Murat Karaboga

Die Entstehung der EU-Datenschutz-Grundverordnung

Das Politikfeld Datenschutz im Spannungsverhältnis zwischen Grundrechtsschutz und Binnenmarktregulierung

Nomos

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Privatheit und Selbstbestimmung in der digitalen Welt

Privacy and Self-Determination in the Digital World

herausgegeben von | edited by
Dr. Michael Friedewald
Prof. Dr. Alexander Roßnagel

Band | Volume 3

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Murat Karaboga

Die Entstehung der EU-Datenschutz-Grundverordnung

Das Politikfeld Datenschutz im Spannungsverhältnis zwischen Grundrechtsschutz und Binnenmarktregulierung

Nomos

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Die Erstellung dieser Arbeit wurde vom Bundesministerium für Bildung und Forschung im Rahmen des Projekts „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“ gefördert.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Frankfurt am Main, Univ., Diss., 2021

u.d.T.: Die Entstehung der EU-Datenschutz-rundverordnung: Policy-Analyse unter besonderer Berücksichtigung der Rolle zeitgenössischer Privatheitsverständnisse

1. Auflage 2024

© Murat Karaboga

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-0841-4
ISBN (ePDF): 978-3-7489-1589-8

DOI: https://doi.org/10.5771/9783748915898

Onlineversion
Nomos eLibrary

D30

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung Nicht kommerziell-Share Alike 4.0 International Public License

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Vorwort und Danksagung

Die Idee zu dieser Arbeit entwickelte ich in einer wunderschönen, lauen Sommernacht Mitte 2013. Die Snowden-Enthüllungen befanden sich auf ihrem Höhepunkt, ich kehrte nach einem interessanten Praktikum am HIIG zurück an meinen damaligen Lebensmittelpunkt in Frankfurt am Main und entschied mich dazu, den Versuch zu wagen, über die Datenschutz-Grundverordnung zu promovieren. Ich hatte bereits im Vorfeld mit Freunden und Bekannten über das Verfassen einer Dissertationsschrift gesprochen, aber so wie es wohl vielen Promovenden geht, ahnte ich zu diesem Zeitpunkt nicht wirklich, auf was ich mich da eingelassen hatte.

Es gibt Menschen, die Einzelgänger sind und damit auch Erfolg haben, es sogar schaffen, Dissertationen im stillen Kämmerlein erfolgreich fertig zu bringen. Ich gehöre nicht zu diesen Menschen. Daher möchte ich an dieser Stelle all jenen Menschen dafür danken, dass sie mich über die Jahre konstant mit ihrer Liebe und Expertise unterstützt haben.

Canım annem ve gurur duyduğum babam: siz, sevginiz ve okumaya odaklı teşvikiniz olmasaydı, ben bu yola girmez, asla bu başarılara imza atamazdım.

Meine herzallerliebste und wundervolle Yeliz: Ich liebe Dich und bin unendlich dankbar für jede Deiner verträumten Blicke, zärtlichen Umarmungen und besänftigenden Worte, die mir auch noch in der schwierigsten dissertationsbedingten Situation Hoffnung gemacht und den nötigen Mut gegeben haben, weiter zu machen und das Projekt erfolgreich zu Ende zu bringen!

Liebe Frau Seubert, vielen Dank, dass Sie mir den nötigen Freiraum gelassen haben, den ich für die Bewerkstelligung dieses Projekts benötigte und dafür, dass Sie trotzdem mit Rat zur Seite standen, wann immer ich auf Sie zugekommen bin.

Einen wesentlichen Anteil an der inhaltlichen Qualität der Arbeit hat auch meine kontinuierliche Einbindung in das BMBF-geförderte interdisziplinäre Forschungsprojekt „Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ gehabt. Durch diese Einbindung hatte ich die Gelegenheit, an zahlreichen Veranstaltungen sowohl teilzunehmen als auch mitzuwirken, die nicht nur meinen fachlichen Horizont erweiterten. Neben den vielen interessanten und lehrreichen Gesprächen mit den Kolleginnen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

und Kollegen geht mein Dank insbesondere an die beiden Projektleiter Peter Zoche und Michael Friedewald, die mir ebenfalls stets mit Rat zur Seite standen, aber auch genügend Raum ließen, mich in den Tiefen der EU-Datenschutzpolitik produktiv zu verlieren.

Michael Friedewald verdient darüber hinaus einen besonderen Dank, da er meine Arbeit über die letzten Jahre als Mentor intensiv betreut und mich besonders in der letzten Phase vor Abgabe auf entscheidende Weise unterstützt hat. Dieser Dank geht gleichzeitig aber auch an das Fraunhofer-Institut für System- und Innovationsforschung ISI und dessen Competence Center Neue Technologien, das mich unter Bedingungen beschäftigt hat, die für Sozialwissenschaftler überdurchschnittlich sind und das den Rahmen für die Projektanbindung, das Mentoring und lehrreiche Weiterqualifikationen gebildet hat.

An meinen früheren Lehrer Peter Zurek geht mein Dank, weil ich insbesondere aufgrund seiner Unterstützung meine Selbstzweifel ablegte und mich trotz meines Gastarbeiterkind-Hintergrunds und gegen den Widerstand der übrigen Lehrerschaft dazu entschied, auf ein Gymnasium zu gehen. Meinem späteren Lehrer Burghardt Rancke möchte ich dafür danken, dass er mich bei meinem Interesse für die Politik, der Wahl des Studiums der Politikwissenschaften und der Wahl von Marburg als Erst-Studienort unterstützt hat. Diese Entscheidungen waren für mich enorm prägend und ich danke Ihnen aufrichtig für die offenen Gespräche, die mich dazu bewogen haben. Ich danke David Salomon dafür, dass er es während meines Studiums der Politikwissenschaften an der Universität Marburg und der Goethe-Universität Frankfurt am Main geschafft hat, dass ich trotz meiner vielen Zweifel letztlich doch den Weg der Wissenschaft eingeschlagen habe – der Funke dieser Begeisterung glüht noch immer und war von entscheidender Bedeutung dafür, dass ich diese Schrift zu Ende verfassen konnte.

Ich danke auch Ralf Lindner, der mir dankenswerterweise den Rat gab, doch „mal das Advocacy Coalitions Framework von diesem Sabatier“ anzuschauen, das letztlich den theoretischen Rahmen meiner Arbeit bilden sollte. In diesem Zusammenhang geht auch ein großer Dank an Lavinia Zinser und Stefan Lindow, mit denen ich im Laufe unzähliger Stunden daran gearbeitet habe, das Advocacy Coalition Framework zu verstehen und zur Anwendung zu bringen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ich danke auch allen Korrekturlesern, HiWis und Diskussionspartnern, die mir viel Arbeit abgenommen bzw. interessante neue Ideen vermittelt haben: Philip Schütz, Dara Hallinan, Nicholas Martin, Christian Geminn, Tanja Martin (geb. Bratsch), Gabriel Letai, Jona Dienst, Robert Fechner, u.v.m.!

Zuletzt möchte ich auch all jenen Freunden und Bekannten danken, deren Namen ich hier nicht aufzählen kann, aber deren Zuneigung, Zuversicht aber auch Nachsichtigkeit mir durch die anstrengende Zeit der Dissertation geholfen haben.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Inhaltsverzeichnis

Abbildungsverzeichnis 19

Tabellenverzeichnis 21

Abkürzungsverzeichnis 29

1 Einleitung 31

1.1 Untersuchungsgegestand und Relevanz 32

1.2 Forschungsstand und Fragestellung 35

1.3 Struktur der Arbeit 41

2 Theoretischer Rahmen und Methodologie 43

2.1 Welche theoretischen Rahmen kommen grundsätzlich infrage? 44

2.1.1 Wahl des theoretischen Rahmens 47

2.2 Das Advocacy Coalition Framework 48

2.2.1 Policy Subsysteme und Kontext 50

2.2.1.1 Kontext – Relativ stabile Parameter und externe, dynamische Systemereignisse 52

2.2.2 Überzeugungssysteme 52

2.2.3 Advocacy-Koalitionen 54

2.2.4 Policy-Wandel als abhängige Variable: Zwei mögliche Pfade 57

2.2.5 Relevante Ergänzungen des ACF 59

2.2.6 Schwächen des ACF 64

2.2.7 Anwendbarkeit des ACF auf politische Entscheidungsprozesse auf der EU-Ebene 66

2.3 Forschungsdesign und methodische Erwägungen 68

2.3.1 Forschungsstrategie: Einzelfallstudie 69

2.3.2 Fallauswahl und Festlegung des zeitlichen Untersuchungsrahmens: Der politische Aushandlungsprozess der DSGVO 72

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.3 Analytischer Rahmen 73
2.3.4 Operationalisierung 78
2.3.4.1 Operationalisierung der Kontextanalyse 78
2.3.4.2 Operationalisierung der Akteurs- und Prozessanalyse 82
2.3.5 Datenerhebung und -analyse 88
2.3.5.1 Begründung der gewählten Datenerhebungsmethoden 92
2.3.5.2 Identifikation und Eingrenzung der Subsystem-Akteure 97
2.3.5.3 Messung der Überzeugungen: Identifikation der Items und Erstellung des Code-Schemas 106
2.3.6 Reflexion über Normativität und Objektivität 107

3 Kontextanalyse 111

3.1 Die Frühphase der Datenverarbeitung und die Divergenz nationaler Datenschutzgesetze 113
3.1.1 OECD-Datenschutz-Richtlinien 115
3.1.1.1 Erste Aktivitäten der OECD mit Datenschutzbezug 115
3.1.1.2 Die politischen Auseinandersetzungen während der Erarbeitung der OECD-Richtlinien 117
3.1.1.3 Inhalt der OECD-Richtlinien 119
3.1.1.4 Zwischenfazit und Bewertung 120
3.1.2 Datenschutz-Konvention des Europarats 121
3.1.2.1 Erste Aktivitäten des Europarats mit Privatheits- und Datenschutzbezug 123
3.1.2.2 Die Erarbeitung der Datenschutz-Konvention Nr. 108 125
3.1.2.3 Inhalt der Datenschutz-Konvention 108 127
3.1.2.4 Zwischenfazit / Bewertung 130
3.2 Die ersten Datenschutz-Instrumente auf Gemeinschaftsebene 132
3.2.1 Struktur und Organe der Europäischen Union 132
3.2.1.1 Europäischer Rat 134
3.2.1.2 Europäische Kommission 135
3.2.1.3 Der Rat der Europäischen Union – Ministerrat 136
3.2.1.4 Europäisches Parlament 137

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.2.2 Die EU-Datenschutz-Richtlinie 95/46/EG 138
3.2.2.1 Erste datenschutzpolitische Bestrebungen auf Gemeinschaftsebene 138
3.2.2.2 Parlament als Befürworter und Kommission als Bremserin von Gemeinschaftsregelungen? 149
3.2.2.3 Der Meinungswandel der Europäischen Kommission 151
3.2.2.4 EG-Richtlinienvorschlag von 1990 159
3.2.2.4.1 Kontext 159
3.2.2.4.2 Grundsätzliche Konfliktlinien 161
3.2.2.4.3 Konkrete Konflikte 163
3.2.2.5 Überarbeiteter Richtlinienvorschlag von 1992 170
3.2.2.5.1 Kontext: Zugeständnisse und Zurückweisungen der Kommission 170
3.2.2.5.2 Weiterhin bestehende und ungelöste grundsätzliche Konfliktlinien 173
3.2.2.5.3 Konkrete Konflikte und Pattsituation bedrohen erfolgreichen Abschluss der Verhandlungen 174
3.2.2.6 Überwindung der politischen Pattsituation 180
3.2.2.6.1 Politische Kompromisse 184
3.2.2.7 Inhalte der DS-RL 189
3.2.2.8 Fazit: Bewertung der DS-RL 198
3.2.2.9 Implementierung der DS-RL in den Mitgliedstaaten 200
3.2.3 Drittstaatentransfers und Safe Harbor-Vereinbarung 203
3.2.4 ISDN-RL 97/66/EG 211
3.2.5 DS-VO 45/2001 213

3.3 Die Datenschutzpolitik der Europäischen Gemeinschaft nach der Jahrtausendwende 216
3.3.1 Hintergrund und Kontext: Wirtschafts- und sicherheitspolitisch bedingte Legitimationskrise des Datenschutzes 216
3.3.1.1 Kommerzialisierung von (personenbezogenen) Daten und IuK-Technologien als Wirtschaftsmotor 216
3.3.1.2 Von 9/11 bis London 2005: Der Einfluss von Terroranschlägen 221

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.2 ePrivacy-Richtlinie 2002/58/EG 223
3.3.2.1 Vorgeschichte zur ePrivacy-Richtlinie 223
3.3.2.2 Veröffentlichung des Kommissionsvorschlags 226
3.3.2.3 Formierung des Gemeinsamen Standpunktes im Ministerrat 227
3.3.2.4 Formierung der Parlamentsposition in erster Lesung: Erster Cappato-Bericht 229
3.3.2.5 Post 9/11: Formierung der Parlamentsposition in erster Lesung: Zweiter Cappato-Bericht 231
3.3.2.6 Interinstitutionelle Auseinandersetzungen und ein schaler Kompromiss 234
3.3.2.7 Zwischenfazit 242
3.3.3 Berichte der Kommission über die Durchführung der DS-RL 243
3.3.3.1 Die Ergebnisse des Berichts: Kritikpunkte 244
3.3.3.2 Die Ergebnisse des Berichts: Lösungsvorschläge und Arbeitsprogramm der Kommission 247
3.3.3.3 Stellungnahme des Europäischen Parlaments 251
3.3.3.4 Folgebericht 253
3.3.3.5 Zwischenfazit 254
3.3.4 Datenschutz-Bestimmungen im Sicherheitsbereich 255
3.3.4.1 Erste Aktivitäten auf dem Gebiet 255
3.3.4.2 Richtlinie 2006/24/EG zur Vorratsdatenspeicherung 259
3.3.4.3 Der Zugriff auf Fluggastdaten zu Sicherheitszwecken 265
3.3.4.3.1 Zwischenfazit 267
3.3.4.4 Die Erarbeitung des JI-Rahmenbeschlusses 2008/977/JHA 268
3.3.4.4.1 Stellungnahmen der Datenschutzaufsichtsbehörden 270
3.3.4.4.2 Positionierung des Parlaments 271
3.3.4.4.3 Verhandlungen im Ministerrat 274
3.3.4.4.4 Stillstand der Verhandlungen 277
3.3.4.4.5 Überwindung der politischen Pattsituation 278
3.3.4.4.6 Zwischenfazit 280

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.5 Novellierung der ePrivacy-RL zur Cookie-Richtlinie 2009/136/EG 283
3.3.5.1 Kommissionsentwurf 288
3.3.5.2 Stellungnahmen des EDSB und der Art. 29-Datenschutzgruppe 290
3.3.5.3 Position des Europäischen Parlaments 292
3.3.5.3.1 Inhalt der Parlamentsposition 293
3.3.5.3.2 Geänderter Vorschlag der Kommission 294
3.3.5.4 Gemeinsamer Standpunkt des Ministerrats 295
3.3.5.5 Einigung im Trilog und Verabschiedung des Kompromisstextes 298
3.3.5.6 Zwischenfazit 300
3.3.6 Fazit 301

3.4 Wandel weiterer relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform entscheidend waren 302
3.4.1 Veränderungen in der grundlegenden verfassungsmäßigen Struktur, im Grad der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des politischen Systems 303
3.4.1.1 Die Erarbeitung der EU-Grundrechtecharta 303
3.4.1.1.1 Entwurfsprozess 305
3.4.1.1.2 Konflikte während des Entwurfsprozesses 306
3.4.1.1.3 Inhalt der Grundrechtecharta 309
3.4.1.1.4 Zwischenfazit 313
3.4.1.2 Der Vertrag von Lissabon 314
3.4.1.2.1 Entwurfsphase 315
3.4.1.2.2 Inkrafttreten der Grundrechtecharta 317
3.4.1.2.3 Institutionelle Neuerungen in Folge des Vertrags von Lissabon 318
3.4.1.3 Das Stockholmer Programm 319
3.4.1.3.1 Empfehlungen der Zukunftsgruppe Inneres 319
3.4.1.3.2 Empfehlungen der Zukunftsgruppe Justiz 321
3.4.1.3.3 Kommissionsentwurf 323

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.1.3.4 Stellungnahme des Europäischen Datenschutzbeauftragten zum Kommissionsentwurf 324
3.4.1.3.5 Ratsentwurf 326
3.4.1.3.6 Parlamentsposition 327
3.4.1.3.7 Das finale Stockholmer Programm 329
3.4.1.3.8 Reaktionen auf das Stockholm-Programm 332
3.4.1.3.9 Umsetzung des Stockholm-Programms: Die formelle Geburt der Datenschutzreform 333
3.4.1.3.10 Zwischenfazit 335
3.4.1.4 Fazit und Auswirkungen auf die Datenschutzpolitik der EU 336
3.4.2 Weitere Faktoren: Veränderung sozioökonomischer Bedingungen und der öffentlichen Meinung 337
3.4.2.1 Zunahme von Datenschutzskandalen 337
3.4.2.2 Wandel in der öffentlichen Meinung gemäß Umfragewerten in den 2000er-Jahren 340
3.4.2.3 Außerparlamentarischer Widerstand 341
3.4.2.3.1 Entstehung europaweiter digitaler Bürgerrechtsgruppen 342
3.4.2.3.2 Zivilgesellschaftlicher Widerstand in Deutschland gegen die Einführung der Vorratsdatenspeicherung 343
3.4.2.4 Policy Entrepreneurship im Europäischen Parlament 345
3.4.2.5 Policy Entrepreneurship auf Ebene der Kommission 348
3.5 Zwischenfazit 349
3.5.1 Zusammenfassung 350
3.5.2 Identifikation von Advocacy-Koalitionen 355
3.5.2.1 Datenschutzbefürworter-Koalition: 356
3.5.2.1.1 Zusammensetzung der Datenschutzbefürworter-Koalition 356
3.5.2.1.2 Überzeugungssystem der Datenschutzbefürworter-Koalition 358

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.5.2.1.3 Ressourcen der Datenschutzbefürworter-Koalition 360
3.5.2.2 Flexibilitätsbefürworter-Koalition 363
3.5.2.2.1 Zusammensetzung der Flexibilitätsbefürworter-Koalition und ihr Verhältnis zur Flexibilitätsbefürworter-Community 364
3.5.2.2.2 Überzeugungssystem der Flexibilitätsbefürworter-Koalition 366
3.5.2.2.3 Ressourcen der Flexibilitätsbefürworter-Koalition 368

4 Akteurs- und Prozessanalyse 371

4.1 Orientierungsphase (2009–2010) 372
4.1.1 Akteursanalyse 374
4.1.1.1 Cluster-Analyse 374
4.1.1.1.1 Grundlegende methodische Erwägungen zur Cluster-Analyse 374
4.1.1.1.2 Ergebnisse der Cluster-Analyse 379
4.1.1.1.3 Zwischenfazit zur Cluster-Analyse 387
4.1.1.2 Datenschutzbefürworter-Community: 388
4.1.1.2.1 Zusammensetzung der Datenschutzbefürworter-Community während der Orientierungsphase 388
4.1.1.2.2 Überzeugungssystem der Datenschutzbefürworter-Community während der Orientierungsphase 390
4.1.1.2.3 Ressourcen der Datenschutzbefürworter-Advocacy-Community während der Orientierungsphase 397
4.1.1.3 Flexibilitätsbefürworter-Community 397
4.1.1.3.1 Zusammensetzung der Flexibilitätsbefürworter-Community 397
4.1.1.3.2 Überzeugungssystem der Advocacy-Community der Flexibilitätsbefürworter während der Orientierungsphase 400

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:08
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.1.1.3.3 Ressourcen der Flexibilitätsbefürworter-Community während der Orientierungsphase 409
4.1.2 Prozessanalyse: Der Pfad zum Datenschutz-Gesamtkonzept der Kommission 409
4.1.2.1 Entscheidende Gründe für das Zustandekommen des Gesamtkonzepts der Kommission 413
4.1.2.2 Zwischenfazit 417
4.2 Entwurfsphase (2010–2012) 419
4.2.1 Akteursanalyse 420
4.2.1.1 Cluster-Analyse 420
4.2.1.2 Datenschutzbefürworter 428
4.2.1.2.1 Zusammensetzung der Datenschutzbefürworter während der Entwurfsphase: Von der Community zur Koalition 428
4.2.1.2.2 Überzeugungssytem der Datenschutzbefürworter-Koalition während der Entwurfsphase 429
4.2.1.2.3 Ressourcen der Datenschutzbefürworter-Koalition während der Entwurfsphase 440
4.2.1.3 Flexibilitätsbefürworter 442
4.2.1.3.1 Zusammensetzung der Flexibilitätsbefürworter: Von der Advocacy-Community zur Advocacy-Koalition 442
4.2.1.3.2 Überzeugungssystem der Flexibilitätsbefürworter während der Entwurfsphase 446
4.2.1.3.3 Ressourcen der Flexibilitätsbefürworter während der Entwurfsphase 471
4.2.1.4 Die Akteursgruppe der Kompromisswilligen 473
4.2.2 Prozessanalyse: Entstehung und Inhalt des DSGVO-Entwurfs der Europäischen Kommission 474
4.2.2.1 Lobbying der Kommission und Verzögerung des Reformpakets 474

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.2.2.2 Der Kommissionsvorschlag zur EU-Datenschutz-Grundverordnung 476
4.2.2.3 Inhalte des DSGVO-Kommissionsentwurfs und Einschätzung des Akteurseinflusses 478
4.2.2.3.1 Konsens-Themen 479
4.2.2.3.2 Von beiden Koalitionen abweichende Positionen der Kommission 481
4.2.2.3.3 Erfüllung der Forderungen der Flexibilitätsbefürworter 483
4.2.2.3.4 Erfüllung der Forderungen der Datenschutzbefürworter 486
4.2.2.4 Entscheidende Gründe für das Zustandekommen des Kommissionsentwurfs 496
4.2.2.5 Zwischenfazit 499
4.3 Konfliktphase (2012–2015) 502
4.3.1 Akteursanalyse 503
4.3.1.1 Cluster-Analyse 503
4.3.1.2 Datenschutzbefürworter 510
4.3.1.2.1 Zusammensetzung der Datenschutzbefürworter 510
4.3.1.2.2 Überzeugungssystem der Datenschutzbefürworter 512
4.3.1.2.3 Ressourcen der Datenschutzbefürworter 526
4.3.1.3 Flexibilitätsbefürworter 529
4.3.1.3.1 Zusammensetzung der Flexibilitätsbefürworter 529
4.3.1.3.2 Überzeugungssystem der Flexibilitätsbefürworter 530
4.3.1.3.3 Ressourcen der Flexibilitätsbefürworter 551
4.3.1.4 Die Akteursgruppe der bedingten Datenschutzbefürworter 552
4.3.2 Prozessanalyse: Das Zustandekommen der DSGVO 554
4.3.2.1 Erste Reaktionen auf den Kommissionsentwurf 554
4.3.2.2 Diskussion des Kommissionsentwurfs in den Parlamentsausschüssen 556
4.3.2.3 Diskussion des Legislativvorschlags im EU-Ministerrat 559

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3.2.4 Höhepunkt der Debatte und Stillstand der Verhandlungen – Blockade in Parlament und Ministerrat 563
4.3.2.5 Überwindung der Pattsituation: Der Einfluss der Snowden-Enthüllungen, die Aufarbeitung des Überwachungsskandals und die Verabschiedung der Parlamentsposition 573
4.3.2.6 Der lange Weg bis zur Überwindung des Stillstands im Ministerrat 578
4.3.2.7 Überblick der Inhalte des DSGVO-Kompromisses 590
4.3.2.8 Reaktionen auf die Einigung im Trilog und die Verabschiedung der DSGVO 593
4.4 Beantwortung der Forschungsfragen: Die Entstehung der DSGVO 594

5 Schluss 601
5.1 Zusammenfassung und Beantwortung der Forschungsfragen 602
5.2 Kritische Reflexion der Ergebnisse und Forschungsdesiderate 617
5.3 Ausblick oder: Quo Vadis Datenschutz? 621

Literaturverzeichnis 623

Anhang 699
1.1 Fraktionen im Europäischen Parlament in den Wahlperioden seit 1979 699
1.2 Partizipation von Akteuren am Subsystem der EU-Datenschutzpolitik bis zur DSGVO 699
1.3 Detaillierte Tabellen für Abschnitt 5 715
1.4 Überblick der formellen LIBE-Ausschusssitzungen zum DSGVO-E 720
1.5 Überblick der formellen Rats-, AStV-, Ratsarbeitsgruppen- und Trilog-Sitzungen zur DSGVO 720
1.6 Vollständige Akteurslisten der Datenschutz-NGOs 732

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Abbildungsverzeichnis

Abbildung 1:	Schema des Advocacy Coalition Framework	64
Abbildung 2:	Überblick über den gewählten analytischen Rahmen	75
Abbildung 3:	Datenschutzpolitische Auseinandersetzungen, die Teil der Kontextanalyse sind	76
Abbildung 4:	Schematische Darstellung des analytischen Rahmens für den Schritt der Akteurs- und Prozessanalyse	77
Abbildung 5:	Einteilung des politischen Aushandlungsprozesses zur DSGVO in drei voneinander getrennte Phasen	78
Abbildung 6:	Vereinfachtes ACF-Schema	82
Abbildung 7:	Netzwerk der Flexibilitätsbefürworter	443

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabellenverzeichnis

Tabelle 2-1: Zugänglichkeit von relevanten Daten der administrativ für die Reform zuständigen Akteure in den EU-Organen (eigene Zusammenstellung) 91

Tabelle 2-2: Teilnehmende Beobachtung - Orte und zentrale Akteure, die beobachtet wurden 92

Tabelle 2-3: Überblick über formelle und informelle Lobbying-Foren zur DSGVO und die Zahl der im Rahmen dieser Foren lobbyierenden Akteure (eigene Zusammenstellung) 99

Tabelle 2-4: Häufigkeit und Zeitpunkt der Beteiligung der Subsystem-Akteure am Datenschutzreformprozess (eigene Auswertung) 104

Tabelle 2-5: Überblick über die Kommentare der Mitgliedstaaten zu den DSGVO-Kapiteln (eigene Auswertung) 105

Tabelle 3-1: Datenschutzgesetze und Umsetzung der der Datenschutz-Konvention in den EG-Mitgliedstaaten und Beitrittskandidaten im Jahr 1990 (eigene Zusammenstellung) 153

Tabelle 3-2: Qualifiziertes Mehrheitswahlrecht bis Ende 1994, Richtliniengegner Ende 1993/Anfang 1994 in Rot (Council of the European Union 2013, 38)(Council of the European Union 2013, 38)(Council of the European Union 2013, 38) 180

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle 3-3: Qualifiziertes Mehrheitswahlrecht nach der EU-Erweiterung im Jahr 1995 und Abstimmungsverhalten (Enthaltung des Vereinigten Königreichs) (Council of the European Union 2013, 39)(Council of the European Union 2013, 39) (Council of the European Union 2013, 39) 189

Tabelle 3-4: Implementierung der DS-RL in den Mitgliedstaaten (Commission of the European Communities 2003, 3; European Commission 2005; Korff 2002, 1) (Commission of the European Communities 2003, 3; European Commission 2005; Korff 2002, 1) (Commission of the European Communities 2003, 3; European Commission 2005; Korff 2002, 1) 201

Tabelle 3-5: 55 Zentrale Akteure der Flexibilitätsbefürworter-Koalition (eigene Zusammenstellung) 366

Tabelle 4-1: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS) 379

Tabelle 4-2: K-Means-Clusteranalyse mit 2 Koalitionen (berechnet mit SPSS) 381

Tabelle 4-3: Finale Cluster-Zentren der K-Means-Clusteranalyse mit 2 Koalitionen (berechnet mit SPSS) 382

Tabelle 4-4: K-Means-Clusteranalyse mit 3 Koalitionen (berechnet mit SPSS) 384

Tabelle 4-5: Distanzen der finalen Cluster-Zentren (berechnet mit SPSS) 384

Tabelle 4-6: Finale Cluster-Zentren der K-Means-Clusteranalyse mit 3 Koalitionen (berechnet mit SPSS) 385

Tabelle 4-7: ANOVA-Ergebnisse für das 2-Cluster-Modell (berechnet mit SPSS) 387

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle 4-8: Die Advocacy-Community der Datenschutzbefürworter 390

Tabelle 4-9: Überblick der Überzeugungen der Datenschutzbefürworter-Community (eigene Erhebung bzw. Berechnung mit SPSS) 392

Tabelle 4-10: Positionierung der Datenschutzbefürworter zu allen relevanten Themen in der Orientierungsphase (eigene Erhebung) 397

Tabelle 4-11: Zentrale Akteure der Flexibilitätsbefürworter-Community (eigene Zusammenstellung) 400

Tabelle 4-12: Überblick der Überzeugungen der Flexibilitätsbefürworter-Advocacy-Community (eigene Erhebung bzw. Berechnung mit SPSS) 402

Tabelle 4-13: Positionierung der Flexibilitätsbefürworter zu allen relevanten Themen in der Orientierungsphase (eigene Erhebung) 408

Tabelle 4-14: Die Positionen der Advocacy-Communities im Vergleich zur Kommissionsposition während der Orientierungsphase (eigene Erhebung, Berechnung mittels SPSS, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum Kommissionsentwurf) 419

Tabelle 4-15: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS) 421

Tabelle 4-16: K-Means Cluster-Analyse mit 2 Clustern (berechnet mit SPSS) 423

Tabelle 4-17: Finale Zentren der K-Means-Clusteranalyse mit 2 Clustern (berechnet mit SPSS) 424

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle 4-18: K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS) 425

Tabelle 4-19: Finale Zentren der K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS) 426

Tabelle 4-20: ANOVA-Ergebnisse für das 3-Cluster-Modell der zweiten Phase (berechnet mit SPSS) 428

Tabelle 4-21: Die Advocacy-Koalition der Datenschutzbefürworter 429

Tabelle 4-22: Überblick der Überzeugungen der Datenschutzbefürworter-Koalition (eigene Erhebung bzw. Berechnung mit SPSS) 439

Tabelle 4-23: Positionierung der Datenschutzbefürworter zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung) 440

Tabelle 4-24: Advocacy-Koalition sowie Advocacy-Community der Flexibilitätsbefürworter 445

Tabelle 4-25: Überblick der Überzeugungen der Flexibilitätsbefürworter (eigene Erhebung bzw. Berechnung mit SPSS) 447

Tabelle 4-26: Positionierung der Flexibilitätsbefürworter zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung) 470

Tabelle 4-27: Akteure der Community der Kompromisswilligen 474

Tabelle 4-28: Die Positionen der beiden Advocacy-Koalitionen bzw. der Community im Vergleich zur Kommissionsposition während der Orientierungsphase (eigene Erhebung, Berechnung der Koalitionspositionen mittels SPSS, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum Kommissionsentwurf) 501

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle 4-29: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS) 504

Tabelle 4-30: Finale Zentren der K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS) 506

Tabelle 4-31: Finale Zentren der K-Means-Clusteranalyse mit 5 Clustern (berechnet mit SPSS) 507

Tabelle 4-32: K-Means-Clusteranalyse mit 5 Clustern (berechnet mit SPSS) 509

Tabelle 4-33: ANOVA-Ergebnisse für das 5-Cluster-Modell der dritten Phase (berechnet mit SPSS) 510

Tabelle 4-34: Akteursliste der Datenschutzbefürworter – Mitglieder der Advocacy-Koalition grau unterlegt (eigene Zusammenstellung) 511

Tabelle 4-35: Positionen aller Datenschutzbefürworter zu allen relevanten Themen (eigene Zusammenstellung) 515

Tabelle 4-36: Akteursliste der Flexibilitätsbefürworter – Mitglieder der Advocacy-Koalition grau unterlegt (eigene Zusammenstellung) 530

Tabelle 4-37: Positionierung der gemäßigten Flexibilitätsbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung) 548

Tabelle 4-38: Positionierung der extremen Flexibilitätsbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung) 550

Tabelle 4-39: Akteursliste der bedingten Datenschutzbefürworter (eigene Zusammenstellung) 554

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle 4-40: Positionen der Kommission, des Ministerrats und des EP im Vergleich zu zur finalen DSGVO sowie zur DS-RL (eigene Codierung der Positionen, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum finalen DSGVO-Text) 592

Tabelle 5-1: Zusammenfassung der zentralen Elemente der Überzeugungssysteme der Datenschutz- und Flexibilitätsbefürworter (eigene Darstellung, inspiriert von Larsen et al. (2006, 217)(2006, 217) (2006, 217)). 614

Tabelle Anhang 1: Häufigkeit und Zeitpunkt der Partizipation aller Akteure am Subystem der EU-Datenschutzpolitik bis zum Beginn des DSGVO-Aushandlungsprozesses 714

Tabelle Anhang 2: Missing Value Analysis für alle 27 infrage kommenden Items in der Orientierungsphase (berechnet mit SPSS) 715

Tabelle Anhang 3: Positionierung der Community der Kompromisswilligen zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung) 717

Tabelle Anhang 4: Positionierung der Gruppe der bedingten Datenschutzbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung) 719

Tabelle Anhang 5: Liste aller mit der DSGVO befassten formellen LIBE-Ausschusssitzungen (eigene Zusammenstellung) 720

Tabelle Anhang 6: Lister aller mit der DSGVO befassten Treffen des Rats in der JI-Konfiguration (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen) 721

Tabelle Anhang 7: Liste aller mit der DSGVO befassten AStV-Sitzungen (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen) 727

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tabelle Anhang 8:	Liste aller mit der DSGVO befassten DAPIX-Ratsarbeitsgruppensitzungen (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen)	730
Tabelle Anhang 9:	Überblick aller Trilog-Sitzungen und der Themen (EPP 2015)(EPP 2015)(EPP 2015)	731
Tabelle Anhang 10:	Unterzeichner-Organisationen des TACD-Briefes an die Rapporteure Albrecht und Comi vom 5. September 2012 (US-Consumer Organizations 2012)(US-Consumer Organizations 2012)(US-Consumer Organizations 2012)	732
Tabelle Anhang 11:	Unterzeichner-Organisationen des NGO-Briefes an die griechische Ratspräsidentschaft vom 28. Januar 2014 (Civil Rights Organisations 2014)(Civil Rights Organisations 2014)(Civil Rights Organisations 2014)	733
Tabelle Anhang 12:	1212 Unterzeichner-Organisationen des NGO-Briefes an den Kommissionspräsidenten Juncker vom 21. April 2015 (EDRi und Access (International) 2015)(EDRi und Access (International) 2015)(EDRi und Access (International) 2015)	735

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Abkürzungsverzeichnis

ADR	Ausschuss der Regionen
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
ALDE (bis 2004: ELDR)	Fraktion der Allianz der Liberalen und Demokraten für Europa (Europäische Liberale, Demokraten und Reformer)
AStV	Ausschuss der Ständigen Vertreter
B2B	Business to Business
BDSG	Bundesdatenschutzgesetz
bDsb	Betriebliche Datenschutzbeauftragte
BfDI	Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
BVerfG	Bundesverfassungsgericht
DAPIX	Ratsarbeitsgruppe "Informationsaustausch und Datenschutz"
Datenschutzgruppe	Art. 29-Datenschutzgruppe
DSGVO	Die finale Datenschutz-Grundverordnung
DSGVO-E	DSGVO-Entwurf der Europäischen Kommission von 2012
DSGVO-PE	DSGVO-Parlamentsentwurf
DSGVO-RE	DSGVO-Ratsentwurf
DSGVO-UE	Der durchgesickerte ursprüngliche DSGVO-Kommissionsentwurf von 2011
DSAB	Datenschutzaufsichtsbehörde
DSFA	Datenschutzfolgenabschätzung
EDD	Europa der Deomkratien und Unterschiede
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EDU	Europa der Demokratien und der Unterschiede (Europe of Democracies and Diversities EDD)
EG	Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
EMPL-Ausschuss	Ausschuss für Beschäftigung und soziale Angelegenheiten

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

EMRK	Europäische Menschenrechtskonvention
EP	Europäisches Parlament
EU-GRCh	Grundrechtecharta der Europäischen Union
Europol	European Police Office
EVP-ED	Fraktion der Europäischen Volkspartei und Europäischer Demokraten
EWSA	Europäischer Wirtschafts- und Sozialausschuss
FISA	Foreign Intelligence Surveillance Act
GD	Generaldirektion
Grüne/EFA	Fraktion der Grünen/Europäischen Freien Allianz
GUE/NGL	Konföderale Fraktion der Vereinten Europäischen Linken/Nordischen Grünen
IMCO-Ausschuss	Ausschuss für Binnenmarkt und Verbraucherschutz
IND/DEM	Fraktion Unabhängigkeit/Demokratie
ITRE-Ausschuss	Ausschuss für Industrie, Forschung und Energie
IuK-Technologien	Informations- und Kommunikationstechnologien
JI	Justiz und Inneres
JURI-Ausschuss	Rechtsausschuss
KMU	Kleine und Mittlere Unternehmen
LIBE-Ausschuss	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres
LIBE-BE	LIBE-Berichtsentwurf
NSA	National Security Agency
PETs	Privacy Enhancing Technologies
RFID	Radio-frequency identification (Identifizierung mit Hilfe elektromagnetischer Wellen)
S&D	Die Fraktion der Progressiven Allianz der Sozialdemokraten im Europäischen Parlament
UEN	Union für das Europa der Nationen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

1 Einleitung[1]

Mittlerweile kann die DSGVO als das zentrale Regulierungselement im digitalpolitischen Geflecht der EU bewertet werden. Zahlreiche Legislativvorhaben und Verordnungen wie der Data Act, Data Governance Act, AI Act, Digital Services Act oder der Digital Markets Act erweitern das digitalpolitische Regulierungsrepertoir der Europäischen Union in ihren jeweiligen Bereichen, während in allen genannten Maßnahmen die DSGVO-Vorgaben den fixen Bezugspunkt bilden. Auch in nicht-verbindlichen Maßnahmen, wie dem European Democracy Action Plan (COM 2020a) oder der KI-Strategie der EU (COM 2020b) werden die DSGVO und ihre Schutzziele affirmiert –selbst in der aus der Regierungszeit Angela Merkels entstadenen Blockchain-Strategie der BRD[2] (BMWi und BMF 2019, 13). Gerade letzteres verdeutlicht, ohne dem Inhalt der Arbeit zu viel vorwegzunehmen, dass sich auch Staaten wie Deutschland, die über viele Jahre hinweg zu den Gegnern der Reform zählten, inzwischen mit der DSGVO arrangiert haben, Ähnliches zeigt sich mit Blick auf die Wirtschaft: Trotz vereinzelter kritischer Stimmen (Bitkom 2020), scheinen sich Akteure aus der datenverarbeitenden Wirtschaft, die enorme Mühen in die Verhinderung bzw. Abschwächung der der DSGVO investiert hatten, mit ihr abgefunden zu haben (AmCham EU 2019; Digitaleurope 2020).

Diese inzwischen ganz selbstverständliche Bezugnahme auf die DSGVO lässt allerdings fast vergessen, wie umstritten der politische Prozess, der zu deren Verabschiedung geführt hat, gewesen ist – und wie mühsam um beinahe jede der DSGVO-Vorgaben, die nun als Standard gelten, gerungen werden musste.

Wie entsteht ein großes EU-Gesetz wie die EU-Datenschutz-Grundverordnung (DSGVO)? Welche politischen und historischen Faktoren wirken als kausale, treibende Faktoren? Die Untersuchung der Entstehung der

1 In diesem Buch werden das generische Maskulinum, das generische Femininum sowie die eindeutige Benennung des männlichen und weiblichen Geschlechts abwechselnd verwendet.

2 Obwohl eine Reihe von Interessenvertretern während der Blockchain-Konsultation der Bundesregierung zum Zwecke eines ungehinderten Blockchain-Einsatzes Änderungen an der DSGVO gefordert hatte, wurde in der Blockchain-Strategie festgehalten, dass sich *aktuell kein Änderungsbedarf* ergebe (BMWi und BMF 2019, 13).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

DSGVO im Kontext der historischen EU-Datenschutzpolitik ist das Ziel der vorliegenden Schrift.

1.1 Untersuchungsgegestand und Relevanz

Die Preisgabe personenbezogener Daten gehört längst zur alltäglichen Praxis: Sobald wir uns auf einer neuen Webseite bzw. bei einem neuen Online-Dienst anmelden, um deren Leistungen zu nutzen. Wenn wir einen Miet- oder sonstigen Vertrag in der Offline-Welt abschließen oder die Anmelde-Passwörter für unsere Online-Accounts in mehr oder weniger regelmäßigen Abständen ändern, damit unsere personenbezogenen Daten, zu denen wir beispielsweise unsere Bankdaten hinzuzählen, nicht kompromittiert werden und in vielen weiteren Fällen. Die ganz selbstverständliche Preisgabe personenbezogener Daten prägt in immer noch ungebremst wachsendem Maße den Alltag der Menschen. Während die sozialen Praktiken im Umgang mit personenbezogenen Daten vielfältige Erscheinungsformen haben und verschiedenen Handlungsmotivationen und -mustern folgen, setzt das Recht eben jenem Umgang objektive Grenzen. Genauer: Das Datenschutzrecht hat zum Ziel zu regeln, wie mit personenbezogenen Daten umzugehen ist, sodass eine Nutzung der Daten weiterhin möglich ist, ohne dass die Menschen, deren personenbezogene Daten Gegenstand der Nutzung sind, negative Auswirkungen erfahren (Simitis 1987).

Unter das Datenschutzrecht fällt beispielsweise, welche Daten einem besonderen Schutz unterliegen, welchen Verpflichtungen wiederum diejenigen unterliegen, denen personenbezogene Daten anvertraut wurden und die aus deren Verarbeitung einen monetären oder sonstigen Nutzen für sich und andere ziehen. Aber auch, welche Strafen die Verletzung der datenschutzrechtlichen Vorschriften nach sich zieht und wer die Regeleinhaltung überwacht und dafür Sorge trägt, dass Rechtsverletzung geahndet werden. Angefangen mit den ersten Datenschutzgesetzen, die vor dem Hintergrund der Zusammenführung öffentlicher Datenbanken zur Verwaltungsautomatisierung und -vereinfachung die ordnungsgemäße Verarbeitung personenbezogener Daten gewährleisten sollten, wurden in den vergangenen knapp 50 Jahren zahlreiche Datenschutzgesetze erlassen (Simitis u. a. 2019).

Gemeinsam ist diesen Gesetzen zweierlei: *Erstens* sind sie Resultat der Nutzbarmachung technologischer Entwicklungen. So hatte es zwar auch schon zuvor vielfältige Gesetze zum Schutze der Persönlichkeitsrechte von Menschen gegeben (Lewinski 2009), doch waren Datenschutzgesetze

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

das spezifische Resultat als Gefährdung wahrgenommener technologischer Entwicklung. Im Laufe der 1960er-Jahre führten die neuen Möglichkeiten der Datenverarbeitung in Teilen der Bevölkerung zu neuen Ängsten, etwa vor einer Unterdrückung auf Grundlage der Daten*macht*, die aus eben jener Verarbeitung resultieren würde. Das augenfälligste Beispiel derartiger Reaktionen ist womöglich die gesellschaftliche Rezeption von George Orwells dystopischem Roman 1984 – historisch wirksam waren in Deutschland aber auch die Erinnerungen an den Holocaust, der durch den systematischen Missbrauch personenbezogener Daten besonders effizient erfolgen konnte (Aly und Roth 2000). Während ein Teil der Bevölkerung und der Politik aufgrund derartiger Bedenken stets ein Interesse an der gesellschaftlichen Einhegung datenverarbeitender Technologien hatte, sah ein anderer Teil eher Vorteile in der Ausschöpfung der Potentiale datenverarbeitender Technologien und wandte sich gegen regulierende Eingriffe des Staates. Das Datenschutzrecht ist das Ergebnis dieser Auseinandersetzungen und hat zum Ziel, mögliche negative Folgen der Datenverarbeitung zu vermeiden während ihre positive Wirkungen erhalten bleiben sollen. Der sowohl europa- als auch weltweit prominenteste Ausdruck dieser Auseinandersetzungen ist die EU-Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 in allen Mitgliedstaaten der EU als unmittelbar anzuwendendes Recht gilt. Mit der DSGVO werden erstmals nicht nur technische Standards oder Marktregeln mittels einer EU-Verordnung festgelegt, sondern unionsweit verbindliche Standards im Hinblick auf ein EU-Grundrecht geschaffen. Als solches war Datenschutz Ende 2000 im Rahmen der EU-Grundrechtecharta (EU-GRCh) verbrieft worden. Mit dem Inkrafttreten des Lissabon-Vertrags wurde die EU-GRCh ab Ende 2009 rechtsbindend und formulierte den Schutz personenbezogener Daten in Art. 16 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) als Regelungsauftrag (Albrecht 2016a, 89).

Zweitens sind Datenschutzgesetze zugleich Ausdruck des Versuchs, Eingriffe in die Privatheit der Menschen zu regulieren. Dieser im umgangssprachlichen Sinne häufig als Privatsphäre bezeichnete Bereich der Gesellschaft wird dabei häufig als Antipode der Öffentlichkeit verstanden: Während die Öffentlichkeit ausmache, dass sie alle Menschen angeht, wird, in westlichen Gesellschaften vielfach als privat angesehen, was nicht die Öffentlichkeit, sondern nur das jeweilige Individuum angehe. Insofern lassen sich Datenschutzgesetze auch als Ausdruck des Schutzes desjenigen privaten Bereichs verstehen, der das Private in Datenform kodifiziert, der Bereich der sogenannten *informationellen Privatheit*: Welchen Taillenumfang habe ich?

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Welche Medien und Inhalte konsumiere ich? Welche sexuellen Vorlieben habe ich? Welche politischen Ansichten vertrete ich? All dies und noch vieles mehr fällt unter den Bereich, der gemeinhin der informationellen Privatheit zugeordnet wird (Rössler 2001, 19; Westin 1967, 7).

Doch das, was personenbezogene Daten für jeden einzelnen Menschen wichtig und schützenswert macht, ist zugleich Grund für deren enorme ökonomische Bedeutung. Waren personenbezogene Daten vor ein paar Jahrzehnten noch vor allem in einzelnen Wirtschaftsbereichen, wie der Kreditbranche, wichtig, sind sie heute zu einer grundlegenden Ressource des Digitalzeitalters quer über verschiedene Wirtschaftsbereiche avanciert. Von der Automobilbranche über den Gesundheitssektor bis hin zu datengetriebenen Nachhaltigkeitstechnologien greifen zunehmend viele Sektoren auf die massenhafte Auswertung personenbezogener Daten zurück, um Innovationen hervorzubringen: Durch die Analyse der Gesundheitsdaten einer Vielzahl von Menschen werden beispielsweise Fortschritte in der Diagnose und Behandlung von Krankheiten ermöglicht. Als entscheidend gilt auch, dass Daten aus unterschiedlichen Quellen zusammengeführt und für neue Zwecke nutzbar gemacht werden: Personenbezogene, Fahrzeug- und Verkehrsdaten sollen die Steuerung von Verkehrsflüssen so optimieren helfen, dass der CO2-Vebrauch gesenkt wird. Abseits solcher, das Gemeinwohl adressierender Vorhaben, sind es aber weiterhin vor allem die großen weltweit agierenden datenverarbeitenden Unternehmen, die personenbezogene Daten unterschiedlichster Art verarbeiten (Edith 2022; Slynchuck 2022). Ein weltweiter Markt, auf dem personenbezogene Daten gehandelt werden, um bessere Vorhersagen über menschliches Handeln zu treffen und sie so besser zu Kaufentscheidungen drängen zu können ist nur ein Aspekt der Verwendung personenbezogener Daten (Zuboff 2018). Wie verschiedene Skandale ans Tageslicht beförderten, werden sie aber auch zur generellen Steuerung bzw. Manipulation menschlichen Handelns verwendet, wie etwa zur Beeinflussung des Wahlverhaltens (Susser, Roessler, und Nissenbaum 2018). Mehr als ein halbes Jahrhundert später scheinen mit den derzeitigen und weiter zunehmenden Möglichkeiten der Datenverarbeitung also gewissermaßen die Träumereien einiger Akteure der 60er-Jahre hinsichtlich Bevölkerungskontrolle und Automation wahr zu werden.

Politische Entscheidungen wie die DSGVO bilden einen politischen Kompromiss ab, der angesichts des konfliktiven Geflechts aus individuellem Grundrecht auf Datenschutz, der Nutzung personenbezogener Daten für Gemeinwohlzwecke und ihrer ökonomischen Verwertung erzielt wurde. Die Reflektion der Entstehungsbedingungen der DSGVO trägt somit

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auch zur Entzerrung der jeweiligen Positionen und einem besseren Verständnis der datenschutzpolitischen Konfliktlinien bei, die sich auch in den gegenwärtigen digitalpolitischen Auseinandersetzungen rund um den Data Act oder AI Act widerspiegeln und es wohl auch in den Debatten über noch kommende Digitalvorhaben tun werden.

Der folgende Abschnitt (1.2) widmet sich der Diskussion des Forschungsstands und der Herausarbeitung der übergeordneten Fragestellung des vorliegenden Dissertationsvorhabens.

1.2 Forschungsstand und Fragestellung

In den vergangenen Jahren haben sich mehrere politikwissenschaftliche Publikationen aus unterschiedlichen Perspektiven mit der Frage der Entstehung der DSGVO auseinandergesetzt. Im Folgenden wird der Forschungsstand anhand dieser Werke vorgestellt und diskutiert.

Im Jahr 2018 erschien die erste umfassende politikwissenschaftliche Untersuchung zur DSGVO. Wie das vorliegende Dissertationsvorhaben auch, verfolgt die Dissertationsschrift von Laima Jančiūtė (2018) das Ziel, die Rolle von Akteursinteressen bei der Verabschiedung der DSGVO zu untersuchen. Jančiūtė verortet ihre Arbeit im Bereich der Forschung zu Kommunikations- bzw. Medienpolitik. Ihr analytischer Rahmen baut auf Elementen von Policy-Netzwerken (Advocacy-Koalitionen, epistemische Communities, Lobbying) sowie Neo-Institutionalismus auf und verwendet als verbindenden Rahmen konkordanzdemokratische Elemente (moderater Staatszentrismus). Mittels Dokumentenanalyse und Interviews untersucht sie die Position von Kommission, Europäischem Parlament, Ministerrat, Datenschutzaufsichtsbehörden, dem europäischen Datenschutzbeauftragten (EDSB), der Europäischen Grundrechteagentur FRA, zivilgesellschaftlichen Datenschützern, Industrievertretern sowie der US-Regierung. Dabei fokussiert sich die Autorin auf die strittigen Punkte „Richtlinie vs. Verordnung", „Delegierte und Durchführungsrechtsakte", „die Kontroverse zum Einbezug des öffentlichen Sektors" sowie „das Prinzip der zentralen Kontaktstelle". In ihren Ergebnissen verweist Jančiūtė schließlich in erster Linie auf den Einfluss der im EU-Ministerrat versammelten EU-Mitgliedstaaten im Hinblick auf die Verabschiedung der DSGVO, die sich insbesondere bei der Ausgestaltung des Prinzips der zentralen Kontaktstelle, den Regelungen zum öffentlichen Sektor sowie der Einführung zahlreicher Öffnungsklauseln niedergeschlagen habe. Die Rolle des Parlaments wiederum sei

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

entscheidend im Hinblick auf die Stärkung des allgemeinen Datenschutzniveaus, die Einführung starker Betroffenenrechte sowie die Einführung hoher und einheitlicher Sanktionsregelungen gewesen. Entsprechend dieser Ergebnisse stellt die Autorin schließlich fest, dass die Vorhersagen der rational choice-Perspektive am ehesten in der Lage seien, den politischen Aushandlungsprozess zur DSGVO zu erklären (ebd.). Insgesamt bietet die Dissertation einen guten Überblick über den Aushandlungsprozess der DSGVO, indem die zentralsten Akteure benannt und ihre Positionen aufgezeigt werden. Andererseits leidet die Arbeit unter der Engführung auf die vier oben genannten Konfliktfelder, sowie auf die interinstitutionellen Verhandlungen zwischen Parlament, Ministerrat und Kommission. Fragen nach der Ausgestaltung der datenschutzrechtlichen Regelungen der DSGVO, bspw. zum Thema Einwilligung, bleiben unberücksichtigt. Fraglich ist daher, ob die Engführung auf die vier Konfliktfelder, in denen mitgliedstaatliche Souveränitätserwägungen die größte Rolle spielten, die Ergebnisse der Arbeit möglicherweise dahingehend prädeterminiert haben, dass die mitgliedstaatlichen Souveränitätserwägungen das entscheidende Kriterium im Aushandlungsprozess gewesen seien. Wie im Laufe der vorliegenden Arbeit noch zu zeigen sein wird, waren weitaus mehr Themen unter den beteiligten Akteuren umstritten und der politische Einfluss von Akteurskoalitionen, die weitaus breiter ausgefächert waren, als jene Akteure, die in Jančiūtės Werk betrachtet werden, war an mehreren Stellen des Aushandlungsprozesses von entscheidender Bedeutung.

Eine weitere Dissertationsschrift, die sich der Erklärung des Zustandekommens der DSGVO widmete, legte Jockum Hildén (2019) vor. Sein Fokus lag auf der Sichtbarmachung des Einflusses von Lobbyisten auf die jeweiligen Positionen der Kommission, des EU-Parlaments, des Ministerrats sowie auf den Text der finalen DSGVO. Hildén zeigt auf, dass der Erfolg von Lobbying bei der Einflussnahme auf DSGVO-Inhalte von der Nähe zu den jeweiligen Entscheidungsinstanzen abhing. Demnach habe die Nähe des Generaldirektors Justiz der EU-Kommission (GD Justiz) zu bürgerrechtlichen Stimmen den Einfluss von Wirtschaftslobbyisten erschwert. Umgekehrt habe die (rechts-)konservative Parteizugehörigkeit von EU-Parlamentsabgeordneten Ministerratsakteuren zu einer verstärkten Einflussnahme von Wirtschaftslobbyisten in Parlament und Ministerrat geführt. Kritisch einzuwenden ist, dass sich auch seine Analysen lediglich auf zwei kritische Aspekte der DSGVO beschränken, die Verankerung des Rechts auf informationelle Selbstbestimmung einerseits und der prozedurale Ansatz zum Schutz personenbezogener Daten andererseits. Auch Hildén

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

vernachlässigt damit weitere im DSGVO-Entscheidungsprozess relevante Diskussionsthemen.

Auch Laurer und Seidl (2021) untersuchen in ihrem Journal-Beitrag die Gründe für die Entstehung der DSGVO. Konkret fragen die beiden, weshalb es zu trotz intensiven Lobbyings zu einer Stärkung des EU-Datenschutzes gekommen ist. Mittels Process Tracing untersuchen sie im ersten Schritt kausale Mechanismen, die von der 1995 verabschiedeten DS-RL zum DSGVO-Kommissionsentwurf im Jahr 2012 führten. In einem zweiten Schritt untersuchen die Autoren mittels discourse network analysis Verschiebungen in den Positionierungen lobbyierender Akteure. Als Datengrundlage dienen Statements unterschiedlicher Akteure über die DSGVO aus US-amerikanischen und europäischen Zeitungen, Mit der New York Times und der Financial Times wurden zwei große für die US-Seite repräsentative Zeitungen ausgewählt. Zur Untersuchung der europäischen Stimmen setzten die Autoren jedoch ausschließlich auf die zwar inhaltlich durchaus einschlägigen, aber im Vergleich zu verschiedenen großen nationalen Publikationen, die tiefgehend über EU-Politikprozesse berichten (wie die FAZ, Der Spiegel, BBC) dennoch eingeschränkten Publikationen Europolitics und Euractiv. Im Hinblick auf den von ihnen als *Agenda Setting Stage* bezeichneten Zeitraum zwischen 1990 bis 2009 resümmieren Laurer und Seidl, dass drei Faktoren ausschlaggebend waren: Erstens und grundlegend habe die mit der Verabschiedung der DS-RL 1995 einhergehende Gründung nationaler Datenschutzaufsichtsbehörden in jenen Mitgliedstaaten, in denen noch keine existierten und der gleichzeitigen Gründung der Art. 29-Datenschutzgruppe (Datenschutzgruppe), unter deren Dach die europäische Kooperation der nationalen Behörden institutionalisiert wurde, eine Pro-Datenschutz-Lobbygruppe im Zentrum der europäischen Politik installiert. Diese haben dann, zweitens, in entscheidender Weise bei der Eingliederung von Datenschutz in der EU-Grundrechtecharta mitgewirkt und, drittens, schließlich auch bei der Gestaltung des Europäischen Verfassungsvertrags bzw. des Lissabon-Vertrags, die entscheidend im Hinblick auf die Geburt der DSGVO waren. Wie sich im Rahmen der vorliegenden Studie noch zeigen wird, ist die Aussage über diese Beeinflussung nicht falsch, aber unterschätzt sowohl die maßgebliche Beteiligung weiterer Akteure, als auch die Wirkung weiterer Faktoren und Mechanismen, die beim Agenda Setting wichtig waren. Im Hinblick auf den als *Policy Formulation Stage* bezeichneten Zeitraum zwischen 2009 und 2012 stellen die Autoren fest, dass die Verortung der institutionellen Zuständigkeit für

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Datenschutzreform beim GD Justiz ausschlaggebend für die Inhalte sowohl des DSGVO-Kommissionsentwurfs als auch der finalen DSGVO war, weil die Nähe des Generaldirektorats Justiz zu Datenschützern und insb. der Art.-29-Datenschutzgruppe zu einer Bevorteilung dieser und einer Benachteiligung von Stimmen aus der Wirtschaftslobby geführt habe. Die Feststellungen der Autoren zu den Faktoren die in der *decision making phase* zwischen 2012 und 2016 maßgeblich für die Verabschiedung der DSGVO waren, stimmen mit den Analysen der meisten anderen Autorinnen und Atoren überein.[3] Demnach stand der Kommissionsentwurf in der ersten Hälfte des Jahres 2013 im EU-Parlament kurz vor seiner Verwässerung, was erst durch den Snowden-Schock verhindert werden konnte. Den Ergebnissen der discourse network analysis zufolge war das entscheidende Argument für die Befürwortung der DSGVO im Nachgang der Snowden-Enthüllungen die Bezugnahme auf die sich in den Überwachungsmaßnahmen widerspiegelnde geopolitische Rivalität zwischen der EU und den USA. Laurer und Seidl geben damit einen instruktiven Einblick in die Post-Snowden-Positionierung der Akteure. Unbetrachtet bleibt bei ihnen jedoch, ob und inwiefern die lobbyierende Akteure es tatsächlich vermocht haben, verschiedene Elemente des Kommissionsvorschlags in ihrem Sinne zu beeinflussen. Zudem wird die vorliegende Studie aufzeigen, dass einige ihrer Aussagen unter Einbeziehung weiterer Informationen widerlegt werden müssen, so etwa die Aussage, dass die deutsche Bundesregierung ihre ablehnende Haltung nach den Snowden-Enthüllungen überdachte habe.

Auch der Journal-Beitrag von Goyal et al. (2021) widmet sich der Erklärung der Entstehung der DSGVO. Aus der Perspektive einer um einen Technology-Stream erweiterten Version des Multiple Stream-Frameworks bestätigen die Autoren einerseits die Ergebnisse anderer Studien. Andererseits argumentieren sie, dass technologischer Wandel einen entscheidenden Effekt auf die DSGVO-Entstehung gehabt habe. Letztlich beschränkt sich ihre Analyse jedoch darauf, dass technologischer Wandel – wie auch von anderen bereits argumentiert wurde (z. B. Burri und Schär 2016, 481 f.) – zur Notwendigkeit der Überarbeitung der DS-RL beigetragen habe, oder in den Worten des Multiple Stream-Frameworks zur Ausreifung des Problemstroms beigetragen habe. Ob und inwiefern technologischer Wandel auch

3 Der Snowden-Effekt auf die DSGVO-Verhandlungen ist Gegenstand mehrerer weiterer Publikationen, die andere Fragen als die Entstehung der DSGVO im Fokus haben (siehe insb. Kalyanpur und Newman 2019; Rossi 2018).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

während des DSGVO-Aushandlungsprozesses eine Rolle spielte, bleibt allerdings unklar.

Schließlich untersuchen Schünemann und Windwehr (2020) in ihrem Journal-Beitrag die Frage, ob die treibenden Kräfte bei der Verabschiedung der DSGVO supranationale EU-Institutionen in Gestalt der EU-Kommission und des EU-Parlaments oder Mitgliedstaaten waren. Ausgehend von einer Analyse der Konflikte zu den Themen Recht auf Vergessenwerden, Recht auf Datenportabilität sowie data protection by design/by default stellen die Autorin und der Autor fest, dass keiner der Mitgliedstaaten, die zum DSGVO-Verhandlungszeitpunkt über ein hohes Datenschutzniveau verfügten, die Verabschiedung der DSGVO mit einem hohen Schutzniveau befürworteten. Dieses Handeln der Mitgliedstaaten führen sie auf drei mögliche Erklärungen zurück: Das erfolgreiche Lobbying durch Wirtschaftsakteure, die Furcht der Mitgliedstaaten, in der kompetitiven Situation weltweiter Digitalmärkte durch restriktive Datenschutzgesetze weitere Anteile zu verlieren sowie die Erwartung, dass Datenschutz als wenig öffentlichkeitswirksames und sehr technisches Thema keine breite öffentliche Unterstützung nach sich ziehen werde. Unbeachtet bleibt dabei, dass bereits die Erwartung, dass einzelne Mitgliedstaaten mit einem höheren Datenschutzniveau als norm entrepreneur ein Interesse daran haben würden, Rechtselemente wie das Recht auf Vergessenwerden, das Recht auf Datenportabilität oder data protection by design/by default unterstützen würden, in die Irre führt: In keinem Mitgliedstaat und auch nicht in jenen Mitgliedstaaten mit einem hohen Datenschutzniveau war eines der genannten Rechtselemente vor der DSGVO vorhanden. Erwartbar wäre also eher gewesen, dass die Mitgliedstaaten mit einem hohen nationalen Datenschutzniveau eine Harmonisierung entlang ihrer Vorschriften begrüßt hätten. Eine Befürwortung der drei genannten Rechtselemente hätte jedoch auch für diese Mitgliedstaaten eine Abweichung von ihren nationalen Normen bedeutet.

Die diskutierten Arbeiten stellen alle einen wichtigen Beitrag zur Erklärung des Zustandekommens der DSGVO dar. Aus ganz unterschiedlichen Perspektiven identifizieren sie ausschlaggebende Faktoren, wie die Bedeutung des institutionalisierten Datenschutzes in Gestalt der Datenschutzgruppe, die Rolle der EU-GrCh, des Lissabon-Vertrags, der Agenda-Setting-Rolle der Kommission und der außerordentlichen Wirkung des Snowden-Schocks auf den Verlauf der interinstitutionellen Verhandlungen. Zudem heben alle Beiträge die Bedeutung von Akteurskoalitionen bei der Entstehung der DSGVO hervor.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Obwohl die diskutierten Beiträge wertvolle Einsichten in die Entstehungsgründe der DSGVO liefern, strebt die vorliegende Arbeit eine umfassendere Betrachtung der einzelnen Elemente an, um den Forschungsstand an entscheidenden Stellen zu ergänzen. Hierzu zählt insbesondere der umfassende Abgleich von Akteurspositionen mit den Ergebnissen politischer Entscheidungen bzw. der Legislativdokumente von Kommission, Parlament, Ministerrat und schließlich der finalen DSGVO selbst. Dies verspricht eine genauere Nachvollziehung der Einflussnahme von Lobby-Akteuren auf den Inhalt der DSGVO, indem klar wird, welche DSGVO-Elemente (bzw. die Positionen von Kommission, Parlament und Ministerrat) in welcher Weise auf das Lobbying der unterschiedlichen Akteure zurückgeführt werden kann. Ein weiteres Kerninteresse der vorliegenden Schrift gilt der Identifizierung kausaler Wirkungsmechanismen, die bei der Entstehung der DSGVO entscheidend waren. Wie noch zu zeigen sein wird, spielten Aspekte wie der Wandel in der öffentlichen Meinung, aber auch das EU-Parlament und einige Mitgliedstaaten bei der Initiierung der Datenschutzreform 2009 eine wichtige Rolle. Bislang vernachlässigt wurde zudem die Rolle einiger Mitgliedstaaten bei der erfolgreichen Verabschiedung der DSGVO.

Die vorliegende Studie soll zu diesen genannten Punkten einen Beitrag leisten und damit zum einen bisher nicht oder wenig beachtete Faktoren bei der Entstehung der DSGVO beleuchten. Zum anderen soll die Untersuchung der Entstehung der DSGVO in den Kontext der historischen EU-Datenschutzpolitik eingeordnet werden.

Die übergeordnete Fragestellung lautet dementsprechend:

Wie lässt sich die Entstehung der EU-Datenschutz-Grundverordnung (DSGVO) vor dem (datenschutz-)polit-historischen Kontext erklären?

Damit wird in der die Arbeit die Beantwortung von zwei miteinander zusammenhängenden Forschungsfragen angestrebt. Die zentrale, erste Forschungsfrage (FF 1) lautet:

FF 1: Wie lässt sich die Entstehung der EU-Datenschutz-Grundverordnung (DSGVO) erklären?

Damit zusammenhängend lautet die zweite Forschungsfrage (FF 2):

FF 2: Welche (datenschutz-)politischen und historischen Faktoren wirkten als kausale, treibende Faktoren auf dem Weg zur DSGVO?

Empirisch leistet die vorliegende Arbeit insbesondere dadurch einen signifikanten Beitrag zu der Debatte um die Entstehung der DSGVO, indem anhand der Inhaltsanalyse des enormen Text-Korpus von an Kommission,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Parlament und Ministerrat gerichteten Lobby-Dokumenten ein tiefgehender Einblick in die von Lobby-Akteuren vertretenen Inhalte und deren inhaltliche Überschneidungen mit den Positionen der EU-Organe ermöglicht wird. Auf theoretischer Ebene leistet die Arbeit einen Beitrag, indem die in bisherigen Studien eher am Rande betrachtete Rolle von Advocacy Koalitionen unter Hinzuziehung weiterer erklärender Faktoren in Form relativ stabiler Parameter und externer, dynamischer Systemereignisse in den Mitttelpunkt der Arbeit gerückt wird.

1.3 Struktur der Arbeit

Die Forschungsfragen der Arbeit werden im Verlauf von einem theoretischen und zwei inhaltlichen Kapiteln beantwortet.

Der folgende Abschnitt spezifiziert den theoretischen Rahmen der Arbeit und die gewählte Methodik. Ausgehend von einer Diskussion verschiedener theoretischer Modelle, die für eine Policy Analyse grundsätzlich infrage kommen, wird das Advocacy Coalition Framework (ACF) als passender theoretischer Rahmen zur Beantwortung der Forschungsfragen gewählt. Im Anschluss werden die für die vorliegende Arbeit zentralen Elemente des ACF erläutert. In Abschnitt 2.3 wird im Rahmen des Forschungsdesigns schließlich ausgeführt, wie das ACF in Kombination mit Process Tracing für die Beantwortung der Forschungsfragen operationalisiert wird. Daran anschließend wird in Abschnitt 2.3.5 ausgeführt, auf welcher Methodik und Datengrundlage die Arbeit aufbaut.

Die empirische Analyse gliedert sich schließlich in zwei voneinander getrennte Schritte. Im Rahmen der Kontextanalyse werden in Abschnitt 3 zunächst die gemäß ACF langfristig relevanten Rahmenbedingungen der EU-Datenschutzpolitik untersucht. Kapitel drei ist in vier Unterabschnitte unterteilt, die sich der Frühphase der Europäischen Datenschutzpolitik (Abschnitt 3.1), den ersten Datenschutz-Instrumenten auf EU-Ebene (Abschnitt 3.2), der EU-Datenschutzpolitik nach der Jahrtausendwende bis 2009 (Abschnitt 3.3) sowie dem Wandel weiterer relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform wichtig waren (Abschnitt 3.4), widmen.

Daran schließt sich die umfassende Untersuchung des Aushandlungsprozesses der DSGVO im Rahmen der Akteurs- und Prozessanalyse in Abschnitt 4 an. Dieses Kapitel ist wiederum in drei empirische Unterkapitel untergliedert, die den Aushandlungsprozess zeitlich in eine Orientierungs-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

phase von 2009 bis 2010 (Abschnitt 4.1), eine Entwurfsphase von 2010 bis 2012 (Abschnitt 4.2) sowie eine Konfliktphase von 2012 bis 2015 (Abschnitt 4.3) aufteilen. In einem vierten Unterkapitel (Abschnitt 4.4) werden schließlich die Forschungsfragen bzw. die übergeordnete Fragestellung der vorliegenden Arbeit beantwortet.

Im Schlussteil der Arbeit werden die Ergebnisse der Arbeit zusammengefasst (6.1), die gewählte Theorie, Methodik und die empirische Analyse bzw. deren Ergebnisse kritisch reflektiert und auf offene Fragen bzw. Forschungsdesiderate eingegangen (6.2). Schließlich wird ein Ausblick auf die weitere Entwicklung der Datenschutzpolitik gewagt (6.3).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2 Theoretischer Rahmen und Methodologie

Die Fragestellung der vorliegenden Studie nach der Entstehung der DSGVO lässt sich zunächst im Bereich der Policy-Analyse verorten. Einer populären und zugleich sehr kompakten Definition nach, besteht das Ziel der Policy-Forschung darin, zu untersuchen: „(1) Was politische Akteure tun, (2) warum sie es tun und (3) was sie letztlich damit bewirken" (Thomas R. Dye, zit. nach: Blum und Schubert 2011, 16). Damit fokussiert die Policy-Forschung auf die Untersuchung konkreter politischer Inhalte, den Policy-Aspekt der Trias der Politikwissenschaft, die aus *policy*, *politics* und *polity* besteht. Das Ziel einer Policy-Analyse besteht also darin, das Zustandekommen einer politischen Maßnahme zu erklären, indem die politics- und polity-Dimensionen als erklärende Faktoren herangezogen werden. Dies wiederum erfolgt, indem theoriegeleitet vorgegangen wird. Der Rückgriff auf Theorien dient dem Zweck, Vergleichbarkeit zwischen unterschiedlichen empirischen Untersuchungen zu gewährleisten, um also vom Einzelfall auf die allgemeine Ebene der Funktionsweise der Politik zu abstrahieren. Die einer Policy-Analyse zugrundeliegenden Theorien berücksichtigen als erklärende Faktoren „rationalistische Handlungs- und Verhandlungskonzepte (z. B. die Spieltheorie) und soziologische Tausch- und Netzwerktheorien und konzipieren politische Prozesse als eine komplexe Verkettung von Tausch- und Entscheidungssituationen, die durch institutionelle Kontexte und Beziehungsstrukturen in den relevanten Akteurskonstellationen beeinflusst werden." (V. Schneider und Janning 2006, 76) Die theoretische Perspektive, mit der ein politisches Phänomen betrachtet wird, prägt dabei auf wesentliche Art und Weise die Ergebnisse der Analyse. Jede theoretische Perspektive fokussiert auf bestimmte Aspekte und Erklärungsperspektiven, die eine möglichst realitätsnahe Beschreibung des Politikphänomens versprechen. Die unterschiedlichen Analyserahmen der Policy-Forschung unterscheiden sich insbesondere darin, „inwieweit sie die Prägekraft von institutionellen Vorgaben, die Auswirkung der ‚Einbettung' von Policy-Interaktionen oder aber die Handlungsspielräume und Präfe-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

renzwahlen der Akteure in den Vordergrund stellen bzw. als erklärende Faktoren betonen." (ebd.)[4]

Welche Perspektive eingenommen wird, hängt schließlich von der Fragestellung, dem Untersuchungsgegenstand, aber auch von den individuellen Präferenzen der Wissenschaftlerin oder des Wissenschaftlers ab. Diese Aspekte gilt es daher besonders gründlich und transparent zu begründen (Bandelow, Kundolf, und Lindloff 2014, 29). Im Folgenden Unterabschnitt 2.1 wird also zunächst die Theorieauswahl diskutiert und begründet. Daran schließt sich die Diskussion des gewählten theoretischen Rahmens in Form des Advocacy Coalition Frameworks (ACF) in Unterabschnitt 2.2 an. Diese Diskussion fokussiert auf die für die Zwecke der vorliegenden Arbeit relevanten Aspekte des ACF. Aus dem ACF wird im Anschluss (vgl. Unterabschnitt 2.3) schließlich das Forschungsdesign abgeleitet und die notwendigen Elemente des Forschungsdesigns in Form der Forschungsstrategie, der Fallauswahl, des analytischen Rahmens, der Operationalisierung, sowie die Details der Datenerhebung und Datenanalyse werden diskutiert und begründet.

2.1 Welche theoretischen Rahmen kommen grundsätzlich infrage?

Wie die Diskussion im Forschungsstand aufgezeigt hat, waren die treibenden Faktoren der EU-Datenschutzpolitik Akteure, die auf Grundlage ihrer Überzeugungen (Datenschutz als Grundrecht betrachtende, überzeugungsgetriebene Akteure wie die Datenschutzgruppe) und unter Nutzung ihrer Ressourcen die Datenschutzpolitik in ihrem Sinne zu beeinflussen strebten. Ins Blickfeld rückt also die politics-Dimension der politischen Akteure: Die Betrachtung ihrer Handlungsmotivationen und Auseinandersetzungen bei der Aushandlung politischer Maßnahmen. Zugleich hat der Forschungsstand aber auch den Einfluss institutioneller Faktoren verdeutlicht. Etwa der institutionellen Gestaltung des politischen Aushandlungsprozesses der EU (Machtausbau des EU-Parlaments in Folge des Inkrafttretens des Lissabon-Vertrags) und der verfassungsrechtlichen Rahmenbedingungen (Datenschutz und Privatheit als unmittelbar geltendes EU-Grundrecht seit dem Inkrafttreten der EU-Grundrechtecharta). Die Literatur weist aber auch auf

4 Die hier allgemein als *Theorie* oder *theoretische Perspektive* diskutierten Zugänge lassen sich intern anhand ihres Abstraktionsgrades (von *wenig abstrakt* zu *sehr abstrakt*) noch einmal unterteilen in: *Konzepte*, *Modelle*, *analytische Rahmen* und *Theorien* (Schubert und Bandelow 2009, 7–12).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

den rasanten technischen Wandel oder auf die Snowden-Enthüllungen und somit auf die Relevanz externer Faktoren hin.

Während der Analyse von Ideen und Überzeugungen vor allem in der deutschen Policy-Forschung eher eine nachgeordnete Rolle zugesprochen wurde (Bandelow 2009), etablierte sich in den vergangenen Jahrzehnten gerade im US-amerikanischen Raum ein reges Interesse an der Ausarbeitung policy-theoretischer Rahmen, in denen Überzeugungen und Ideen eine zentrale Rolle einnehmen. Im Folgenden sollen kurz der Multiple Streams-Ansatz, die Punctuated Equilibrium-Theorie, das Narrative Policy Framework, sowie das Advocacy Coalition Framework, die alle als theoretischer Rahmen für das Dissertationsvorhaben in Frage kommen könnten, kurz vorgestellt und meine Entscheidung für das ACF begründet werden.

Der *Multiple Streams* Ansatz (MSA) von John Kingdon fokussiert auf der Interaktion zweier Arten von Ideen: Ein erster Typus an neuen Ideen, die im Hinblick auf die Lösung von Politik-Problemen geeignet sein könnten sowie ein zweiter Typus an etablierten Ideen, denen zumeist die relevanten politischen Entscheider in einem Politikfeld anhängen, wodurch die Akzeptanz neuer Ideen aufgehalten oder verzögert wird. Dem MSA nach sind drei Ströme im Hinblick auf die Veränderung von Politiken entscheidend: Der Problem-, der Politics- sowie Policy-Strom. Der Problem-Strom besteht aus Sachverhalten, „die als Probleme wahrgenommen werden, veränderlich sind und politisch geändert werden sollten." (Herweg 2015, 328) Der Politics-Strom beschreibt das Feld der politischen Auseinandersetzungen, auf dem sich die öffentliche Meinung, Interessengruppen und Akteure aus der unmittelbaren und mittelbaren Politik aufeinandertreffen und um die Lösung von Problemen ringen. Der Policy-Strom schließlich beschreibt die Summe aller Ideen, die im Hinblick auf die Lösung eines Problems existieren. Dabei wird nicht von der Existenz einer rationalen Problemlösung ausgegangen, sondern davon, dass unterschiedliche Akteure Probleme und Lösungen unterschiedlich wahrnehmen. Neue Ideen finden dem Ansatz nach dann Eingang in politische Programme und Maßnahmen, wenn es einem *Policy Entrepreneur* gelingt, die drei Ströme während eines *politischen Gelegenheitsfensters* miteinander erfolgreich zu verbinden und einen Wandel zu bewirken. Allerdings liegt das zentrale Erkenntnisinteresse des MSA nicht auf der Erklärung der konkreten Ausgestaltung einer Policy, sondern auf der Erklärung des Zeitpunkts eines Wandels (Cairney und Zahariadis 2016; Heikkila und Cairney 2017).

Auch die *Punctuated-Equilibrium-Theorie* legt das Hauptaugenmerk darauf, zu untersuchen, wie sich neue Ideen gegenüber älteren, etablierten

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ideen durchsetzen. Dass auf lange Phasen politischer Stabilität unter bestimmten Bedingungen sehr abrupte und tiefgreifende Veränderungen folgen können ist sowohl Ausgangspunkt als auch Untersuchungsgegenstand der Punctuated-Equilibrium-Theorie. Zur Erklärung wird auf negative Feedback-Zyklen, die der Bewahrung des Status Quo dienen, und positive Feedback-Zyklen, die der politischen Innovationen dienen, verwiesen. Ein abrupter und tiefgreifender politischer Wandel ist demnach möglich, wenn neue politische Akteure und neue Zuständigkeitsbereiche aufgrund der spezifischen Bedingungen der betrachteten politischen Thematik und der sonstigen Umweltbedingungen (z. B. öffentliche Meinung) Eingang in den Entscheidungsfindungsprozess finden (Beyer, Boushey, und Breunig 2015; Heikkila und Cairney 2017).

Das Advocacy Coalition Framework (ACF) stellt Überzeugungen in den Mittelpunkt der Untersuchung. Dem ACF nach besteht das Kerninteresse politischer Akteure darin, ihre eigenen Überzeugungen in politische Maßnahmen zu übersetzen. Akteursüberzeugungen werden im ACF detailliert auf drei Stufen konzipiert (Grundüberzeugungen, Policy-Kernüberzeugungen und Sekundärüberzeugungen). Des Weiteren wird angenommen, dass sich Akteure zum Zwecke der wirkungsvolleren politischen Einflussnahme auf Grundlage geteilter Überzeugungen zu verschiedenen sog. Advocacy-Koalitionen zusammenschließen und in politischen Entscheidungsprozessen gegeneinander antreten. Dieser Schritt ist sowohl eine Annahme des ACF, dass Akteure sich also tatsächlich in Koalitionen zusammenschlössen. Er wird aber auch explizit als eine Methodik angesehen, mit der sich das ACF besonders dazu eigne, komplexe politische Auseinandersetzungen abzubilden, indem auf die wesentlichen Argumente der wesentlichen Akteure, die als Koalitionen betrachtet werden, zurückgegriffen wird. Welcher Advocacy-Koalition es gelingt, sich durchzusetzen, wird wiederum von den institutionellen Bedingungen und insb. von externen Schocks abhängig gemacht (Heikkila und Cairney 2017; Jenkins-Smith u. a. 2017).

Das *Narrative Policy Framework* räumt Ideen ebenfalls einen zentralen Platz ein: Demnach greifen politische Akteure auf Narrative (stilisierte Vorstellungen der Herkunft politischer Forderungen, ihrer Ziele und möglichen Auswirkungen), zurück, um politischen Einfluss auszuüben. Zudem wird argumentiert, dass sich politische Akteure auf Basis geteilter Narrative zu Advocacy-Koalitionen zusammenschließen, um ihr Narrativ in der politischen Auseinandersetzung mit stärkerem politischem Gewicht zu vertreten und so einen Wandel in der Politik zu bewirken (Heikkila und Cairney 2017; Shanahan u. a. 2017).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.1.1 Wahl des theoretischen Rahmens

Ein theoretischer Rahmen, der den Erfordernissen der im Rahmen dieser Studie untersuchten Fragestellungen gerecht wird, muss also in erster Linie den Überzeugungen der an politischen Entscheidungsprozessen beteiligten Akteure einen möglichst großen Platz einräumen, um nachvollziehen zu können, ob und inwiefern diese ihre Überzeugungen in Politik-Ergebnisse gießen konnten. Zudem muss der theoretische Rahmen es erlauben, eine größere Bandbreite an Akteuren zu erfassen und eine Vielzahl an externen Einflussfaktoren zu berücksichtigen.

Der nun folgenden Diskussion sei vorangestellt, dass sich alle aufgelisteten theoretischen Rahmen grundsätzlich zur Bearbeitung der Fragestellung eignen. Mehr noch, kann die Anwendung eines voraussichtlich weniger gut passenden Rahmens wertvolle, von anderen Erklärungen abweichende Erkenntnisse im Hinblick auf den Untersuchungsgegenstand oder auch im Hinblick auf die Theoriediskussion liefern (Weible 2014, 393). Alle genannten theoretischen Rahmen greifen die zentralen, im Forschungsstand vorgestellten Elemente meines Untersuchungsgegenstandes auf. Aufgrund von Nuancen fiel meine finale Entscheidung jedoch für das Advocacy Coalition Framework aus. Diese Entscheidung möchte ich im Folgenden begründen.

So fokussieren sowohl MSA, als auch PET und ACF auf die Erklärung von Policy-Wandel. Obwohl Akteursüberzeugungen in allen drei Ansätzen eine zentrale Rolle spielen, sticht das ACF dennoch gegenüber MSA als auch PET hervor: Während letztere stärker auf das Moment eines abrupten Policy-Wandels nach Phasen längerer Stabilität fokussieren, nimmt ACF zusätzlich in den Blick, welchen Einfluss die überzeugungsgetriebenen Auseinandersetzungen zwischen politischen Akteuren langfristig auf politische Entwicklungen haben. Inwiefern sich ein maßgeblicher Policy-Wandel ereignete, steht beim ACF nicht so sehr im Vordergrund wie bei den übrigen Ansätzen. Zudem erlaubt der gleichzeitige starke Fokus des ACF auf Akteure und Überzeugungen die detaillierte Offenlegung des Beziehungsgeflechts der beteiligten Akteure. Die Beantwortung der Frage, *wer auf Grundlage welcher Überzeugungen wie miteinander kooperiert hat*, ist eine der Stärken des ACF. Schließlich spricht für das ACF, dass eine Vielzahl an institutionellen und externen Einflussfaktoren Berücksichtigung findet.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.2 Das Advocacy Coalition Framework

Das vorliegende Kapitel dient der Vorstellung des ACF, das dem Dissertationsvorhaben als theoretischer Rahmen zugrunde liegt. Eingangs wird kurz in die Entstehung und Entwicklung des ACF eingegangen. Die sich daran anschließenden Unterabschnitte gehen auf die einzelnen zentralen Aspekte des Frameworks ein und fokussieren insbesondere auf die Elemente des ACF, die auch im Rahmen des empirischen Teils dieser Arbeit stärkere Berücksichtigung finden werden.

Das Advocacy Coalition Framework (ACF) wurde im Laufe der 1980er-Jahre unter der Ägide des US-amerikanischen Policy-Forschers Paul Armand Sabatier entwickelt (Sabatier 1987). Sabatier entwickelte das ACF, da er mit den damals dominanten Ansätzen der Policy-Analyse aus drei Gründen nicht zufrieden war. Erstens kritisierte er den damals üblichen Rückgriff auf die Phasenheuristik (Blum und Schubert 2011, 105, 133–37; V. Schneider und Janning 2006, 49) dafür, dass diese keine kausalen Erklären anbiete (Sabatier 2007, 6 f.). Zweitens wurden die bestehenden Erklärungsansätze dafür kritisiert, dass sie entweder auf top-down- oder auf bottom-up-Erklärungen fokussierten, aber eine Verbindung beider Erklärungsansätze nicht in ausreichendem Maße in Erwägung zogen. Drittens sah Sabatier – weil das ACF im Umfeld der Debatten um Umweltpolitik entstand – die Notwendigkeit, der politischen Verarbeitung wissenschaftlicher Kenntnisse in einem theoretischen Rahmen einen Platz einzuräumen (Jenkins-Smith und Sabatier 1993b, 1 f. Weible, Sabatier, und McQueen 2009, 122). In einer Zeit, in der die institutionelle Zugehörigkeit eines Akteurs und insbesondere die von politischen Entscheidungsträgern innerhalb politischer Institutionen zumeist als entscheidend im Hinblick auf eine Akteursposition interpretiert wurde, intervenierte das ACF mit der Vorstellung, dass Individuen innerhalb von Organisationen auf Grundlage ihrer individuellen Überzeugungen durchaus auch abweichende Forderungen unterstützen und sich auf dieser Grundlage mit anderen Akteuren zu Advocacy-Koalitionen zusammenschließen würden (Sabatier 1998, 107).

Ursprünglich hatte das ACF das Ziel, konkreten Policy-Wandel durch Policy-Lernen über einen Zeitraum von mehr als zehn Jahren zu erklären, doch wird es zunehmend häufiger als allgemeines Konzept zur Policy-Analyse genutzt (Petridou 2014: 14) und auch von maßgeblichen Akteuren der ACF-Forschung für eine Policy-Analyse empfohlen (Weible et al. 2011: 357).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Aufgrund seines Ursprungs, aber auch aufgrund des anfänglichen Fokus der Elemente des ACF auf die US-amerikanische Politik waren die frühen Jahre vor allem durch Anwendungen dominiert, die auf den US-amerikanischen Raum bezogen waren. Nachdem im Laufe der 1990er-Jahre verschiedene Schwierigkeiten bei der Anwendbarkeit des ACF auf europäische politische Systeme auftauchten, folgte die erste größere Revision, mit der das ACF dahingehend modifiziert wurde, Spezifika europäischer politischer Systeme besser zu berücksichtigen (Sabatier 1998).

Das ACF konnte in der Zwischenzeit zu einem der am häufigsten verwendeten theoretischen Rahmen der Policy-Forschung avancieren (Herweg 2013, 323). Nach der Revision des ACF zur besseren Berücksichtigung europäischer politischer Systeme stieg die Anzahl der auf Europa bezogenen Anwendungen deutlich an und erreichte schließlich das Niveau der auf die Vereinigten Staaten bezogenen Analysen (Jenkins-Smith u. a. 2014, 210). In zahlreichen Anwendungen wurden zudem die Elemente und Thesen des ACF im Hinblick auf eine Vielzahl von Untersuchungsgegenständen getestet (ebd.). Die Hauptprotagonisten des ACF, Sabatier, Christopher Weible und Paul Jenkins-Smith wiederum nutzten die Erfahrungen aus den empirischen Anwendungen stets dazu, das ACF zu aktualisieren, indem neue Konzepte und Elemente eingeführt oder deren Verwendung zumindest angeraten wurde (Weible u. a. 2011; Weible und Sabatier 2007b; Weible, Sabatier, und McQueen 2009).

Die vorliegende Arbeit stützt sich auf den Rahmen des ACF in der von Weible ausführlich beschriebenen Fassung von 2007, ergänzt diese allerdings zusätzlich um die Vorschläge und Anregungen aus jüngeren Publikationen (Jenkins-Smith u. a. 2014, 2017; Weible und Sabatier 2007b).

Das Interesse der vorliegenden Schrift an Überzeugungen und den Auseinandersetzungen der Akteure beim Zustandekommen der DSGVO legt die Fokussierung auf die ACF-Elemente *Überzeugungssysteme* (2.2.2) und *Advocacy-Koalitionen* (2.2.3) nahe.[5] Daneben sind auch die im ACF beschriebenen Kontextbedingungen von Interesse, sodass zuvor in Unterabschnitt 2.2.1 auf *relativ stabile Parameter* und *dynamische externe Systemereignisse* eingegangen wird. Entsprechend werden im Folgenden die Grundannahmen des ACF vorgestellt (Policy Subsysteme, Überzeugungssysteme, Advocacy-Koalitionen). Darauf folgt in Unterabschnitt 2.2.4 die Vorstellung

5 Seitens der zentralen ACF-Expert:innen wird die Fokussierung auf einzelne Elemente des ACFs ausdrücklich befürwortet, da der gleichzeitige Fokus auf alle drei Elemente aus forschungspraktischer Sicht in der Regel zu mühsam sei (Weible u. a. 2011, 354).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der klassischen Erklärung von Policy-Wandel gemäß ACF, die auf die Bedeutung von Lernprozessen und externen Schocks abhebt. Nach der Vorstellung des grundlegenden ACF-Konzepts geht Unterabschnitt 2.2.5 schließlich auf die für die Zwecke der vorliegenden Arbeit relevanten Ergänzungen des ACF in Form langfristig wichtiger politischer Gelegenheitsstrukturen, kurzfristig wichtiger Koalitionsressourcen, subsystem-interner Schocks und ausgehandelter Kompromisse ein. Darauf folgt eine kurze Diskussion der Schwächen des ACF (in Unterabschnitt 2.2.6) sowie der Anwendbarkeit des ACF auf politische Entscheidungsprozesse auf EU-Ebene (in Unterabschnitt 2.2.7), bevor im folgenden Abschnitt 2.3 schließlich auf das Forschungsdesign und methodologische Vorgehensweise eingegangen wird.

2.2.1 Policy Subsysteme und Kontext

Eine Grundannahme des ACF ist, dass politische Entscheidungsprozesse aufgrund der Komplexität moderner Politik in den meisten Fällen durch das Wirken hoch spezialisierter Akteure innerhalb von „Policy Subsystemen" verhandelt werden. Entsprechend bildet das Policy Subsystem die Untersuchungseinheit des ACF. Dabei unterscheidet sich das ACF-Verständnis eines Policy Subsystems von systemtheoretischen oder institutionalistischen Perspektiven, weil nicht von einer typischen Strukturierung der Akteurskonfiguration (beispielsweise in Gestalt von Parlament, Bürokratie und Interessengruppen, wie im Falle des US-amerikanischen sog. *iron triangle*) ausgegangen wird, sondern die spezifische Konfiguration eines Policy Subsystems als empirische Frage offengelassen wird. Dabei berücksichtigt das ACF nicht nur Politiker, Beamte und Lobbyisten als potentielle Mitglieder eines Policy Subsystems, sondern auch Wissenschaftler, Journalisten und andere fachspezifischen Experten. Ob ein Akteur als Teil des Subsystems betrachtet wird, hängt also etwa nicht von dessen Zugehörigkeit zu einer vordefinierten Gruppe, sondern allein davon ab, ob er sich in relevantem Maße am Subsystem beteiligt hat (Weible und Sabatier 2007b, 192). Als Grundregel zur Identifizierung von Subsystemen schlagen Sabatier und Weible (2007b, 193) vor, sich am inhaltlichen und geographischen Geltungsbereich der Institutionen zu orientieren, die die relevanten Interaktionen strukturieren.

Ähnlich wie bei Politikfeldern, werden Policy Subsysteme nicht als geschlossene Entitäten konzipiert, sondern als semi-unabhängige soziale

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Konstellationen, sie sich im Laufe der Zeit auch verändern können. So können sich Policy Subsysteme beispielsweise überlappen oder auch in andere Policy Subsysteme eingebettet sein. Jenkins-Smith et al. (2017, 139) führen als Beispiel an, dass sich das energiepolitische Subsystem Colorados mit der Nahrungsmittelpolitik desselben Bundesstaates teilweise überlappt, während es zugleich eingebettet ist in das umfassendere nationale energiepolitische Subsystem der Vereinigten Staaten. Zudem lassen sich Policy Subsysteme aber auch in ihrem Reifegraf in „reife" und „entstehende" Subsysteme unterscheiden. Ein Policy Subsystem kann gemäß ACF dann als reif bezeichnet werden, wenn zwei Bedingungen erfüllt sind. *Erstens* dann, wenn eine Reihe von spezialisierten Akteuren für sich eine Expertise in Bezug auf eine politische Problematik beansprucht und politische Entscheidungsprozesse bzw. deren Inhalte in dieser Hinsicht über einen längeren Zeitraum (ca. 10 Jahre) zu beeinflussen versucht. Und *zweitens* dann, wenn zu diesen Akteuren neben staatlichen auch Vertreter aus anderen gesellschaftlichen Teilbereichen wie Interessengruppen und Forschungseinrichtungen zählen, die sich in Form von Untergruppen in Bezug auf die jeweilige politische Problematik spezialisieren und in regelmäßigen Abständen positionieren (Sabatier 1998, 111, 114; Weible und Sabatier 2007b, 192 f., 210). Die Unterscheidung zwischen reifen und entstehenden Subsystem wird deshalb als wichtig angesehen, da der ACF die Annahme vertritt, dass größere Policy-Veränderungen sich in der Regel als schwierig gestalten, weil die Überzeugungssysteme der Akteure, auf deren Basis ihr Handeln innerhalb reifer Subsysteme erfolgt, als stabil und nur schwer veränderlich angesehen werden (ebd.).

Die Unterteilung von Politikfeldern in Subsysteme ist für die Auseinandersetzung mit dem Thema Datenschutz auch deshalb sinnvoll, da in der politikwissenschaftlichen Forschung kaum Einigkeit in Bezug auf die Definition eines Politikfelds besteht (Blum und Schubert 2011, 14; für einen Konzeptvorschlag für Politikfelder, siehe jüngst: Reiberg 2018) und das politische Thema Datenschutz sich gegenüber den etablierten Politikfeldern wie Wirtschaftspolitik, Verbraucherschutz, Innenpolitik und Außenpolitik als Querschnittsthema verhält und somit schwer im Sinne eines klassischen Politikfelds greifbar wäre. Die Identifikation eines Datenschutz-Subsystems kann jedoch anhand der oben beschriebenen Bedingungen vergleichsweise einfach erfolgen. Wie bereits der kurze Überblick im Forschungsstand (vgl. 1.2) zeigte und später auch das Kontext-Kapitel (Abschnitt 3) ausführlich darlegt, handelt es sich bei der Datenschutz-Politik um ein reifes Subsystem.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.2.1.1 Kontext – Relativ stabile Parameter und externe, dynamische Systemereignisse

Das ACF bettet da Handeln von Akteuren in einem Policy Subsystem in einen breiten politischen und sozioökonomischen Kontext bestehend aus zwei Sets exogener Faktoren ein. Das sind einerseits *relativ stabile Parameter* und andererseits *externe, dynamische Systemereignisse.* Die Differenzierung erfolgt dabei nach ihrem Verhalten in der Zeit. Jene Faktoren, die ihre Stabilität über ein Jahrzehnt und länger bewahren, werden als relativ stabil und solche, die sich im Verlauf weniger Jahre ändern können als dynamisch aufgefasst (Weible und Sabatier 2007b, 192 f.).

Zu relativ stabilen Parametern zählen: (1) die grundlegenden Merkmale des betrachteten Problems, (2) die Verteilung natürlicher Ressourcen, (3) grundlegende soziokulturelle Wertvorstellungen und die Sozialstruktur sowie (4) die grundlegende verfassungsmäßige Struktur. Diese sind bedeutsam, da sie den Kontext des betrachteten Phänomens strukturieren, die den Akteuren zur Verfügung stehenden Ressourcen verteilen, die Regeln und Prozeduren festlegen, nach denen kollektive Regelsetzungsmechanismen funktionieren und den allgemeinen Möglichkeitsraum handlungsleitender Orientierungen umreißen und damit die Vielfalt möglicher Alternativen begrenzen, auf deren Basis das Handeln von Advocacy-Koalitionen erfolgen kann. (ebd.)

Zu externen, dynamischen Systemereignissen zählen: (1) der Wandel in den sozioökonomischen Bedingungen, (2) der Wandel in der öffentlichen Meinung, (3) der Wandel maßgeblicher (Regierungs-)Koalitionen und (4) Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen. Eine Veränderung zumindest einer dieser Faktoren wird als Bedingung für einen Policy-Wandel angesehen. (ebd.)

2.2.2 Überzeugungssysteme

Die zweite Grundannahme des ACF baut auf Arbeiten in den Bereichen der Kognitions- und Sozialpsychologie auf. In diesen wird angenommen, dass Individuen die Welt entlang von kognitiven Vorprägungen erleben, die ihnen in komplexen Situationen eine heuristische Handlungsorientierung ermöglichen. Diese kognitiven Vorprägungen werden im ACF in Form von *Überzeugungssystemen* (Belief Systems) operationalisiert und beschreiben ein „Set von grundlegenden Wertvorstellungen, Kausalannahmen und

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Problemperzeptionen" (Sabatier 1993, 127). Vorherrschende Überzeugungen bilden somit eine Art Wahrnehmungsfilter, den eine Information zunächst durchdringen muss. Dies bedingt, dass ein und dieselbe Information von Akteuren – sofern diese über unterschiedliche Überzeugungssysteme verfügen – ganz unterschiedlich wahrgenommen werden kann. Hierbei kommt insb. dem Phänomen sog. *devil shift* (Verteufelung) eine wichtige Rolle zu: Dadurch, dass Akteure mit unterschiedlichen Überzeugungen die Welt auch unterschiedlich wahrnehmen, entsteht Misstrauen. In der Folge tendieren Akteure dazu, ihre Gegner als weniger vertrauenswürdig, böser und mächtiger zu betrachten, als sie es wahrscheinlich sind. Der devil shift verstärkt somit die Bereitschaft politischer Akteure, gegenüber Gleichgesinnten intensivere Verbindungen aufzubauen, während zugleich die Bereitschaft zum Konflikt mit der politischen Konkurrenz erhöht wird. Schließlich wird angenommen, dass das Bestehen von Wahrnehmungsfiltern dazu führt, dass Informationen, die den bestehenden Überzeugungen widersprechen eher ignoriert werden als Informationen, die der Bestätigung der eigenen Überzeugungen dienlich sind. Allerdings unterscheidet das ACF Überzeugungen danach, welche Reichweite sie haben und wie stabil sie sind. Diese Unterscheidung wird im ACF durch eine hierarchische Dreiteilung von Überzeugungssystemen erzielt:

Auf der ersten und umfassendsten Ebene befinden sich die kaum veränderlichen *allgemeinen Kernüberzeugungen* (Deep Core Beliefs). Allgemeine Kernüberzeugungen beinhalten normative Werte und ontologische Axiome, die sich auf alle Policy Subsysteme beziehen können. Entsprechend allgemeiner Natur können auch die allgemeinen Kernüberzeugungen der untersuchten politischen Akteure sein und sich beispielsweise auf Aussagen über die Natur des Menschen (von Grund auf gut vs. von Grund auf böse), die angemessene Verteilung von Kompetenzen zwischen Staat und Markt (Staatsdirigismus Vs. Laissez-faire), die traditionelle links-/rechts-Skala in der Politik, oder die relative Priorisierung unterschiedlicher höchster Werte wie Freiheit, Sicherheit, Macht, Wissen, Gesundheit u. v. m. beziehen. Weil allgemeine Kernüberzeugungen als das Ergebnis frühkindlicher und jugendlicher Sozialisation angesehen werden, gelten sie als nicht oder nur sehr schwer veränderlich (Weible und Sabatier 2007b, 194).

Auf der nächsten Ebene befinden sich die relativ stabilen, aber noch veränderlichen *Policy-Kernüberzeugungen* (Policy Core Beliefs). Diese leiten sich unmittelbar aus den allgemeinen Kernüberzeugungen ab und geben Individuen im Hinblick auf ein spezifisches Policy Subsystem Handlungsorientierung. Somit beziehen sich allgemeine Kernüberzeugungen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zwar nicht unmittelbar auf ein Policy Subsystem, aber da sich die Policy-Kernüberzeugungen direkt aus den allgemeinen ableiten, lassen sich Policy-Kernüberzeugungen als der policy-bezogene Ausdruck der allgemeinen Kernüberzeugungen begriffen werden. Policy-Kernüberzeugungen können sich auf sämtliche Aspekte eines Policy Subsystems beziehen (Weible und Sabatier 2007b, 194 f.). Sabatier und Jenkins-Smith (Sabatier und Jenkins-Smith 1999, 133) definieren elf mögliche Bestandteile von Policy-Kernüberzeugungen, etwa was die Akteure als grundlegendes Problem betrachten, was sie für die Ursachen dieses Problems halten, welche Policy-Instrumente priorisiert werden (allgemeingültige Verordnung, Empfehlungen, Bildung der Bevölkerung, steuerrechtliche Anreize, usw.). Policy-Kernüberzeugungen gelten ebenfalls als schwer veränderlich, aber da diese nicht in der frühkindlichen und jugendlichen Sozialisation verinnerlicht werden, kann es unter besonderen Umständen (z. B. aufgrund subsystem-interner Schocks) zu einem Wandel kommen (Weible und Sabatier 2007b, 194 f.).

Auf der dritten Ebene befinden sich schließlich die *Sekundärüberzeugungen* (Secondary Beliefs/Aspects). Diese haben eine geringere Reichweite als Policy-Kernüberzeugungen und beziehen sich lediglich auf Teilaspekte eines Policy Subsystems (Weible und Sabatier 2007b, 196). Bei Sekundärüberzeugungen handelt es sich um spezifische Überzeugungen und Einstellungen, „etwa in Bezug auf die Wahl von Instrumenten zur Verwirklichung von Kernüberzeugungen." (Bandelow 2015, 309) Da mit Sekundärüberzeugungen zumeist taktische Absichten im Hinblick auf die Verwirklichung der Policy-Kernüberzeugungen verknüpft werden, gelten diese als am leichtesten veränderbar.

2.2.3 Advocacy-Koalitionen

Die dritte Grundannahme des ACF baut auf der Literatur zur Erforschung von Politik-Netzwerken auf und hebt die Rolle von informellen Netzwerken beim Zustandekommen von politischen Ergebnissen hervor. Das ACF nimmt an, dass politische Akteure danach streben, wichtige Aspekte ihrer Überzeugungssysteme in politische Programme, Maßnahmen usw. zu übersetzen, bevor dies ihren Gegner gelingt. Weiter wird angenommen, dass diese Akteure zur Erhöhung ihrer Erfolgschancen bei dem Versuch der Beeinflussung politischer Entscheidungsprozesse nach Alliierten suchen, Ressourcen teilen und vergleichbare Strategien anwenden. Der oben erwähnte

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

devil shift wird auch in dieser Hinsicht als relevant gesehen, da er die Akteure zusätzlich – aus Angst vor einer Niederlage gegen die als mächtiger und böser wahrgenommene politische Konkurrenz – dazu anhalte, ihr Verhalten mit politischen Verbündeten abzustimmen und mit diesen Kooperationsbeziehungen einzugehen. Schließlich wird angenommen, dass Akteure eine *Advocacy-Koalition* bilden, sobald auf Basis geteilter Überzeugungen ein nichttrivialer Grad an Zusammenarbeit besteht.[6] Zudem argumentieren Sabatier et al., dass die Aggregation von Akteuren in Advocacy-Koalitionen zugleich auch aus wissenschaftlicher Perspektive der effektivste Weg zur analytischen Durchdringung der politischen Positionen von einer Vielzahl von Akteuren sei (Weible und Sabatier 2007b, 196).

Dieser Aspekt des ACF war in der Vergangenheit in besonderem Maße Gegenstand akademischer Auseinandersetzungen. Auf verschiedene Kritiken hin, setzten sich zahlreiche ACF-Forscherinnen und -Forscher intensiv mit der Advocacy-Koalitionen-Grundannahme auseinander und verfeinerten diesen Strang des ACF. Die Hauptelemente dieser Fortentwicklungen, die auch dem vorliegenden Dissertationsvorhaben Handlungsorientierung bieten, sollen im Folgenden skizziert werden.

Das Konzept von dominanten und Minderheitenkoalitionen:

Gemäß diesem Konzept wird davon ausgegangen, dass viele Policy Subsysteme durch die Existenz einer dominanten Koalition und einer Minderheitenkoalition gekennzeichnet sind. Dieses Konzept beruht auf der Annahme, dass politische Akteure stets danach streben, ihre Überzeugungen in politische Ergebnisse zu übersetzen. Sofern in einem Policy Subsystem also politische Ergebnisse vorzufinden sind, wird angenommen, dass diese auf das Wirken jener Advocacy-Koalition zurückzuführen sind, die mittels Nutzung ihrer Ressourcen entscheidenden Einfluss auf die Gestaltung einer Politik nehmen konnte. Demgegenüber wird jene Advocacy-Koalition, die es nicht vermochte, ihre Überzeugungen in politische Ergebnisse zu übersetzen, als die Minderheitenkoalition bezeichnet (Jenkins-Smith u. a. 2017, 150).

6 Es wird zudem davon ausgegangen, dass in jedem Policy Subsystem in aller Regel zwei bis fünf Advocacy-Koalitionen vorzufinden sein werden (Weible und Sabatier 2007b, 196). Abweichend, kann ein weniger konfliktreiches Policy Subsystem auch aus nur einer Koalition bestehen (Bandelow 2015, 312). Eine empirische Auswertung von ACF-Studien ergab, dass die absolute Mehrzahl der Studien zwei Koalitionen identifizieren konnte, während drei Koalitionen in 19 Prozent, 4 und 5 Koalitionen dagegen in nur 6 bzw. 3 Prozent der Studien identifiziert wurden (Hohage 2013, 110; Weible, Sabatier, und McQueen 2009, 131 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Das Konzept der Überwindung von Problemen kollektiven Handelns:

Ein rege diskutierter Debattenstrang im ACF setzt sich mit den Problemen kollektiven Handelns auseinander. Im Kern geht es dabei darum, dass die Annahme des ACF, wonach sich Akteure vor allem auf Grundlage geteilter Überzeugungen zu Advocacy-Koalitionen zusammenschlössen, dahingehend kritisiert wird, dass andere, möglicherweise entscheidende, Gründe für die Entstehung von Gruppen oder Schwierigkeiten beim Aufbau einer Koalition auf Grundlage geteilter Überzeugungen vernachlässigt würden. Angeführt wird etwa, dass Akteure neben ihren Überzeugungen auch materielle Selbstinteressen verfolgen und es daher zur Entstehung des Trittbrettfahrerproblems komme, bei dem der Anschluss an eine Koalition nicht primär aus Überzeugung sondern aufgrund eines erwarteten materiellen Mehrwerts erfolgt (aber auch: Sabatier 1998, 116; siehe insbesondere die Kritik von: Schlager 1995, 263). Der aktuelle Stand im Hinblick auf diese Debatte ist (Jenkins-Smith u. a. 2017, 150), dass Akteure aus drei Gründen in der Lage seien, Probleme des kollektiven Handelns zu überwinden und Koalitionen einzugehen. *Erstens* würden die Transaktionskosten zur Partizipation an einer Advocacy-Koalition dadurch geringgehalten, dass die Akteure auf gemeinsamen Überzeugungen bauen können in deren Ergebnis sie einander mehr vertrauen und auf eine faire Kostenverteilung Wert legen. *Zweitens* würden Akteure sich in unterschiedlichem Maße in Policy Subsystemen engagieren und daher teils nur eine schwache Form der Kooperation pflegen (Abstimmung des eigenen Programms auf das der anderen Akteure, ggf. Informationsaustausch) während ein anderer Teil der Akteure starke Kooperationsformen praktiziere (Entwicklung und Umsetzung gemeinsamer Aktionspläne). Schwache Koordination könne gerade in denjenigen Fällen von Bedeutung sein, wenn die Koordination über verschiedene Organisationstypen hinweg zu erklären ist, sobald etwa Interessengruppen, Forschungsorganisationen und administrative Stellen die potentiellen Mitglieder einer Advocacy-Koalition darstellen. Zudem bietet das Konzept schwacher Koordination eine hilfreiche Grundlage, auf der der Zusammenhalt von Akteuren über längere Perioden (also etwa ein Jahrzehnt und länger) hinweg bestimmt werden kann. Schließlich gebe es zwar durchaus Advocacy-Koalitionen, die auf Basis einer starken Koordination über längere Zeiträume kooperierten, doch ein Großteil der Zusammenarbeit auf Basis starker Koordination fokussiere (z. B. aufgrund der hohen Kosten einer starken Koordination) auf die Erreichung eher kurzfristiger Policy-Ziele. Schwache Koordination biete damit gerade im Hinblick auf längere Zeiträume den Vorteil, für die Beeinflussung eines Subsystems

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

einzutreten, während die Koordinationskosten möglichst geringgehalten werden (Zafonte und Sabatier 1998, 479 f.).

Sofern Akteure auf Grundlage gemeinsamer Überzeugungen ihre Aktivitäten in starkem Maße koordinieren und in dieser Hinsicht miteinander kooperieren, kann von einer *Advocacy-Koalition* gesprochen werden. Wenn hingegen von einer Gruppe von Akteuren die Rede ist, die zwar Überzeugungen teilt, aber nicht im Sinne starker Koordination miteinander kooperiert, kann diese als *Advocacy-Community* bezeichnet werden (Stritch 2015, 438).[7]

Das Konzept der Haupt- und Nebenakteure innerhalb von Koalitionen:

Weil das ACF typischerweise auf langfristige politische Wandlungsprozesse (die sich über Zeiträume von mehr als zehn Jahren erstrecken) fokussiert, wird angenommen, dass Akteure aufgrund beschränkter Ressourcen sich nicht zu jedem Zeitpunkt im selben Maße für eine Sache einsetzen werden. Entsprechend wird zwischen Hauptakteuren und Nebenakteuren innerhalb einer Koalition unterschieden. Hauptakteure würden in stärkerem Maße und regelmäßiger an Koalitionsaktivitäten partizipieren, während sich Nebenakteure eher in unregelmäßigen Abständen oder nur für eine kurze Zeitdauer an Koalitionsaktivitäten beteiligen würden (Jenkins-Smith u. a. 2017, 150).

2.2.4 Policy-Wandel als abhängige Variable: Zwei mögliche Pfade

Ein zentrales Ziel des ACF ist die Erklärung von Policy-Wandel. Wie bereits dargestellt, fußt das ACF auf der zentralen Annahme, dass politische Entscheidungen, Maßnahmen, usw. Ausfluss der Überzeugungen der dominanten Koalition sind. Politische Programme spiegeln aus ACF-Perspektive somit Überzeugungen, „also gleichermaßen einen abstrakten Kern von allgemeinen Zielen und Wahrnehmungen und einen konkreten Rand instrumenteller Veränderungen. Entsprechend kann das Ergebnis politischer Prozesse in einer Veränderung des Policy-Kerns liegen, dann handelt es sich um einen signifikanten politischen Wandel [Anm. d. Autors: *major policy change*]." (Bandelow 2015, 310) Berührt eine Veränderung hingegen die Sekundärüberzeugungen, handelt es sich um einen geringfügigen politi-

7 Eine Gruppe von Akteuren, die keine Überzeugungen teilt, aber miteinander in starkem Maße kooperiert wird als coordination network bezeichnet (Matti und Sandström 2011).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schen Wandel (*minor policy change*). Dass die Überzeugungssysteme der Koalitionen und Veränderungen politischer Programme auf diese Weise in Beziehung zu einander gesetzt werden, hat weitreichende Folgen für Veränderungsprozesse. Weil Policy-Kernüberzeugungen als schwer veränderlich gesehen werden, wird davon ausgegangen, dass ein signifikanter politischer Wandel die Ausnahme bildet und so lange unwahrscheinlich ist, wie die dominante Advocacy-Koalition an der Macht bleibt. Demgegenüber könne geringfügiger politischer Wandel vergleichsweise häufig der Fall sein (Jenkins-Smith u. a. 2017, 145).

Entsprechend wird ein geringfügiger politischer Wandel im klassischen ACF auf Lernprozesse, die auf Ebene des Subsystems stattfinden, zurückgeführt. Drei Faktoren seien hierbei in besonderem Maße entscheidend: Erstens sollte das Konfliktniveau in einem Subsystem möglichst gering sein. Zweitens sollten bestehende Konflikte sich möglichst auf technisch-naturwissenschaftlich bearbeitbare Sachfragen und nicht auf sozialwissenschaftliche Auseinandersetzungen beziehen, da die Generierung von allgemein anerkanntem Fachwissen bei ersteren einfacher sei. Drittens sollte ein ausreichend prestigeträchtiges und professionelles Forum existieren, das dazu imstande ist, konkurrierende Koalitionen zu einem Dialog zu bewegen (Weible und Sabatier 2007b, 198).

Während ein geringfügiger politischer Wandel als eine Möglichkeit der Veränderung im Kontext des Subsystems selbst konzipiert ist, sieht der zweite mögliche Pfad für politischen Wandel vor, dass ein signifikanter politischer Wandel nur als Reaktion auf Subsystem-externe Einflussfaktoren stattfinden kann. Derartige externe Shocks sind dadurch definiert, dass sie außerhalb der Kontrolle der Subsystem-Akteure liegen. Veränderungen in den sozioökonomischen Bedingungen, Regimewechsel, Auswirkungen anderer Subsysteme oder Naturkatastrophen können die Wirkung eines derartigen externen Schocks entfalten. Zwar wird auch angenommen, dass externe Schocks zu einer unmittelbaren Veränderung der Policy-Kernüberzeugungen der dominanten Koalition führen können (Zafonte und Sabatier 2004), doch wird ein signifikanter politischer Wandel eher darauf zurückgeführt, inwiefern die Minderheitenkoalition in der Lage ist, aus dem Schock politisch zu profitieren, indem z. B. die Ressourcen im Subsystem neu verteilt werden, es zu einer Verschiebung der öffentlichen Meinung hin zu den Überzeugungen der Minderheitenkoalition kommt oder die Aufmerksamkeit zentraler politischer Entscheidungsinstanzen gewonnen werden kann. Ein signifikanter politischer Wandel würde demnach dann stattfinden, wenn es der Minderheitenkoalition unter Rückgriff auf derarti-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ge Veränderungen und unter geschicktem Einsatz ihrer Ressourcen gelingt, selbst zur dominanten Koalition aufzusteigen (Weible und Sabatier 2007b, 198 f.).

2.2.5 Relevante Ergänzungen des ACF

Im Jahr 2007 erfuhr das ACF eine Ergänzung um drei Elemente. Der erste Aspekt betrifft die Spezifizierung der politischen Gelegenheitsstrukturen, die den Kontext bilden, innerhalb dessen Advocacy-Koalitionen handeln. Diese Erweiterung war eine Reaktion auf die Kritik, dass das ACF zu stark auf das US-amerikanische politische System bezogen sei, deren Hauptmerkmale hochprofessionalisierte Interessengruppen, missionsorientierte Regulierungsbehörden, schwache politische Parteien, zahlreiche politische Schauplätze und die Notwendigkeit der Erreichung von absoluten Mehrheiten seien. Demgegenüber fänden die besonderen Merkmale europäischer politischer Systeme (gekennzeichnet durch weniger Offenheit, langwierige Entscheidungsprozesse und konsensorientierte Entscheidungsgrundsätze) kaum Berücksichtigung im ACF. Um dieser Kritik entgegenzukommen wurde das ACF um das Variablenset *langfristig wichtiger politischer Gelegenheitsstrukturen* ergänzt. Diese sind konzipiert als Mediator zwischen relativ stabilen Parametern und dem Policy Subsystem. Demnach beziehen sich politische Gelegenheitsstrukturen auf relativ beständige Merkmale eines politischen Systems und wirken sich auf die Ressourcen, Möglichkeiten und Zwänge von Subsystem-Akteuren aus. Zunächst beinhaltete das neue Variablenset zwei Variablen: (1) Den *Grad der erforderlichen Zustimmung für wesentlichen Wandel* und (2) die relative *Offenheit eines politischen Systems*. Der Grad der erforderlichen Zustimmung für wesentlichen Wandel postuliert, dass Akteure bzw. Koalitionen in stärker konsensorientierten politischen Systemen strukturell eher dazu gedrängt werden, eine inklusive Politik zu praktizieren, Kompromisse zu schließen, Informationen auch über Koalitionsgrenzen hinweg zu teilen und die Verteufelung der Gegner zu reduzieren. Die relative Offenheit eines politischen Systems bezieht sich einerseits auf die Anzahl der legislativen Entscheidungsinstanzen, die eine Policy bis zur Verabschiedung passieren muss und andererseits auf die Zugänglichkeit der entsprechenden Entscheidungsinstanzen. Hier ist die Annahme, dass geschlossenere (korporatistische) politische Systeme teilnehmende politische Akteure eher dazu drängen, Kompromisse einzugehen und Anreize für Policy Broker

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schaffen, als vermittelnde Akteure zu agieren, während offenere (pluralistische) politische Systeme geringere Anreize zur Kompromissschließung schaffen (Weible und Sabatier 2007b, 200 f.).

Später wurde das Variablenset langfristig wichtiger politischer Gelegenheitsstrukturen noch um eine dritte Variable *traditioneller Konfliktlinien* („societal cleavages") ergänzt.[8] Diese baut auf den Vorarbeiten der Politikwissenschaftler Lipset und Rokkan auf, die in ihren Arbeiten argumentieren, dass die Politik westlicher Industriegesellschaften seit dem 19. Jahrhundert in entscheidendem Maße von vier großen Konfliktlinien geprägt war, die sich auf den Konflikt zwischen Kapital und Arbeit, Kirche und Staat, Stadt und Land sowie Zentrum und Peripherie beziehen. Hierbei ist die Annahme, dass politische Akteure zur Erreichung ihrer politischen Ziele in Situationen, in denen traditionelle Konfliktlinien berührt werden, besondere Sorgfalt walten lassen müssen, um Kompromisse zu erzielen und nicht in die traditionellen Konfliktmuster zu verfallen, wodurch die Zielerreichung gefährdet werden könnte (siehe z. B. D. Nohrstedt 2010, 16 f.).[9]

Die zweite wichtige Spezifizierung des ACF im Jahr 2007 betrifft die Festlegung von sechs Typen *kurzfristig wichtiger Koalitionsressourcen* (Weible und Sabatier 2007b, 201–4):[10]

8 Interessanterweise äußern sich die Hauptprotagonisten des ACF an sehr wenigen Stellen zu dieser Variable. Meines Wissens nach wurde das Thema erstmals in einer Vortragsverschriftlichung von Sabatier und Weible aus dem Jahr 2005 erwähnt. Darin wurde argumentiert, dass die Gefahr des Betretens eines den traditionellen Konfliktlinien entsprechenden politischen Terrains auf Seiten der Akteure Anreize schafft, einen korporatistischen Policy-Stil zu wählen, Kompromisse einzugehen usw. (Sabatier und Weible 2005, 8 f.). In der zentralen Erweiterung des ACF aus dem Jahr 2007 war die Variable hingegen nicht enthalten (Weible und Sabatier 2007b). Das Schaubild aus der Bestandsaufnahme des ACF aus dem Jahr 2011 listet traditionelle Konfliktlinien („overlapping societal cleavages") schließlich als dritte Variable auf (Weible u. a. 2011, 352). Etwas ausführlicher äußerte sich später Nohrstedt zu der Variable (Daniel Nohrstedt und Weible 2010, 16 f.).

9 Gemeint sein könnte beispielsweise, dass eine politische Auseinandersetzung, die ansonsten zugunsten einer Advocacy-Koalition ausfallen würde, in Falle, dass beispielsweise der historische Konflikt zwischen Arbeit und Kapital berührt wird, zu einer Neuordnung der Unterstützer und Gegner führt und auf diese Weise das politische Ergebnis verändert wird.

10 Weniger gut untersucht ist hingegen weiterhin die Frage, mittels welcher kausalen Mechanismen welche dieser Ressourcen unter welchen Bedingungen wie dazu beitragen, dass ein (signifikanter) politischer Wandel vonstattengehen kann (Jenkins-Smith u. a. 2017; Daniel Nohrstedt und Weible 2010, 11).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(1) *Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse*, Gemäß dem ACF können einzelne Individuen, die wichtige Entscheidungsfunktionen in politischen Aushandlungsprozessen wahrnehmen Teil einer Advocacy-Koalition sein. Dass eine Koalition mehr ihrer Mitglieder in solche Positionen einbinden kann als es gegnerische Koalitionen dazu imstande sind, wird daher als eine zentrale Koalitionsressource betrachtet, die maßgeblich über den Erfolg einer Advocacy-Koalition entscheidet.

(2) *Unterstützung durch die Öffentliche Meinung*, Der öffentlichen Meinung kommt eine unterstützende Rolle in zweifacher Hinsicht zu. Zum einen wird davon ausgegangen, dass die unmittelbare Beeinflussung der Entscheidungen politischer Autoritäten zugunsten der eigenen Überzeugungen eher möglich sein wird, sofern man sich auf der Seite der öffentlichen Meinung wähnt. Zum anderen wird davon ausgegangen, dass die Unterstützung durch die öffentliche Meinung dazu führen kann, dass neutrale oder gegnerische politische Repräsentanten abgewählt und an deren Stelle Individuen gewählt werden, die eher bereit sind, die eigenen Überzeugungen umzusetzen.

(3) *Informationen/Informationshoheit*. Solange keine ungewollte Pattsituation besteht, wird davon ausgegangen, dass Informationen eine wichtige Rolle im Handeln von Advocacy-Koalitionen spielen. Besonders in Policy Subsystemen, in denen technischen Informationen eine große Rolle zukommt, kann Informationshoheit zur Festigung der Mitgliedschaft in einer Koalition dienen, die Überzeugungen politischer Gegner wirksam infrage stellen und politische Entscheider bzw. die öffentliche Meinung von der Unterstützung der eigenen Sache überzeugen.

(4) *Fähigkeit zur politischen Mobilisierung*, Gerade im Falle geringer finanzieller Ressourcen, wie dies häufig bei zivilgesellschaftlichen Akteuren der Fall ist, kommt der Fähigkeit zur politischen Mobilisierung Gleichgesinnter eine wichtige Rolle zu, um den politischen Druck zu verstärken. Eine solche Mobilisierung kann in erster Linie die Form der Durchführung von Demonstrationen annehmen, aber auch bei Wahlkampagnen oder der Mittelbeschaffung von Relevanz sein.

(5) *Finanzielle Ressourcen*. Finanzielle Ressourcen können für vielfältige Zwecke verwendet werden, mittels derer wiederum Einfluss auf politische Entscheidungsprozesse genommen werden kann. Darunter fallen beispielsweise die Finanzierung von gleichgesinnten Forscher(-inne)n und Denkfabriken, die Unterstützung gleichgesinnter politischer Repräsentanten, die Finanzierung von Medienkampagnen zur Vergröße-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

rung der öffentlichen Unterstützung und die Bewerbung der eigenen Positionen zur Erhöhung der Zahl mobilisierbarer Aktivisten.

(6) das *Vorhandensein einer fähigen Führung*. Policy Entrepreneuren wird eine wichtige, übergeordnete Rolle bei der Führung und Festigung einer Koalition, der effizienten und effektiven Nutzung aller verfügbaren Ressourcen und der Erschließung neuer Ressourcen beigemessen. Zudem wird angenommen, dass externe Schocks besonders dann eine große Wirkung auf politische Entscheidungsprozesse entfalten können, wenn es Policy Entrepreneuren unter geschicktem Ressourceneinsatz gelingt, den Schock zur Umsetzung der eigenen Ziele wirksam zu kanalisieren.

Die dritte zentrale Ergänzung, die das ACF 2007 erfuhr, betrifft schließlich die Identifizierung zwei weiterer, möglicher Pfade für einen signifikanten politischen Wandel. Wie oben dargestellt, postulierte das ACF, dass für einen signifikanten politischen Wandel in einem Subsystem das Auftreten eines externen Shocks, der außerhalb des Einflussbereichs der Subsystem-Akteure liegt, eine notwendige Bedingung darstellt, weil Lernprozesse, also Änderungen der (Kern-)Überzeugungen der Akteure als (sehr) unwahrscheinlich gelten. In Reaktion auf Kritiken am ACF, dass zu stark auf externe Faktoren im Hinblick auf signifikanten politischen Wandel fokussiert werde, ergänzten Sabatier und Weible das ACF um zwei weitere Möglichkeiten signifikanten politischen Wandels: subsystem-interne Schocks und ausgehandelte Kompromisse (Weible und Sabatier 2007b, 204 f.).

Subsystem-interne Schocks: Demnach kann ein signifikanter politischer Wandel auch die Folge eines *subsystem-internen Schocks* sein, der nach einem politischen Debakel, gestalterischen Fehlschlägen, persönlichen Skandalen usw. eintritt. Die zwei zentralen Annahmen in dieser Hinsicht sind, dass interne Schocks zum einen kritische politische Ressourcen (öffentliche Unterstützung, finanzielle Ressourcen) in einem Subsystem umverteilen und damit die Machtbalance im entsprechenden Subsystem zugunsten der Minderheitenkoalitionen verändern können. Zum anderen können interne Schocks auch koalitionsinterne Wandlungsprozesse auslösen, indem insbesondere infolge großer politischer Fehlentscheidungen Zweifel an den Kernüberzeugungen der dominanten Koalition genährt werden und die Bereitschaft der Koalitionsmitglieder zur Unterstützung der Koalitionsziele sinkt oder diese die Koalition verlassen. Auf Seiten der Minderheitenkoalitionen können derartige Schocks dagegen zur Festigung der eigenen Überzeugungen dienen. Da ein interner Schock als notwendige,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

aber nicht zugleich auch hinreichende Bedingung für einen signifikanten politischen Wandel gilt, kommt, wie bei externen Shocks, den Minderheitenkoalitionen eine zentrale Rolle bei der Ausnutzung des Schocks für den Ausbau der eigenen Machtposition zu (ebd.).

Ausgehandelte Kompromisse: Schließlich wurde das ACF in Reaktion auf signifikante politische Wandlungsprozesse in Kontexten, die durch kollaborative Institutionen und korporatistische Regime geprägt sind und in denen sich zuvor weder interne noch externe Schocks ereigneten, um die Möglichkeit eines signifikanten politischen Wandels in Folge ausgehandelter Kompromisse ergänzt. Sabatier und Weible definieren neun Bedingungen, unter denen die Wahrscheinlichkeit eines ausgehandelten Kompromisses in einem Subsystem steigt. Als erste und wichtigste Bedingung gilt dabei das Vorliegen einer von Seiten miteinander im Konflikt liegender Koalitionen *unerwünschten politischen Pattsituation*. Eine solche unerwünschte Pattsituation tritt dann ein, wenn alle beteiligten Koalitionen der Meinung sind, dass der Status Quo nicht tragbar ist, aber diese sich zugleich weigern, ihren Gegnern Zugeständnisse zu machen. Von einer unerwünschten Pattsituation ist eine gewöhnliche Pattsituation zu unterscheiden, in der eine Seite einen Prozess auch aus dem Grunde blockieren kann, weil sie in der Blockade bzw. der Bewahrung des Status Quo Vorteile für sich erkennt. Die weiteren Bedingungen gehen auf (2) die möglichst ausgeglichene Komposition der am Aushandlungsprozess beteiligten Akteure, (3) das Vorhandensein neutraler Policy Broker, (4) dem Bestehen eines konsensorientierten Entscheidungsmechanismus, das den einzelnen Akteuren Vetomächte einräumt, (5) Finanzierung, (6) wie lange und kontinuierlich die gegnerischen Akteure aufeinander treffen, (7) welche Rolle naturwissenschaftlich-empirische Fragestellungen spielen, (8) das Vorhandensein und der Ausbau von Vertrauen und (9) das Fehlen alternativer Entscheidungsarenen, in die politische Akteure zur Erreichung ihrer Ziele ausweichen können (Weible und Sabatier 2007b, 205–7).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Somit ergibt sich folgendes Schaubild des ACF:

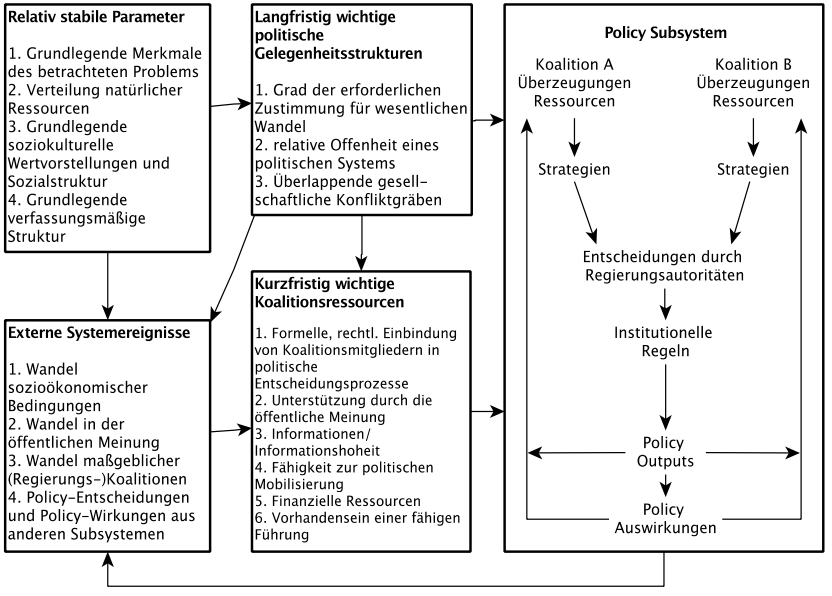

Abbildung 1: Schema des Advocacy Coalition Framework (Quelle: Eigene Übersetzung von Weible 2011: 352)

2.2.6 Schwächen des ACF

Wie der Überblick gezeigt hat, stellt das ACF einen umfassenden und umfangreichen theoretischen Rahmen dar, der seine Anwendbarkeit in vielen Kontexten unter Beweis gestellt hat. Diese Vielfältigkeit des ACF hat bei Policy-Analysen allerdings auch seine Nachteile. So legen die Hauptprotagonisten des ACF zwar großen Wert auf die Erfüllung der Kriterien einer wissenschaftlichen Theorie, d. h. der Bestimmung falsifizierbarer Hypothesen und kausaler Faktoren, doch hat der gleichzeitig mitformulierte Anspruch der Gewährleistung einer breiten Anwendbarkeit des ACF (Sabatier 1998, 122) den Nachteil, dass die Wechselbeziehungen zwischen den Variablen und die kausalen Wirkungsmechanismen unterspezifiziert

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

bleiben.[11] Mauersberger (2016, 65) verweist im Zusammenhang mit dieser Kritik etwa darauf, dass wichtige ACF-Studien (z. B. Matti und Sandström 2011) den theoretischen Rahmen aus diesem Grunde nur wenig strukturiert anwenden und eher als grobe konzeptionelle Anleitung heranzögen. Wie Mauersberger (2016, 65) es ausdrückt, vermag das ACF aufgrund der Unterspezifizierung nicht als mathematisches Modell zu fungieren, in das eine Forscherin Daten eingibt und auf Grundlage der darauffolgenden Berechnungen zielführende Ergebnisse erhält. Stattdessen bedinge der theoretische Rahmen des ACF, dass Forscherinnen und –Forscher dazu angehalten werden, einen theoretischen Fokus zu setzen, um auf bestimmte Variablen zu fokussieren. Diese theoretischen Schwerpunkte beziehen sich im ACF auf die Fokussierung einer Untersuchung entweder auf Advocacy-Koalitionen bzw. Überzeugungen (z. B. Henry 2011; und: Pierce 2011), auf den Lernaspekt (z. B. Albright 2011) oder auf Policy-Wandel (z. B. Ingold 2011; und: Daniel Nohrstedt 2011). Diese Fokussierung auf einzelne Elemente des ACFs wird auch seitens der ACF-Experten befürwortet, da der gleichzeitige Fokus auf alle drei Elemente aus forschungspraktischer Sicht in aller Regel zu aufwendig sei (Weible u. a. 2011, 354). Ich teile die Perspektive von Mauersberger (2016, 65), wonach dieses Fokussieren nicht als Schwäche, sondern als Anerkennung der Komplexität der realen Welt zu deuten ist. Entscheidend wird an diesem Punkt also, im Rahmen einer Forschungsarbeit jene Elemente des ACF zu spezifizieren, denen eine handlungsanleitende Funktion zukommt. Aufgrund dieser Einsicht, fokussierte der vorliegende Abschnitt bereits auf Advocacy-Koalitionen bzw. Überzeugungen und klammerte den Themenkomplex Policy-Lernen aus. Diese Fokussierung wird im Rahmen des folgenden Unterabschnitts (vgl. 2.3), in dem ich den analytischen Rahmen des vorliegenden Dissertationsvorhabens darlege, weiter spezifiziert.

Eine weitere, in der englischsprachigen ACF-Literatur allerdings nur wenig beachtete Kritik (Hajer und Laws 2008, 255 f.), bezieht sich auf eine innere, wissenschaftstheoretische Diskrepanz des ACF (Bandelow 2015, 320 f.). So verweist der Fokus auf die Überzeugungssysteme von Akteuren, die deren Handeln vorstrukturieren auf das kritische Potential des Rahmens. Auf der anderen Seite verstand Sabatier sich selbst stets als Szientist und verfolgte mit dem ACF das Ziel, *objektive* Erkenntnisse über die Funktions-

11 Bandelow führt diese Unübersichtlichkeit des Rahmens teilweise auf die unsystematische, induktive Weiterführung der theoretischen Fundierung des ACF auf Basis empirischer ACF-Studien zurück (Bandelow 2015, 305, 307).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

weise der Politik zu generieren. Während also bei der Analyse politischer Prozesse davon ausgegangen wird, dass keine objektiven Wahrheiten existieren, weil jede Weltwahrnehmung der Akteure durch ihre Überzeugungssysteme geprägt ist, wird dieselbe kritische Perspektive im Hinblick auf die Forschenden, die sich mit politischen Prozessen auseinandersetzen, verworfen und angenommen, dass diese tatsächlich imstande seien, objektive Erkenntnisse zu generieren. Um dieser, meines Erachtens sehr berechtigten Kritik entgegenzukommen, werde ich den letzten Unterabschnitt dieses Teils der Arbeit (vergleiche Unterabschnitt 2.3.6) der Reflexion meiner eigenen Überzeugungen und auf deren möglichen Einfluss auf meine Forschung widmen.

2.2.7 Anwendbarkeit des ACF auf politische Entscheidungsprozesse auf der EU-Ebene

Galt das ACF in den Anfangsjahren noch als eine auf die US-Politik beschränkte Forschungsperspektive, ist es aufgrund der zahlreichen Weiterentwicklungen der vergangenen Jahrzehnte (Jenkins-Smith u. a. 2017, 201; Sabatier 1998; Weible und Sabatier 2007b) mittlerweile problemlos auf politische Prozesse auf EU-Ebene anwendbar (Rozbicka 2013). Dies zeigt sich an zahlreichen Anwendungen des ACF, etwa auf die EU-Steuerpolitik (Radaelli 1999), die historische EU-Stahlpolitik (Dudley und Richardson 1999), die EU-Finanzpolitik (Quaglia 2010) oder die EU-Arzneimittelpolitik (Brooks 2018).

Zentrale Charakteristiken des politischen Systems der EU sind deren Offenheit und die Involvierung einer großen Zahl an Akteuren. Private als auch öffentliche Akteure aus allen Ebenen (lokal, national, europäisch) bilden EU-weite komplexe Akteursnetzwerke, die in Abhängigkeit von den behandelten Themen, potentiell auf allen Ebenen im Hinblick auf die Beeinflussung von Politiken aktiv sind. Zudem gilt als ausreichend belegt, dass administrative Akteure, privatwirtschaftliche und zivilgesellschaftliche Interessengruppen sowie Wissenschaftler aus verschiedenen EU-Mitgliedstaaten z. B. ökologisch oder privatwirtschaftlich motivierte überzeugungsbasierte Koalitionen auf EU-Ebene bilden (Rozbicka 2013, 843 f.). Das ACF eignet sich zur Erfassung dieser komplexen Akteurs- und Vernetzungsstrukturen sowie zur Durchdringung der komplexen inhaltlichen Dynamiken besonders gut. Hilfreich ist dabei zum einen die Forschungsperspektive des ACF, die auf langfristige Wandlungsprozesse fokussiert, sowie die Unter-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

scheidung zwischen gewöhnlichem und signifikantem Policy-Wandel. Dass sich ein signifikanter Policy-Wandel ereignet, gilt angesichts der komplexen Entscheidungsstrukturen der EU als besonders schwierig und überlappt sich somit auch mit der entsprechenden Annahme des ACF. Schließlich gilt die Bedeutung, die das ACF dem Kontext zuspricht, innerhalb dessen ein Policy-Wandel stattfindet, als eine der Stärken des ACF (ebd., 843-848).

An ihre Grenzen stoße die Erklärungskraft des ACF hingegen insbesondere bei der Untersuchung der Formierung von Advocacy-Koalitionen, die auf EU-Ebene tätig sind. So bestätige ein Teil der Literatur die Grundannahme des ACF, dass Akteure sich langfristig zu strategischen Advocacy-Koalitionen zusammenschlössen während ein anderer Teil der Literatur gegenläufige Strukturlogiken identifiziert habe, wonach sich Akteure auf EU-Ebene eher zaghaft und nur kurzfristig zu themenspezifischen und strategischen Koalitionen zusammenfinden. Rozbicka resümiert diesbezüglich, dass das politische System der EU auch chaotischen, nur wenig organisierten Koalitionen die Möglichkeit biete, ihre politischen Ziele zu erreichen, sodass eher die Untersuchung der Zielerreichung selbst in den Vordergrund und damit der Fokus des ACF auf strategische, überzeugungsbasierte Koordination in den Hintergrund rücke (ebd., 847 f.).

Von den verschiedenen Vorschlägen, die zur Adressierung der hieraus resultierenden Herausforderungen gemacht werden, möchte ich zwei an dieser Stelle hervorheben: Zum einen bietet der Rückgriff auf das Policy Entrepreneur-Konzept die Möglichkeit, dynamische Entwicklungen, die ansonsten aus der Perspektive des ACF herausfallen, damit zu erklären, dass fähige Führungskräfte es mittels geschickten Ressourceneinsatzes vermögen, Policy-Wandel herbeizuführen. Zum anderen könne unter Rückgriff auf interessenbasierte Ansätze die auf Überzeugungen fokussierende Perspektive des ACF dadurch erweitert werden, dass Koalitionen sich nicht allein auf Basis geteilter Überzeugungen, sondern auch auf Basis geteilter Interessen und gegenseitiger Abhängigkeiten formen (ebd., 849 f.). Das Modell des Policy-Entrepreneurs ist Teil des ACFs. Explizit enthalten ist es in der Ressource Vorhandensein einer fähigen Führung und wird daher auch im weiteren Verlauf der Arbeit Berücksichtigung finden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3 Forschungsdesign und methodische Erwägungen

Bis hierhin habe ich das ACF als einen theoretischen Rahmen vorgestellt, der im Allgemeinen dafür geeignet ist, Policy-Wandel unter Berücksichtigung der Spezifika meines Forschungsgegenstandes zu untersuchen. Davon ausgehend möchte ich nun einen analytischen Rahmen entwickeln, mit dessen Hilfe das ACF für die Zwecke der vorliegenden Arbeit gewinnbringend angewendet werden kann. Dabei orientiere ich mich an den Empfehlungen von Gschwend und Schimmelfennig (2007, 18), die eine Unterscheidung zwischen Analyseeinheit, Fall und Beobachtung nahelegen. Unter Analyseeinheit ist dabei das zu untersuchende abstrakte Gebilde zu verstehen (z. B. Staaten, Institutionen, Entscheidungen, politische Entwicklungen). Falls die Analyseeinheit „Staat" ist, könnte eine Einzelfallstudie sich also beispielsweise dem Staat bzw. „Fall" Schweden widmen. Mittels Beobachtung wird schließlich die (Nicht-)Interaktion zwischen unabhängigen und abhängigen Variablen erklärt (Gschwend und Schimmelfennig 2007, 18). Daher stelle ich im Folgenden (2.3.1) zunächst meine Forschungsstrategie vor, die auf einer Einzelfallstudie beruht, gefolgt von der Begründung der Fallauswahl (2.3.2). Im darauffolgenden Unterabschnitt (2.3.3) stelle ich schließlich den analytischen Rahmen der Arbeit vor. Der darauffolgende Unterabschnitt widmet sich der Operationalisierung (2.3.4), gefolgt von der Vorstellung der Datenerhebung und -analyse (2.3.5). Abschließend reflektiere ich in Unterabschnitt 2.3.6 schließlich über Normativität und Objektivität.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.1 Forschungsstrategie: Einzelfallstudie

Die vorliegende Arbeit stützt sich zum Zwecke der Untersuchung der Fragestellung auf die Forschungsstrategie der Einzelfallstudie bzw. Einzelfallanalyse (Hering und Schmidt 2014). Zur Bearbeitung des Einzelfalls greife ich auf die Untersuchungsmethode der *Prozessanalyse* (Process Tracing) zurück (Blatter, Langer, und Wagemann 2018, 236). Für die Erklärung des Zustandekommens der DSGVO bietet sich diese Vorgehensweise an. Nur mittels der Möglichkeiten der Einzelfallanalyse kann der Aushandlungsprozess in seiner ganzen Komplexität und im Hinblick auf kausale Mechanismen angemessen erfasst werden. Der Rückgriff auf die Prozessanalyse erfolgt insbesondere deshalb, weil das ACF zwar einen umfassenden theoretischen Rahmen bietet, allerdings selbst keine Untersuchungsmethode darstellt, mittels derer die Wirkungen der einzelnen Elemente des Rahmens untersucht werden können (Mauersberger 2016, 66 ff. Pierce, Peterson, und Hicks 2016, 23).

Mein Forschungsinteresse am Zustandekommen der DSGVO legt ein *Y-zentriertes* Forschungsdesign nahe (Gschwend und Schimmelfennig 2007, 22). Von den fünf möglichen Zielsetzungen, die mit Fallstudien grundsätzlich verfolgt werden können (Blatter, Langer, und Wagemann 2018, 175 f.), fokussiert die vorliegende Fallstudie auf die folgenden zwei Zielsetzungen: Einerseits geht es mir um die *sinnvolle und systematische Beschreibung von Phänomenen*, in meinem Fall des Zustandekommens der DSGVO. Andererseits geht es mir um die *Identifikation von kausalen Bedingungen und Mechanismen*, mittels derer das spezifische Politikergebnis der DSGVO erklärt werden kann. Die von mir gewählte Vorgehensweise ist somit zu unterscheiden von der *deskriptiv-vergleichenden Fallanalyse*, der *fallvergleichenden Fallanalyse* sowie der *Kongruenzanalyse* (Blatter, Langer, und Wagemann 2018, 173 ff.).[12]

Die Analyseeinheit (Gschwend und Schimmelfennig 2007, 18) der durchzuführenden Einzelfallstudie bildet die „Politische Regulierung des Schutzes personenbezogener Daten in der Europäischen Union", kurz: „Die EU-Datenschutzpolitik".

Die seitens einiger Vertreter quantitativer Ansätze vorgebrachte Perspektive auf Politikwissenschaft, wonach große statistische Studien mit einer

12 Eher nachrangig geht es mir aber auch um die Beeinflussung von theoretischen Perspektiven und Paradigmen, welche den (wissenschaftlichen oder praktischen) Diskurs in einem Themenfeld strukturieren (Blatter, Langer, und Wagemann 2018, 176).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

möglichst hohen Fallzahl Studien mit geringerer Fallzahl vorzuziehen seien (und: King, Keohane, und Verba 1994; vgl. insb.: Lijphart 1971), weise ich unter Verweis auf moderne Vertreter qualitativer Studien zurück (Blatter, Langer, und Wagemann 2018; George und Bennett 2005; Hall 2008; Mahoney 2010). Auf der allgemeinsten Ebene kann als gemeinsamer Nenner zwischen quantitativen und qualitativen Ansätzen das Streben nach besseren Erklärungen gelten, indem die Erklärungskraft von Theorien auf Basis quantitativer oder qualitativer (Fallstudien-)Daten getestet wird und die Theorien in der Folge den Ergebnissen entsprechend bestätigt oder modifiziert werden (George und Bennett 2005, 32 f.). Während die quantitative Vorgehensweise ausgehend von einer bestimmten Zahl an Variablen Gemeinsamkeiten und Unterschiede (vor allem auf Basis von Korrelationen) zwischen einer hohen Fallzahl zu finden sucht, wird bei der qualitativen Vorgehensweise der Fokus auf die Identifikation von kausalen Schlussfolgerungen bzw. Erklärungen gelegt (Mahoney 2007). Ich folge qualitativen Forschenden in der Annahme:

> *„[D]ass nicht der Effekt einer unabhängigen Variablen auf eine abhängige Variable im Vordergrund stehen sollte, sondern die Untersuchung des kausalen Mechanismus: Sie gehen davon aus, dass der Mechanismus nicht als Ganzes beobachtbar ist, sondern aus empirischen Beobachtungen weitgehend indirekt erschlossen werden muss. […] Bestimmte Beobachtungen von Zuständen und Ereignissen können demnach als empirische Implikationen eines Mechanismus verstanden werden, insbesondere wenn sie in dem Kontext und der Reihenfolge auftreten, die theoretisch erwartbar ist."* *(Starke 2015, 456 f.)*

Mechanismus soll in diesem Kontext als die Verbindung von Ursache und Wirkung verstanden werden. Kausale Mechanismen sind allerdings nicht mit intervenierenden Variablen gleichzusetzen: Entgegen einer intervenierenden Variablen beeinflussen sie nicht nur ein Ergebnis, sondern sie generieren vielmehr selbst die Wirkung (ebd.).

In den vergangenen zwei Jahrzehnten haben qualitativ Forschende große Fortschritte im Hinblick auf die Systematisierung qualitativer Forschungsansätze geleistet. So stellen prozessanalytische Techniken typischerweise in fast allen Fallstudien ein Teil des Vorgehens dar. Was die moderne Prozessanalyse von früheren Anwendungen fundamental unterscheidet, ist die theoretische Rückbindung und methodische Fundierung und Reflexion neuerer Ansätze (Blatter, Langer, und Wagemann 2018, 237). Die theoretische Rückbindung der durchzuführenden Prozessanalyse ist bereits im vor-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

angegangenen Theorieteil erfolgt. Als theoretischer Ausgangspunkt fungiert das Advocacy Coalition Framework und als grobe Orientierung die vier vorgestellten möglichen Pfade eines Policy-Wandels.

Durch diese Form der Orientierung an der Erarbeitung endgültiger Erklärungen grenze ich mich zudem von postmodernen qualitativen Forschungsansätzen ab. Ausgehend von der sinnstiftenden Bedeutung von Sprache, verweisen postmoderne Ansätze auf die Schwierigkeit der Identifikation von objektiven Wahrheiten und legen den Fokus der Analyse verstärkt auf die diskursive Konstruktion der mittels Machtstrukturen als wahr konstruierten Versionen von Ereignissen (Diez 2010). Von hermeneutischer Seite wurde zudem hervorgehoben, dass die Analyse sozialer Phänomene nicht in Unabhängigkeit von den Phänomenen – in anderen Worten: nicht objektiv – durchgeführt werden kann, weil die Forschenden selbst auch immer Teil der von ihnen untersuchten sozialen Welt sind und daher von dieser geprägt werden. (George und Bennett 2005, 186 f.) Die von mir eingenommene Perspektive nimmt diese Einwände ernst (vgl. Unterabschnitt 2.3.6 zur *Reflexion über Normativität und Objektivität*), sodass die von mir im Laufe dieser Schrift herausgearbeiteten Verallgemeinerungen Repräsentativität stets nur im Hinblick auf den spezifischen Kontext und Zeitrahmen, innerhalb dessen sie formuliert werden, erheben. Die Kritik an positivistischen Vorgehensweisen verleitet mich also dazu, Selbstreflexion ernst zu nehmen, während ich zugleich weiterhin danach strebe, objektiv gültige Aussagen über den Untersuchungsgegenstand treffen zu können. Entscheidend ist auch, dass Theorien lediglich deduktive Orientierung bieten, sie aber immer induktiv wiederlegt oder ergänzt werden können (George und Bennett 2005, 186 f.). Dass sozialwissenschaftliche Theorien nicht immer ein vollständiges Bild des Untersuchungsgegenstandes liefern können, liegt in der Natur sozialwissenschaftlicher Forschung. Insofern stellt die von mir im Rahmen der vorliegenden Arbeit eingenommene Perspektive eine von vielen möglichen Erklärungsansätzen (wie sie beispielsweise bereits im Forschungsstand in Kapitel 1.2 diskutiert wurden) für den untersuchten Fall dar, ohne eine alle anderen möglichen Erklärungen ausschließende alleinige Gültigkeit zu beanspruchen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.2 Fallauswahl und Festlegung des zeitlichen Untersuchungsrahmens: Der politische Aushandlungsprozess der DSGVO

Ausgehend von der Analyseeinheit „EU-Datenschutzpolitik" wird als der zu untersuchende Fall der vorliegenden Schrift der *politische Aushandlungsprozess der Datenschutz-Grundverordnung* gewählt. Der zeitliche Rahmen der Arbeit fokussiert daher in erster Linie auf den Zeitraum zwischen dem Beginn des politischen Aushandlungsprozesses der DSGVO 2008/2009 und ihrer Verabschiedung im Jahr 2016. Da er für den politischen Aushandlungsprozess, der zur DSGVO führte, von enormer Bedeutung ist, wird zudem – allerdings in geringerem Umfang – auch die Entstehung der DS-RL (1970er bis 1990er) sowie der Zeitraum zwischen der Verabschiedung der DS-RL im Jahr 1995 und dem Beginn der Aushandlung der DSGVO (2009) mituntersucht. Für die Festlegung dieser Zeitrahmen haben zwei Gründe gesprochen, ein praktischer und ein theoretischer. Viele sowohl politikwissenschaftliche als auch juristische Publikationen, in denen Aussagen im Hinblick auf die Datenschutzpolitik getroffen werden, verweisen auf die große Bedeutung des Akteurshandelns sowie der institutionellen und verfassungsmäßigen Struktur im Hinblick auf das Zustandekommen von Datenschutzpolitiken. Insofern liegt die nähere Betrachtung dieser möglichen kausalen Faktoren, die in der Literatur Erwähnung finden, nahe.

Zudem misst auch das ACF selbst diesen Elementen eine wichtige Rolle im Hinblick auf das Zustandekommen politischer Entscheidungen zu. Wie in Unterabschnitt 2.2.1 dargestellt wurde, kommt laut ACF dem Kontext in Form von relativ stabilen Parametern, externen Systemereignissen und langfristig wichtigen politischen Gelegenheitsstrukturen eine entscheidende Rolle in politischen Aushandlungsprozessen bzw. im Hinblick auf Policy-Wandel zu. Daneben entspricht die Untersuchung politischer Prozesse über einen Zeitraum von mindestens einem Jahrzehnt hinweg eher der Forschungsperspektive des ACF, die einen Fokus auf langfristige Wandlungsprozesse liegt (Weible und Sabatier 2007a).[13]

13 In der aktuellsten Fassung des ACF stellten die Autorinnen und Autoren allerdings klar, dass diese Fokussierung auf langfristige Veränderung eher auf Grundlage der Beobachtung realer Aushandlungsprozesse entstand und eine Orientierung bieten soll, aber keine Notwendigkeit darstellt (Jenkins-Smith u. a. 2017).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.3 Analytischer Rahmen

Der analytische Rahmen einer Forschungsarbeit dient typischerweise zwei Zielen: Zum einen spezifiziert er die unabhängigen und die abhängige(n) Variable(n). Zum anderen gibt er eine Antwort auf die Frage, wie die unabhängigen Variablen die abhängige Variable erklären. Sofern ein ausreichend gut erforschter Forschungsstand vorliegt, können dann seitens eines Forschenden Theorien eingesetzt werden, die möglichst klare Antworten auf diese Fragen liefern, sodass der Forschende die postulierten kausalen Muster anhand eines empirischen Falls untersucht. Zentrale Bedeutung kommt also der theoriegeleiteten Spezifizierung der zu untersuchenden Variablen und kausalen Faktoren zu (A. Bennett und Checkel 2015a; Collier 2011; George und Bennett 2005; Hall 2008). Zudem wird die möglichst detaillierte Spezifizierung theoretischer Vorhersagen auch deshalb angeraten, da auf diese Weise ausufernden Erklärungen entgegengewirkt werden soll (Schimmelfennig 2015, 105 f.).

Wie im Forschungsstand (1.2) aufgezeigt wurde, kommen eine Reihe von unabhängigen Variablen als erklärende Faktoren infrage, darunter Veränderungen der verfassungsmäßigen und institutionellen Struktur der EU, eine Vielfalt an Akteuren, die überzeugunsbasiert nach der Beeinflussung von Politik-Ergebnissen streben und ein externer Schock in Form der Snowden-Enthüllungen. Ausgehend von diesen Einflussfaktoren wurde das ACF als theoretischer Rahmen ausgewählt. Daher leitet sich der analytische Rahmen dieser Arbeit auch unmittelbar aus dem ACF ab. Aufgrund des breiten Akteursverständnisses des ACF kommen nicht nur politische Verantwortliche als mögliche relevante Akteure des Policy-Subsystems EU-Datenschutzpolitik infrage, sondern auch Wirtschaftsvertreter, Vertreter der Zivilgesellschaft, zivilgesellschaftliche Bewegungen, Journalisten und Wissenschaftler. Ausgehend vom Forschungsstand zur Datenschutzpolitik sowie zur DSGVO und unter Rückgriff auf ACF-Studien, die auf die Überzeugungen der Akteure und ihren Interaktionen fokussieren (Fenger und Klok 2001; Larsen, Vrangbæk, und Traulsen 2006; Mauersberger 2016; Pierce 2011; Schlager 1995; Zafonte und Sabatier 2004), bestimme ich als die zentralen, zu untersuchenden unabhängigen Variablen die Kerncharakteristiken der Advocacy-Koalitionen: Die *Überzeugungssysteme*, *Zusammensetzung* und *Ressourcen* einer jeden Koalition. Ich gehe davon aus, dass diese drei Variablen in entscheidender Weise den Erfolg und Misserfolg einer Koalition bei ihrem Versuch, Einfluss auf politische Entscheidungsprozesse zu nehmen, determinieren. Als abhängige Variable der Arbeit ist die Verabschiedung der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutz-Grundverordnung definiert. Das Ziel ist es daher zu erklären, inwiefern und auf welche Weise die Advocacy-Koalitionen die Gestaltung der DSGVO prägen konnten.

Wie bereits dargestellt, besteht eine der Schwächen des ACF in der Unterspezifizierung des Mechanismus, wie genau die unabhängigen Variablen – also überzeugungsbasierte Advocacy-Koalitionen mittels Ressourceneinsatzes und der Anwendung von Strategien – die abhängige Variable – also die Entscheidungen durch politische Autoritäten und damit die beschlossenen institutionellen Regeln bzw. Policy Outputs – zu ihren Gunsten beeinflussen.[14] Die Hilfestellung, die das ACF an dieser Stelle bietet, ist die Benennung von vier möglichen kausalen Pfaden (externe Schocks, Policy-Lernen, interne Schocks und ausgehandelte Kompromisse) auf dem Weg zu einem Policy-Wandel. Wie genau die unabhängigen Variablen und die Pfade zu einem Policy-Wandel jedoch miteinander interagieren und die abhängige Variable beeinflussen, bleibt weitgehend eine Black Box. Da das ACF an diesem Punkt an eine Grenze stößt, bediene ich mich zur Untersuchung der kausalen Mechanismen der Untersuchungsmethode der Prozessanalyse. Mittels der Prozessanalyse werden die kausalen Wechselbeziehungen zwischen Akteurshandeln und politischen Entscheidungen herausgearbeitet.

Der gewählte analytische Rahmen der vorliegenden Arbeit (vgl. Abbildung 2) stützt sich somit auf einen *ersten* einführenden Schritt in Form einer Kontextanalyse der Geschichte der Europäischen Datenschutzpolitik und einen zweiten Schritt der detaillierten Akteurs- und Prozessanalyse des Zustandekommens der DSGVO.

Das Ziel des ersten Analyseschrittes besteht darin, die relevanten Kontextbedingungen in Form der relativ stabilen Parameter, externen Systemereignisse im Vorfeld der DSGVO sowie langfristig wichtige politische Gelegenheitsstrukturen zu ermitteln, die entscheidend im Hinblick auf das Zustandekommen der DSGVO waren. Am Ende der Kontextanalyse soll feststehen, was die grundlegenden Merkmale des betrachteten Problems sind, wie natürliche Ressourcen ggf. verteilt sind, welche grundlegenden soziokulturellen Wertvorstellungen und welche Elemente der Sozialstruktur im Hinblick auf das Subsystem der EU-Datenschutzpolitik relevant sind

14 Vgl. hierzu etwa auch das vorgestellte Schaubild des ACF (Abbildung 1), das als Platzhalter lediglich „Strategien" zwischen den Aktivitäten einer Koalition und den Entscheidungen durch Regierungsautoritäten setzt, allerdings nicht näher bestimmt, welche Strategien dies sein könnten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

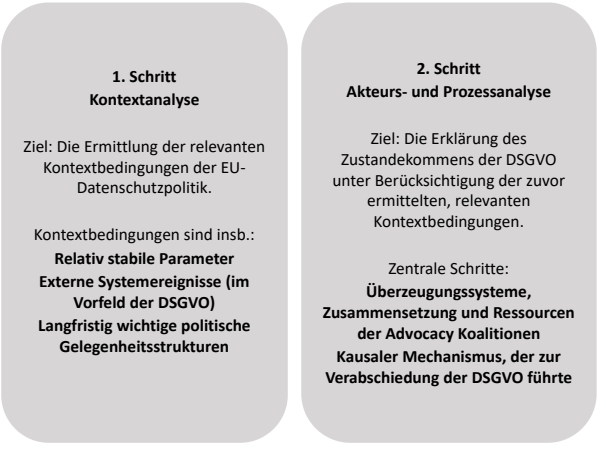

Abbildung 2: Überblick über den gewählten analytischen Rahmen (eigene Zusammenstellung)

und wie die grundlegende verfassungsmäßige Struktur, innerhalb dessen die EU-Datenschutzpolitik verortet ist, aufgebaut ist. Zudem sollen die langfristigen wichtigen politischen Gelegenheitsstrukturen der EU-Datenschutzpolitik ermittelt werden, sodass am Ende der Grad der erforderlichen Zustimmung für wesentlichen Wandel, die relative Offenheit des untersuchten politischen Systems und mögliche, traditionelle Konfliktlinien feststehen. Schließlich untersuche ich den Einfluss von externen Systemereignissen auf datenschutzpolitische Entwicklungen, die historisch vor der DSGVO verortet sind. Diese Herausarbeitung der relevanten Kontextbedingungen stützt sich auf die Analyse der zentralen datenschutzpolitischen Auseinandersetzungen auf EU-Ebene. Diese sind:[15]

15 Ausgenommen von der Analyse sind folgende Vorhaben: Die Entstehung der RFID-Empfehlungen der Kommission, die Untersuchung der PET-Strategie der Kommission sowie der gescheiterte Versuch der Kommission, im Jahr 2004 eine Richtlinie zum Arbeitnehmerdatenschutz zu erlassen (Albrecht 2016a, 97).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

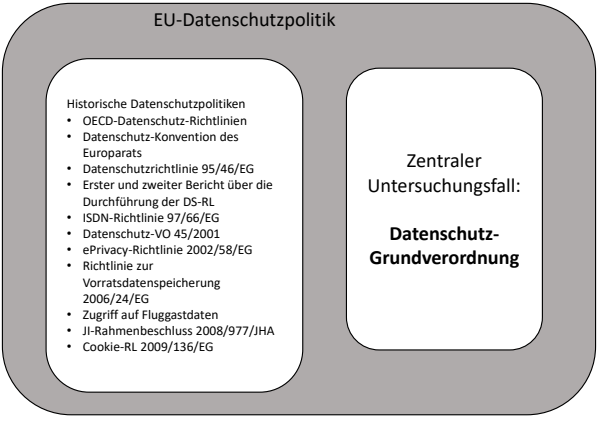

Abbildung 3: Datenschutzpolitische Auseinandersetzungen, die Teil der Kontextanalyse sind (eigene Zusammenstellung)

Auf die Kontextanalyse folgt im zweiten Schritt schließlich die Akteurs- und Prozessanalyse. Die Struktur der Akteurs- und Prozessanalyse kann 2.3.3 entnommen werden. Die Analyse beginnt mit der Untersuchung der Advocacy-Koalitionen. Dazu werden die Überzeugungssysteme, Zusammensetzung und Ressourcen jeder Koalition einzeln analysiert. Darauf folgt im zweiten Schritt die Untersuchung der Aktivitäten der Koalitionen im Rahmen der jeweils betrachteten Phase des politischen Entscheidungsprozesses zur DSGVO. In diesem Schritt kommt die Untersuchungsmethode der Prozessanalyse zum Einsatz. Mit Hilfe der Prozessanalyse werden die kausalen Wirkungsmechanismen und Wechselbeziehungen zwischen den verschiedenen Akteuren, ihren Aktivitäten, den externen Systemereignissen und langfristig wichtigen politischen Gelegenheitsstrukturen usw. untersucht. Auf diese Weise werden die Zusammenhänge zwischen den unabhängigen Variablen, den Pfaden zu einem Policy-Wandel und den abhängigen Variablen offengelegt.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

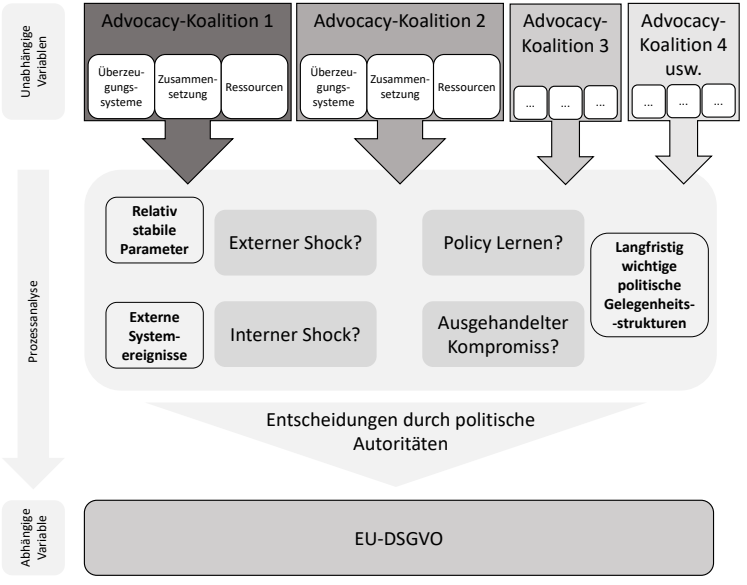

Abbildung 4: Schematische Darstellung des analytischen Rahmens für den Schritt der Akteurs- und Prozessanalyse (in Anlehnung an Mauersberger 2016: 72)

Schließlich unterteilte ich den politischen Aushandlungsprozess zur DSGVO in drei Phasen (siehe Abbildung 5): Die Orientierungsphase (Phase 1), Entwurfsphase (Phase 2) sowie die Konfliktphase (Phase 3). Die Einteilung in Phasen diente dazu, den Einfluss der Akteursüberzeugungen auf den politischen Entscheidungsprozess besser untersuchen zu können, Die Akteurs- und Prozessanalyse wird für jede der drei Phasen wiederholt. Die erste Phase bildet den Zeitraum der ersten Konsultationsphase ab, die zwischen dem 19. Mai 2009 und dem 3. November 2010 stattgefunden hat. Die zweite Phase bildet die sich an die erste unmittelbar anschließende, zweite Konsultationsrunde, die zwischen dem 4. November 2010 und dem 24. Januar 2012 stattfand und mit der Veröffentlichung des Kommissionsentwurfs abgeschlossen wurde. Die dritte Phase umfasst den Zeitraum zwischen der Veröffentlichung des Kommissionsentwurfs am 25. Januar 2012 bis zur Annahme der DSGVO im Trilog bzw. ihrer endgültigen Verabschiedung am 27. April 2016.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

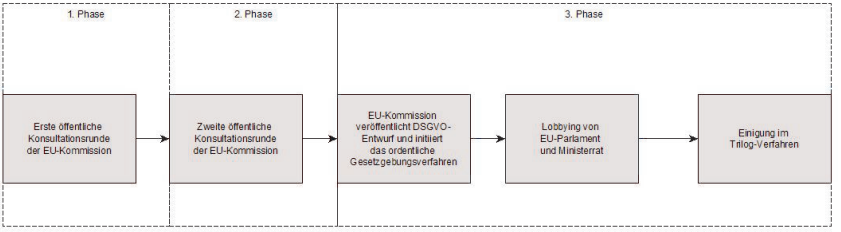

Abbildung 5: Einteilung des politischen Aushandlungsprozesses zur DSGVO in drei voneinander getrennte Phasen (eigene Darstellung)

2.3.4 Operationalisierung

In einer allgemeinen Definition dient der Schritt der Operationalisierung der Zuordnung der zuvor festgelegten theoretischen Begriffe zu empirisch beobachtbaren Sachverhalten, indem Indikatoren zugewiesen werden, mittels derer eine Messung der Erklärungskraft der theoretischen Begriffe möglich wird (Stein 2014, 138). Während diesem Schritt bei quantitativ orientierter Forschung eine enorme Bedeutung im Hinblick auf die Festlegung von Messskalen, -größen, usw. zukommt, orientiert sich qualitative Forschung eher an einer iterativen Vorgehensweise bei der sowohl Deduktion als auch Induktion eine wichtige Rolle zukommt (Przyborski und Wohlrab-Sahr 2014, 118). Da sich der analytische Rahmen der vorliegenden Arbeit auf einen *ersten* einführenden Schritt in Form einer Kontextanalyse der Geschichte der Europäischen Datenschutzpolitik und einen zweiten Schritt der detaillierten Akteurs- und Prozessanalyse des Zustandekommens der DSGVO stützt, stelle ich im Folgenden zunächst vor, wie die Kontextanalyse operationalisiert wird und im Anschluss daran die Operationalisierung der Akteurs- und Prozessanalyse.

2.3.4.1 Operationalisierung der Kontextanalyse

Die Operationalisierung der Kontextanalyse folgt einer qualitativen Vorgehensweise. Die Identifikation insbesondere der relativ stabilen Parameter, der langfristig wichtigen politischen Gelegenheitsstrukturen sowie der externen Systemereignisse erfolgt mittels einer Nominalskala (vgl. überblickshalber auch die vereinfachte Darstellung des ACF in Abbildung 6).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bei der Operationalisierung dieser Kategorien stellt sich – insbesondere im Hinblick auf relativ stabile Parameter und externe Systemereignisse – erneut das Problem der Unterspezifizierung.[16] Die folgende Beschreibung der Eckpfeiler zur Operationalisierung stützen sich insbesondere auf die Hinweise, die in Sabatier und Jenkins-Smith (1993), in Weible und Sabatier (Weible und Sabatier 2007a, 125 f.) sowie in Jenkins-Smith et al. (2014, 144) zu finden sind.

In einer allgemeinen Definition werden zu den *relativ stabilen Parametern*, die den Kontext, in den ein Subsystem eingebettet ist, bilden, die grundlegenden sozialen, kulturellen, ökonomischen, physischen institutionellen Strukturen hinzugezählt. Zudem wird darauf hingewiesen, dass zwischen subsystem-externen Faktoren und -internen Faktoren unterschieden werden kann. Zu den subsystem-externen Faktoren zählen Jenkins-Smith et al. (2014, 144) die grundlegende verfassungsmäßige Struktur und zu den subsystem-internen Faktoren die materiellen Besonderheiten des untersuchten Subsystems:

Grundlegende Merkmale des betrachteten Problembereichs: In den für die Entstehung des ACF zentralen Arbeiten zu den politischen Auseinandersetzungen um den Lake Tahoe werden zu dieser Kategorie jene Attribute der betrachteten Auseinandersetzung gezählt, die den materiellen Kontext des Problems umreißen. Da es sich bei der Auseinandersetzung um ein natürliches Phänomen handelt, beschreiben die Autoren folglich die materielle Beschaffenheit des Sees: Aus welchem Material sich das Seebecken zusammensetzt, welcher Anteil des Sees auf die Niederschlagsmenge zurückgeht und welche sonstigen Besonderheiten den See auszeichnen (vgl. z. B. Weible und Sabatier 2007a, 126).

Verteilung natürlicher Ressourcen: Dieser Aspekt bezieht sich auf die Verteilungskämpfe im Hinblick auf ein politisches Thema. Im Zusammenhang mit dem Lake Tahoe interessierte die Autoren beispielsweise, ob der Zugang zum Seewasser umstritten ist oder ob die Auseinander-

16 Im Hinblick auf die erste Kategorie verweisen die Hauptprotagnisten des ACF regelmäßig (Jenkins-Smith u. a. 2014, 193 f. 2017, 144) auf die Arbeiten von Heclo (1974) und Hofferbert (1974), führen aber nicht im Detail aus, inwiefern der Transfer ihrer Forschungsergebnisse für das ACF erfolgen könnte oder sollte. Die einzige mir bekannte Ausnahme bildet eine frühe Publikation Sabatiers, in der er den Forschungsstand der Theorien des Politikprozesses auswertet und dabei erwähnt, welche Aspekte der Arbeiten der beiden Autoren er schätzt und welche er kritisiert (Sabatier 1991). Eine nähere Anleitung, wie die Kategorien im Rahmen einer ACF-Studie eingesetzt werden können, findet sich allerdings auch dort nicht.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

setzung eher um die Landnutzung im Seebecken kreist. Folglich schildern die Autoren, wie sich die Nutzung des Sees im Laufe der Jahrzehnte entwickelt hat (ebd.).

Grundlegende soziokulturelle Wertvorstellungen und Sozialstruktur: Die Auseinandersetzungen um das Lake Tahoe kreisten um eine Gruppe von Naturschützern einerseits und eine Gruppe von Landnutzern andererseits. Folglich identifizierten die Autoren als die zentralen soziokulturellen Wertvorstellungen, die relevant im Hinblick auf das untersuchten Thema sind, die grundlegende Orientierung der US-amerikanischen Kultur an der Überzeugung eines minimalen Staates und der Verteidigung der Freiheiten des Individuums, die insbesondere als Verteidigung der Eigentumsrechte zu deuten sei. Zudem weisen die Autoren als übergeordnete Konfliktkategorie auf den Konflikt zwischen individuellem Wohl und Allgemeinwohl hin (ebd.).

Grundlegende verfassungsmäßige Struktur: Mit Blick auf die Verfassungen westlicher Staaten argumentieren Sabatier et al., dass die Verfassungen westlicher Staaten über viele Jahrzehnte hinweg unverändert bleiben und einen grundlegenden Handlungsrahmen für jedes Policy-Subsystem vorgeben. Wichtig in einer ACF-Studie ist insbesondere die Identifizierung der relevanten rechtlichen Vorgaben, die das zu untersuchende Subsystem strukturieren (Hohage 2013, 116).

Langfristig wichtige politische Gelegenheitsstrukturen bezeichnen die Autoren als relativ beständig (Weible und Sabatier 2007b, 199 f.). Zudem leitet sich dieses Variablenset aus den relativ stabilen Parametern ab und hat Einfluss auf die Strategien und Ressourcen von Akteuren in politischen Prozessen (vgl. auch Abbildung 6). Folgende Elemente zählen zu diesem Variablenset:

Grad der erforderlichen Zustimmung für wesentlichen Wandel: Der Hauptzweck dieser Variablen besteht darin, Aussagen darüber zu ermöglichen, wie konsens- oder konfliktorientiert politische Aushandlungsprozesse aufgrund des institutionellen Rahmens ausgestaltet sein können. Die grundlegende Annahme in diesem Zusammenhang ist, dass konsensorientierte politische Systeme die beteiligten politischen Akteure eher zur Zusammenarbeit drängen, während weniger konsensorientierte – beispielsweise autoritäre – Systeme es einer geringeren Zahl von Akteuren auch erlauben, konfliktorientiert vorzugehen, sofern sie die politische Macht innehaben (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Relative Offenheit eines politischen Systems: Diese Variable zeichnen zwei Aspekte aus: Einerseits beschreibt sie die Anzahl legislativer Entscheidungsinstanzen, die eine Policy bis zur Verabschiedung passieren muss und andererseits die Zugänglichkeit der Entscheidungsinstanzen (Weible und Sabatier 2007b, 200 f.). Bezogen auf das Beispiel des Lake Tahoe könnte das politische System dann als offen beschrieben werden, sofern nur ein Bezirk oder eine Stadt für das Subsystem zuständig wäre. Da die Zuständigkeiten komplex verteilt sind und nach einer Entscheidung auf Bezirksebene die Bundesstaats- als auch die US-föderale Ebene weiterhin Einfluss nehmen können, betrachten die Autoren das Subsystem als eher geschlossen. In ähnlicher Weise kann ein solches, komplexes (Mehrebenen-)Zuständigkeitssystem auch deshalb als eher geschlossen bezeichnet werden, weil davon auszugehen ist, dass alle Entscheidungsinstanzen nur einem kleinen Kreis an Akteuren stets offenstehen.

Traditionelle Konfliktlinien: Zu dieser Kategorie zählen die Autoren die großen Konfliktlinien der westlichen Weltgeschichte in Gestalt des Konflikts zwischen Kapital und Arbeit, Kirche und Staat, Stadt und Land sowie Zentrum und Peripherie. Ob eine politische Auseinandersetzung auf Subsystemebene eine der traditionellen Konfliktlinien tangiert, wird deshalb als bedeutsam angesehen, weil angenommen wird, dass diese Konfliktlinien eine eigene übergeordnete Form der Parteilichkeit bedingen, die es einer Koalition erschweren oder erleichtern kann, Verbündete zu gewinnen, erwünschte politische Entscheidungen durchzusetzen usw.

Das Variablenset der *externen Systemereignisse* zählt zur Kategorie jener Faktoren, die sich innerhalb kürzerer Zeiträume (≤10 Jahre) verändern können. Diese sind: *Wandel sozioökonomischer Bedingungen*, *Wandel in der öffentlichen Meinung*, *Wandel maßgeblicher (Regierungs-)Koalitionen* sowie *Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen*. Im Hinblick auf jede der Variablen gilt, dass eine Veränderung in der Variablen zu einer Umverteilung der Ressourcen politischer Akteure führen kann (vgl. auch Abbildung 6), wodurch die Machtbalance in dem Subsystem kippen und es zu einem politischen Wandel kommen kann (Weible und Sabatier 2007b, 199). Da externe Systemereignisse als notwendiges, aber nicht zugleich auch hinreichendes Kriterium für politischen Wandel gelten, bedarf es zusätzlich eines externen Ereignis der Kanalisierung des Ereignisses seitens politischer Entrepreneure (Daniel Nohrstedt 2011).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

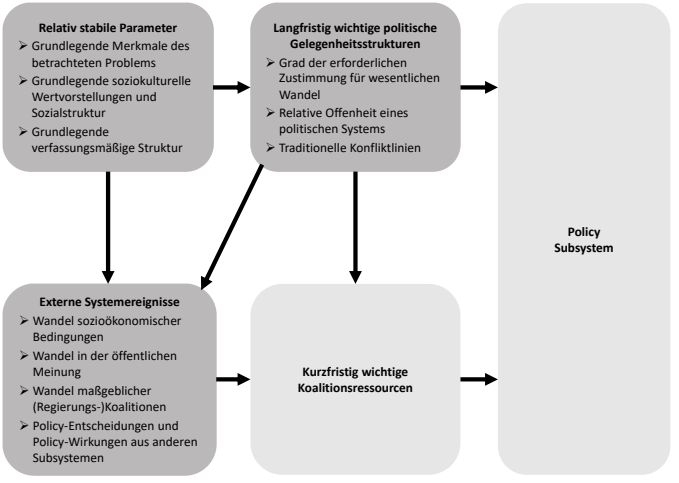

Abbildung 6: Vereinfachtes ACF-Schema (Eigene Darstellung)

2.3.4.2 Operationalisierung der Akteurs- und Prozessanalyse

Nachdem die Zusammensetzung, Überzeugungssysteme und die Ressourcen einer Koalition im Rahmen des analytischen Rahmens als die zentralen unabhängigen Variablen definiert wurden, müssen diese nun operationalisiert werden. Zur Untersuchung der Variablen kommen sowohl quantitative Intervallskalen zur Geltung als auch qualitative Nominal- bzw. Ordinalskalen. Im Folgenden möchte ich jedem der jeweiligen unabhängigen Variablen Indikatoren zuweisen, um nachvollziehbar zu machen, wie eine Messung der Variable erfolgen soll.

Akteursanalyse

Die *Untersuchung des Überzeugungssystems* einer Koalition bildet den Ankerpunkt einer jeden ACF-Analyse. Die Identifikation des Überzeugungssystems dient sowohl der politischen Verortung von Koalitionen als auch der Bestimmung ihrer Mitglieder. Das ACF sieht für die Untersuchung des Überzeugungssystems eine Analyse auf drei Ebenen vor: Grundüberzeugungen, Policy-Kernüberzeugungen und Sekundärüberzeugungen. Die Identifikation des Überzeugungssystems eines Akteurs erfolgt auf Grundlage der in einem politischen Prozess getätigten Aussagen des jeweiligen Akteurs. Die Identifikation der jeweiligen Advocacy-Koalitionen erfolgt schließlich auf Grundlage der quantitativen Einordnung aller Akteursposi-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tionen auf einer Intervallskala (5-Punkte-Likert-Skala) und einer daran anschließenden Cluster-Analyse (für die Details, vgl. Unterabschnitt 4.1.1.1).

Sobald die Advocacy-Koalitionen bestimmt wurden, erfolgt die *Untersuchung ihrer Zusammensetzung*. Dieser qualitativ orientierte Untersuchungsschritt beinhaltet genau genommen zwei Teilschritte in Form einerseits der Bestimmung der einzelnen Koalitionsmitglieder sowie andererseits der Bestimmung des Grads ihrer Kooperation. Hierbei werden sowohl Individuen als auch Organisationen als Akteure in den Blick genommen. Im nächsten Schritt erfolgt die Unterteilung der Akteure in Akteursgruppen: Politische Akteure, Wirtschaftsvertreter, Vertreter der Zivilgesellschaft, Wissenschaftler. Die Zugehörigkeit zu einer Akteursgruppe dient zugleich als ein wichtiger Vorschritt, damit die Untersuchung der Koalitionsressourcen ermöglicht bzw. vereinfacht wird. Die Bestimmung des Grads der Kooperation der Koalitionsmitglieder erfolgt sowohl auf Grundlage der von den Akteuren geäußerten Überzeugungen als auch auf Grundlage konkreter, gemeinsamer Aktivitäten.

Nachdem die Überzeugungssysteme und die Zusammensetzung der Advocacy-Koalitionen bestimmt wurden, erfolgt schließlich die *Untersuchung ihrer Ressourcen*. Die Ressourcen einer Koalition bestimmen das Potential einer Koalition, Einfluss auf politische Entscheidungsprozesse zu nehmen. Die im Sinne des ACF relevanten Ressourcen, die auch Gegenstand der vorliegenden Analyse sein werden, sind (Weible und Sabatier 2007b, 201–3): (1) *Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse*, (2) *Unterstützung durch die Öffentliche Meinung*, (3) *Informationen/Informationshoheit*, (4) *Fähigkeit zur politischen Mobilisierung*, (5) *Finanzielle Ressourcen* und (6) das *Vorhandensein einer fähigen Führung*. Die Untersuchung der Ressourcen erfolgt mittels qualitativer Maßstäbe, da eine Quantifizierung bei diesem Schritt keinen Mehrwert böte.[17]

Prozessanalyse

Auf den Schritt der Akteursanalyse folgt schließlich die Prozessanalyse. Das zentrale Ziel der Prozessanalyse besteht in der Beantwortung der Forschungsfrage, wie die DSGVO entstanden ist. In der Literatur wird zwischen drei Typen der Prozessanalyse unterschieden: (1) deduktiv-theo-

17 Entscheidend ist beispielsweise nicht die Anzahl oder der Rang der in Entscheidungspositionen sitzenden Koalitionsmitglieder, sondern ihre konkrete Ausfüllung der eingenommenen Entscheidungsposition.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

rietestende Prozessanalysen, (2) induktiv-theoriegenerierende Prozessanalysen und solche (3), die der Erklärung eines spezifischen Politik-Ergebnisses dienen, indem sie sich auf eine deduktiv-induktive Vorgehensweise stützen, die jene kausalen Mechanismen offenlegt, die das Ergebnis herbeigeführt haben (Beach und Pedersen 2013; A. Bennett und Checkel 2015a). Aufgrund des Fehlens umfassender politikwissenschaftlicher Theorien zur Entstehung der DSGVO kommt der erste Typus nicht infrage. Der zweite würde hingegen vor allem dann infrage kommen, wenn mein Forschungsziel in der Theoriegenerierung auf Grundlage des vorliegenden Falls liegen würde. Aufgrund des Fokus auf das Zustandekommen des spezifischen Politik-Ergebnisses der DSGVO liegt also der Rückgriff auf den dritten Typus am nächsten.

Die grundlegende handlungsanleitende Vorgabe einer jeden Prozessanalyse ist die möglichst klare Benennung fallspezifischer beobachtbarer Sachverhalte, die aus der verwendeten Theorie abgeleitet werden (A. Bennett und Checkel 2015a, 18). Wie bereits dargestellt legt die Verwendung des ACF nahe, dass ein Politik-Ergebnis, im vorliegenden Fall also die Verabschiedung der DSGVO, auf das überzeugungsbasierte Handeln der Akteure zurückzuführen sein müsste. Darüber hinaus legt das ACF nahe, dass die Kontextbedingungen des betrachteten Subsystems entscheidenden Einfluss auf das Politik-Ergebnis entfalten müssten, und dass das entsprechende Ergebnis bzw. ein Policy-Wandel auf einen der vier möglichen Pfade zurückgeführt werden können muss.

Zur Untersuchung des Aspekts, inwiefern das Policy-Ergebnis auf die Überzeugungen der Akteure zurückgeführt werden kann, stütze ich mich auf die Kombination aus Prozessanalyse und Präferenzerzielung (*preference attainment*). Letztere Untersuchungsmethode geht davon aus, dass sich der Erfolg von Akteuren im Hinblick auf die Beeinflussung eines Politik-Ergebnisses insbesondere darin äußern müsste, dass sich die Inhalte des Politik-Ergebnisses und der Gestaltungsvorschläge der Akteure überlappen (Dür 2008). Der Vorteil der Untersuchungsmethode der Präferenzerzielung liegt darin, dass die Überprüfung der inhaltlichen Überlappung Einflussnahme auch dort sichtbar macht, wo diese unsichtbar erfolgte. Eine Schwierigkeit dieser Untersuchungsmethode liegt in der Erhebung der Präferenzen der Akteure. Schwierigkeit wird insbesondere dem Umstand zugesprochen, dass Akteure ihre *wahren Präferenzen* in öffentlichen Statements, Interviews usw. häufig verschleiern, während sie zugleich hinter den Kulissen auf Grundlage ihrer wahren Überzeugungen tatsächlichen Einfluss auf politische Prozesse nehmen (Dür 2008, 567 f.). Dieses Problem ist mir

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

bewusst, doch denke ich, dass die Tragweite dieses Problems in starkem Maße davon abhängt, um was für ein Policy-Subsystem es sich bei einem Fall handelt. Die Grundannahme des ACF besagt, dass die Anordnung von Akteuren in reifen Subsystemen über viele Jahre und Jahrzehnte grundsätzlich stabil bleibt und dass sich größere Veränderungen nur unter bestimmten (Kontext-)Bedingungen ereignen. Diese Annahme hat wiederum zur Grundlage, dass die Policy-Kernüberzeugungen der Akteure in der Regel über längere Zeiträume stabil bleiben und lediglich Sekundärüberzeugungen spontaneren Veränderungen unterliegen. Daher gehe ich davon aus, dass die Identifikation der tatsächlichen Überzeugungen der Akteure in ausreichendem Maße möglich sein sollte, sofern eine langfristige Analyseperspektive eingenommen wird, die nicht nur auf singuläre Ereignisse setzt. Entscheidend im Hinblick auf Präferenzerzielung ist, dass Akteure verschiedene Strategien anwenden können, um ihre Ziele zu erreichen. Wichtig ist auch der Hinweis, dass sich politischer Erfolg im Hinblick auf die Beeinflussung politischer Inhalte nicht immer nur an der inhaltlichen Überlappung äußert. Es kann auch sein, dass sich die Präferenzen von Akteuren zwar nicht unmittelbar in einem Politik-Ergebnis äußern, diese aber trotzdem Einfluss auf das Ergebnis nehmen konnten, indem sie die Verabschiedung eines in noch radikalerem Maße ihren Forderungen nicht entsprechenden Ergebnisses verhindern konnten (ebd., 561 f.). Die Überprüfung der Präferenzerzielung muss zudem auch reflektieren, dass einige Akteure auf einige wenige, ihnen aber zugleich sehr wichtige Themen fokussieren und lediglich diese versuchen zu ihren Gunsten zu beeinflussen suchen könnten (ebd., 568 f.). Eine weitere Herausforderung ergibt sich aus der Grundannahme, die der Untersuchungsmethode der Präferenzerzielung zugrunde liegt: Dass eine inhaltliche Überlappung zwischen Akteurspräferenzen und Politik-Ergebnis vorhanden ist, sagt alleine noch nichts darüber aus, ob das Ergebnis tatsächlich auf das Akteurshandeln zurückgeführt werden kann oder ob stattdessen andere Faktoren, die womöglich nichts mit dem Akteurshandeln zu tun haben, entscheidend waren. Unklar bleibt auch, falls eine aktive Beeinflussung stattgefunden hat, welche Kanäle der Beeinflussung gewählt wurden und wie genau diese erfolgte (Dür 2008, 561 f. Klüver 2013, 63). Sofern die geäußerten Überzeugungen der Akteure ausreichend gut gemessen werden können, stellt sich das Problem der Zusammenstellung von ausreichender Evidenz, um den Mechanismus zu entschlüsseln, durch den die Überzeugungen der Akteure politische Entscheidungen beeinflusst haben (Jacobs 2014, 46).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Diese Rolle kommt der Untersuchungsmethode der Prozessanalyse zu. Die Wichtigkeit der dabei gezogenen Schlussfolgerungen bemisst sich nicht allein an der Anzahl von Beobachtungspunkten. Vielmehr kann einzelnen Beweisstücken ein besonderes Gewicht beigemessen werden (A. Bennett und Checkel 2015a, 16). Dementsprechend wird die Prozessanalyse häufig mit kriminalistischen Ermittlungen, juristischer Beweisführung oder klinischer Diagnostik verglichen. Grundlegend baut die Prozessanalyse auf vier Arten qualitativer Tests („straw-in-the-wind test", „hoop test", „smoking gun test" und „doubly-decisive test"), mittels derer die *Gewissheit* (certainty) und die *Trennschärfe* (uniqueness) einer Hypothese analysiert wird. Trennschärfe beschreibt dabei die Wahrscheinlichkeit, mit der eine Hypothese stimmt, wenn gewisse Evidenz vorliegt oder, dass diese nicht stimmt, sofern es entsprechender Evidenz mangelt. Trennschärfe beschreibt dagegen die Wahrscheinlichkeit, mit der bei Nichtvorliegen automatisch die alternative Hypothese korrekt ist. Im Folgenden möchte ich die vier Arten qualitativer Tests nach Starke (2015, 467 f.) vorstellen:

- „Der ‚straw-in-the-wind test' ist der schwächste der vier Tests, da er sich weder durch besonders große Gewissheit noch durch Trennschärfe auszeichnet. Van Evera (1997, S. 32) nennt hier als Beispiel das Fehlen eines schriftlichen Führerbefehls zum Holocaust. Weder ist ein solches Dokument notwendig, um zu argumentieren, dass Hitler persönlich den Holocaust befahl; noch erlaubt seine Abwesenheit automatisch starke Schlüsse darüber, dass Hitler ihn nicht unterstützte oder über alternative historische Ursachen für die national sozialistische Vernichtungspolitik. Würde man ein solches Dokument finden, so hätte es sicher seinen Platz in der Argumentation, würde aber nicht ausreichen, um alternative Erklärungen zu entkräften.
- Beim ‚hoop test' sind Beobachtungen gewiss, aber nicht trennscharf. Negative Evidenz kann eine Hypothese zwar entkräften, aber positive Evidenz hat nur sehr geringe Aussagekraft. Das Beispiel hier ist etwa die Anwesenheit des Verdächtigen in der Stadt, in der ein Verbrechen stattfand. Kann ein Beschuldigter beweisen, dass er außer Landes war, so ist er wohl unschuldig, seine Anwesenheit selbst beweist aber nur, dass es ihm möglich war, die Tat zu begehen, nicht aber, dass er sie begangen hat.
- Bei einem ‚smoking gun test' verhält es sich genau anders herum. Geringe Gewissheit und hohe Trennschärfe eines solchen Tests bewirken, dass zwar ein positiver Nachweis entscheidend sein kann, eine Hypothese

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ihren Alternativen vorzuziehen, ein negativer Befund jedoch nicht. Der Verdächtige mit dem rauchenden Colt war wohl der Täter. Nur, weil ein Verdächtiger keinen rauchenden Colt in der Hand hält, kann er allerdings noch nicht als entlastet gelten.

- Der ‚doubly-decisive' Test ist vergleichbar mit Aufnahmen eines Verbrechens (z. B. eines Banküberfalls) durch eine Überwachungskamera. Einerseits ist positive Evidenz (z. B. ein deutlich erkennbares Gesicht) in hohem Maße inkriminierend (= hohe Gewissheit), andererseits kann sie als entlastend gelten, wenn der Beschuldigte nicht zu sehen ist (= Trennschärfe)."

Entscheidend im Hinblick auf die Untersuchung der Diffusion von Überzeugungen in politische Entscheidungen ist ihre Übernahme oder bereits zuvor erfolgte Verinnerlichung seitens der Entscheidungsträger (Jacobs 2014, 66 f.).[18] Das bedeutet z. B., dass Veränderungen des Outcomes auf den Eintritt einzelner überzeugungsgetriebener Policy Entrepreneure in den politischen Prozess zurückgeführt werden können müssen (ebd., 67).

Der Überprüfung der Überschneidung zwischen den von den Akteuren getragenen Überzeugungen und dem politischen Ergebnis kommt beispielsweise die Aussagekraft eines Hoop-Tests (notwendig, aber nicht hinreichend) zu. Denn um den Einfluss von Akteuren bestimmen zu können ist es notwendig, aufzeigen zu können, dass die von den Akteuren vertretenen Positionen sich in einer später verabschiedeten Policy wiederspiegeln. Wenn die Inhalte einer Policy keine der von den Akteuren geforderten Punkte wiederspiegelt, kann weitestgehend ausgeschlossen werden, dass die Akteure einen Einfluss auf den Entscheidungsprozess nehmen konnten. Dies stellt allerdings alleine noch keine hinreichende Begründung dafür dar, dass der Grund für die inhaltliche Gestaltung der Policy auch tatsächlich die Übernahme der entsprechenden Akteurspositionen gewesen ist und nicht andere Faktoren ursächlich waren (Jacobs 2014, 71).[19]

18 Hier besteht also grundsätzlich die Möglichkeit, dass Entscheidungsträger entweder schon vorher gewisse Überzeugungen verinnerlicht haben oder im Laufe politischer Entscheidungsprozesse durch Policy-Lernen einzelne – bedeutsamere oder weniger bedeutsame – Elemente ihrer Überzeugungen verändern.

19 Abweichungen von überzeugungsbasierten politischen Ergebnissen müssen jedoch nicht notwendigerweise bedeuten, dass Überzeugungen keine Rolle spielten. Möglich ist etwa auch, dass ein Outcome Ergebnis sowohl von überzeugungsbasiertem Akteurshandeln als auch anderer Faktoren ist: „This complication is not intractable, however; indeed, it can be turned into a testable hypothesis. By closely examining the decision-making process alongside the details of the outcome, the analyst should

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Mittels der Prozessanalyse wird nun das Ziel verfolgt, geeignete Evidenz für möglichst starke Tests zu finden. Besondere Bedeutung wird hierbei der Spezifizierung der empirischen Implikationen der verwendeten Theorie beigemessen: „Was sind die empirischen Erwartungen, wenn Theorie A stimmt? Aber auch: Was dürfte nicht zu beobachten sein? Wie überraschend sind bestimmte Beobachtungen?“ (Starke 2015, 469) Das Advocacy Coalition Framework bildet den theoretischen Rahmen der vorliegenden Arbeit. Die zu überprüfenden empirischen Erwartungen leiten sich daher aus dem ACF ab. Insbesondere die vorgestellten vier möglichen Pfade für einen Policy-Wandel (externe Schocks, Policy-Lernen, interne Schocks und ausgehandelte Kompromisse) stellen somit die zu überprüfenden empirischen Erwartungen der vorliegenden Arbeit dar. Entscheidend im Hinblick darauf, ob und inwiefern einer der vom ACF postulierten Pfade tatsächlich einen Policy Wandel bewirkt, ist wiederum, ob und inwiefern es Advocacy-Koalitionen unter Berücksichtigung der relevanten Kontextbedingungen (relativ stabile Parameter, externe Systemereignisse, langfristig wichtige politische Gelegenheitsstrukturen, kurzfristige wichtige Koalitionsressourcen) gelingt, geeignete Strategien anzuwenden, um die Entscheidungen politischer Entscheidungsträger so zu beeinflussen, dass die eigenen Überzeugungen in möglichst hohem Maße berücksichtigt werden.

Da sich Gesetzgebungsprozesse meist über mehrere Phasen erstrecken (mind. eine Entwurfsphase sowie eine Gesetzgebungsphase) (Dür 2008, 561 f.), bietet es sich zudem an, die Einflussnahme auf politische Aushandlungsprozesse entlang unterschiedlicher Phasen zu untersuchen. Dies eröffnet die Möglichkeit nachzuvollziehen, welche Gestaltungsvorschläge seitens der Akteure gemacht wurden und inwiefern diese Vorschläge im Aushandlungsprozess diskutiert wurden (Jacobs 2014, 61).[20]

2.3.5 Datenerhebung und -analyse

Zur Bearbeitung meiner Forschungsfragen kombiniere ich verschiedene Datenquellen und Datenerhebungsmethoden.

---

be able to determine how well any departures from the prescriptive logic of an idea held by one set of actors “fit” the demands of other actors with veto power or strong bargaining leverage.” (Jacobs 2014, 71)

20 Dadurch wird folgender Test möglich: “if an option was removed from the menu of active alternatives for ideational (or material) reasons at stage S, then we should be able to observe actors who plausibly held that idea (or who had that material interest) centrally engaged in the policymaking process at or before S.” (Jacobs 2014, 61)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die einführende Kontextanalyse basiert überwiegend auf einer Durchsicht der einschlägigen Sekundärliteratur. Das Ziel der Kontextanalyse ist es, die (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik zu identifizieren, die in entscheidendem Maße Einfluss auf die Verabschiedung der DSGVO hatten. Hier kann zunächst auf einige politikwissenschaftliche Publikationen zurückgegriffen werden, die auf verschiedene wichtige Entwicklungen und politische Zusammenhänge hinweisen. Ergänzend liegt zudem eine Vielzahl juristischer Publikationen (z. T. von Akteuren, die selbst an den entsprechenden politischen Entscheidungsprozessen direkt oder indirekt beteiligt waren) vor, in denen sich ebenfalls hilfreiche Analysen politischer Zusammenhänge finden lassen. Zur Ausfüllung von Leerstellen in der Sekundärliteratur greife ich auf Primärdokumente (in Form von Policy-Dokumenten, Stellungnahmen, Plenar- und Sitzungsprotokollen, Resolutionen etc.) und die Medienberichterstattung zurück. Die Darstellung der Entwicklung der EU-Datenschutzpolitik erfolgt im weitesten Sinne narrativ, d. h. insbesondere, dass anders als in der Akteurs- und Prozessanalyse die Identifikation der Advocacy-Koalitionen nicht den Anfangspunkt der Untersuchung bildet, sondern ihren Endpunkt.

Die zentrale Akteurs- und Prozessanalyse stützt sich im ersten Schritt auf eine systematische, quantitative Dokumentenanalyse der Stellungnahmen aller Subsystem-Akteure. Mittels dieses Erhebungsschrittes wird es möglich, auf intersubjektiv nachvollziehbare Weise die Überzeugungen der Subsystem-Akteure zu identifizieren. Auf Grundlage der bei diesem Schritt erhobenen Daten unterziehe ich die Subsystem-Akteure im Anschluss einer Cluster-Analyse (für Details, siehe Unterabschnitt 4.1.1.1), um zunächst auf Grundlage der geäußerten Überzeugungen Akteurscluster, d. h. potentielle Advocacy-Koalitionen zu identifizieren. Unter Hinzuziehung ergänzender qualitativer Informationen überprüfe ich zudem den Kooperationsgrad der Akteure. Auf diese Weise wird es möglich, zu untersuchen, welche Akteure Überzeugungen miteinander teilen ohne miteinander in nicht-trivialem Maße zu kooperieren (Advocacy-Communities) und welche Akteure zusätzlich zu den geteilten Überzeugungen aktiv im Hinblick auf die Beeinflussung der EU-Datenschutz-Grundverordnung miteinander kooperiert haben (Advocacy-Koalitionen).[21] Zur Identifikation der Akteursressourcen greife ich vor allem auf Sekundärliteratur und auf die Medienberichterstat-

21 Um aussagekräftigere Ergebnisse zu erzielen ergänzte ich diesen Schritt im Falle der Fleexibilisierungsbefürworter in der zweiten der untersuchten drei Phsaen zudem um eine Netzwerkanalyse (für Details, siehe Unterabschnitt 4.2.1.3.1).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tung zurück. Die Prozessanalyse, mit der der Einfluss der Akteursüberzeugungen auf den politischen Entscheidungsprozess untersucht wird, stützt sich schließlich insbesondere auf die Auswertung von Primärdaten (in Form von Policy-Dokumenten, Stellungnahmen, Plenar- und Sitzungsprotokollen, Resolutionen etc.) sowie teilweise auf die Sekundärliteratur und die Medienberichterstattung zur DSGVO. Die diesem Schritt zugrundeliegende Datenlage kann Tabelle 2-1 entnommen werden. Die zentralen Dokumente aus Parlament und Ministerrat waren – beim Ministerrat auch dank der zahlreichen Leaks – verfügbar. Zur Analyse der Meinungsbildung in der Kommission musste ich mich hingegen auf Presseinformationen, Medienberichte und die weitere Sekundärliteratur verlassen, da keine Dokumente zu den Kommissions- bzw. Referatssitzungen existieren.[22]

Organ	Einheit	Dokumententyp	Verfügbarkeit
Europäische Kommission	Generaldirektion Justiz und Verbraucher	Tagesordnung	Nein
		Grobes Protokoll/ Ergebnisse	Nein
		Wortprotokoll	Nein
	Referat C.3 „Datenschutz" in der Direktion C „Grundrechte und Rechtsstaatlichkeit" in der Generaldirektion Justiz und Verbraucher	Tagesordnung	Nein
		Grobes Protokoll/ Ergebnisse	Nein
		Wortprotokoll	Nein
Europäisches Parlament	LIBE-Ausschuss	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Ja (Video)
	ITRE-Ausschuss	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Ja (Video)
	EMPL-Ausschuss	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Ja (Video)
	IMCO-Ausschuss	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Ja (Video)
	JURI-Ausschuss	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Ja (Video)

22 Ich stellte eine Informationsfreiheitsanfrage an das Datenschutz-Referat der Kommission und bat um Zugang zu potentiell vorhandenen internen Dokumenten, Protokollen usw. In der Antwort wurde mir mitgeteilt, dass keine Tagesordnungen und Protokolle erstellt würden, da die Referatssitzungen einen Ort des informellen Austauschs darstellten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Organ	Einheit	Dokumententyp	Verfügbarkeit
Rat der Europäischen Union	Ratspräsidentschaften	Interne Arbeitsdokumente	ja
	Tagungen des Rats der Europäischen Union (Justiz und Inneres)	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Nein
	Tagungen des AStV	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Nein
	Treffen der JI-Referenten	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Nein
		Wortprotokoll	Nein
	Treffen der „Freunde des Vorsitzes“	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Nein
		Wortprotokoll	Nein
	Treffen der Ratsarbeitsgruppe DAPIX	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Nein
Europäischer Rat	Treffen des Europäischen Rats	Tagesordnung	Ja
		Grobes Protokoll/ Ergebnisse	Ja
		Wortprotokoll	Nein

Tabelle 2-1: Zugänglichkeit von relevanten Daten der administrativ für die Reform zuständigen Akteure in den EU-Organen (eigene Zusammenstellung)

Die beschriebenen Datenerhebungen wurden durch informelle Interviews und teilnehmende Beobachtung ergänzt. Die in den Jahren 2015 bis 2016 geführten vier informellen Interviews dienten der Exploration des Forschungsfeldes und wurden mit drei Personen aus dem akademischen Umfeld (davon zwei aus der Bundesrepublik und eine Person aus dem internationalen Umfeld) sowie einer Person aus dem Kontext des institutionalisierten Datenschutzes geführt. Ergänzend konnte ich, aufgrund der Projektanbindung meines Dissertationsvorhabens, in verschiedenen Kontexten auf die teilnehmende Beobachtung zurückgreifen (siehe Tabelle 2-2 für einen Überblick über die Orte und beobachteten Akteure). Diese diente überwiegend dem Zweck der Verifizierung der übrigen Daten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Orte Beobachtete Akteure	CPDP 2015	Republica 2015	CPDP 2016	CPDP 2017	CAST-Workshop 2018	CPDP 2018
MEP & BE: Jan Philipp Albrecht (Grüne/EFA//Grüne)	x	x	x	x		
MEP & S-BE: Axel Voss (EVP//CDU)	x		x			
Vertreter der deutschen Ratsdelegation			x	x		x
BITKOM					x	
Viviane Reding EU-Justizkommissarin	x		x			

Tabelle 2-2: Teilnehmende Beobachtung - Orte und zentrale Akteure, die beobachtet wurden

Im Folgenden möchte ich noch auf einige kritische Aspekte bei der Datenerhebung bzw. -Auswertung eingehen, bei denen es mir wichtig erscheint, Einblicke in die Erhebungs- bzw. Auswertungsweise zu geben. Dies betrifft zunächst die Begründung meiner Erhebungsmethodik, die Identifizierung der zu untersuchenden Subsystem-Akteure sowie die darauffolgende Messung ihrer Überzeugungen, aber auch die Vorgehensweise auf die sich die Prozessanalyse stützt sowie die Frage, wie ich den Einfluss der beteiligten politischen Akteure auf den Aushandlungsprozess gemessen habe.

2.3.5.1 Begründung der gewählten Datenerhebungsmethoden

Im Folgenden möchte ich die Auswahl meiner Datenerhebungsmethoden begründen. Zur Identifizierung der Überzeugungen von Akteuren eignen sich sowohl die Dokumentenanalyse als auch die Durchführung von Interviews, da sich Überzeugungen in der Regel am deutlichsten in Form sprachlichen Ausdrucks manifestieren, d. h. in den sprachlichen oder schriftlichen Aussagen, die seitens eines Akteurs getätigt werden. Durch die Untersuchung der Aussagen, die von den Akteuren während des politischen Entscheidungsprozesses und im Hinblick auf diesen gemacht werden, kann also *erstens* bestimmt werden, welche Überzeugungen die Akteure haben, und *zweitens* kann dieses Wissen als Nachweis dafür dienen, dass die von den Akteuren getragenen Überzeugungen auf die zur Debatte stehende politische Entscheidung angewendet wurden (Jacobs 2014, 49 ff.). Da sich zur Erhebung von Akteursüberzeugungen sowohl ein interviewbasiertes als auch ein dokumentenanalytisches Vorgehen eignet, möchte ich kurz

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

begründen, weshalb im Rahmen der vorliegenden Arbeit die Analyse von Dokumenten die geeignetere Vorgehensweise darstellte.

Ein erster, wichtiger Grund, der für die Dokumentenanalyse spricht, ist die Reduktion der Gefahr strategischer Antworten. So besteht bei der Durchführung von Interviews im Nachgang eines politischen Aushandlungsprozesses stets die Gefahr, dass die befragten Akteure die Positionen, die sie während der Verhandlungen vertreten hatten[23] im Nachhinein auf verzerrte Weise wiedergeben (Behrens 2003; Krosnick 1999). Diese Gefahr besteht bei der Dokumentenanalyse in geringerem Maße, da die Akteure in schriftlichen Stellungnahmen in aller Regel ihre tatsächlichen politischen Ziele äußern und kein oder nur ein sehr geringes Interesse daran haben, ihre tatsächlichen Absichten zu verschleiern.[24] Die Analyse von schriftlichen Stellungnahmen, die in den politischen Prozess eingebracht wurden, ermöglicht es also, die Akteurspositionen in adäquatem Maße zu erheben (Jenkins-Smith und Sabatier 1993a, 243). Die Bedeutung der Untersuchung sprachlicher Beweise nimmt zudem in dem Maße zu, indem durch empirische und logische Argumentation strategische Motive der Akteure ausgeschlossen werden können (Jacobs 2014, 55). Zur Reduktion der Restgefahr einer Verschleierung der tatsächlichen Überzeugungen oder der kurzfristigen materiellen Interessen hinter populären Überzeugungen und Forderungen, um eine größere Unterstützung für ihre Sache zu gewinnen, als dies auf Grundlage ihrer eigentlichen Überzeugungen möglich wäre, habe ich insbesondere auf die Strategie der Gegenprüfung der untersuchten

23 Wenn im Folgenden von *tatsächlichen Überzeugungen* die Rede ist, meine ich diejenigen Überzeugungen eines Akteurs, die auf den politischen Prozess angewendet wurden. Zu unterscheiden sind tatsächliche Überzeugungen somit sowohl von Überzeugungen, die aus strategischen Gründen auf verzerrte Weise wiedergegeben werden als auch von im psychoanalytischen Sinne *wahren* Überzeugungen.

24 Durchaus denkbar ist, dass Akteure in dem Wissen, dass schriftliche Stellungnahmen publik gemacht werden, *besonders brisante Forderungen* eher in informellen Einzelgesprächen mit Entscheidungsträgern ansprechen werden. In meiner Untersuchung der Akteurspositionen sind aber keine solchen Differenzen zwischen öffentlichen Statements und geleakten Gesprächsinhalten sichtbar geworden. Dass ein Akteur in einer schriftlichen Stellungnahme *alle seine Forderungen* verzerrt, halte ich hingegen für sehr unwahrscheinlich – und ich konnte auch keine Hinweise auf derart abweichende Positionierungen finden (Blatter und Haverland 2012, 117 ff. Blatter, Langer, und Wagemann 2018, 255).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Aussagen mit weiteren Statements der Akteure und Dokumenten über die Akteure gesetzt (Jacobs 2014, 46).[25]

Zweitens erlaubte die Dokumentenanalyse die flächendeckende Analyse aller relevanten Subsytem-Akteurspositionen. Schließlich war eins der Ziele der vorliegenden Studie, die in anderen Arbeiten zur Entstehung der DSGVO vorfindbaren Analysen, die sich meist auf die Analyse weniger Akteure stützen um eine umfassende Akteursanalyse zu ergänzen. Diese Analyse wäre bei einem interviewbasierten Vorgehen nicht möglich gewesen und hätte sich aus Ressourcengründen auf eine Stichprobenauswahl einzelner Akteure beschränken müssen.

Neben öffentlich getätigten mündlichen oder schriftlichen Äußerungen können Akteure allerdings auch Aussagen in eher privatem Rahmen treffen. So kann davon ausgegangen werden, dass Akteure – insb. jene der politischen Elite zugehörigen – in öffentlichen Kontexten eher dazu tendieren werden, ihre Vorschläge, Forderungen und Entscheidungen in gesellschaftlich akzeptable Worte zu hüllen. In eher privaten Kontexten besteht dagegen die Möglichkeit, dass die Wahl der Aussagen weniger vorsichtig getroffen wird. Dies betrifft in besonderem Maße solche Kontexte, in denen Akteure mit überwiegend ähnlichen politischen Zielen aufeinandertreffen. In derartigen Situationen ist davon auszugehen, dass die Überzeugungen der Akteure besonders klar kommuniziert werden und dass auch Aussagen zu Strategien getroffen werden, wie die politischen Ziele erreicht werden sollen (A. Bennett und Checkel 2015b, 25).

Idealerweise müssten dafür private Korrespondenzen zwischen den am politischen Aushandlungsprozess beteiligten Akteuren untersucht werden. Doch der Zugriff auf private Korrespondenzen im Hinblick auf aktuelle Politiken ist im Gegensatz zur Untersuchung veröffentlichter Archiv-Dokumente in Fällen weiter in der Vergangenheit liegender politischer Entschei-

25 Auf diese Weise konnte ich die sog. European Privacy Association (EPA) (vgl. Unterabschnitt 4.2.1.3.3) als Astroturf-Organisation enttarnen. Bei Akteuren, wie der EU-Justizkommissarin Viviane Reding, die regelmäßig vor verschiedenen Zuhörerschaften sprach, spiegelte ich beispielsweise ihre vor Datenschutz-Organisationen getätigten Aussagen mit jenen Aussagen, die sie gegenüber Wirtschaftskreisen tätigte, um strategische Aussagen herauszufiltern und um auf diese Weise dem Kern ihrer Überzeugungen näherzukommen. So war es mir möglich, den Unterschied in den Überzeugungen Viviane Redings und Jan Philipp Albrechts herauszuarbeiten. Während Reding tatsächlich überzeugt davon war, dass ein hohes Datenschutzniveau das Vertrauen in datenverarbeitende Dienste stärken und damit als Vorteil für diese Anbieter fungieren würde, übernahm Albrecht dieses Argument im Verlauf des Aushandlungsprozesses aus strategischen Gründen (vgl. auch Unterabschnitt 4.3.2.4).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

dungen in der Regel nicht oder nur sehr schwer systematisch möglich (Jacobs 2014, 52 ff.). Die Ausnahme bilden hier durchgesickerte Kommunikationsfragmente. Diese (bspw. Briefverkehre zwischen den Akteuren, aber auch vermeintlich anonym erfolgtes Lobbying[26]) sind Teil der vorliegenden Untersuchung, allerdings sollte der Wert durchgesickerter Informationen nicht überhöht werden, insbesondere dann nicht, wenn diese Leaks nicht alle Akteure gleichermaßen umfassen.[27] Eine andere Möglichkeit, um Akteure in eher privaten Kontexten beobachten zu können bildet die teilnehmende Beobachtung bei Veranstaltungen die in die Kategorie eher privater Veranstaltungen eingeordnet werden können (Thierbach und Petschick 2014). Die oben beschriebene Partizipation an mehreren Veranstaltungen diente sowohl der Beobachtung der politischen Akteure beim Aufeinanderprallen in Diskussionen als auch der Beobachtung zentraler Akteure in eher privaten Kontexten, um mehr über deren Überzeugungssysteme zu erfahren.[28]

Die teilnehmende Beobachtung erfüllte allerdings nur eine ergänzende Rolle, da die Teilnahme sich auf Schauplätze beschränkte, die von Privatheitsbefürwortern dominiert waren.[29] Mögliche negative Effekte dieses Datenschutzbefürworter-Bias', würde ich nicht nur ergänzend auf diese

26 Siehe hierzu meine Ausführungen zu den veröffentlichten Korrespondenzen zwischen Interessenvertretern und den für die Verhandlungen zur DSGVO federführend zuständigen Beamten des Bundesinnenministeriums in Unterabschnitt 4.3.2.6.

27 So stieß ich bei meinen Recherchen beispielsweise – obwohl es diese zweifellos gegeben hat – auf keine durchgesickerte Korrespondenz zwischen den für die DSGVO Verantwortlichen aus der EU-Kommission und Interessenvertretern.

28 So sind beispielsweise die in Fn. 25 beschriebenen Erkenntnisse im Hinblick auf die Überzeugungssysteme Redings und Albrechts teilweise auf teilnehmende Beobachtung zurückzuführen.

29 Die seit dem Jahr 2007 stattfindende CPDP (Brüssel) zählt zu den größten interdisziplinären Datenschutz-Konferenzen Europas, auf der Akteure aus Wissenschaft, Politik (insbesondere aus den EU-Organen) und Wirtschaft aufeinandertreffen und über zahlreiche datenschutzrelevante Themen diskutieren. Veranstaltet wird die CPDP federführend von Paul de Hert, der Teil der Datenschutzbefürworter-Koalition ist (CPDP 2019). Die ebenfalls seit dem Jahr 2007 stattfindende re:publica (Berlin) bringt ebenfalls Akteure aus Wissenschaft, Politik und Wirtschaft zusammen, ist allerdings thematisch breiter in der Netzpolitik verortet und deckt in stärkerem Maße das aktivistische Spektrum der Datenschutzbefürworter ab. Die Organisatoren kommen aus dem netzpolit-aktivistischen Spektrum (Das Weblog Spreeblick und die Nachrichtenplattform Netzpolitik.org) (Wikipedia 2019c). Der CAST-Workshop wird vom CAST e. V. veranstaltet, einem seit Anfang 2004 bestehenden Verein, der sich der Förderung der gesellschaftlichen Debatte rund um IT-Sicherheitsthemen widmet. Inhaltlicher Verantwortlicher ist Alexander Roßnagel, ein Datenschutz-Ju-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Beobachtungen zurückgreifen, wären zum Beispiel, dass die Positionen der Datenschutzbefürworter im empirischen Teil der vorliegenden Arbeit in unverhältnismäßig stärkerem Maße Berücksichtigung finden könnten oder, dass mir potentiell wichtige Einblicke in die Verhaltensweisen der wirtschaftsnahen Akteure entgehen könnten.

Die Erklärung für das Bias liegt einerseits in individuellen und andererseits in strukturellen Gründen. Individuell entscheidend war mein persönliches Interesse am Thema Privatheit aus einer eher privatheitsbefürwortenden Perspektive, was zur Folge hatte, dass ich im Laufe der Arbeit eher auf die Idee kam, solche Veranstaltungen zu besuchen, die bzw. deren Teilnehmer und Besucher tendenziell für mehr Privatheitsschutz eintraten. Strukturell entscheidend war hingegen, dass Veranstaltungen, die sich eher als neutraler Austragungsort von Datenschutzdebatten verstehen (gerade deshalb, weil sie sich nicht nur bzw. nicht primär an die Datenschutz-/Privatheits-Community, sondern vor allem an Unternehmen richten) eine vergleichsweise sehr hohe Teilnahmegebühr verlangen[30] oder sich gegenüber der Teilnahme Außenstehender gleich ganz verschließen.[31] Als strukturellen Grund würde ich auch bezeichnen, dass die Forschungscommunity der Privatheits- und Datenschutzforscher, zu denen ich mich hinzuzähle, tendenziell aus Privatheitsbefürwortern besteht und auf den entsprechenden, sich mit diesen Themen befassenden, E-Mail-Verteilern eher datenschutzbefürwortende Veranstaltungen geteilt werden, mir also sehr wahrscheinlich viele Möglichkeiten der Beobachtung von datenschutzkritischen Veranstaltungen schlicht entgangen sind.

---

rist, der ebenfalls dem Spektrum der Datenschutzbefürworter zuzuordnen ist (CAST e.V 2017).

30 So verlangte etwa der stärker als andere Veranstaltungen auf Neutralität bedachte 20. Datenschutzkongress 2019 eine Eintrittsgebühr von 2100,- € für die Teilnahme an beiden Veranstaltungstagen (vgl. https://www.euroforum.de/datenschutz-kongress/anmelden/). Es sind keine Rabatte vorgesehen. Die CPDP 2019 dagegen kostete für Unternehmensmitarbeiterinnen und -mitarbeiter für alle drei Veranstaltungstage 1025,- €. Für Forschende beläuft sich der rabattierte Eintrittspreis auf 500,- € und Studenten und Mitglieder von NGOs zahlen immerhin nur 200,- € (vgl. https://www.cpdpconferences.org/registration).

31 Eine Teilnahme an der von Hubert Burda Media durchgeführte DLD-Konferenz (Digital Life Design), auf der im Jahr 2014 u. a. EU-Justizkommissarin Viviane Reding vor Wirtschaftsvertretern sprach, war entweder nur auf Einladung möglich oder nach der Bewerbung auf eine begrenzte Anzahl von Plätzen für *young creatives*, *students* und *NGOs* möglich (vgl. https://web.archive.org/web/20131102074853/https://dld-conference.com/DLD14).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.5.2 Identifikation und Eingrenzung der Subsystem-Akteure

Eine Schwierigkeit, die bei der Untersuchung des Subsystems der EU-Datenschutzpolitik besteht, liegt in der Trennung von relevantem Stakeholder-Input (also dem Input der Subsystemakteure) von irrelevantem Input (von Nicht-Subsystemakteuren).

Gemäß ACF sollen zwei Aspekte bei der Identifikation von Subsystemakteuren handlungsleitend sein: Erstens, ob sich ein Akteur – aus Wirtschaft, Wissenschaft, Zivilgesellschaft, allen Ebenen der Politik, aber auch Bürgerinnen und Bürger ohne organisationale Anbindung oder Journalisten – in das Subsystem eingebracht hat (also bei Anhörungen etc. partizipiert hat) bzw. qua Funktion Teil des Subsystems ist (Datenschutzaufsichtsbehörden, Ministerialbeamte in den für Datenschutz zuständigen Abteilungen usw.) und, zweitens, da es die Intention des ACFs ist, die Änderung von Überzeugungen im Verlauf von mehreren Jahren zu messen, wie häufig ein Akteur am Subsystem partizipiert hat. In der Regel wird mit Bezug auf Jenkins-Smith und Sabatier (1993a, 241) auf zwei Teilnahmen innerhalb eines Zeitraums von zwei Jahren verwiesen.

Gerade das US-amerikanische Anhörungswesen aber auch europäische korporatistische Systeme bieten relativ klare Maßstäbe für die Beurteilung der Partizipation von Akteuren.[32] Als deutlich schwieriger gestaltet sich dies dagegen beim quasi-korporatistischen Regime der Europäischen Union, das eine Mischung aus geregeltem und ungeregeltem Transfer von Stakeholder-Input darstellt. Geregelte Formen des Transfers stellen beispielsweise die formalisierten öffentlichen Konsultationen der Europäischen Kommission oder Anhörungen in den EU-Parlamentsausschüssen dar. Daneben ist es aber auch üblich, dass sowohl Kommission, als auch Parlament und Ministerrat in zahlreichen intransparenten informellen Kontexten lobbyiert werden. Würde sich also eine Analyse nur auf das geregelte Lobbying beschränken, bestünde die Gefahr, dass potentiell wichtiges, informelles Lobbying unsichtbar bleibt. Wird dagegen versucht, informelles Lobbying miteinzubeziehen, besteht die Gefahr darin, dass nur ein Teil dieses Lobbyings sichtbar wird. Schließlich greifen Akteure auf informelles Lobbying gerade deshalb zurück, weil sie auf unsichtbare Weise Einfluss nehmen

32 Zahlreiche ACF-Studien bieten klare Hinweise bezüglich der Datenerhebung im Kontext der Vereinigten Staaten (Jenkins-Smith u. a. 2014, 210) oder auch im Kontext einzelner europäischer Staaten (Fritz 2013; Moyson 2016; vgl. z. B. D. Nohrstedt 2010).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wollen und geben sich entsprechend viel Mühe dieses Lobbying unsichtbar zu halten (Coen und Richardson 2009; Dialer und Richter 2019; Klüver 2013). Teilweise kann informelles Lobbying sichtbar gemacht werden, z. B. mittels Informationsfreiheitsanfragen (Meister 2015) oder durch Leaks. Dies gewährleistet allerdings nicht auf zuverlässige Weise, dass jedes relevante Lobbying auch tatsächlich sichtbar gemacht werden kann. Auch existierende ACF-Studien, die sich mit Themen auf EU-Ebene auseinandersetzen, helfen an dieser Stelle nicht weiter, da diese mit einem vergleichsweise kleinen Akteurskreis hantieren. So fokussieren bestehende Studien zur EU-Steuerpolitik (Radaelli 1999), zur EU-Stahlpolitik (Dudley und Richardson 1999) oder EU-Finanzpolitik (Quaglia 2010) auf die klassischen staatlichen oder besonders staatsnahen Akteure, also die drei EU-Organe und weiteren EU-Institutionen sowie die Mitgliedstaaten, Demgegenüber umfasst das Subsystem der EU-Datenschutzpolitik ein weitaus breiteres Akteursspektrum.[33]

Da der Aushandlungsprozess der DSGVO einen Fall darstellt, bei dem verschiedene Formen des Lobbyings seitens einer enorm großen Aktuersspanne angewendet wurden (Jančiūtė 2018; Schildberger 2016), und eine Begrenzung auf geregeltes Lobbying also wahrscheinlich die Ausblendung wichtiger Akteure und Position zur Folge hätte, beschloss ich, auch das informelle Lobbying miteinzubeziehen. Zu diesem Zweck identifizierte ich zunächst alle formellen Lobbying-Foren (vgl. hellgrau unterlegte Zeilen in Tabelle 2-3). Im Anschluss ergänzte ich die Liste um alle informellen Foren bzw. Kanäle, die ich im Rahmen meiner Recherchen identifizieren konnte (vgl. weiß unterlegte Zeilen in Tabelle 2-3).

Nach der Identifikation der Lobbying-Foren erweiterte ich die Tabelle zunächst um alle Akteure, die an den formellen Foren partizipierten und erhielt auf diese Weise eine Liste mit insgesamt 612 Akteuren.[34] Zur Bestim-

33 Deutlich wird dies an verschiedenen Punkten: Bereits an der ersten öffentlichen Konsultation der EU-Kommission nahmen 168 Akteure teil (EU Commission 2010). Von verschiedenen Seiten war zu hören, dass das Lobbying zur Datenschutzreform ein auf EU-Ebene bis dahin nie da gewesenes Maß gehabt hätte (Schildberger 2016, xxxvii, xliv, lxiv). Später dokumentierte auch LobbyPlag (LobbyPlag 2013) einen Teil des umfangreichen Lobbyings.

34 Akteure, die gemeinsam mit weiteren Akteuren Stellungnahmen einreichten, behandelte ich stets als individueller Akteur. So nahm ich in der Excel Tabelle beispielsweise die Verbände EMMA und ENPA jeweils einzeln in einer eigenen Zeile als individuelle Akteure auf, auch wenn diese eine gemeinsame Stellungnahme eingereicht hatten. Dadurch umfasste die Akteursliste der ersten öffentlichen Konsultationsrunde am Ende 184 Akteure statt 168 Akteure.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datum	Lobbying-Forum	Grad der Formalität	Anzahl der Beteiligten
19.05.2009	Konferenz der EU-Kommission "More use - more Protection?"	Formell	30
09.07.2009 - 31.12.2009	Erste öffentliche Konsultationsrunde der EU-Kommission	Formell	184
04.11.2010 - 15.01.2011	Zweite öffentliche Konsultationsrunde der EU-Kommission	Formell	297
01.07.2010	Nicht-öffentliche Konsultation mit Schlüsselakteuren „Consultation with Key Stakeholders“	Informell	48
28.01.2011	Joint high-level meeting on data protection: "Data protection (30 years later) - from European to international standards"	Formell	10
19.03.2012	EU Conference "Privacy and Protection of Personal Data"	Formell	37
29.05.2012	LIBE Workshop on the proposed Data Protection Regulation	Formell	10
09.10.2012	Interparlamentarische LIBE-Ausschusssitzung mit einzelstaatlichen Parlamenten	Formell	37
17.12.2012	ITRE Mini-Anhörung zum Thema "Perspektiven der Datenschutz-Grundverordnung für die Bereiche Industrie und Forschung"	Formell	7
25.01.2012 - 21.10.2013	Der Zeitraum, in dem die Möglichkeit bestand, die Europaparlamentarier zu lobbyieren	Informell	173
25.01.2012 - 11.06.2015	Der Zeitraum, in dem die Möglichkeit bestand, die Mitgliedsataaten zu lobbyieren	Informell	
		Gesamt	**833**

Tabelle 2-3: Überblick über formelle und informelle Lobbying-Foren zur DSGVO und die Zahl der im Rahmen dieser Foren lobbyierenden Akteure (eigene Zusammenstellung)

mung der Subsystemzugehörigkeit differenzierte ich die Beteiligungen der Akteure im nächsten Schritt im Hinblick auf die drei Phasen, in die ich den politischen Aushandlungsprozess der DSGVO zuvor unterteilt hatte. Das ACF-Kriterium zur Bestimmung der Subsystem-Zugehörigkeit (zweimalige Partizipation an einem Subsystem) (Jenkins-Smith und Sabatier 1993a, 241) modifizierte ich aufgrund der hohen Zahl an Akteuren dahingehend, dass als Subsystem-Akteure nur jene Akteure infrage kamen, die mindestens über zwei Phasen hinweg dreimal am politischen Aushandlungsprozess der DSGVO partizipierten. Die auf diese Weise erarbeitete Liste der Akteure

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des Subsystems der EU-Datenschutzpolitik[35] ergänzte ich im nächsten Schritt um alle Akteure, die im Rahmen informeller Foren am Aushandlungsprozess partizipierten. Das Ergebnis war eine Akteurstabelle mit 833 Einträgen bestehend aus 322 einzelnen Akteuren (vgl. Tabelle 2-3).[36]

Im Folgenden filterte ich alle Akteure aus der Akteurstabelle heraus, die das Subsystem-Relevanzkriterium nicht erfüllten, da sie nicht innerhalb von zwei Phasen dreimal am Reformprozess partizipiert hatten. Im nächsten Schritt nahm ich einen Vergleich zwischen vollständiger und gefilterter Liste vor. Das Relevanzkriterium fand letztlich allerdings keine strenge Anwendung um keine potentiell wichtigen Akteure aus dem Blick zu verlieren. Bei den folgenden Akteuren, von denen aus verschiedenen Gründen (z.B. weil das ordentliche Gesetzgebungsverfahren den Einbezug von ADR und EWSA vorsieht) davon auszugehen war, dass sie Subsystem-Akteure sind, fand die Regel keine strenge Anwendung: Datenschutzaufsichtsbehörden, mit Datenschutzthemen befasste EU-Institutionen (FRA – EU-Grundrechteagentur, Eurojust und ENISA), verschiedene US-amerikanische staatliche Akteure, sowie die am ordentlichen Gesetzgebungsprozess der EU beteiligten EU-Parlamentsausschüsse, der Europäische Ausschuss der Regionen (ADR), der Europäische Wirtschafts- und Sozialausschuss (EWSA) und alle EU-Mitgliedstaaten. Die finale Akteursliste, die auf Basis von Tabelle 2-3 erstellt wurde, umfasste am Ende 114 Akteure. Tabelle 2-4 listet alle 114

35 Genauer: Des Subsystems der EU-Datenschutzpolitik im Kontext der Aushandlung der DSGVO. Die hier vorgenommene Strategie zur Identifizierung von Subsystem-Akteuren blendet freilich die Partizipation von Akteuren an vorherigen Policy-Prozessen wie der Aushandlung der DS-RL, ePrivacy-Richtlinie usw. aus.

36 Zugang zu der Liste jener Akteure, die Teil der am 01. Juli 2010 erfolgten nicht-öffentlichen Konsultation mit Schlüsselakteuren waren, erhielt ich in Folge einer Informationsfreiheitsanfrage bei der Europäischen Kommission. Mehrere im Internet auffindbare Repositorien (neben lobbyplag auch laquadraturedunet und dataskydd)), die die Stellungnahmen zahlreicher Akteure zugänglich machten, deren Lobbying an Parlament und Ministerrat adressiert war, erleichterten die Erstellung der Akteurstabelle. Für den Fall, dass die auf diese Weise erarbeitete Akteurstabelle unvollständig ist, führte ich schließlich noch eine strukturierte Internet-Recherche durch, bei der ich nach weiteren Stellungnahmen zur Datenschutzreform suchte, die von Akteuren eingereicht wurden, die bereits zweimal und häufiger in meiner Akteurstabelle auftauchten. Die Suchformeln, die bei diesem Schritt in eine Online-Suchmaschine eingegeben wurden, folgten dem Schema:
„Organisation A“ + „Stellungnahme“ + Datenschutz-Grundverordnung
„Organisation A“ + „Stellungnahme“ + DSGVO
„Organisation A“ + „Stellungnahme“ + GDPR
„Organisation A“ + „Opinion“ + Datenschutz-Grundverordnung
Usw.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Akteure auf und zeigt zudem auf, welcher Akteur wann und wie häufig am Subsystem partizipiert hat.

Akteure	2009	2010	2011	2012	2013	2014	2015	Gesamt
Alle Akteure	78	95	22	149	59	19	3	425
Art. 29-Datenschutzgruppe	1		1	5	7			14
EDPS	2	1	1	3	3	3		13
BITKOM	1	2		2	3	2	1	11
Viviane Reding			1	2	6	1		10
Microsoft	2	3		3	2			10
BEUC	2	2		5				9
EDRi	2	1		6				9
ENPA	1	2		3	2	1		9
FEDMA	3	2	1	1	1		1	9
GRC - Ratspräsidentschaft						9		9
AmCham EU	1	2	1	2	1			7
DigitalEurope	2	1	1	3				7
eBay	1	2		3	1			7
EPC	2	1	1	1	1	1		7
IRL - Ratspräsidentschaft				1	6			7
UEAPME	1	2		2	1		1	7
ACT	2	2	1	1				6
EMMA				3	2	1		6
Eurofinas	1	2		3				6
EuroISPA	1	2	1	2				6
GSMA	1	2		2	1			6
IAB Europe	2	2	1	1				6
ICO	1	1		2	2			6
Telefonica		2		3	1			6
US FTC		1		5				6
ACCIS	1	2		2				5
BSA	1	1	1	2				5
CDT	1	1		2	1			5
DEU - Regierung		2		2	1			5
ETNO	1	2		1	1			5
Facebook		1		4				5
GDD	2	2		1				5

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Akteure	2009	2010	2011	2012	2013	2014	2015	Gesamt
Intel	2	2			1			5
TechAmerica, AEA	1	2	1	1				5
US DoC				5				5
BT	1	2		1				4
CEPS	1	1	1	1				4
EBF	1	1		2				4
EMOTA	1	1	1	1				4
FBF	1	1		2				4
GDV	1	2		1				4
LTU - Ratspräsidentschaft					4			4
Nokia		2		2				4
PI	1	1		2				4
VDZ	1	2		1				4
WFA	1	1	1	1				4
Yahoo	1	2		1				4
ZAW	1	1		2				4
vzbv	1	1		1	1			4
BDIU	1	1		1				3
BRAK		1		2				3
Christopher Kuner (EPOF&Hunton&Williams LLP)	2	1						3
CPME		1		2				3
CYP - Ratspräsidentschaft				3				3
DDV	1	1		1				3
DSAB - CAN		1	1	1				3
ECTA	1	1			1			3
EPIC			1	2				3
Europ. Datenschutzbeauftragte			1	1	1			3
FRA - EU-Grundrechteagentur	1			2				3
FRA - Regierung	1			1	1			3
GBR - Regierung	1	1		1				3
Google	1			2				3
ICC	1	1			1			3
Liberty Global	2	1						3
Patrick Breyer	2	1						3

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Akteure	2009	2010	2011	2012	2013	2014	2015	Gesamt
Paul de Hert	2		1					3
EPA	1	1	1					3
AdR (CoR)				2				2
AUT - Regierung	1	1						2
DEU - Parlament	1			1				2
DNK - Ratspräsidentschaft				2				2
Douwe Korff	1	1						2
DSAB - BEL	1	1						2
DSAB - DE - Land	1			1				2
DSAB - ESP	1	1						2
DSAB - NLD	1			1				2
EU-KOM		1		1				2
Eurojust		1		1				2
Europäischer Rat					1	1	1	3
Europarat			1	1				2
EWSA				2				2
FRA - Parlament				2				2
JP Albrecht				1	1			2
SWE - Parlament				2				2
BEL - Parlament				1				1
CYP - Parlament				1				1
Dimitris Droutsas				1				1
DSAB - AUT		1						1
DSAB - CHR			1					1
DSAB - DEU		1						1
DSAB - FRA	1							1
DSAB- IT	1							1
DSAB - LIE		1						1
DSAB - NOR		1						1
DSAB - PL				1				1
DSAB - PRT		1						1
DSAB - SVN	1							1
DSAB - SWE		1						1
EMPL-Bericht					1			1
ENISA				1				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Akteure	2009	2010	2011	2012	2013	2014	2015	Gesamt
FIN - Regierung		1						1
GBR - Parlament				1				1
IMCO-Bericht					1			1
ITA - Parlament				1				1
ITRE-Bericht					1			1
JURI-Bericht					1			1
LVA - Regierung		1						1
NLD - Parlament				1				1
NLD - Regierung	1							1
PL - Regierung		1						1
SWE - Regierung				1				1
US DoJ				1				1
US Gov				1				1

Tabelle 2-4: Häufigkeit und Zeitpunkt der Beteiligung der Subsystem-Akteure am Datenschutzreformprozess (eigene Auswertung)

Die Partizipation der Mitgliedstaaten erfasste ich separat (vgl. Tabelle 2-5). Als Datengrundlage dienten hierbei insb. die Kommentare der Delegationen der Mitgliedstaaten. Diese Kommentare werden seitens der jeweiligen Ratspräsidentschaft gesammelt und in gebündelter Form veröffentlicht. Das erste derartige Dokument umfasste beispielsweise die Art. 1 bis 10 der DSGVO-Kapitel 1 und 2 (vgl. die zweite Spalte in Tabelle 2-5). Ergänzend wurden auch die – ebenfalls seitens der zu einem gegebenen Zeitpunkt federführenden Ratspräsidentschaft veröffentlichten – internen Arbeitsdokumente des Ministerrats verwendet, in denen in Form einer sog. konsolidierten Fassung des debattierten Legislativvorschlags der gegenwärtige Stand der Debatte im Ministerrat dargestellt und in den Fußnoten strittige Fragen thematisiert werden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Mitgliedstaat	Art. 1 - 10 (Kap. 1 und 2)	Art. 11-27 (Kap. 3 bis 4)	Art. 28-39 (Kap. 4)	Art. 40-45 (Kap. 5)	Kap. 6 & 7	Kap. 8	Kap. 9 & 10	Gesamt
Austria				1				1
Belgium	1	1	1	1	1			5
Bulgaria		1	1					2
Cyprus	1							1
Czech Republic	1	1	1	1	1		1	6
Denmark		1						1
Estonia	1	1						2
Finland		1	1	1	1			4
France	1	1	1	1			1	5
Germany	1	1	1	1	1	1	1	7
Greece				1	1			2
Hungary	1	1						2
Ireland	1	1					1	3
Italy	1	1	1	1	1			5
Latvia	1		1				1	3
Liechtenstein	1							1
Lithuania		1	1					2
Luxembourg	1	1	1	1	1			5
Netherlands		1	1	1	1			4
Norway		1	1	1	1	1		5
Poland	1	1	1	1		1	1	6
Portugal			1	1	1		1	4
Romania	1	1	1	1		1	1	6
Slovak Republic	1	1	1	1		1	1	6
Slovenia	1	1				1		3
Spain	1	1	1	1	1	1		6
Suisse				1	1			2
Sweden	1	1		1	1		1	5
Switzerland		1						1
United Kingdom	1	1	1	1	1			5
Gesamt	**19**	**23**	**18**	**19**	**14**	**7**	**10**	**110**

Tabelle 2-5: Überblick über die Kommentare der Mitgliedstaaten zu den DSGVO-Kapiteln (eigene Auswertung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2.3.5.3 Messung der Überzeugungen: Identifikation der Items und Erstellung des Code-Schemas

Dieser Unterabschnitt widmet sich der Beschreibung der Erstellung der Item-Liste und des Code-Schemas, mittels derer die Überzeugungen der Akteure gemessen wurden. Anknüpfend an Jenkins-Smith und St. Clair (1993) ging ich dabei deduktiv-induktiv vor: Die Items des Code-Schemas wurden zunächst identifiziert auf Grundlage (1) der zum Thema DSGVO vorhandenen Literatur (Albrecht 2013g; De Hert und Papakonstantinou 2012; Dix u. a. 2013; P. de Hert und Papakonstantinou 2016; Hornung 2012; Knyrim 2013; Mantelero 2013; Roßnagel 2017; Sloot 2014). Im nächsten Schritt (2) wurden diese Items mittels Inhaltsanalyse einer Stichprobe der vorliegenden Dokumente bestätigt und erweitert. Dieses Vorgehen diente der Zeitersparnis, sodass insb. die Wahrscheinlichkeit verringert wird, dass wichtige Items aus dem Blick geraten und erst während der Codierungsphase in die Item-Liste aufgenommen werden, damit keine erneute Durchsicht der bereits codierten Dokumente im Hinblick auf die neu hinzugekommenen Codes notwendig wird.

Dadurch besteht die Item Liste aus insgesamt 101 Items,[37] darunter 3 Items der Kategorie Grundüberzeugungen, 11 Items der Kategorie Policy-Kern-Überzeugungen und 87 Items der Kategorie Sekundärüberzeugungen.[38]

Die Akteurspositionen pro Phase wurden im Anschluss codiert und jedes codierbare Item mit einem Wert auf einer 5-Punkte-Likert-Skala versehen. Die Werte an den beiden Enden der Skala verweisen auf die für jedes Item spezifischen Extrempositionen der jeweiligen Debatte während die 1 immer für eine extreme Ablehnung regulatorischer Vorgaben codiert wurde und die 5 immer für die weitestgehende Regulierungsforderung gewählt wurde. Mit einer 3 wurde dann immer die Mittelposition einer jeden Debatte codiert.

Die am Ende jeder Phase stehenden Dokumente („Kommissionsmitteilung Gesamtkonzept für den Datenschutz in der EU", „Verordnungsvorschlag", „Parlamentsposition" sowie „Ratsposition") wurden ebenfalls

37 Die entsprechenden Item-Listen, Excel-Daten, der Codierbogen, die SPSS-Auswertungen und sonstige relevante Dokumente lassen sich unter dem folgenden Link erreichen: https://zenodo.org/records/10656864

38 Aus forschungspraktischen Gründen wurde auf einen Reliabilitätstest verzichtet. Aufgrund bisheriger Erfahrungen (Bandelow 1999, 167) ist allerdings davon auszugehen, dass keine im statistischen Sinne exakte Messung erfolgte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

codiert. Indem die codierten Akteurspositionen der Phase eins mithilfe einer Clusteranalyse mit der „Kommissionsmitteilung Gesamtkonzept …" korreliert wurden, konnte ich herausfinden, welche Akteure vergleichbare Positionen wie die Kommission vertreten haben (welche Akteure demselben Cluster zugeordnet werden können und wie weit die inhaltlichen Positionen der Akteure voneinander entfernt sind). Indem diese Vorgehensweise auf alle Phasen angewendet wurde, konnte eine Beurteilung der Verarbeitung des Stakeholder-Inputs durch die Europäische Kommission, das Parlament und den Rat im Hinblick auf die Datenschutz-Grundverordnung erfolgen.

2.3.6 Reflexion über Normativität und Objektivität

Eine der Schwächen des ACF ist dessen Herangehensweise an das Thema der Normativität und Objektivität auf Seiten des ACF-Forschenden selbst. Wie bereits in Unterabschnitt 2.2.6 geschildert, wird im ACF zwar angenommen, dass in politischen Auseinandersetzungen kein objektives Wissen existiert und jede Weltwahrnehmung und Äußerung von den Überzeugungssystemen der an politischen Prozessen beteiligten Akteure geprägt wird. Im Hinblick auf Forschende, die mittels des ACF auf politische Prozesse blicken, wird diese Prämisse hingegen vollständig verworfen und angenommen, dass die Forschenden imstande seien, objektive Erkenntnisse über die Funktionsweise der Politik zu generieren. Um diese Diskrepanz nicht unberücksichtigt zu lassen, möchte ich mit diesem Unterabschnitt eine kurze Reflexion meiner eigenen Position im Kontext des Dissertationsvorhabens anstellen.

Das zentrale Moment der Reflexion meiner eigenen Position im Rahmen der vorliegenden Arbeit betrifft meine persönliche Haltung zum Thema Privatheit und Datenschutz. So ordne ich mich selbst fraglos dem Lager der Datenschutzbefürworter zu. Ich schätze Privatheit und Datenschutz als wichtige Stützpfeiler sowohl eines jeden Individuums und dessen sozialpsychologischer Verfassung als auch einer demokratischen und selbstbestimmten Gesellschaft ein. Im Hinblick auf die Frage der konkreten Ausgestaltung eines sinnvollen Privatheitsschutzes bin ich allerdings relativ leidenschaftslos.

Grundsätzlich besteht hierbei das Problem des sog. *Bestätigungsbias*, wonach Forschende grundsätzlich der Neigung ausgesetzt sind, zu überprüfende empirische Implikationen und das empirische Material auf eine

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Weise auszuwählen, zu erheben und zu interpretieren, dass die eigenen (theoretischen) Erwartungen bestätigt werden (Nickerson 1998). Um den Bestätigungsbias möglichst zu vermeiden, achtete ich während aller Analyseschritte insbesondere darauf, Positionen, die nicht meinen eigenen Überzeugungen entsprechen, so authentisch wie möglich wiederzugeben und zugleich stets die stärksten Aspekte der gegnerischen Argumente hervorzuheben. Zudem stützte ich meine Analyse nicht allein auf Deduktion, sondern versuchte stets offen für induktive Erkenntnisse zu bleiben (Starke 2015, 475). Hilfreich sind auch die von Bennett und Checkel (2014, 21) aufgestellten Gütekriterien für Prozessanalysen:

1) „Wirf das Netz für alternative Erklärungen möglichst weit aus
2) Beurteile alternative Erklärungen gleich streng
3) Beachte die Möglichkeit der Verzerrung durch die verwendeten Quellen
4) Überlege, ob der Fall „most likely" oder „least likely" für alternative Erkärungen ist
5) Begründe die Entscheidung, an welcher Stelle du beginnst
6) Sei unerbittlich beim Sammeln von unterschiedlichen und relevanten Daten, aber begründe die Entscheidung, wann du mit dem Sammeln aufhörst
7) Kombiniere die Prozessanalyse mit Fallvergleichen, wenn es für das Forschungsziel nützlich und machbar ist
8) Sei offen für induktive Erkenntnisse
9) Verwende Deduktion für die Frage: „Welcher spezifische Prozess muss zu meinem Outcome führen, wenn meine Erklärung stimmt?"
10) Denke daran, dass eine schlüssige Prozessanalyse zwar gut, aber nicht jede Prozessanalyse schlüssig ist" (Übersetzung von Bennett und Checkel (2014, 21) nach Starke (2015, 476))

Abschließend möchte ich noch darauf hinweisen, dass ich selbst nicht Teil einer Advocacy-Koalition gewesen bin. Aufgrund meiner Rolle als wissenschaftlicher Mitarbeiter an einer außeruniversitären Forschungseinrichtung und als Mitarbeiter in einem großen, interdisziplinären Forschungsprojekt zu Privatheit und Datenschutz[39] konnte ich zwar an einigen themenrelevanten Veranstaltungen teilnehmen und Koalitionsakteure unmittelbar be-

39 Das BMBF-geförderte Forschungsprojekt Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt: www. forum-privatheit.de

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

obachten, partizipierte selbst aber nicht in einem Maße am Aushandlungsprozess, der die Einstufung als Subsystem-Akteur rechtfertigen würde.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

3 Kontextanalyse

Für die Erklärung politischer Entwicklungen mithilfe des Advocacy Coalition Frameworks ist zunächst die Identifikation der wesentlichen politischen Rahmenbedingungen eines Policy-Subsystems erforderlich. Das Ziel der Kontextanalyse ist es, die relevanten (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik zu identifizieren, die in entscheidendem Maße Einfluss auf das Zustandekommen der DSGVO hatten.

Die Analyse folgt den Vorgaben des gewählten theoretischen Rahmens in Gestalt des ACF und hat zunächst zum Ziel, die Entwicklung der EU-Datenschutzpolitik von ihren Anfängen in den 1970er-Jahren bis zum Beginn des Aushandlungsprozesses der DSGVO im Hinblick auf das Variablenset relativ stabiler Parameter zu untersuchen, von denen im ACF angenommen wird, dass sie über längere Zeiträume (etwa zehn Jahre) stabil bleiben. Das Variablenset relativ stabiler Parameter umfasst (1) die grundlegenden Merkmale des betrachteten Problems, (2) die Verteilung natürlicher Ressourcen, (3) grundlegende soziokulturelle Wertvorstellungen und die Sozialstruktur sowie (4) die grundlegende verfassungsmäßige Struktur. Die Kontextanalyse hat darüber hinaus zum Ziel, die langfristig wichtigen politischen Gelegenheitsstrukturen insb. in Form des Grads der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des untersuchten politischen Systems herauszuarbeiten und zu untersuchen, inwiefern traditionelle Konfliktlinien in den untersuchten datenschutzpolitischen Auseinandersetzungen berührt werden. Schließlich soll im Rahmen der Kontextanalyse untersucht werden, inwiefern die Datenschutzpolitik durch externe, dynamische Systemereignisse beeinflusst wurde, von denen angenommen wird, dass sie sich innerhalb von weniger als zehn Jahren verändern können. Zum Variablenset der externen, dynamischen Systemereignisse zählt (1) der Wandel in den sozioökonomischen Bedingungen, (2) der Wandel in der öffentlichen Meinung, (3) der Wandel maßgeblicher (Regierungs-)Koalitionen und (4) Policy-Entscheidungen oder -Wirkungen aus anderen Subsystemen.

Anders als in der Akteurs- und Prozessanalyse des späteren DSGVO-Abschnitts (vgl. Unterabschnitt 4), wird bei der Kontextanalyse größerer Wert auf die Herausarbeitung von Entwicklungstendenzen gelegt und daher in geringerem und weniger systematischem Maße auf die Positionen der an

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

den Aushandlungsprozessen beteiligten Akteure eingegangen. Die Analyse fokussiert sich daher auf die zentralen und insb. institutionellen Akteure der entsprechenden Policy-Debatten.

Die Kontextanalyse umfasst die relevantesten datenschutzpolitischen Auseinandersetzungen bzw. Entwicklungen, die bis zur Verabschiedung der DSGVO insb. auf EU-Ebene geführt wurden bzw. sich ereigneten. Zu diesem Zweck teilt sich der Abschnitt in vier inhaltliche Unterabschnitte auf zweiter Ebene, plus einen fünften Unterabschnitt, in dem ein Zwischenfazit gezogen wird, auf. Zu Beginn werden in Unterabschnitt 3.1 die Frühphase der Datenverarbeitung und die Entstehung der OECD-Datenschutz-Richtlinien sowie der Datenschutz-Konvention des Europarats untersucht. Im zweiten Unterabschnitt (3.2) folgt die Analyse der Aushandlung der ersten Datenschutz-Instrumente, die auf Gemeinschaftsebene verabschiedet wurden, darunter insb. die DS-RL, aber auch das Safe Harbor-Abkommen, die ISDN-RL und die Datenschutz-VO. Der dritte Unterabschnitt (3.3) widmet sich der Analyse der Datenschutz-Politiken bzw. datenschutzrelevanten sicherheitspolitischen Maßnahmen, die unter veränderten politischen Rahmenbedingungen nach der Jahrtausendwende verhandelt wurden, darunter insb. die ePrivacy-RL, die Berichte der Kommission über die Durchführung der DS-RL, die Richtlinie zur Vorratsdatenspeicherung, die Gewährung des Zugriffs auf Fluggastdaten, der JI-Rahmenbeschluss sowie die Aushandlung der Cookie-RL.

Der vierte inhaltliche Unterabschnitt (3.4) widmet sich der Untersuchung des Wandels relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform von entscheidender Bedeutung waren. Zu diesem Zweck wird zunächst entlang der Analyse der Entstehung der EU-Grundrechtecharta, des Vertrags von Lissabon und des Stockholmer Programms der Wandel in der grundlegenden verfassungsmäßigen Struktur, des Grads der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des politischen Systems aufgezeigt. Daran schließt sich die Untersuchung der Veränderung sozioökonomischer Bedingungen und der öffentlichen Meinung in der EU an.

Im fünften Unterabschnitt (3.5) werden die Ergebnisse der Kontextanalyse schließlich zusammengefasst sowie auf Grundlage der Erkenntnisse aus der Kontextanalyse ein erster Überblick über die Advocacy-Koalitionen im Bereich der EU-Datenschutzpolitik geliefert.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.1 Die Frühphase der Datenverarbeitung und die Divergenz nationaler Datenschutzgesetze

Am Anfang der Debatten über den gesetzlichen Schutz personenbezogener Daten stand die Diskussion staatlich-behördlicher Kontrollvorstellungen, die ihren Höhepunkt am Ende der 1960er-Jahre fanden. Mittels Verwaltungsautomation sollten Datenbestände automatisch zusammengeführt und ausgewertet werden können, um die Vereinfachung von Verwaltungsabläufen, Kostensenkungen und eine Optimierung staatlicher Planungsmaßnahmen zu erreichen. Zeitgleich warnten Kritiker vor den negativen Folgen dieser Pläne. So würde die grenzenlose Erhebung und Zusammenführung personenbezogener Daten nicht nur ein nie dagewesenes Maß an Durchleuchtung des Einzelnen ermöglichen, die computergestützte Auswertung der Daten könne zudem neues Wissen über Personen generieren, „das unter Umständen weit über das hinausgehe, was diese selbst über sich wissen." (Berlinghoff 2013a, 16) Schließlich würde der wachsende Informationsbestand auf Seiten der Exekutive die Informationsasymmetrie zwischen Regierung und parlamentarischer wie außerparlamentarischer Opposition verschärfen und somit zu einer Untergrabung des demokratischen Gemeinwesens führen (ebd.).

Als Reaktion auf diese Kritiken entstand das weltweit erste Datenschutzgesetz, das am 30. September 1970 im deutschen Bundesland Hessen verabschiedet wurde.[40] Weniger als drei Jahre später folgte das erste nationale Datenschutzgesetz, das am 11. Mai 1973 in Schweden verabschiedet wurde sowie zahlreiche weitere Datenschutzgesetze Staats- als auch Landesebene, wie der US Privacy Act (1974) oder das BDSG (1977) (Simitis u. a. 2019, 159 ff.).

Die Herausforderung, mit der alle frühen Datenschutzgesetze konfrontiert waren, lag darin, die mit der automatisierten Datenverarbeitung verbundenen Probleme in einer Zeit anzugehen, in der sich die potentiellen Probleme zwar noch nicht äußerten, jedoch auch nicht ignoriert werden konnten (ebd., 179, Rn. 72). In der Folge bildeten sich drei Regelungsmodelle heraus, in denen diese Herausforderung auf ganz unterschiedliche

40 Parallel zu Europa war auch in den Vereinigten Staaten eine Debatte über die automatisierte Datenverarbeitung entbrannt (Ware 1973; Westin 1967). Anders als in Europa beschränkte sich die politische Diskussion allerdings auf mögliche negative Folgen einzelner Verarbeitungsbereiche bzw. insb. auf den Kreditsektor. In der Folge wurde nur wenige Tage nach dem Hessischen Landesdatenschutzgesetz der US Fair Credit Reporting Act am 26. Oktober 1970 verabschiedet (Simitis u. a. 2019, 159 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Weise adressiert wurde. Das deutsche BDSG und das österreichische DSG hatten die Etablierung einer allumfassenden Regelung zum Ziel, die detaillierte Vorgaben zur Erhebung und dem Verarbeitungsverlauf machte und versuchten, einen Kompromiss zwischen einer möglichst umfassenden und einer möglichst flexiblen Regelung dadurch zu erreichen, dass eine Vielzahl von Generalklauseln weite Spielräume für die Datenverarbeiter offenließ (ebd., Rn. 73). Das schwedische Datenschutzgesetz (in ähnlicher Weise auch das norwegische Datenschutzgesetz) machte hingegen keinerlei Prozessvorgaben und setzte stattdessen auf die Genehmigung einer jeden automatisierten Verarbeitung personenbezogener Daten durch eine Kontrollinstanz (ebd., Rn. 74). Die USA wiederum stellten zwar einige Vorgaben zum Ablauf des Verarbeitungsprozesses auf, verzichteten aber auf eine allgemeine Datenschutzregelung zugunsten eines bereichsspezifischen Ansatzes, bei dem nur jene Bereiche reguliert wurden, in denen negative Folgen der Datenverarbeitung vermutet wurden (ebd., 75).

Die sowohl grundrechtliche Bedeutung, die der Verarbeitung von (personenbezogenen) Daten zugeschrieben wurde, als auch die wirtschaftliche bzw. politische Bedeutung in Kombination mit der Verabschiedung voneinander divergierender nationaler Datenschutzgesetze veranlasste gleich zwei internationale Organisationen dazu, internationale Instrumente zum Zwecke der Harmonisierung der divergierenden nationalen Datenschutzgesetze zu erarbeiten. Das erste dieser Instrumente sind die 1980 verabschiedeten *OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten*. Das andere und weitaus wirkungsvollere Instrument ist das Anfang 1981 verabschiedete *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten* des Europarats, das besser unter dem Namen Datenschutz-Konvention Nr. 108 bekannt ist. Der folgende Unterabschnitt widmet sich der Entstehung und Aushandlung dieser beiden wegweisenden internationalen Datenschutz-Instrumente.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.1.1 OECD-Datenschutz-Richtlinien

Die *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung* bzw. OECD[41] ging aus der 1948 gegründeten *Organisation für europäische wirtschaftliche Zusammenarbeit* (OEEC - Organisation for European Economic Co-operation*)* hervor. Die OEEC diente der keynesianisch motivierten Verwaltung der im Rahmen des Marshallplans seitens der Vereinigten Staaten von Amerika gegenüber (west-)europäischen Staaten gewährten finanziellen Hilfen zum Zwecke des wirtschaftlichen Wiederaufbaus und der Zusammenarbeit in Europa nach Ende des Zweiten Weltkrieges (Woodward 2004, 114). Mit der Gründung der OECD im Jahre 1961 und der Überführung der OEEC in diese wurden die anfänglichen, stark am Wiederaufbau Europas orientierten politischen Ziele zunehmend in die Richtung allgemeiner marktwirtschaftlich motivierter wirtschaftspolitischer Kooperation der Mitgliedstaaten und des Abbaus von Handelshemmnissen geändert (ebd.).[42] Zur Erreichung ihrer Ziele kann die OECD auf verschiedene rechtliche Instrumente zurückgreifen. Zu unterscheiden ist vor allem zwischen rechtlich bindenden Instrumenten wie Entscheidungen oder internationalen Vereinbarungen und nicht-bindenden Instrumenten wie Empfehlungen und Deklarationen (OECD 2017).[43]

3.1.1.1 Erste Aktivitäten der OECD mit Datenschutzbezug

Der Beginn der Auseinandersetzung der OECD mit Fragen von Computer-Technologien lässt sich bis März 1968 zurückverfolgen, als auf einem Ministertreffen der OECD-Länder zum Thema Wissenschaft bestehende Technologiedifferenzen thematisiert wurden. Zur weiteren Untersuchung Computer-relevanter Themen richtete die OECD im Juni 1968 die sog. „Computer Utilisation Group" ein, die in den Folgejahren mehrere einschlägige Studi-

41 Ausnahmsweise wird hier auf die Verwendung der deutschen Abkürzung OWZE verzichtet, da sich auch im deutschen Sprachgebrauch die englische Abkürzung OECD (*Organisation for Economic Co-operation and Development*) weitgehend durchgesetzt hat.

42 Mit der Verallgemeinerung ihrer politischen Ziele ging auch eine gewisse Verbreiterung der mitgliedstaatlichen Basis einher: Italien (1962), Japan (1964), Finnland (1968), Australien (1971) und Neuseeland (1973) (Woodward 2004, 115).

43 Die überwiegende Mehrzahl der erlassenen Instrumente sind nicht-bindender Natur. Gemäß dem Stand des Jahres 2018 sind 25 Entscheidungen, 174 Empfehlungen und 27 Deklarationen in Kraft (OECD 2018).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

en zur Nutzung von Datenbanken und den damit zusammenhängenden Datenschutzproblemen veröffentlichte.[44] Weil sich durch die Studien die Einschätzung, dass Datenschutz ein wirtschaftlich und gesellschaftlich relevantes Thema sei, bestätigte, setzte die „Computer Utilisation Group" 1972 zwei neue Gremien zur weiteren Untersuchung ein: Das „Data Bank Panel" sowie das „Panel on Policy Issues of Computer/Communications Interaction". Ersteres veranstaltete im Juni 1974 das „OECD Seminar on Policy Issues in data protection and privacy", auf dem verschiedene Datenschutzthemen und darunter erstmals auch die Frage nach grenzüberschreitenden Datenströmen thematisiert wurden, dem späteren Kernanliegen der OECD Privacy Guidelines.[45] Das Seminar brachte etwa 100 bedeutsame Entscheidungsträger aus den verschiedenen OECD-Mitgliedstaaten für einen Wissens- und Meinungsaustausch zusammen. Bedeutung und Notwendigkeit dieses Erfahrungsaustauschs rührten auch daher, dass in der Zwischenzeit mehrere OECD-Mitgliedstaaten – neben dem Bundesland Hessen (1970) auch Schweden (1973) und die Vereinigten Staaten (1974) – Datenschutzgesetze erlassen hatten, deren Regulierungsmodelle sich stark voneinander unterschieden (Gassmann 2010, 2). Das besonders restriktive schwedische Modell sah zum Beispiel die Genehmigung seitens der Datenschutzaufsichtsbehörde für jede einzelne grenzüberschreitende Datenübertragung vor, damit die Gefahr der Übertragung von (personenbezogenen) Daten zum Zwecke der Umgehung nationaler Regulierungen an sog. Datenoasen (*data havens*) – Staaten mit weniger strengen Datenschutzregelungen – möglichst vermieden wird. Diese Befürchtung teilten im Grundsatz auch weitere europäische Staaten, die in den Folgejahren Datenschutzgesetze erließen (Kirby 1980, 3 f.).

Die OECD wiederum, deren primäres Ziel in der Förderung wirtschaftlichen Wachstums durch internationale Kooperation auf dem Gebiet der Wirtschaftspolitik liegt, sah in der Verabschiedung voneinander divergierender nationaler Datenschutzbestimmungen die Gefahr der Erschwerung grenzüberschreitender Datenflüsse und daraus resultierender volkswirtschaftlicher Wachstumseinbuße. Schließlich organisierte das Data Bank

44 Die beiden 1971 veröffentlichen Studien widmeten sich den Themen „Computerised data banks in public administration", „Digital information and the privacy problem" sowie „Policy Issues in Data Protection and Privacy". Eine dritte Studie „Computer and Communications" wurde 1973 veröffentlicht (Gassmann 2010, 1 f.).

45 Neben dem Thema der grenzüberschreitenden Datenströme widmeten sich zwei weitere Panels den Themen „The Personal Identifier and Privacy" bzw. „Right of Citizen Access to their File" (WPISP 2011, 9).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Panel im Jahr 1977 das „Symposium on Transborder Data Flows and the Protection of Privacy", das sich dann auch explizit der Frage grenzüberschreitender Datenflüsse widmete. Auf dieser Veranstaltung trafen etwa 300 Persönlichkeiten aus den OECD-Mitgliedstaaten, der Privatwirtschaft und aus inter-gouvernementalen Organisationen aufeinander. Ein Kommentar des damaligen Präsidenten der französischen Datenschutzaufsichtsbehörde *Commission nationale de l'informatique et des libertés* (CNIL), Louis Joinet, der später eine entscheidende Rolle bei der Erarbeitung der OECD Privacy Guidelines einnehmen sollte, machte in besonderem Maße den gesellschaftlichen und politischen Wert deutlich, der grenzüberschreitenden Datenflüssen zugesprochen wurde:

> *„Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows." (WPISP 2011, 10)*

3.1.1.2 Die politischen Auseinandersetzungen während der Erarbeitung der OECD-Richtlinien

Im Ergebnis des Symposiums wurde das Data Bank Panel aufgelöst und stattdessen Anfang 1978 die *OECD Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data*[46] ins Leben gerufen. Die Gruppe wurde mit der Erarbeitung von Richtlinien zum Umgang mit personenbezogenen Daten bei grenzüberschreitenden Datenströmen beauftragt. Zur Lektüre der Expertengruppe zählten Texte von Westin, dessen früherem Forschungsassistenten David Flaherty, sowie verschiedene weitere Studien (González Fuster 2014, 78). Zudem stand die Expertengruppe im Austausch mit dem Europarat, der sich ebenfalls seit geraumer Zeit mit Fragen des Schutzes personenbezo-

46 Den Vorsitz der Expertengruppe übernahm der Australier und damalige Vorsitzende der australischen Kommission für Rechtsreformen, die zu dem Zeitpunkt ein Bundesdatenschutzgesetz für Australien vorbereitete, Michael Kirby. Den Vize-Vorsitz hatte der seinerzeitige CNIL-Präsident Louis Joinet inne. Daneben waren Jan Freese (Leiter der schwedischen Datenschutzaufsichtsbehörde), Jon Bing (Leiter der norwegischen Datenschutzaufsichtsbehörde), Stefano Rodotà aus Italien, Spiros Simitis aus Deutschland sowie William Fishman (US-Handelsministerium) und Lucy Hummer (US-Außenministerium) Teil der Expertengruppe (Kirby 2011, 7 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gener Daten auseinandersetzte, sowie mit der Europäischen Kommission (Kirby 2011, 8).

Die Erarbeitung der Richtlinien gestaltete sich angesichts der Beteiligung zahlreicher Akteure aus europäischen Datenschutzaufsichtsbehörden und dem Feld der Menschenrechtspolitik als äußerst zäh. Der Grund dafür waren Meinungsverschiedenheiten zwischen europäischen und nicht-europäischen Vertretern. Während erstere Datenschutzregelungen als realen Schutz von Individuen unter Betonung der menschenrechtlichen Dimension und vor dem Hintergrund der zu diesem Zeitpunkt noch relativ frischen Erinnerungen an die durch den Missbrauch personenbezogener Daten ermöglichten Verbrechen des NS-Regimes befürworteten, sahen letztere datenschutzrechtliche Bestimmungen als Mittel für wirtschaftliche Zwecke. Die europäischen Vertreter waren mit dem Vorwurf konfrontiert, dass der europäische Ansatz zu bürokratisch sei, nicht ausreichend Rücksicht auf die wirtschaftlichen Erfordernisse grenzüberschreitender Datenflüsse nehme und möglicherweise auch protektionistisch motiviert sei, um europäischen Informationstechnologien einen künstlichen Vorteil gegenüber nicht-europäischen Wettbewerbern zu verschaffen. Die europäischen Vertreter sahen die Vorstellungen der nicht-europäischen Mitglieder hingegen als den Versuch der Erzielung einer Einigung zugunsten vereinfachter Datenverarbeitungen an, ohne dass zugleich praktische Verbesserungen auf dem Gebiet des Schutzes personenbezogener Daten erreicht würden (Kirby 2011, 4). So forderten die europäischen Vertreter eine Orientierung an der Sprache des Europarats, der zu diesem Zeitpunkt bereits zwei Europaratsempfehlungen ausgesprochen hatte (vgl. auch 3.1.2) und die darin befürworteten Datenschutzmaßnahmen ausschließlich auf den Schutz von Menschen bezog.

Nach langwierigen Debatten konnten sich schließlich die nicht-europäischen Vertreter mit ihren Forderungen weitgehend durchsetzen, sodass die Empfehlungen der Expertengruppe vorsahen, eine Balance zwischen den miteinander konkurrierenden Werten individueller Privatheit einerseits und dem Informationsbedarf einer informationsabhängigen Gesellschaft andererseits zu erzielen (González Fuster 2014, 78). Die Hoffnung der US-Delegation bestand darin, dass die Festlegung gemeinsamer Datenschutzstandards die OECD-Mitgliedstaaten dazu veranlassen würde, datenprotektionistische Maßnahmen zurückzufahren und dadurch grenzüberschreitende Datenflüsse zu erleichtern (WPISP 2011, 10). Allerdings war bereits der Versuch, eine Balance zu erzielen, hoch problematisch, wie die folgende

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Abwägung unterstreichen soll: Wie viel Datenschutz darf zugunsten möglichst freier grenzüberschreitender Datenflüsse geopfert werden, sofern eine Diskrepanz im Datenschutzniveau der OECD-Mitgliedstaaten festzustellen ist?[47] Da allerdings beide Seiten tendenziell unzufrieden mit dem politischen Ergebnis waren, lief die Wahl des Instruments letztlich auf nicht-bindende OECD-Empfehlungen hinaus (Kirby 2011, 4). Die *OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten* wurden schließlich am 23. September 1980 vom obersten Rat der OECD in Form von OECD-Empfehlungen angenommen (OECD 1980b).

3.1.1.3 Inhalt der OECD-Richtlinien

Die Richtlinien sind in fünf Teile unterteilt, die sich je unterschiedlichen Aspekten widmen. Teil 1 „Allgemeines" beinhaltet Begriffsbestimmungen und den Anwendungsbereich der Richtlinien. So werden unter Nr. 1 „alle Informationen, die sich auf eine bestimmte oder bestimmbare Person […] beziehen", als personenbezogene Daten definiert und Nr. 2 sieht vor, dass die Richtlinien öffentliche wie nicht-öffentliche Stellen gleichermaßen einbeziehen. Zudem machen die OECD-Richtlinien keinen Unterschied zwischen automatisierter und manueller Verarbeitung personenbezogener Daten. Teil 2 widmet sich den Grundprinzipien der innerstaatlichen Anwendung. Darunter fallen die Verpflichtung zur Rechtmäßigkeit bei der Erhebung personenbezogener Daten ggf. mit Wissen bzw. Einwilligung des Betroffenen (Nr. 7), Vorgaben zur Zweckbindung (Nr. 8–10), zu Sicherheitsmaßnahmen (Nr. 11), Transparenzvorgaben (Nr. 12) Vorgaben zu Auskunftsrechten des Betroffenen (Nr. 13) sowie die Rechenschaftspflicht des Verantwortlichen zur Einhaltung der genannten Vorgaben (Nr. 14). Die Teile 3 und 4 widmen sich schließlich der Gewährleistung möglichst ungehinderter grenzüberschreitender Datenflüsse, indem Vorgaben zum freien Datenverkehr und zu legitimen Beschränkungen in den Nrn. 15–18 sowie zu internationaler Kooperation und Interoperabilität in den Nrn. 20–22 gemacht werden. Erwähnenswert ist zudem noch, dass die Vorgaben zur Umsetzung in nationales Recht in Teil 4 (Nr. 19) Maßnahmen zum Schutz

47 Diesem Problem wird sich auch in der Begründung der OECD-Richtlinien gewidmet, dort heißt es: „[…] There is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth." (OECD 1980a Explanatory Memorandum, Nr. 19 h)).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

personenbezogener Daten auf Grundlage von Selbstregulierung, wie z. B. Verhaltenskodizes (Nr. 19 b.) auf dieselbe Stufe setzen wie gesetzliche Regelungen zum Schutz personenbezogener Daten (Nr. 19 a.) (ebd.).

3.1.1.4 Zwischenfazit und Bewertung

Da die Entscheidungen der OECD im Konsens getroffen werden, können die Ergebnisse in Form der OECD-Richtlinien als der größte gemeinsame Nenner zwischen allen beteiligten Mitgliedstaaten im Hinblick auf den Umgang mit der Materie des Schutzes personenbezogener Daten und grenzüberschreitenden Datentransfers interpretiert werden. Letztlich überbewertete die in den OECD-Richtlinien angestrebte Balance jedoch dem institutionellen Selbstinteresse der OECD entsprechend die Bedeutung der volkswirtschaftlichen Folgen reglementierter Datentransfers, während die Gewährleistung eines hohen Datenschutzniveaus nur so lange befürwortet wurde, wie dieser zu keiner Beschränkung des grenzüberschreitenden Transfers personenbezogener Daten führen würde. Entsprechend gering war letztlich der Einfluss der Richtlinien auf die nationalen Gesetzgebungen. Eine gewisse Harmonisierungswirkung konnten die Richtlinien allerdings trotz ihrer Unverbindlichkeit entfalten, sowohl was nationale Datenschutzgesetze (Schiedermair 2012, 150 f.), als auch weitere internationale Harmonisierungsbestrebungen angeht (Schiedermair 2012, 152 ff. WPISP 2011, 12–15). Zudem sind die in den OECD-Richtlinien vorgesehen Verarbeitungsgrundsätze – allerdings mit teils erheblichen Erweiterungen – noch heute Bestandteil vieler nationaler Datenschutzgesetze und insb. sowohl der DS-RL als auch der DSGVO.

Im Rückblick auf die Erarbeitung der OECD-Richtlinien kann festgehalten werden, dass bereits zu diesem vergleichsweise frühen Zeitpunkt zentrale Konfliktlinien der Datenschutzpolitik offen zu Tage traten, die bis hin zu den Verhandlungen zur Datenschutz-Grundverordnung auch weiterhin prägend für die Datenschutzdebatten sein sollten. Hierzu zählt insbesondere der Konflikt zwischen einer Grundrechtsorientierung einerseits und einer wirtschaftlichen Orientierung von Regelungen zum Schutz personenbezogener Daten andererseits. Der Kern dieses Spannungsfelds entfaltet sich entlang der Frage, wie die Balance im Detail auszusehen hat. Die OECD-Richtlinien versuchen, ein Mindestmaß an Ordnung in die internationale Verarbeitung personenbezogener Daten hineinzubringen, indem die Einschränkung grenzüberschreitender Datentransfers dann in Kauf genommen wird, wenn ein anderer Mitgliedstaat wesentliche Teile der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

OECD-Richtlinien nicht einhält oder lediglich als Transit-Staat zur Umgehung von Datenschutzbestimmungen im eigenen Land fungiert (OECD 1980b Teil 3, Nr. 17). Problematisch dabei ist aber zugleich, dass die OECD-Richtlinien aufgrund ihres unverbindlichen Charakters und ihrer Vermeidung der Festlegung auf gesetzliche Vorgaben ohnehin nur bedingt wirksam sein konnten im Hinblick auf die Harmonisierung von nationalen Datenschutzregelungen. Letztlich zeigte sich anhand der Umsetzung der OECD-Richtlinien erstmals, wie der Versuch eine den Datenschutz wahrende Balance zwischen Datenschutz- und Wirtschaftsinteressen auf Basis von Selbstregulierung zu erzielen scheiterte. In den späten 1980er-Jahren wurde zunehmend klar, dass die OECD-Richtlinien eher national divergierenden und inhaltlich unzureichenden Selbstregulierungspraktiken zuträglich waren statt der Harmonisierung eines effektiven Schutzniveaus bzw. -regimes (C. J. Bennett und Raab 2006, 87 ff.).

3.1.2 Datenschutz-Konvention des Europarats

Der Europarat wurde mit der Unterzeichnung des Londoner Vertrags durch zehn westeuropäische Staaten[48] am 5. Mai 1949 ins Leben gerufen. Damit ist der Europarat die älteste europäische internationale Organisation. Wie die Gründung der OECD (3.1.1) und der Vorgänger-Organisationen der EU (3.2.1), ist auch die Entstehung des Europarats im zeithistorischen Kontext des zweiten Weltkrieges zu verstehen. Entscheidend waren dabei einerseits das politische Leitmotiv des *„Nie wieder"* und andererseits die Einschätzung der Sowjetunion als eine gegen Europa gerichtete militärische und gesellschaftspolitisch-ideologische Bedrohung, der entgegengetreten werden müsse. Mit der Gründung des Europarats sollte der Friede in Europa gewahrt werden, indem die Mitgliedstaaten durch politische Kooperation enger zusammenrücken. Jene Europaratsbefürworter (darunter insb. die Benelux-Länder und Frankreich), die für eine supranationale Organisationsform und damit für die Abtretung nationalstaatlicher Kompetenzen an eine übergeordnete Instanz eintraten, konnten sich allerdings gegenüber den Befürwortern eines Organisationsmodells auf Basis zwischenstaatlicher Kooperation (darunter insb. Großbritannien) nicht durchsetzen (Brummer

48 Neben den fünf Mitgliedern des Brüsseler Pakts (Frankreich, Großbritannien, Belgien, Luxemburg und die Niederlande) waren dies Dänemark, Norwegen, Schweden, Irland und Italien (Brummer 2008, 23).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

2008, 21–23). Der Wunsch, den Europarat in Gestalt einer supranational verfassten Europäischen Union zu errichten, scheiterte also schon vor ihrer Gründung. Am Ende blieb ein politischer Kompromiss, den insbesondere die institutionelle Struktur der Organisation wiederspiegelt: Tonangebend sind die Regierungen der Mitgliedstaaten im Ministerkomitee (ebd., 33 ff.), während die Parlamentarische Versammlung vorrangig beratende Tätigkeiten wahrnimmt (ebd., 93 ff).

Anfangs noch vor dem Hintergrund des Ost-West-Konflikts deutlich schwächer ausgeprägt, war der Europarat vor allem seit den 1960er-Jahren darum bemüht, sich als möglichst offene Organisation zu verstehen, indem sie allen Staaten, die ihr noch nicht beitreten konnten oder wollten, die Möglichkeit des Beitritts niedrigschwellig offenhielt, sofern die Wertretrias des Europarats bestehend aus Demokratie, Menschenrechten und Rechtsstaatlichkeit grundsätzlich eingehalten wurde (Brummer 2008, 17). So zählte der Europarat Ende der 1970er-Jahre bereits 22 Mitgliedstaaten und umfasst heute nach mehreren größeren Erweiterungsrunden die mit dem Beitritt Montenegros 2007 ihr vorläufiges Ende fanden, mit 47 Mitgliedstaaten nunmehr beinahe alle europäischen Staaten (ebd., 28 f.). Zwar ging mit diesem enormen Mitgliederzuwachs auch eine Steigerung des Handlungsspielraums einher, doch leidet der Europarat seit einigen Jahrzehnten unter der Aufweichung seiner zentralen Prinzipien der Demokratie, Menschenrechte und Rechtsstaatlichkeit, da mehrere Mitgliedstaaten diese untergraben, während sie zugleich kaum nennenswerte Folgen zu befürchten haben (ebd., 31 f.).[49]

Zur Erfüllung seiner Aufgaben kann der Europarat auf verschiedene Instrumente zurückgreifen. Relevant für die Aktivitäten des Europarats auf dem Feld der Datenschutzpolitik sind vor allem zwei Instrumente: Konventionen und Empfehlungen. Sowohl die Ausarbeitung einer Konvention als auch ihre Annahme erfolgen seitens des Ministerkomitees. Damit Konventionen Bindungswirkung entfalten können, müssen Staaten der Konvention zunächst beitreten, d. h. diese ratifizieren (ebd., 62 ff.). Empfehlungen entfalten im Gegensatz zu Konventionen keine Bindungswirkung gegenüber den Mitgliedstaaten. Sie dienen vielmehr dem Versuch der allgemeinen Orientierung der Mitgliedstaaten auf neuen oder strittigen thematischen Feldern (Brummer 2008, 66).

Bereits achtzehn Monate nach Gründung des Europarats wurde am 4. November 1950 das wohl bekannteste Dokument des Europarats, die Eu-

49 Vgl. z. B. den Umgang mit den russischen Menschenrechtsverletzungen (Ackeret 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ropäische Menschenrechtskonvention (EMRK), zur Zeichnung aufgelegt. Nach dem Erreichen der erforderlichen Zahl von zehn Staaten, die das Dokument ratifiziert hatten, trat die EMRK schließlich am 3. September 1953 in Kraft (143 f.). Die EMRK orientiert sich inhaltlich und terminologisch klar an der *Allgemeinen Erklärung der Menschenrechte* (AEMR) der Vereinten Nationen vom Dezember 1948. Zum einen wird in der EMRK der universelle Charakter der Menschenrechte, wie er in der AEMR festgeschrieben wurde, nachdrücklich unterstützt. Zum anderen aber bildet die EMRK den Versuch, „die ersten Schritte auf dem Weg zu einer kollektiven Garantie bestimmter in der Allgemeinen Erklärung aufgeführter Rechte zu unternehmen." (Europarat 2010 Präambel) Die Durchsetzbarkeit der in der EMRK dargelegten Menschenrechte wurde insbesondere über die Einführung des Individualbeschwerdeverfahrens möglich, mit der Einzelpersonen erstmals Rechte nach internationalem Recht erhielten, die unabhängig von den Rechten ihrer Heimatstaaten existierten. Den bedeutendsten Baustein des EMRK-Kontrollmechanismus bildet daher auch der Europäische Gerichtshof für Menschenrechte (EGMR), der seine Arbeit Anfang 1959 aufnahm (Brummer 2008, 143 ff.).

3.1.2.1 Erste Aktivitäten des Europarats mit Privatheits- und Datenschutzbezug

Datenschutz und Privatheit waren in den ersten Jahrzehnten seines Bestehens zunächst noch kein Thema für den Europarat (González Fuster 2014, 82). Dies änderte sich 1967. Auf einer Sitzung der Beratenden Versammlung des Europarats[50] wurde Art. 8 EMRK[51] dahingehend uminterpretiert, dass fortan nicht mehr nur das Privatleben (im Sinne räumlicher, häuslicher Privatheit)[52], sondern Privatheit im Allgemeinen als von dem Artikel umfasst verstanden wurde. Diese Neubestimmung des Begriffs fand im Kontext von Debatten über die Auswirkungen wissenschaftlicher und tech-

50 Die „Beratende Versammlung" wurde 1974 in „Parlamentarische Versammlung" umbenannt (Brummer 2008, 93).

51 „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz." (Europarat 2010 Art. 8 (1)).

52 An dieser Stelle sei auf Fusters Analyse der Sprachverwendung in AEMR und EMRK verwiesen. Dabei wird deutlich, dass der in der englischen Originalfassung der AEMR verwendete Term „privacy" kurz vor der Finalisierung der EMRK durch „private life" ersetzt wurde, aber in Anlehnung an das „vie priveé" im Französischen doch dasselbe meint (González Fuster 2014, 81 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nologischer Entwicklungen auf den Schutz der Menschenrechte, statt. Im Anschluss beauftragte die Beratende Versammlung ihren Rechtsausschuss mit der Erstellung von zwei Anträgen: Einer Resolution zum Thema der Menschenrechte und moderner wissenschaftlicher Entwicklungen im Allgemeinen und einer weiteren Resolution, die sich mit der Problematik technischer Vorrichtungen zum Zwecke des Eindringens in und Abhörens von privaten Räumen auseinandersetzen und Regulierungsmöglichkeiten unterbreiten sollte (ebd., 83). Die vom Rechtsausschuss erarbeitete Antwort führte zu weiteren Diskussionen in der Beratenden Versammlung darüber, ob und inwiefern Art. 8 EMRK aber auch das nationale Recht der Mitgliedstaaten des Europarats dafür geeignet seien, den Schutz von Privatheit angesichts neuartiger wissenschaftlich und technologisch bedingter Risikoszenarien zu gewährleisten (ebd.).[53] Im Ergebnis dieser Debatten hielt die Beratende Versammlung im Rahmen der Empfehlung 509 (1968) fest, „that newly developed techniques […] are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights" (Parliamentary Assembly of the CoE 1968 Paragraph 3). Die Beratende Versammlung rief das Ministerkomitee schließlich dazu auf, das Expertenkomitee für Menschenrechte mit der Frage zu befassen, ob die mitgliedstaatliche Rechtslage einen ausreichenden Schutz vor Verletzungen des Rechts auf Privatheit bietet, die durch den Einsatz moderner wissenschaftlicher und technologischer Mittel entstehen können (ebd., Paragraph 8). Die Ministerkonferenz entsprach der Empfehlung der Beratenden Versammlung und beauftragte das Expertenkomitee mit der Erarbeitung einer Studie. In dieser 1970 fertiggestellten Studie wurde schließlich, entgegen den Erwartungen der Beratenden Versammlung, festgestellt, dass die in der Empfehlung genannten Risikogründe (das Abhören von Telefonen bzw. Abhöraktivitäten im Allgemeinen, versteckte Überwachung usw.) ausreichend unter Kontrolle seien. Allerdings wies das Expertenkomitee darauf hin, dass die Verbreitung von Rechnern ein Problem für die Privatheit darstelle, das womöglich nicht ausreichend von Art. 8 EMRK abgedeckt sei, da die Vorgaben des Art. 8 lediglich auf den öffentlichen aber nicht auch auf den nicht-öffentlichen Bereich anwendbar seien. Ein weiteres Unterkomitee, das sich ab 1971 mit derselben Materie auseinandersetze, grenzte das Problem schließlich auf

53 Der österreichische Wortführer des Rechtsausschusses (aber auch die übrigen Mitglieder) waren laut Fuster (2014, 83) besonders mit der Arbeit von Alan Westin vertraut.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Nutzung elektronischer Datenbanken ein, sodass im Jahr 1973 zunächst die Empfehlung (73) 22 (Council of Europe 1973) und ein Jahr später die Empfehlung (74) 29 (Council of Europe 1974) durch den Europarat angenommen wurde. Ausgehend von der Auffassung, „the right to privacy, which is, by its very nature a matter belonging to the European public order" (Council of Europe 1974 Explanatory Report, Nr. 8), wurde mit ihnen das Ziel verfolgt, bis zur möglichen Ausarbeitung eines international verbindlichen Dokuments der Entstehung weiterer Divergenzen auf dem Gebiet nationaler Datenschutzregelungen entgegenzuwirken (Council of Europe 1973). In der Begründung der Empfehlung (73) 22 wurde ausgehend von der Feststellung, dass Art. 8 EMRK keinen ausreichenden Schutz der informationellen Privatheit („data privacy") vor technologisch bedingten Beeinträchtigungen biete, betont, dass der Privatsektor besonderen Anlass zur Sorge schaffe, weil dieser im Gegensatz zum öffentlichen Bereich einen eindeutig grenzüberschreitenden Fokus mit sich bringe und das Fehlen von Schutzregelungen in vielen Mitgliedstaaten die Position der Individuen schwäche (Council of Europe 1973 Explanatory Report, § 6). Inhaltlich orientierten sich die Empfehlungen an den miteinander übereinstimmenden Elementen bestehender nationaler Datenschutzgesetze, wie sich an den vorgeschlagenen Prinzipien zeigt: Vorgaben zur Rechtmäßigkeit bei der Erhebung (Nr. 1, 3)[54] und Verwendung (Nr. 9) personenbezogener Daten, Vorgaben zur Zweckbindung (Nr. 2, 5), Speicherfristen (Nr. 4), Transparenzvorgaben (Nr. 6), Datenqualität (Nr. 7), Sicherheits- (Nr. 8), Anonymisierungs- und Pseudonymisierungsmaßnahmen (Nr. 10).

3.1.2.2 Die Erarbeitung der Datenschutz-Konvention Nr. 108

Nach Verabschiedung der beiden Empfehlungen setzte der Europarat seine Tätigkeiten auf dem Gebiet des Datenschutzes fort, indem deren Implementierung in den Europaratsmitgliedstaaten im Hinblick auf die weitere Entwicklung der Divergenz nationaler Datenschutz-Bestimmungen verfolgt wurde. Zu diesem Zweck wurde im Jahr 1975 vom Sekretariat des Europarats eine Studie erarbeitet. In dieser wurde festgestellt, dass zwischen den

54 Da die Prinzipien beider Empfehlungen weitgehend übereinstimmend sind, beziehen sich die genannten Ziffern auf Empfehlung (73) 22. Erwähnenswert ist, dass Empfehlung (74) 29 zusätzlich (nationale) Ausnahmen von der Zweckbindung und bei den Speicherfristen für statistische, wissenschaftliche oder historische Zwecke unter Einhaltung von Garantien vorsieht (Nr. 4).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutzgesetzen der Mitgliedstaaten sowohl wesentliche Gemeinsamkeiten als auch entscheidende Diskrepanzen vorhanden waren (González Fuster 2014, 86). Die anhaltenden Diskrepanzen wurden 1976 schließlich seitens des Ministerkomitees zum Anlass für die Einrichtung eines Expertenkomitees[55] genommen, das mit der Erarbeitung einer Europaratskonvention *zum Schutze der Privatheit bei der Datenverarbeitung im Ausland und bei der grenzüberschreitenden Datenverarbeitung*[56] beauftragt wurde (Council of Europe 1981 Nr. 13).

Der Europarat war spätestens seit diesem Zeitpunkt an einer möglichst breiten Wirkung der auszuarbeitenden Europaratskonvention interessiert. So hatte bereits die erste Sitzung des Expertenkomitees einen Briefwechsel mit der OECD zur Folge, in dessen Rahmen sich die beiden Institutionen Zusammenarbeit und gegenseitige Unterstützung zusicherten. Einig waren sich beide Institutionen insbesondere dahingehend, dass eine künftige Europaratskonvention den von der OECD unterstützten Grundsatz des freien grenzüberschreitenden Informationsflusses respektieren und keine Hindernisse für den internationalen Handel mit personenbezogenen Daten errichten sollte (Council of Europe 1981 Nr. 14; González Fuster 2014, 87). Außerdem nahmen an den Sitzungen des Expertenkomitees Vertreter sowohl der OECD und vier ihrer nichteuropäischen Mitgliedstaaten (Australien, Kanada, Japan und die Vereinigten Staaten) als auch der Europäischen Kommission und damit der Europäischen Gemeinschaften teil. Im Laufe der Beratungen intensivierte sich die Kooperation zwischen dem Europarat und den Europäischen Gemeinschaften noch weiter. Während die Europäische Kommission sich jedoch später dazu entschied, das Ergebnis

55 Das *Commitee of Experts on Data Protection* war zwischen November 1976 und May 1979 tätig und wurde 1978 in *Project Group on Data Protection* (CJ-PD) umbenannt. Institutionell war es dem *Ausschuss für rechtliche Zusammenarbeit* (CDCJ – European Committee on Legal Co-operation) untergeordnet. Seit Ende 1974 war im Europarat zudem die Vorstellung vorherrschend geworden, dass sich in der Zwischenzeit die Verwendung des Begriffspaars „Data Protection" für die mit dem Schutz informationeller Privatheit bzw. dem Schutz personenbezogener Daten zusammenhängenden Problemstellungen in Europa durchgesetzt habe, sodass der Europarat eine allmähliche Umstellung des Europaratsvokabulars von *privacy* auf *data protection* vollzog (González Fuster 2014, 86 f.). Gemäß Frits W. Hondius (1975, 4), einem der wesentlichen Verantwortlichen bei der Erarbeitung der Datenschutz-Konvention, wurden Datenschutzrechte als ein Aspekt von Privatheit verstanden, nämlich der informationellen Privatheit.

56 Eigene Übersetzung. Im Original: „to prepare a convention for the protection of privacy in relation to data processing abroad and transfrontier data processing" (Council of Europe 1981 Nr. 13).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Europaratsaktivitäten auf dem Felde der Harmonisierung nationaler Datenschutzbestimmungen abzuwarten, hielt das Europäische Parlament (EP) an der Erarbeitung von Gemeinschaftsregelungen zum Datenschutz in der EG fest (vgl. auch 3.2.2.1). In einem Brief an den Generalsekretär des Europarats signalisierte der Generalsekretär des Europäischen Parlaments allerdings auch das Interesse des Parlaments an den Arbeiten des Europarats. So wurde in der ebenfalls mitversendeten EP-Resolution aus dem Jahre 1979 nicht nur der Erlass eigener Gemeinschaftsstandards, sondern auch der Beitritt der EG zur Europaratskonvention gefordert (González Fuster 2014, 87). Die parlamentarische Versammlung des Europarats nahm Anfang 1980 zur Haltung des EP Stellung und lud dieses mittels einer Europaratsempfehlung dazu ein, die Harmonisierung mitgliedstaatlicher Datenschutzbestimmungen bzw. den Erlass harmonisierter Datenschutzbestimmungen entlang der – sich kurz vor ihrer Finalisierung befindenden – Europaratskonvention zu unterstützen (Parliamentary Assembly of the CoE 1980 Nr. 10). Eine möglichst breite Wirkung der Europaratskonvention sollte zudem auch dadurch erzielt werden, dass beschlossen wurde, dass auch nichteuropäische Staaten ihr beitreten können sollten. Dass die Datenschutz-Konvention nicht als Europaratskonvention, sondern schlicht als Konvention benannt wurde, spiegelt diesen Anspruch wider (Council of Europe 1981 Nr. 24).

Nachdem das zuständige Expertenkomitee 1979 eine erste Fassung der Datenschutz-Konvention vorbereitet hatte, wurde diese zunächst im Rahmen eines weiteren Expertenkomitees im April 1980 überarbeitet, finalisiert und schließlich am 17. September 1980 seitens des Ministerkomitees angenommen, aber erst am 28. Januar 1981 zur Unterzeichnung aufgelegt (Council of Europe 1981 Nr. 17; González Fuster 2014, 88).[57]

3.1.2.3 Inhalt der Datenschutz-Konvention 108

Im Gegensatz zu den OECD-Richtlinien, die zwei einander widerstrebende Ziele zu vereinen suchten, verfolgte die Datenschutz-Konvention des Europarats vielmehr das Ziel, „im Hoheitsgebiet jeder Vertragspartei für

57 Die Erstunterzeichner-Staaten sind: Dänemark, Deutschland, Frankreich, Luxemburg, Österreich, Schweden und die Türkei. Die Ratifizierung seitens einiger dieser Staaten erfolgte allerdings mit – teils erheblicher – Verzögerung. Im Extremfall der Türkei lagen 35 Jahre zwischen Unterzeichnung und Ratifizierung (Council of Europe 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden (‚Datenschutz')" (Europarat 1981). Zwar sah auch die Europaratskonvention vor, dass *der bloße Hinweis* (Simitis u. a. 2019, 186, Rn. 103) auf den Schutz der Persönlichkeit des Betroffenen nicht dazu legitimiert, grenzüberschreitende Datenflüsse zu verbieten oder von einer besonderen Genehmigung abhängig zu machen (Europarat 1981, Art. 12 Abs. 2). Dennoch wurde nicht der ungehinderte Fluss von Informationen als Angelpunkt der Materie festgelegt: „Erst die Existenz einer von allen Vertragsstaaten akzeptierten Mindestregelung ebnet vielmehr den Weg zu einem grenzüberschreitenden Transfer der Daten" (Simitis u. a. 2019, 186, Rn. 103). Simitis zufolge ist Art. 12 Abs. 2 der Datenschutz-Konvention vielmehr als Kompromiss zu deuten, den der Europarat, insb. gegenüber den Nicht-Mitgliedstaaten, eingehen musste, um den erfolgreichen Abschluss der Konvention nicht zu gefährden (Simitis 2001, 102 f.).

Gonzáles-Fuster (2014, 89 f.) weist zudem darauf hin, dass eine herausragende Besonderheit der Datenschutz-Konvention ihre Verknüpfung der Forderung nach möglichst freien, grenzüberschreitenden Datenflüssen mit der Freiheit der Meinungsäußerung ist. Dazu verband die Präambel der Datenschutz-Konvention den „freien Informationsaustausch […] zwischen den Völkern" mit der Forderung nach „Informationsfreiheit ohne Rücksicht auf Staatsgrenzen" (Europarat 1981). Im erläuternden Bericht[58] zur Datenschutz-Konvention wurden die Vorgaben aus Art. 12 der Datenschutz-Konvention zum grenzüberschreitenden Verkehr personenbezogener Daten schließlich eindeutig in Bezug zu Art. 10 EMRK[59] gesetzt. Entsprechend wird konstatiert, dass der freie grenzüberschreitende Verkehr von Informationen nicht allein für Staaten von Bedeutung ist, sondern auch für Individuen (Council of Europe 1981 Nr. 9). Die von der OECD und insbesondere von ihren nichteuropäischen Mitgliedern vorgebrachte wirtschaftspolitisch motivierte Forderung nach möglichst freien grenzüberschreitenden Datenflüssen zur Vermeidung von Handelshemmnissen wird also in der Datenschutz-Konvention um eine menschenrechtspolitische Dimension ergänzt.

58 Vergleichbar einer Gesetzesbegründung, Erwägungsgründen, etc.

59 In diesem heißt es: „Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben." (Europarat 2010)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Davon abgesehen umfasst der Anwendungsbereich der Konvention ebenso wie die OECD-Richtlinien sowohl den öffentlichen als auch den nicht-öffentlichen Bereich, beschränkt sich aber im Gegensatz zu den OECD-Richtlinien nicht auf die automatisierte Verarbeitung personenbezogener Daten.[60] Die Definition personenbezogener Daten umfasst „jede Information über eine bestimmte oder bestimmbare natürliche Person" (Art. 2 a).[61] Art. 5 legt schließlich die Grundsätze dar, die den *harten* Kern des Datenschutzes ausmachen und die bis heute weitgehend intakt geblieben sind: Personenbezogene Daten müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden (Art. 5 a); sie dürfen nur für festgelegte und rechtmäßige Zwecke verarbeitet werden (Art. 5 b); sie müssen für den jeweiligen Verarbeitungszweck relevant und vom Umfang her angemessen sein (Art. 5 c); sie müssen sachlich richtig und auf dem neuesten Stand sein (Art. 5 d) und so aufbewahrt werden, dass ein Betroffener lediglich innerhalb der für den jeweiligen Zweck erforderlichen Verarbeitungszeit identifiziert werden kann (Art. 5 e).

Die Datenschutz-Konvention enthält in Art. 6 zudem Vorgaben zur Verarbeitung besonderer Arten personenbezogener Daten. Aufgelistet werden solche zur rassischen Herkunft, zu politischen, religiösen oder anderen Überzeugungen sowie Angaben zur Gesundheit, zum Sexualleben und zu Vorstrafen.[62]

Art. 8 schreibt schließlich die Betroffenenrechte fest. So müssen Betroffene im Rahmen ihres Auskunftsrechts die Möglichkeit haben, beim Verantwortlichen Informationen über die verwendeten personenbezogenen Daten, die Verarbeitungszwecke, aber auch über den gewöhnlichen Aufent-

60 Den Vertragsstaaten steht es allerdings gemäß Art. 3 Abs. 2 lit. c frei, darüber zu entscheiden, den Anwendungsbereich auf die manuelle Verarbeitung personenbezogener Daten auszudehnen.

61 Auch in diesem Bereich räumt die Konvention den Vertragsstaaten die Möglichkeit ein, den Anwendungsbereich auch auf Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stellen mit oder ohne juristische Persönlichkeit auszudehnen (Art. 3 Abs. 2 lit. b).

62 Im erläuternden Bericht wurde allerdings unter Verweis auf die Bedeutung des Kontexts bei der Datenverarbeitung versucht klarzustellen, dass die Auflistung in der Konvention lediglich eine Orientierung zu bieten vermöge, Ergänzungen und Spezifizierungen im nationalen Recht also notwendig sein würden: "The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views." (Council of Europe 1981 Nr. 48)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

haltsort oder den Sitz des Verantwortlichen zu erhalten (Art. 8 a). Art. 8 b schreibt zudem vor, dass diese Mitteilung in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten sowie in verständlicher Form zu erfolgen hat. Art. 8 c schreibt die Rechte auf Berichtigung und Löschung fest und Art. 8 d sieht die Bereitstellung von Rechtsmitteln im nationalen Recht zum Zwecke der Durchsetzung der Betroffenenrechte vor.

Ein bedeutender Unterschied zu den OECD-Richtlinien liegt in Art. 10 vor, der die Schaffung von Sanktionsstrukturen und Rechtsmitteln im nationalen Recht für Verletzungen der Vorgaben der Datenschutz-Konvention vorsieht.

Zum Zwecke der verbesserten Anwendung der Konvention wurde sowohl die gegenseitige Unterstützung der Vertragsstaaten (Art. 13) als auch die Einrichtung eines Beratenden Ausschusses (Art. 18–20) vorgesehen. Der Ausschuss konnte unter anderem Änderungen vorschlagen und somit die Weiterentwicklung des Instruments sicherstellen.[63]

3.1.2.4 Zwischenfazit / Bewertung

Die Datenschutz-Konvention trat, nachdem sie durch fünf Mitgliedstaaten (Deutschland, Frankreich, Norwegen, Schweden, Spanien) ratifiziert wurde, am 1. November 1985 in Kraft. Stand Anfang 2019 wurde die Datenschutz-Konvention von insgesamt 54 Staaten, darunter 7 Nicht-Mitgliedstaaten, ratifiziert (Council of Europe 2019). Damit ist sie das erste und bis heute einzige verbindliche internationale Datenschutz-Instrument (P. de Hert und Papakonstantinou 2014, 635). Gegenüber den OECD-Richtlinien unterscheidet die Datenschutz-Konvention außerdem noch die vergleichsweise klare Adressierung von Datenschutz als zentralem Ziel und die Bevorzugung staatlicher Regulierung anstelle von Selbstregulierung zur Erreichung dieses Ziels. Viele der nach der Annahme der Datenschutz-Konvention erlassenen nationalen Datenschutzgesetze wurden von dieser geprägt. Die in der Konvention dargelegten Datenschutz-Grundsätze fungierten als Grundlage jeder weiteren europäischen Regelung auf dem Gebiet des Datenschutzrechts (Zerdick 1995, 81) bzw. als Grundlage auch im Hinblick

63 Aufgrund von mitgliedstaatlichen Meinungsverschiedenheiten enthält die Konvention keine Vorgaben zur Einrichtung unabhängiger Aufsichtsinstanzen (Simitis u. a. 2019, 186, Rn. 101).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auf die Überarbeitung der bestehenden nationalen Regelungen (González Fuster 2014, 93).[64]

Trotz dieser Vorzüge verfehlte die Konvention letzten Endes das Ziel der Schaffung eines ausreichend harmonisierten Datenschutzniveaus. Dies lag einerseits daran, dass die in den Artikeln 13 und 18–20 vorgesehen Maßnahmen bzw. der Beratende Ausschuss nur bedingt dazu geeignet waren, die einheitliche Anwendung der Konvention sicherzustellen. Während die Erarbeitung der Konvention noch seitens unabhängiger Sachverständiger erfolgte, gingen die Regierungen der Vertragsstaaten nach dem Beitritt zur Konvention dazu über, den Beratenden Ausschuss mit Regierungsvertretern zu besetzen, sodass die Chancen einer möglichst unabhängigen und wissenschaftlichen Beurteilung der Anwendung der Konvention verloren gingen, weil keine ernsthaften Änderungsvorschläge gemacht wurden (Simitis u. a. 2019, 187 f., Rn. 110). Schließlich verfehlte die Konvention das Harmonisierungsziel insbesondere in Bezug auf den Anwendungsbereich (Einbezug manueller Verarbeitung vs. ausschließlicher Einbezug automatisierter Verarbeitungen sowie Einbezug juristischer Personen vs. ausschließlicher Einbezug natürlicher Personen) sowie die konkrete Ausgestaltung der Verarbeitungsvoraussetzungen (Ausgestaltung der Auskunftsrechte bzw. genereller Verarbeitungstransparenz und die Verarbeitung besonderer Arten personenbezogener Daten) (Commission of the European Communities 1990, 2 f.).

Die Europäische Kommission, die bereits seit Jahren als Beobachterin an der Erarbeitung der Konvention beteiligt war, forderte die Mitgliedstaaten der Europäischen Gemeinschaften Mitte 1981 – und damit bereits kurz nach der Freigabe der Konvention zur Unterschrift – in einer Empfehlung dazu auf, die Datenschutz-Konvention noch im selben Jahr zu unterzeichnen und im Laufe des Jahres 1982 zu ratifizieren (Commission of the European Communities 1981). Die Nichtbefolgung dieser Kommissionsempfehlung sollte einige Jahre später schließlich ein ausschlaggebender Grund für die Erarbeitung der EU-DS-RL sein. Wie die Europäische Union mit der Herausforderung der zunehmenden Verarbeitung personenbezogener Daten umging und wie es zur Verabschiedung von EU-Maßnahmen zum Datenschutz kam, ist Gegenstand der folgenden Unterabschnitte.

64 Genannt werden das britische (1984), das irische (1988), das finnische (1987) sowie das niederländische Datenschutzgesetz (1989) (González Fuster 2014, 93 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.2 Die ersten Datenschutz-Instrumente auf Gemeinschaftsebene

Die Regulierung der Verarbeitung personenbezogener Daten durch die EU lässt sich bis in die 1970er-Jahre zurückverfolgen. Nachdem die Europäische Kommission zunächst nur wenig Interesse an einer Harmonisierung der nationalen Datenschutzregelungen hatte, änderte sie diese Einstellung mit dem Scheitern der OECD-Datenschutz-Richtlinien und der Datenschutz-Konvention des Europarats. In der Folge wurde zunächst die Datenschutz-Richtlinie 95/46/EG im Jahr 1995 und im Anschluss daran viele weitere Datenschutzbestimmungen verabschiedet und das Feld der Datenschutzpolitik zunehmend durch Europäische Regulierungen geprägt.

Die Verabschiedung der DS-RL markiert einen wichtigen Wendepunkt in der Geschichte des Datenschutzes, der in den Folgejahren nicht nur für die Mitgliedstaaten, sondern auch für viele Staaten weltweit von großer Bedeutung sein sollte. Die DSGVO stellt die Nachfolgerin der DS-RL dar. Das Ziel dieses Unterabschnitts ist die Erklärung des Zustandekommens der Richtlinie. Dazu wird zunächst ein Überblick über die frühesten Aktivitäten auf Gemeinschaftsebene geboten (vgl. 3.2.2.1 bis 3.2.2.2), der Aushandlungsprozess und die Rahmenbedingungen kurz skizziert sowie im Anschluss der Aushandlungsprozess inkl. der Konfliktlinien im Detail erörtert sowie eine Zusammenfassung der wichtigsten Inhalte der Richtlinie geliefert (vgl. 3.2.2.4 bis 3.2.2.8). Darauf folgt eine kurze Betrachtung ihrer Implementierung in den Mitgliedstaaten (vgl. 3.2.2.9).

Bevor jedoch der konfliktreiche Aushandlungsprozess der DS-RL beleuchtet wird, gibt der folgende Unterabschnitt 3.2.1 für ein besseres Verständnis der Aushandlungsprozesse und Konfliktkonstellationen auf EU-Ebene zunächst einen Überblick über die Struktur und Organe der Europäischen Union, die bis hin zum Aushandlungsprozess der DSGVO prägend für die datenschutzpolitischen Auseinandersetzungen auf EU-Ebene waren.

3.2.1 Struktur und Organe der Europäischen Union

Die Europäische Union in ihrer heutigen Form kann als staatsähnliches Gebilde charakterisiert werden, das wesentliche Bereiche des wirtschaftlichen, sozialen und politischen Lebens in den Mitgliedstaaten prägt (Wessels 2008, 20). Ein entscheidendes Merkmal der EU besteht allerdings in ihrem bis heute anhaltenden Fokus auf die Integration durch wirtschaftliche Kooperation, die erst allmählich und zuletzt vor allem durch das In-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

krafttreten der EU-Grundrechtecharta eine andere Qualität angenommen hat, und die unter anderem für die Reform des EU-Datenschutzrechts entscheidend gewesen ist (Lelieveldt und Princen 2015; Tinnefeld 2009; Wessels 2008).

Der Fokus auf wirtschaftliche Integration hat seine Wurzeln in der Unterzeichnung des Pariser Vertrags zur Europäischen Gemeinschaft für Kohle und Stahl (EGKS) im Jahr 1951 sowie der Römischen Verträge im Frühjahr 1957. Ersterer fokussierte sich auf die Vergemeinschaftung der kriegswichtigen Güter Kohle und Stahl und letztere erweiterten die wirtschaftliche Zusammenarbeit in Richtung der Schaffung eines gemeinsamen Binnenmarktes vor dem Hintergrund der Idee europäischer Völkerverständigung, nachdem der weitergehende Vorstoß in Form der Europäischen Verteidigungsgemeinschaft (EVG), die eine Kooperation im militärischen und politischen Bereich vorgesehen hatte, von der französischen Nationalversammlung 1954 abgelehnt worden war (Wessels 2008, 66 ff.). Neben der Gründung der Europäischen Wirtschaftsgemeinschaft (EWG) sahen die Römischen Verträge auch die Gründung der Europäischen Atomgemeinschaft (EURATOM) zum Zwecke der Sicherstellung der friedlichen Verwendung der Atomenergie vor. Die sechs Unterzeichnerstaaten waren Belgien, Frankreich, die Bundesrepublik Deutschland, Italien, Luxemburg und die Niederlande. Mit dem Inkrafttreten des EG-Fusionsvertrags am 1. Juli 1967 wurden die drei bestehenden Gemeinschaften (EGKS, EWG und EURATOM) in den Europäischen Gemeinschaften zusammengeführt. Institutionell bedeutete dies, dass die bestehenden drei Ministerräte (der EGKS, der EWG und der EURATOM) zum Rat der Europäischen Union (bzw. geläufiger auch als Ministerrat[65] bekannt) sowie die bestehenden zwei Kommissionen (der EWG und des EURATOM) zur Kommission der Europäischen Gemeinschaften (die heutige Europäische Kommission) fusionierten.[66] Schon vor der Unterzeichnung des Fusionsvertrages teilten sich die drei Gemeinschaften eine parlamentarische Versammlung (das heutige Europäische Parlament), einen Gerichtshof (Europäischer Gerichtshof – EuGH) sowie einen Wirtschafts- und Sozialausschuss (WSA – heutiger Name: Europäischer Wirtschafts- und Sozialausschuss EWSA). In

65 Wenn im weiteren Verlauf des Textes die Rede vom *Rat* ist, ist stets der Ministerrat gemeint.

66 Um Verwirrungen aufgrund der Verwendung der unterschiedlichen Begrifflichkeiten zu vermeiden, werden im weiteren Verlauf durchgängig die aktuellen Bezeichnungen verwendet, also Ministerrat, Europäische Kommission, Europäisches Parlament usw.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

mehreren Erweiterungsrunden wuchs die Zahl der Mitgliedstaaten von ursprünglich sechs auf bis zu 28 an.[67] Mit dem Inkrafttreten des Maastrichter Vertrags Ende 1993 wurde die intergouvernementale Zusammenarbeit der EG über die Wirtschaftskooperation (nunmehr als erste Säule bezeichnet) hinaus auf die teil-vergemeinschafteten Politikbereiche der gemeinsamen Außen- und Sicherheitspolitik (GASP) (zweite Säule) sowie der Justiz- und Innenpolitik (JI)[68] (dritte Säule) ausgeweitet. Nachdem der bislang weitest gehende Integrationsversuch in Form der EU-weiten Annahme des Europäischen Verfassungsvertrags an den Referenden in Frankreich und den Niederlanden 2005 scheiterte, wurden dessen wesentliche Elemente in Form des Vertrags von Lissabon umgesetzt. Dieser hob u. a. die zuvor geschaffene Säulenstruktur und damit auch die Unterscheidung zwischen supranationalem Gemeinschaftsrecht (Binnenmarkt) und intergouvernementalem Unionsrecht (PJZS – Polizeiliche und justizielle Zusammenarbeit) auf und weitete das für datenschutzpolitische Fragen bedeutsame, sog. Mitentscheidungsverfahren auf die PJZS aus. Bedeutsam war zudem, dass mit dem Inkrafttreten des Lissabon-Vertrags am 1. Dezember 2009 auch die bereits 2000 proklamierte EU-Grundrechtecharta Rechtskraft erlangte. In Folge des Inkrafttretens des Reformvertrages bilden nunmehr der EUV (Vertrag über die Europäische Union) sowie der AUEV (Vertrag über die Arbeitsweise der Union, ehemals EC Treaty) die primärrechtlichen Grundlagen der EU (Europäische Union 2010).

Im Folgenden werden kurz die zentralen Organe der EU und ihre Rolle im politischen Geflecht der Unionspolitiken vorgestellt.

3.2.1.1 Europäischer Rat

Der 1974 gegründete Europäische Rat versammelt neben dem Präsidenten des Europäischen Rates, dem Präsidenten der Europäischen Kommission

67 1973 traten das Vereinigten Königreich, Dänemark und Irland der Gemeinschaft bei, 1981 folgte Griechenland, 1986 Portugal und Spanien, 1995 Finnland, Österreich und Schweden, 2004 Estland, Lettland, Litauen, Polen, Tschechien, Slowenien, die Slowakei, Ungarn, Malta sowie Zypern, 2007 Rumänien und Bulgarien und schließlich 2013 Kroatien. Aktuell (Stand: Mitte 2020) steht der freiwillige Austritt Großbritanniens aus der EU bevor.

68 Nachdem die justizielle Zusammenarbeit in Zivilsachen und die flankierenden Maßnahmen zum freien Personenverkehr mit dem Vertrag von Amsterdam 1997 in die erste Säule verschoben worden waren, verblieben die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) in der dritten Säule, die fortan entsprechend bezeichnet wurde (Wessels 2008, 94).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

und dem hohen Vertreter der Union für Außen- und Sicherheitspolitik außerdem die Staats- und Regierungschefs der Mitgliedstaaten. Er gilt als „oberstes" Gremium der EU (Wessels 2008, 155), da er der Union „die für ihre Entwicklung erforderlichen Impulse [gibt] und […] die allgemeinen politischen Zielvorstellungen und Prioritäten hierfür fest[legt]" (Europäische Union 2010, Art. 15 (1)).

Dazu gehört sowohl die Befassung mit und die Setzung von Schwerpunkten im Hinblick auf eine enorm breite Themenpalette an Politikfeldern als auch die Initiierung neuer Tätigkeitsbereiche wie etwa im Bereich der Innen- und Justizpolitik seit Ende der 1990er sowie im Rahmen der Terrorismusbekämpfung seit 2001 (Wessels 2008, 163 f.). Besonders sichtbare und einflussreiche Eckpunkte dieser Politik sind die Mehrjahresprogramme, die von Kommission und Ministerrat erarbeitet und vom Europäischen Rat verabschiedet werden. Darunter fallen das Tampere Programm (Europäischer Rat 1999b), das Haager Programm (Europäischer Rat 2005a) sowie das Stockholmer Programm (Europäischer Rat 2010).

3.2.1.2 Europäische Kommission

In der institutionellen Architektur der EU kommt der Europäischen Kommission eine wesentliche Rolle bei der *Vorbereitung*, *Verabschiedung*, *Durchführung* und *Kontrolle* von verbindlichen Entscheidungen zu (Wessels 2008, 225). So hat die Kommission im Regelfall[69] das Initiativrecht zur Einbringung von Legislativvorschlägen inne, sodass sie im Rahmen der *Vorbereitung*sphase häufig als Agenda-Setterin fungiert (Fouilleux, Maillard, und Smith 2005, 617). Das Parlament und der Ministerrat können die Kommission lediglich dazu auffordern, gesetzgeberisch aktiv zu werden. Bei der Wahrnehmung ihrer Aufgaben ist die Kommission gemäß ihres vertraglich festgelegten Auftrags dazu verpflichtet, die „allgemeinen Interessen" der Union zu fördern (Europäische Union 2010, Art. 17) – womit die Kommission ein Gegengewicht zum Ministerrat bilden soll, in dem einzelstaatliche Partikularinteressen verfolgt werden (Wessels 2008, 228 f.). In der Phase der *Verabschiedung* eines Legislativvorschlags ist die Kommission in

69 Die einzige Ausnahme existiert im Bereich der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit, wo neben der Kommission auch mind. ein Viertel der EU-Mitgliedsstaaten einen Legislativvorschlag unterbreiten können (Lelieveldt und Princen 2015, 86). Zudem können Parlament und Ministerrat die Kommission dazu auffordern, einen Legislativvorschlag für ein Themengebiet anzufertigen (EU-Ministerrat 2017; Europäisches Parlament 2020).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Beratungen und Verhandlungen zwischen Ministerrat und Parlament als Mitgestalterin sowie im Rahmen von Vermittlungsausschüssen oder informellen Trilog-Verhandlungen als Vermittlerin eingebunden. Sobald eine verbindliche Entscheidung von Parlament und Ministerrat beschlossen wurde, kommt der Kommission die Gewährleistung der *Durchführung* derselben zu. Schließlich wacht die Kommission im Rahmen der *Kontrolle* über die Einhaltung des Vertragsrechts („Primärrecht") und der auf dieser Grundlage gefassten Beschlüsse („Sekundärrecht"), also Verordnungen, Richtlinien usw. (Wessels 2008, 229).

Im Zuge der Vertragsänderungen seit ihrer Gründung im Jahr 1951 hat sich das Aufgaben- und Kompetenzspektrum der Kommission stetig erweitert. Zuletzt wurden mit dem Inkrafttreten des Lissabon-Reformvertrages die Strukturen der EU sowie die Kompetenzen und Funktionsweisen ihrer Organe reformiert. Auf Grundlage dieser jüngsten Vertragsänderungen kann sich die Kommission bei der Auswahl ihrer Themen idealtypisch sowohl an den Vorgaben höherer politischer Ebenen (jährliches Arbeitsprogramm der Kommission, Vorschläge des Parlament oder der Mitgliedstaaten im Rahmen von Ministerrat oder Europäischem Rat) orientieren als auch eine Route *von unten* nehmen, indem die Kommission unter Bezugnahme auf bestehende Regelungen selbst zur Agenda-Setterin wird (Princen und Rhinard 2006a).

Dabei kann die Kommission auf verschiedene Legislativinstrumente zurückgreifen. Mittels einer Richtlinie kann die Kommission den Mitgliedstaaten verbindlich zu erreichende Ziele vorgeben, während das Wie, also Form und Mittel der Zielerreichung, den Mitgliedstaaten überlassen bleibt. Demgegenüber hat eine Verordnung unmittelbar geltende Wirkung in jedem Mitgliedstaat. Empfehlungen und Stellungnahmen der Kommission entfalten schließlich keinerlei bindende Wirkung (Wessels 2008, 196). Neben diesen vertraglich vorgesehenen Dokumenten veröffentlicht die Kommission zudem auch Grünbücher und Weißbücher, um Konsultationsprozesse anzustoßen bzw. einen Kommissionsstandpunkt darzulegen sowie Mitteilungen, in denen sich die Kommission zu verschiedenen Themen äußert (EU-Ministerrat 2017).

3.2.1.3 Der Rat der Europäischen Union – Ministerrat

Der Ministerrat war lange Zeit das zentrale Entscheidungsorgan der EU. Bis zur Gründung des Europäischen Rats war der Ministerrat das einzige Organ, in dem die Regierungen der Mitgliedstaaten – in Form von Minis-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

tern oder Staatssekretären – repräsentiert waren. Trotz des allmählichen Aufstiegs des Parlaments zum Mitgesetzgeber, der mit dem Inkrafttreten des Lissabon-Vertrags seinen vorläufigen Höhepunkt erreichte, kommt dem Rat in der Hierarchie der EU-Organe, insbesondere aufgrund ihrer Nähe und des Einflusses auf den Europäischen Rat, immer noch eine zentrale Rolle zu (Naurin 2014). Denn obwohl die wegweisenden Entscheidungen der EU auf den Treffen des Europäischen Rats getroffen werden, erfolgt die meiste tatsächliche politische Arbeit der Mitgliedstaaten auf der Ebene des Ministerrats und der ihm unterstellten Vorbereitungsgremien (Hayes-Renshaw 2017; Naurin 2014). Dem Ministerrat kommen sowohl legislative als auch budgetäre sowie exekutive Aufgaben zu. Zudem fungiert der Ministerrat als Unterstützungs- und Umsetzungsgremium der Beschlüsse des Europäischen Rates (Europäische Union 2010, Art. 16). Der Ministerrat verabschiedet aber nicht nur Rechtsakte, wie es in den europarechtlichen Verträgen vorgesehen ist, sondern beispielsweise auch Schlussfolgerungen und Entschließungen. In diesen Dokumenten, die vertraglich nicht vorgesehen sind und die daher auch keine Rechtswirkung entfalten, äußert sich der Ministerrat zu unterschiedlichen Themen im Zusammenhang mit den Tätigkeitsbereichen der EU (EU-Ministerrat 2017).

3.2.1.4 Europäisches Parlament

Seit seinem Bestehen hat das Europäische Parlament zunehmend an Bedeutung gewonnen, sodass die ehemalige Dominanz von Kommission und Ministerrat immer mehr – und insbesondere seit dem Inkrafttreten des Lissabon-Vertrags – einem institutionellen Dreieck gewichen ist, in dem das Parlament zunehmend als Mitentscheider und Vetospieler, statt nur als Berater, auftritt (Wessels 2008, 119).

In den ersten Jahrzehnten, die auf seine Gründung folgten, war das EP zunächst (anfänglich unter dem Namen „Versammlung") als Diskussionsforum ohne Entscheidungsbefugnisse konzipiert, sodass ein Großteil seiner Tätigkeit im Bereich weniger bedeutsamer Prozesse verlief. Der Prozentsatz der politischen Entscheidungen, an denen das Parlament als Mitentscheider partizipiert, hat sich nach der erstmaligen Einführung des Mitentscheidungsverfahrens im Rahmen des Vertrags von Maastricht 1993 zunächst mit dem Inkrafttreten des Vertrags von Amsterdam 1999 und später den Verträgen von Nizza und Lissabon signifikant erhöht (Pittella, Vidal-Quadras, und Papastamkos 2014; Wessels 2008, 124).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Aufgrund seiner Macht-*Ferne* galt das Europäische Parlament über viele Jahre als ein im Vergleich zu Kommission und Rat offener Diskussionsort für umweltschutz-, verbraucherschutz- oder auch geschlechterpolitische Interessengruppen (sog. diffuse Interessen) aus der Zivilgesellschaft (Dür, Bernhagen, und Marshall 2013; Kluger Dionigi 2017; D. J. Marshall 2012). Mit dem Aufstieg zum Mitgesetzgeber hat sich diese Rolle des Parlaments allerdings deutlich gewandelt. So gilt das Parlament (bzw. die Ausschussvorsitzenden und zuständigen Rapporteure) inzwischen als einer der zentralen Adressaten für Interessengruppen jeglicher Couleur, sodass sich auch in den Entscheidungen des Parlaments immer weniger die Vertretung diffuser Interessen erkennen lässt. Sinnbildhaft im Bereich der Datenschutzpolitik war in diesem Zusammenhang das Abweichen des Parlaments von seiner früheren Position im Zusammenhang mit der EU-Richtlinie zum Zugriff auf Fluggastaten (Greis 2015) sowie zur Vorratsdatenspeicherung (Ripoll Servent 2013).[70]

In seiner Rolle als Mitgesetzgeber veröffentlicht das Parlament Berichte, in denen es seinen Standpunkt im Hinblick auf einen von der Kommission unterbreiteten Legislativvorschlag festlegt. Zudem kann auch das Parlament mittels Entschließungen/Resolutionen und Empfehlungen zu verschiedenen Fragen im Zuständigkeitsbereich der EU rechtsunverbindlich Stellung beziehen (Europäisches Parlament 2020).

3.2.2 Die EU-Datenschutz-Richtlinie 95/46/EG

3.2.2.1 Erste datenschutzpolitische Bestrebungen auf Gemeinschaftsebene[71]

Die ersten Aktivitäten auf Gemeinschaftsebene lassen sich bis in die frühen 1970er-Jahre zurückverfolgen. Vor dem Hintergrund der zunehmenden Verbreitung von Computern und der Zunahme der volkswirtschaftlichen Bedeutung der Datenverarbeitung setzten sich Kommission und Parlament mit der Frage auseinander, wie die EG auf diesem zukunftsträchtigen Wirtschaftsgebiet gemeinsam agieren könnte, um angesichts der drohenden Marktdominanz der Vereinigten Staaten bestehen zu können (Commission of the European Communities 1972). Zum Zwecke der Steigerung der

70 Vgl. auch die Unterabschnitte 3.3.4.3 bzw. 3.3.4.2 zum Thema der Fluggastdatenspeicherung bzw. zur Vorratsdatenspeicherung.

71 Die grundlegende Struktur dieses Abschnittes orientiert sich an der instruktiven Darstellung von Gloria Gonzáles-Fuster (2014), legt allerdings andere Schwerpunkte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

europäischen Wettbewerbsfähigkeit auf diesem Gebiet trat die Kommission schließlich Ende 1973 mit einem Entschließungsvorschlag für eine „gemeinschaftliche Politik auf dem Gebiet der Datenverarbeitung" mittels einer Kommissionskommunikation an den Ministerrat heran (Commission of the European Communities 1973). In diesem wirtschaftspolitisch motivierten Dokument, das sich der Schaffung möglichst günstiger Bedingungen für die weitere Verbreitung von Computern, Datenverarbeitungen, Datenbanken usw. widmete, setzte sich die Kommission in einem Punkt mit der Bedeutung der Frage auseinander, wie der Zugriff auf in zunehmendem Maße international verwaltete Datenbanken, die Informationen über Individuen enthalten, aussehen müsste. Einerseits forderte die Kommission darin die Durchführung öffentlicher Experten-Anhörungen und andererseits wurde vorgeschlagen, „to seek a genuine political consensus on this matter now with a view to establishing common ground rules, than to be obliged to harmonise conflicting national legislation later on." (Commission of the European Communities 1973, 13 Nr. 39) Der Ministerrat unterstützte im Anschluss an die Aufforderung der Kommission zwar die Schaffung einer *gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung* und leitete entsprechende dahingehende Schritte im Rahmen einer Ministerratsentschließung vom 14. Juli 1974 ein, doch wurden die von der Kommission ebenfalls aufgeworfenen datenschutzpolitischen Fragen dabei vollständig ignoriert (Ministerrat 1974) und auch nicht anderweitig aufgegriffen (González Fuster 2014, 113).

Vor dem Hintergrund der öffentlich-medialen Debatte um die Zentralisierung von staatlichen Datenbanken in Frankreich[72] brachte der französische Europaparlamentsabgeordnete Pierre Bernard Cousté das Thema im März 1974 zudem im Europäischen Parlament ein und richtete eine mündliche Anfrage an den Ministerrat. Darin nahm Cousté Bezug auf die bereits erfolgte und noch laufende Einrichtung großer Datenbanken in verschiedenen EG-Mitgliedstaaten und erkundigte sich danach, ob der Ministerrat „zum Schutz der Bürger vor Eingriffen in ihre Privatsphäre im Rahmen der gemeinschaftlichen Informationspolitik geeignete Maßnahmen, wie insbesondere strenge gesetzliche Vorschriften über den Zugang zu solchen Informationen, zu treffen [gedenkt]." (Cousté 1974, 21)

Die Antwort auf Cousté kam seitens des amtierenden Präsidenten des Ministerrates, Hans Apel, dem seinerzeitigen von der SPD gestellten parlamentarischen Staatssekretär beim Bundesminister des Auswärtigen. Dieser

72 Das sog. *Projekt S.A.F.A.R.I.* (vgl. González Fuster 2014, 61 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

teilte zunächst die geäußerten Bedenken und das Ziel des Schutzes personenbezogener Daten: „It is true that here we need strict provisions on access to this information, as you rightly say, Mr Cousté, to protect the private life of the individual." (European Communities 1974, 35) Apel stellte aber sodann die Notwendigkeit einer gemeinschaftlichen Politik, wie sie seitens der Kommission als möglicherweise erforderlich dargestellt worden war, infrage, da diese Frage zunächst im Ministerrat zu klären sei: „The prime aim is to protect private life. Whether this is to be achieved at national or Community level is a question of practical feasibility, not a matter for a European discussion of principle. […] Since it is not a matter of ideology, I think it should be quite easy to discuss." (ebd.) Am Ende der Parlamentsdebatte kündigte Cousté schließlich an, dass der Ausschuss für Wirtschaft und Währung des Europäischen Parlaments (ECON-Ausschuss - Committee on Economic and Monetary Affairs) bereits dabei war, einen einschlägigen Bericht zu erarbeiten (ebd., 37). Die Arbeiten an jenem Bericht waren tatsächlich bereits im Vorfeld der Plenardebatte am 13. Februar 1974 mit einem an den Rechtsausschuss (Legal Affairs Committee) gerichteten Brief des Parlamentspräsidenten initiiert worden. Der Parlamentspräsident forderte den Rechtsausschuss darin auf, eine Stellungnahme für den ECON-Ausschuss zu der Mitteilung der Kommission an den Rat über die Politik der Kommission im Bereich der Datenverarbeitung abzugeben (Legal Affairs Committee of the EP und Lord Mansfield 1975, 10).

Der Rechtsausschuss folgte der Aufforderung und überreichte seine Stellungnahme im Mai 1974 an den ECON-Ausschuss (ebd., 14). Vonseiten der Kommission war an dem Prozess der damalige Kommissar für das Ressort Industrie und Handel, Altiero Spinelli, beteiligt. In einem Brief an den Parlamentspräsidenten im März 1974 unterstrich Spinelli, selbst überzeugter Europäer, der Zeit seines Lebens für eine verstärkte Europäische Integration eintrat (Pinder 2007), die Bedeutung der Thematik und dass die „Commission realizes that the communication of data across frontiers will be a European problem likely to require harmonization" (Spinelli, zit. nach González Fuster 2014, 114). Allerdings sah es Spinelli aufgrund der verfassungsrechtlichen Bedeutung des Schutzes personenbezogener Daten als angemessener an, wenn sich das Parlament zunächst insb. in Gestalt öffentlicher Experten-Anhörungen tiefergehend mit der Thematik auseinandersetzt. Im Anhang des Briefes übersandte Spinelli zudem weitergehende Informationen der Kommission zu den Herausforderungen von Datenbanken für den Schutz der Freiheit der Individuen, konkrete Gestaltungsvorschläge für einen mit dem Thema befassten Parlamentsausschuss sowie

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Angaben zu wesentlichen Aspekten des Themas, die einer tiefergehenden Untersuchung bzw. politischer Entscheidungen bedürften. Dass es sich bei dem Thema des Schutzes von Individuen im Kontext von Datenbanken um ein brisantes Thema handelte, bestätigte ein weiterer Brief, diesmal seitens des Vize-Präsidenten der Europäischen Kommission. Darin wurde dargelegt, dass, aufgrund des ausgesprochen politischen Charakters des Themas, die Befassung des Parlaments mit der Materie angemessener sei (González Fuster 2014, 114).

Diese Auffassung wurde allerdings auf Seiten des Parlaments nicht vollends geteilt. Dies hatte mehrere Gründe: Zum einen war das Parlament in den 1970er-Jahren eine noch weitgehend machtlose Diskussionsplattform. Ohne eigene Kompetenz hinsichtlich der Unterbreitung von Gesetzesvorschlägen konnte sie gegenüber der Kommission in Form von Parlamentsresolutionen lediglich ihren Wunsch äußern, gesetzgeberisch tätig zu werden, ohne dass die Kommission verpflichtet war, dem Wunsch nachzukommen. Gleichzeitig lag die Entscheidungsmacht in der EG in den 1970er-Jahren noch stärker als heute eindeutig bei den Mitgliedstaaten. Mit der 1974 erfolgten Gründung des Europäischen Rates, die seitens der Supranationalitätsbefürworter kritisiert wurde (Pinder 2007; Wessels 2008, 155 ff.), verfestigte sich diese Macht zudem noch weiter. Entsprechend wurde die Meinung vertreten, dass die Befassung des Parlaments mit der Materie lediglich als Vorbereitung dienen könne, während die *Sammlung von Fakten und Informationen, auf deren Grundlage die Kommission Gemeinschaftsvorschriften vorlegen könne, allerdings eine Aufgabe sei, die allein die Kommission zu erfüllen vermag*[73] (Legal Affairs Committee of the EP und Lord Mansfield 1975, 14). Zum anderen taten sich im Laufe der Auseinandersetzung des Parlaments mit der Materie Schwierigkeiten im Hinblick auf die Zuständigkeit auf. So war die Verwaltung von Datenbanken eine Frage, die in den Verantwortungsbereich der EG-Industriepolitik fiel. Das Interesse an der Befassung mit der Materie des Schutzes von Individuen beim für diesen Bereich zuständigen ECON-Ausschuss hielt sich dagegen in Grenzen, sodass der Ausschuss am 8. Juli 1974 alle weiteren Arbeiten einstellte. Erst als Kommissar Spinelli am 22. Juli 1974 den dahingehenden Wunsch der Kommission, dass das Parlament Stellung zu dem Thema nehme, bekräftigte, sicherte der Rechtsausschuss am 12. September 1974 schließlich die Erarbeitung eines entsprechenden Dokuments unter der Federführung

73 Eigene Übersetzung der entsprechenden Passage.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

von Lord Mansfield[74] zu (ebd., 15). Das Verhalten des ECON-Ausschusses lässt sich wohl am ehesten mit dem verinnerlichten Selbstverständnis des Ausschusses erklären, der vielmehr als Vertreter bestimmter Interessen und nicht bloß als neutraler Austragungsort von Interessenkämpfen fungiert.[75] So zählt zum Kern-Themenportfolio des ECON-Ausschusses die Förderung der wirtschaftlichen Integration und des wirtschaftlichen Wachstums in der EU, jedoch nicht der Schutz von Verbraucherinteressen oder von Menschenrechten.[76] Dies darf aber nicht verwundern, da die Gründung der EG zu diesem Zeitpunkt erst sieben Jahre zurücklag und letztlich ohnehin nur deshalb Erfolg hatte, weil nach dem Scheitern weitergehender Integrationsbemühungen der Kompromiss die Fokussierung auf wirtschaftspolitische Kooperation vorsah (vgl. 3.2.1). Während es also nicht verwunderlich ist, dass der ECON-Ausschuss das Thema nicht aus der ihm vorgegebenen Menschenrechtsperspektive aufgegriffen hat, ist es dagegen durchaus verwunderlich, weshalb der Ausschuss das Thema nicht analog zur OECD aus einer wirtschaftspolitischen Perspektive heraus betrachtet hat. Die Antwort auf diese Frage mag darin liegen, dass der ECON-Ausschuss innerhalb seiner kurzen Tätigkeitsspanne (nur wenige Monate) nicht auf das für die Wirtschaftspolitik relevante Problem der grenzüberschreitenden Datenflüsse gestoßen war. Schließlich war selbst die – in ähnlichem Maße stark wirtschaftspolitisch motivierte – OECD, die sich zu diesem Zeitpunkt bereits seit Jahren mit dem Thema beschäftigte, erst im Juni 1974 auf den Themenkomplex grenzüberschreitender Datenflüsse aufmerksam geworden (vgl. 3.1.1).

Ende Februar 1975 wurde der vom Rechtsausschuss ausgearbeitete Vorschlag schließlich vom EP-Plenum in Form der *Entschließung über den Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung* angenommen. Diese nahm Bezug auf die im Jahr 1973 an den Rat gerichtete Kommissionskommunikation, stellte allerdings zugleich zwei Ziele für

74 Lord Mansfield, mit bürgerlichem Namen William Murray, war zu dieser britischer Parlamentarier und Mitglied der britischen Delegation an das EP (Jackson 1993).

75 So zeigt die Forschung zum Ausschusswesen des Europäischen Parlaments, dass Ausschüsse im Allgemeinen dazu neigen, ihr eigenes Themenportfolio gegenüber den Themenportfolios anderer Ausschüsse zu begünstigen (Kluger Dionigi 2017, 156).

76 Diese Schwierigkeiten sollten später während des politischen Entscheidungsprozesses der DSGVO in Form der Torpedierung starker gesetzlicher Vorgaben in der DSGVO seitens der in erster Linie mit Wirtschaftsthemen beschäftigten Ausschüsse (insb. der ITRE-, aber auch der IMCO-Ausschuss) wiederkehren (vgl. Unterabschnitt 4.3).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

eine künftige EG-Richtlinie auf, „nicht nur um sicherzustellen, daß die Bürger der Gemeinschaft einen maximalen Schutz vor Mißbrauch oder Defekten der Datenverarbeitungsverfahren genießen, sondern auch, um das Entstehen einander widerstreitender nationaler Rechtsvorschriften zu verhindern" (Europäisches Parlament 1975, 48 Nr. 1). Trotz der Empfehlung, dass eine Richtlinie *dringend notwendig* sei, bot die Resolution allerdings keine konkreten inhaltlichen Gestaltungsvorschläge für eine solche Richtlinie, sondern war vor allem darum bemüht, die Einsetzung eines Sonderausschusses in die Wege zu leiten, der sich mit dem Themenkomplex auseinandersetzen und Gestaltungsvorschläge erarbeiten sollte (ebd., Nr. 2 & 3). Nachdem die Einsetzung des Sonderausschusses doch nicht mehr erfolgte, beauftragte das Parlamentsplenum im Rahmen einer weiteren Entschließung Anfang April 1976 den Rechtsausschuss[77] mit der weiteren Berichterstattung zu laufenden und einzuleitenden Gemeinschaftsaktivitäten (Europäisches Parlament 1976, 27 Nr. 2). Daneben wurde die Europäische Kommission noch einmal darum ersucht, die Erarbeitung einer Gemeinschaftsregelung zum *Schutz der Rechte der einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung* voranzutreiben (ebd., Nr. 1).

Der Rechtsausschuss nominierte im Anschluss den sozialdemokratischen Europaabgeordneten Alfons Bayerl als Berichterstatter. Dieser veranlasste daraufhin die Einsetzung eines Sonderunterausschusses,[78] der sich zwischen Juni 1977 und März 1979 mit dem Themenkomplex auseinandersetzte. Bedeutende Eckpunkte dieser Auseinandersetzung waren eine seitens des Sonderunterausschusses organisierte öffentliche Experten-Anhörung im Jahr 1978, an der neben Kommissionsvertretern auch Beobachter der OECD und des Europarates teilnahmen, sowie die Veröffentlichung des sog. Bayerl-Berichts Mitte 1979, in dem die Ergebnisse des Unterausschusses zusammengetragen wurden (Bayerl 1979).

Der Bayerl-Bericht diente dem EP Mitte 1979 schließlich als Grundlage für die Verabschiedung einer dritten Entschließung (Europäisches Parlament 1979). Gegenüber den vorherigen Resolutionen stellt die 1979er Resolution eine deutliche inhaltliche Entwicklung dar. Erstens wurde darin gesetzgeberisches Handeln nicht mehr nur gefordert, sondern auch konkrete

77 Der Rechtsausschuss sollte dann auch bis zur deutlich später erfolgten Gründung des LIBE-Ausschusses (Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten) für Datenschutzfragen (darunter insbesondere die Verhandlungen zur DS-RL) auf Seiten des EP zuständig bleiben (Karaboga 2018, 151 ff.).

78 Das sog. *Data Processing and Individual Rights Sub-committee* (Bayerl 1979, 2).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Vorschläge hinsichtlich der Gestaltung der geforderten Rechtsvorschriften dargelegt. Zweitens hatte sich die Herangehensweise des Parlaments an das Thema von einer grundrechtsorientierten hin zu einer wirtschaftspolitisch motivierten verschoben. So wurde die Erforderlichkeit der in der Resolution geforderten Maßnahmen damit begründet, dass „eine harmonische Entwicklung der Wirtschaftstätigkeit im Rahmen des Gemeinsamen Marktes die Verwirklichung eines echten gemeinsamen Datenverarbeitungsmarktes voraussetzt, innerhalb dessen der freie Warenverkehr und der freie Dienstleistungsverkehr sichergestellt und der Wettbewerb nicht verzerrt ist" (ebd., 35 Nr. 1) und dass sich die Verabschiedung divergierender einzelstaatlicher Vorschriften „unmittelbar auf die Errichtung und das Funktionieren des Gemeinsamen Marktes auswirken" (ebd., 35 Nr. 2). Viele der Punkte, die in der Entschließung genannte wurden, sollten später Teil der DS-RL werden.

Noch im Begründungsteil wurde zum Zwecke der Überwachung der Anwendung der gewünschten Regelungen die Gründung eines Ausschusses von Vertretern der nationalen Organe der Mitgliedstaaten, also eine Art Datenschutzaufsichtsbehörde auf Gemeinschaftsebene vergleichbar der späteren Art. 29-Datenschutzgruppe bzw. dem heutigen Europäischen Datenschutzausschuss (EDSA) (ebd., S. 36 Nr. 13) – allerdings unter dem Vorsitz eines Parlamentsvertreters – vorgeschlagen (ebd., Nr. 14). Entsprechend wurde in der eigentlichen Entschließung dann auch die Einrichtung unabhängiger Aufsichtsbehörden zur Überwachung der Anwendung der vorgeschlagenen Regelungen auf mitgliedstaatlicher Ebene empfohlen (ebd., 37 Nr. 10–12).

Als Anwendungsbereich wurde sowohl die manuelle als auch die automatisierte Verarbeitung personenbezogener Daten vorgesehen sowie die Verarbeitung (ebd., 37 Nr. 1) und auch die Zusammenführung von Datenbanken (Nr. 6 und 7) einer vorgelagerten, generellen Melde- und Genehmigungspflicht unterlegt. Daneben betonte die Entschließung die Grundsätze der rechtmäßigen Erhebung personenbezogener Daten, der Zweckbindung (inkl. der Betonung der Notwendigkeit zur Einholung einer Einwilligung bei der Erhebung sensibler personenbezogener Daten), der Datenminimierung und -richtigkeit sowie Speicherbegrenzung (ebd., 37 Nr. 2). Regelugen zur Haftung (für materielle sowie immaterielle Schäden) (Nr. 3), zu Sanktionen (Nr. 16), zu den Informationspflichten des Verantwortlichen gegenüber dem Betroffenen (Nr. 4), zu Betroffenenrechten (Transparenz, Löschung, Berichtigung), sofern die Betroffenen ihren gewöhnlichen Aufenthalt im Hoheitsgebiet eines Mitgliedstaates haben (Nr. 8), inklusive der Garantie, diese Rechte *innerhalb einer angemessenen Frist und ohne Gebüh-*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ren und Kosten wahrnehmen zu können (Nr. 9), wurden ebenfalls vorgesehen. Interessanterweise sah der Vorschlag auch vor, dass die genannten Grundsätze sowohl für den Schutz von personenbezogenen Daten gelten sollten als auch für den Schutz von gruppenbezogenen Daten und für die Rechte von Gruppen (Nr. 17).

Für grenzüberschreitende Datenübertragungen innerhalb der Gemeinschaft (Nr. 13) wurde eine Meldepflicht und für Übertragungen in Drittstaaten (Nr. 14) eine Genehmigungspflicht seitens der Datenschutzaufsichtsbehörde auf Gemeinschaftsebene gefordert. Zudem drückte das Parlament seine Unterstützung für die Aktivitäten des Europarats aus und forderte die Kommission auf, zu überprüfen, ob die EG als solche (und nicht jeder Mitgliedstaat für sich) der künftigen Datenschutz-Konvention des Europarats beitreten könnte (EG Nr. 15).

In der Zwischenzeit hatte die Kommission auf die EP-Resolution aus dem Jahr 1976 hin, in der die Kommission erneut zur Erarbeitung einer Gemeinschaftsregelung zum Schutz der Rechte der Einzelnen aufgefordert worden war, einen Austausch mit Ministerratsvertretern zur Eruierung von Harmonisierungsmöglichkeiten initiiert (Commission of the European Communities 1976, 8 Nr. 2.4.4). Zugleich signalisierte die Kommission ihre Unterstützung für die in der Europaratsempfehlung (74) 29 vorgeschlagenen Prinzipien, die bereits seitens einzelner Mitgliedstaaten in nationales Recht umgesetzt worden waren (Commission of the European Communities 1976, 8 Nr. 2.4.4). Im April 1977 verabschiedeten Parlament, Rat und Kommission zudem eine gemeinsame Erklärung, in der sich alle drei Organe zur Wahrung der Grundrechte „wie sie insbesondere aus den Verfassungen der Mitgliedstaaten sowie aus der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten hervorgehen“ (EG 1977) verpflichteten.

Zum Zwecke der verbesserten Entscheidungsfindung hinsichtlich der Erarbeitung einer EG-Richtlinie unterbreitete die Kommission dem Ministerrat schließlich einen Vorschlag zur Ausarbeitung einer Studie, in der „die wichtigsten Probleme der Harmonisierung der in der Gemeinschaft geltenden Rechtsvorschriften über den Schutz der Privatsphäre und die Ausarbeitung von Anwendungskodexen sowie entsprechenden Normen“ (Ministerrat 1977, 26) untersucht werden sollten. In dieser vom Ministerrat im September 1977 (ebd.) genehmigten und zwischen 1978 und 1979 erstellten Studie (Commission of the European Communities 1982, 7) wurde festgestellt, dass trotz der Bestrebungen der Mitgliedstaaten, Divergenzen zu vermeiden, weiterhin mehrere Mitgliedstaaten gar keine Datenschutzrege-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

lungen verabschiedet hatten. Während in Italien und Irland noch keinerlei gesetzgeberische Aktivitäten auf dem Gebiet des Datenschutzes festgestellt wurden, hatten Belgien, das Vereinigte Königreich und die Niederlande immerhin bereits Gesetzesvorschläge oder vorbereitende, einschlägige Studien eingebracht bzw. in Bearbeitung (González Fuster 2014, 118). Während einer parlamentarischen Fragerunde Ende 1979 unterrichtete der konservative Vizepräsident der Europäischen Kommission, Lorenzo Natali, schließlich das Parlament darüber, dass sich die Kommission der Notwendigkeit internationaler Regeln für den Schutz personenbezogener Daten zwar vollkommen bewusst sei, jedoch den Ausgang der Europaratsaktivitäten abzuwarten bevorzuge (ebd., 120).

Als die Datenschutz-Konvention 108 des Europarats schließlich Anfang 1981 verabschiedet wurde, teilte die Kommission Mitte 1981 in Form einer Empfehlung mit, dass sie die Konvention für ein geeignetes Instrument zur Herbeiführung eines einheitlichen Datenschutzniveaus auf europäischer Ebene halte und empfahl allen Mitgliedstaaten die Unterzeichnung der Konvention noch im laufenden Jahr und ihre Ratifikation vor Ende 1982. Für den Fall, dass die Mitgliedstaten die Konvention nicht binnen einer angemessenen Zeitspanne unterzeichnen und ratifizieren würden, behielt sich die Kommission zudem vor, einen eigenen Rechtsakt gemäß EWG-Vertrag vorzuschlagen (Europäische Kommission 1981). In der Folge finanzierte die Kommission weitere Studien zur Untersuchung der Entwicklungen auf dem Gebiet der Verarbeitung und des rechtlichen Schutzes personenbezogener Daten. Auf Grundlage der 1979er Studie verständigten sich die Kommission und der Ausschuss einzelstaatlicher Sachverständiger der Kommission auf die Fokussierung auf die folgenden sechs Unterthemen: (1) die Qualität und Quantität grenzüberschreitender Datenflüsse; (2) den organisatorischen Charakter und das technische Funktionieren von Datenschutzbehörden; (3) die Probleme hinsichtlich der Rechtspersönlichkeit (natürliche und juristische Personen); (4) die internationalen wirtschaftlichen Aspekte der Datensicherheit und Vertraulichkeit; (5) die technischen Aspekte des Rechts auf Zugang zu Datenbanken; sowie (6) die Kontrolle, Prüfung und Umsetzung der Anforderungen an die Vertraulichkeit und deren Umsetzung im Bereich der Datensicherheit (Commission of the European Communities 1982, 7 Nr. 1.2.2.). Das daraus resultierende Arbeitsprogramm, das 1981 initiiert wurde, hatte wiederum zum Ziel, die *Anforderungen an die Harmonisierung der Rechtsvorschriften sowie Empfehlungen und Normen zur Vertraulichkeit von Daten* zu prüfen und widmete sich der Untersuchung von:

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

- Datenschutz im Hinblick auf die neuen Informations- und Kommunikationstechnologien;
- Technologien für den Datenschutz und die Datensicherheit;
- personenbezogenen Daten und automatischen Entscheidungsprozessen;
- den Auswirkungen internationaler Datenschutzbestimmungen auf die Wirtschaftsbereiche, die am stärksten von der Informationsverarbeitung betroffen sind;
- Systemdesign und Datenschutz;
- freiem Zugang zu Informationen und Datenschutz;
- sowie von Datenbanken, verteilten Systemen und Datenschutz (Commission of the European Communities 1982, 29 f.)

Der an alle EG-Mitgliedstaaten gerichteten Kommissionsempfehlung, die Datenschutz-Konvention noch vor Ende 1981 zu unterzeichnen, kamen schließlich lediglich fünf der zehn EG-Mitgliedstaaten nach.[79] Das Europäische Parlament, das bereits seit 1975 für harmonisierte Gemeinschaftsregelungen zum Datenschutz eingetreten war und seitens Rat und Kommission mit dem Verweis auf intergouvernementale Harmonisierungbestrebungen insb. des Europarats vertröstet worden war, nahm die Verabschiedung der Konvention und die zögerliche Unterzeichnung bzw. Ratifikation dieser zum Anlass für eine weitere Resolution im März 1982. Trotz der Begrüßung der Verabschiedung der Datenschutz-Konvention des Europarats (Europäisches Parlament 1982, 40 Nr. 1) äußerte das Parlament seine Bedenken im Hinblick darauf, „daß nicht abzusehen ist, wann schließlich alle Mitgliedstaaten der Gemeinschaft dieses Europäische Übereinkommen unterzeichnet und ratifiziert haben werden" (ebd., Nr. 2) und drückte sein Bedauern darüber aus, dass die EG-Mitgliedstaaten der Kommissionsempfehlung nur teilweise nachgekommen waren (ebd., Nr. 13). Entsprechend bekräftigte das Parlament seine bereits 1979 geäußerte Meinung, dass die EG als solche der Datenschutz-Konvention beitreten sollte (Nr. 16). Mehr aber noch vertrat das Parlament – nunmehr auch unter Verweis auf Art. 100 des EWG-Vertrags, also im Hinblick auf die Errichtung oder das Funktionieren des Gemeinsamen Marktes[80] – die Position, dass der Erlass einer EG-Richtlinie

79 Diese waren: Dänemark, Deutschland, Frankreich, Luxemburg sowie das Vereinigte Königreich. Zu diesem Zeitpunkt noch nicht unterzeichnet wurde die Konvention dagegen von: Belgien, Italien, Irland, Griechenland und den Niederlanden (Council of Europe 2019).

80 „Der Rat erläßt einstimmig auf Vorschlag der Kommission und nach Anhörung des Europäischen Parlaments und des Wirtschafts- und Sozialausschusses Richtlinien für

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

trotz des Bestehens der Datenschutz-Konvention weiterhin nötig und erwägenswert sei (Nr. 3, 17). Als Eckpunkte einer künftigen Regelung wurden die Gleichbehandlung des öffentlichen und nicht-öffentlichen Bereichs, Zugangs- und Berichtigungsrechte, Regelungen zur Haftung sowie die Unterstellung des Betriebs von Datenbanken einer vorherigen Anmelde- und Genehmigungspflicht genannt (Nr. 17).

Allerdings hatte auch diese vierte Resolution des EP keine weiteren Auswirkungen auf die Datenschutzpolitik der EG. Kommission und Rat hielten daran fest, abzuwarten, inwieweit eine Harmonisierung mittels der Datenschutz-Konvention erreicht werden könne (Simitis 1995). Die Aktivitäten der EG auf dem Gebiet des Datenschutzes beschränkten sich in den Folgejahren auf die Erarbeitung von wissenschaftlichen Studien im Kontext der gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung (González Fuster 2014, 121 f.). So genehmigte der Ministerrat zunächst im April 1984 die Ausschreibung weiterer Studien, u. a. mit dem für eine mögliche Harmonisierungspolitik relevanten Ziel der „Prüfung der in den Mitgliedstaaten geltenden oder in Ausarbeitung befindlichen Rechtsvorschriften und Erörterung der Angleichungsmöglichkeiten sowie der Instrumente, die auf Gemeinschaftsebene eingesetzt werden könnten" (Ministerrat 1984a, 31, Nr. 1.3.4). Aufgrund einer Ministerratsentschließung vom Juli 1984, in der die Gemeinschaftspolitik auf dem Gebiet der Datenverarbeitung dahingehend aktualisiert wurde, „mittelfristig ein systematisches Programm der Gemeinschaft zur Förderung der Forschung, industriellen Entwicklung und Anwendung der Datenverarbeitung aufzustellen" (Ministerrat 1984b, 49), wurde der Fokus der zu fördernden Studien allerdings erheblich verändert. Als alleiniges Ziel im Bereich des Datenschutzes wurde die „Fortsetzung der Untersuchungen über Datensicherung und Daten- und Softwareschutz, um die Entwicklung praktischer Werkzeuge für die Verwender zu fördern" (Ministerrat 1984b, 52, Nr. 1.3.3), festgelegt. In der folgenden Ausschreibung der Kommission ging es dann auch nicht mehr um die Arbeit an gemeinschaftsrechtlichen Grundlagen, sondern stattdessen vor allem um die Förderung praxisorientierter Projekte zum technischen (Selbst-)Datenschutz.[81]

---

die Angleichung derjenigen Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die sich unmittelbar auf die Errichtung oder das Funktionieren des Gemeinsamen Marktes auswirken." (Europäische Gemeinschaften 1957, Artikel 100)

81 Lediglich im Bereich „Erfordernisse der Benutzer hinsichtlich der künftigen Gesetzgebung zu Fragen der Sicherheit und der Vertraulichkeit von Daten" fand sich auch

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.2.2.2 Parlament als Befürworter und Kommission als Bremserin von Gemeinschaftsregelungen?

Spiros Simitis, der an mehreren Stellen[82] in die politischen Beratungs- und Entscheidungsprozesse der damaligen Zeit involviert gewesen ist, lässt keinen Zweifel daran, dass die Kommission – aufgrund ihrer wirtschaftspolitischen Motivation – zu keinem Zeitpunkt tatsächliches Interesse an einer Harmonisierung von Datenschutzregelungen hatte. Simitis zufolge lässt sich der datenschutzpolitische Hauptkonflikt der 1970er und 1980er-Jahre dahingehend zusammenfassen, ob Datenschutzregelungen im Sinne des Schutzes fundamentaler Menschenrechte verstanden oder als wirtschaftspolitische Maßnahme aufgefasst wurden. Ein menschenrechtlich orientierter Regulierungsansatz – wie er seitens des EP verfolgte worden war – hätte daher notwendigerweise all jene Übertragungen personenbezogener Daten effektiv beschränken müssen, bei denen kein ausreichendes Schutzniveau vorhanden gewesen wäre. Die Kommission, und insbesondere die Binnenmarkt-Generaldirektion, habe daher, aufgrund ihrer Gebundenheit an die Gemeinschaftsverträge,[83] Datenschutz notwendigerweise einzig im Kontext der Wirtschaftspolitik bzw. insbesondere im Kontext der gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung betrachten können. Diesem Verständnis gemäß waren personenbezogene Daten ein handelbares wirtschaftliches Gut wie jedes andere Gut auch – ohne besondere Schutzerfordernisse. Daher erschienen aus einer solchen wirtschaftspolitischen Perspektive heraus auch jegliche Datenschutzgesetze zunächst als Hindernisse beim Aufbau eines gemeinsamen, also grenzüberschreitenden europäischen Informations- bzw. Datenmarktes, da sie den grenzüberschreitenden Transfer personenbezogener Daten in Staaten ohne Datenschutzgesetze oder mit nur unzureichenden Datenschutzgesetzen er-

---

das Ziel „die Meinungen der Benutzer sowohl bezüglich der anzuwendenden Prinzipien als auch bezüglich der Verfahrensregeln, die in die künftige Gesetzgebung eingehen müßten, zusammenzustellen." (Europäische Kommission 1985, 4, Nr. 3.3.2)

82 Vor allem zu nennen sind hier: Datenschutzbeauftragter des Landes Hessen zwischen 1975 und 1991, Vorsitzender des Datenschutz-Experten-Komitees des Europarats zwischen 1982 und 1986, Berater der Europäischen Kommission in Datenschutzfragen seit 1988 bis ca. zur Jahrtausendwende, Berater des International Labour Office zur Erarbeitung von Beschäftigtendatenschutzregeln zwischen 1991 und 1994 (Simitis 2001, 99).

83 Gemäß EWG-Vertrag waren die Ziele der Gemeinschaft, die Gewährleistung des freien Warenverkehrs (Art. 9), die Freizügigkeit von Arbeitnehmern (Art. 48), von Dienstleistungen (Art. 59) sowie von Kapital (Art. 67).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schwert oder verhindert hätten. Dem seitens der Kommission verfolgten wirtschaftspolitischen Ansatz gemäß dienten Datenschutzregelungen somit allenfalls – und damit ganz im Gegenteil zum Parlamentsverständnis – dazu, einen möglichst ungehinderten Austausch von Informationen zu gewährleisten. Simitis zufolge war selbst die Unterstützung der Datenschutz-Konvention seitens der Kommission der Existenz von Art. 12 Abs. 2 der Datenschutz-Konvention geschuldet, mit dem die Blockierung von grenzüberschreitenden Datenflüssen auf Grundlage von Datenschutzgesetzen verhindert werden sollte (Simitis 1995, 446, 2001, 101; Simitis u. a. 2019, 193, Rn. 133).

Andere Autoren benennen hingegen die Anerkennung des Europarats als entscheidenden Faktor für die Zurückhaltung der Kommission. So hatte die Kommission ohnehin angekündigt, dass sie ein EG-Datenschutzinstrument vorschlagen würde, sofern die Mitgliedstaaten nicht von selbst der Konvention beitreten und harmonisierte Datenschutzgesetze erlassen. Dass die Kommission aber zunächst auf die Konvention setzte sei vor allem darauf zurückzuführen, dass der Europarat über mehr Mitglieder verfügte und die potentielle Harmonisierungswirkung einer Europaratskonvention größer sein könnte als die der EG (Burkert 1988, 756; Schmahl und Breuer 2017, 711).

Newman weist zudem darauf hin, dass bei der Kommission über lange Zeit das – seit der Verbreitung von Computern überholte – Verständnis vorherrschend gewesen sei, wonach die Verarbeitung personenbezogener Daten in erster Linie eine den öffentlichen Sektor betreffende Frage wäre, die folglich am besten auf mitgliedstaatlicher Ebene zu lösen sei, da die Gemeinschaft bei Fragen, die den öffentlichen Sektor betreffen, schlicht keine Kompetenz inne hatte (A. L. Newman 2008a, 110 f.).

Neben der Kommission opponierten aber auch die EG-Mitgliedstaaten gegen die Erarbeitung supranationaler Datenschutzregeln. Die drei großen Mitgliedstaaten Deutschland, Frankreich und insbesondere Großbritannien waren bis zuletzt Gegner jeglicher supranationalen Aktivität auf dem Gebiet des Datenschutzrechts (A. Newman 2007a, 131 f.). Ebenso wandten sich Vertreter der europäischen Wirtschaft klar gegen die Einführung einer gemeinschaftsweiten Harmonisierung der Datenschutzregelungen. Britische Unternehmen gingen – unter Verweis auf für die Wettbewerbsfähigkeit drohende, negative Konsequenzen – am intensivsten gegen europäische Regelungen vor. Aber auch deutsche Unternehmen, die aufgrund des in der Bundesrepublik herrschenden hohen Datenschutzniveaus am ehesten für die Unterstützung der Anhebung des Schutzniveaus in anderen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Ländern in Frage kamen, stellten sich gegen Harmonisierungsbestrebungen (Computerwoche 1990; A. L. Newman 2008a, 111 f.).

3.2.2.3 Der Meinungswandel der Europäischen Kommission

Mit der Veröffentlichung mehrerer Vorschläge im Hinblick auf den Schutz personenbezogener Daten im September 1990 wurde deutlich, dass sich die Haltung der Kommission schlagartig geändert hatte. Doch was waren die ausschlaggebenden Gründe für diesen bedeutungsschweren Meinungswandel, in dessen Folge die EU bis heute zur weltweiten Vorreiterin in Datenschutzfragen werden sollte?

Laut aktuellem Stand der Forschung zu den Gründen für die Erarbeitung der DS-RL waren vor dem Hintergrund der massiven Zunahme grenzüberschreitender Datenübertragungen am Ende der 1980er-Jahre vor allem zwei miteinander zusammenhängende und sich gegenseitig verstärkende Faktoren entscheidend. Die von dieser Zunahme am stärksten betroffenen Bereiche waren: Personalabteilungen; Banken, Versicherungen, Kreditkartenunternehmen und Kreditbüros; Direktmarketing; Fluggesellschaften, Reisebüros und andere am Tourismus beteiligte Unternehmen; Unternehmen, die Waren an internationale Kunden liefern oder anderweitig mit internationalen Kunden handeln wollen; und innerhalb der öffentlichen Verwaltung: Polizei, Zoll, Steuerbehörden und öffentliche Rentenversicherungsträger (Ellger 1990, 108–29).

Erstens war das Auftreten der Datenschutzaufsichtsbehörden als politischer Akteurinnen und Lobbyistinnen von entscheidender Bedeutung. Waren die Aufsichtsbehörden ursprünglich mit dem Ziel gegründet worden, einerseits die Einhaltung der Datenschutzregelungen bei den jeweiligen Verarbeitungen zu überwachen und andererseits Beratungsfunktionen im Hinblick auf den Umgang mit den oftmals auch für die Verantwortlichen selbst neuen Verarbeitungssystemen zu übernehmen, verschob sich ihre Rolle im Laufe der Zeit zunehmend hin zur Politikberatung. So kam mit steigender Erfahrung im Laufe der 1970er- und 1980er-Jahre zu der Überwachungs- und Beratungsrolle die kritische Hinterfragung bestehender gesetzlicher Regelungen und die proaktive Skizzierung von Fortentwicklungsmöglichkeiten des Datenschutzrechts hinzu (A. Newman 2007a, 132; Simitis 2001, 135 f.). Die auf die entsprechenden Aufsichtsbehörden-Positionen berufenen Individuen entstammten wiederum der epistemischen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Community Datenschutzregelungen befürwortender Privatheitsexperten, waren also überzeugungsgetriebene Akteure (A. Newman 2007a, 132).[84]

Als sich die Befürchtungen, dass Unternehmen ihre Datenverarbeitungen in jene Staaten ohne Datenschutzgesetze auslagern würden, seit Ende der 1970er-Jahre zunehmend bewahrheiteten, initiierten die nationalen Aufsichtsbehörden zunächst Formate zur internationalen Kooperation.[85] In der Folge kooperierten Vertreter der nationalen Aufsichtsbehörden im Rahmen von internationalen Arbeitsgruppen zu Themen wie Binnenmarkt- oder Telekommunikationspolitik und brachten abgestimmte Politikvorschläge in ihren jeweiligen Heimatländern ein. Im Vordergrund stand dabei die Befürwortung supranationaler Regelungen, um das EG-weit stark divergierende Datenschutzniveau zu vereinheitlichen und auf diese Weise die sog. Daten-Oasen trocken zu legen (A. L. Newman 2008a, 113). Schließlich war im Laufe der 1980er immer klarer geworden, dass die von der Kommission gewünschte und vom Parlament bezweifelte Harmonisierungswirkung der Datenschutz-Konvention, trotz aller Appelle an die EG-Mitgliedstaaten, nicht eintreten würde. Selbst im Jahr 1990 existierten in fünf[86] von zwölf EG-Mitgliedstaaten noch immer keine Datenschutzgesetze (Vgl. die Übersicht in Tabelle 3-1).

Als die Mitgliedstaaten und die Kommission trotz der anhaltenden offenkundigen Probleme weiterhin tatenlos blieben, begannen die Aufsichtsbehörden schließlich, Gebrauch von ihren neu erlangten Befugnissen zu machen, um den Datentransfer in Länder ohne Datenschutzgesetze zu stoppen. So verhinderte z. B. bereits die schwedische Datenschutzaufsichtsbehörde, das *Data Inspection Board*, im Jahre 1980 die Übertragung von Gesundheitsdaten über die schwedische Bevölkerung zum Zwecke der Herstellung von Gesundheitskarten aus Plastik in das Vereinigte Königreich, da dieses zu dem Zeitpunkt noch über keine Datenschutzregelungen verfügte (Bignami 2005, 844). Deutlich mehr Aufmerksamkeit erhielt hingegen die Entscheidung der französischen CNIL im Juli 1989, den

84 Entgegen etwa jenen primär im Dienste ihrer jeweiligen Regierungen stehenden Individuen, die in den beratenden Ausschuss berufen wurden, der im Zuge der Unterzeichnung der Datenschutz-Konvention des Europarats gegründet worden war (Simitis u. a. 2019, 187 f., Rn. 110).

85 Die erste der seither jährlich stattfindenden „Internationalen Konferenz der Datenschutzbeauftragten" fand 1979 in Bonn statt (ICDPPC 2017).

86 Belgien, Griechenland, Italien, Portugal und Spanien. Das Scheitern der Datenschutz-Konvention wurde besonders gut am Beispiel Spaniens deutlich: Trotz der Unterzeichnung der Konvention im Jahr 1982 sowie ihrer Ratifizierung im Jahr 1984 verfügte das Land 1990 noch immer über kein Datenschutzgesetz.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

EG-Mitglieder (Stand: 1990)	DS-Gesetze vorhanden (Stand 1990)	Datenschutz-Konvention …		
		… unterzeichnet	… ratifiziert	… als Gesetz in Kraft getreten
Belgien	Nein	07.05.1982	28.05.1993	01.09.1993
BRD	Ja	28.01.1981	19.06.1985	01.10.1985
Dänemark	Ja	28.01.1981	23.10.1989	01.02.1990
Frankreich	Ja	28.01.1981	24.03.1983	01.10.1985
Griechenland	Nein	17.02.1983	11.08.1995	01.12.1995
Irland	Ja	18.12.1986	25.04.1990	01.08.1990
Italien	Nein	02.02.1983	29.03.1997	01.07.1997
Luxemburg	Ja	28.01.1981	10.02.1988	01.06.1988
Niederlande	Ja	21.01.1993	24.08.1993	01.12.1993
Portugal	Nein	14.05.1981	02.09.1993	01.01.1994
Spanien	Nein	28.01.1982	31.01.1984	01.10.1985
Verein. Kön.	Ja	14.05.1981	26.08.1987	01.12.1987
Neue EG-Mitglieder (seit 1.1. 1995)	**DS-Gesetze vorhanden (Stand 1990)**	**Datenschutz-Konvention …**		
		… unterzeichnet	**… ratifiziert**	**… als Gesetz in Kraft getreten**
Finnland	Nein	10.04.1991	02.12.1991	01.04.1992
Österreich	Ja	28.01.1981	30.03.1988	01.07.1988
Schweden	Ja	28.01.1981	29.09.1982	01.10.1985

Tabelle 3-1: Datenschutzgesetze und Umsetzung der der Datenschutz-Konvention in den EG-Mitgliedstaaten und Beitrittskandidaten im Jahr 1990 (eigene Zusammenstellung)

Datentransfer von Beschäftigtendaten der französischen Fiat-Tochter an das italienische Mutterunternehmen zu stoppen, weil Italien zu diesem Zeitpunkt noch immer über keine Datenschutzregelungen verfügte. Der Transfer durfte nach mehreren Wochen des Haderns letzten Endes erst dann stattfinden, als beide Fiat-Stellen einen Vertrag unterzeichnet hatten, in dem sie sich zur Einhaltung der französischen Datenschutzregelungen verpflichteten (Schwartz 1994, 491 f.). Zudem modifizierte das Netzwerk der Aufsichtsbehörden gegen Ende der 1980er-Jahre auch die Rahmung des Themas: Waren zuvor vor allem menschenrechtliche Erwägungsgründe in den Vordergrund gestellt worden, bemühte man sich fortan, die Existenz von Datenschutzregeln als eine Vorbedingung für die erfolgreiche administrative und Binnenmarktintegration in der Europäischen Gemeinschaft zu definieren (A. L. Newman 2008a, 113). So etwa in der Resolution der inter-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nationalen Konferenz der Datenschutzbeauftragten des Jahres 1989, in der die Kommission und Mitgliedstaaten zu supranationalem Handeln aufgefordert wurden (ICDPPC 1989). Angesichts der anhaltenden Untätigkeit von Kommission und Mitgliedstaaten drohten die Datenschutzbeauftragten bei einem weiteren Zusammentreffen im März 1990 schließlich damit, grenzüberschreitende Datentransfers in die fünf EG-Mitgliedsstaaten ohne Datenschutzgesetze vollständig zu unterbinden, sollten bis zur Vollendung des Binnenmarktes im Jahre 1992 keine gemeinschaftlichen und gleichwertigen Datenschutzstandards existieren. Der einige Monate zuvor gestoppte Datentransfer zwischen der französischen Fiat-Zweigstelle und dem italienischen Mutterkonzern – neben weiteren, vergleichbaren Transfer-Verboten – demonstrierte, dass die Behörden ihren Worten auch Taten folgen lassen würden (A. L. Newman 2008a, 114 f.).

Zweitens fanden, zusammenhängend mit dem ersten Grund, vertragsrechtliche Verschiebungen auf oberster EG-Ebene statt, die auch für den Datenschutz folgenreich sein sollten. Bereits seit den 1970er-Jahren wurde die intergouvernementale Kooperation im, zur damaligen Zeit noch nicht vergemeinschafteten Bereich Justiz und Inneres vorangetrieben (González Fuster 2014, 122 f.). Das wichtigste Ergebnis dieser Kooperation der Mitgliedstaaten war die Unterzeichnung der *Schengener Abkommen zur Abschaffung der stationären Grenzkontrollen* und weiterer Folgeabkommen zwischen den EG-Mitgliedstaaten[87] seit Mitte 1985. Zum Zwecke der darin angestrebten Abschaffung der Binnengrenzen wurden Ausgleichsmaßnahmen vorgesehen, mit denen die innere Sicherheit trotz offener Binnengrenzen gewährleistet werden sollte. Das zentrale Element dieser Sicherheitsmaßnahmen war der Aufbau des Schengener Informationssystems (SIS), mit dem die grenzüberschreitende Kooperation der fünf Vertragsstaaten hinsichtlich der automatisierten Personen- und Sachfahndung im Rahmen eines vernetzten Datenbestandes eingerichtet wurde. Im Kontext der Errichtung dieses für damalige Verhältnisse gigantischen Datenverarbeitungssystems wurde Datenschutzfragen allerdings zunächst keine Beachtung geschenkt. Besonders problematisch war, dass mit Belgien ein Staat am SIS teilnehmen sollte, der noch immer keinerlei Datenschutzgesetze verabschiedet hatte. Da die luxemburgische Datenschutzaufsichtsbehörde alleine nur wenig Handlungsmacht innehatte, setzte sie die Vertreter der

87 Zunächst zwischen der Bundesrepublik und Frankreich, gefolgt von Belgien, Luxemburg und den Niederlanden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

französischen und deutschen Aufsichtsbehörden auf der internationalen Konferenz der Datenschutzbeauftragten des Jahres 1988 schließlich über die Datenschutzgefahren des SIS im Zusammenhang mit der vertraglichen Einbindung Belgiens in Kenntnis. Gemeinsam traten die französischen, deutschen und luxemburgischen Vertreter in der Folge an die für das SIS zuständigen Stellen heran und teilten diesen mit, dass das SIS in seiner vorgesehenen Form gegen geltendes nationales Datenschutzrecht verstoße. Die Verhandlungen gerieten daraufhin ins Stocken, bis einige, am – verglichen mit den geltenden Datenschutzregelungen jener Staaten – niedrigen Schutzlevel der Datenschutz-Konvention des Europarats orientierte, Datenschutzvorkehrungen implementiert wurden.[88] Belgien musste sich zudem verpflichten, schnellstmöglich Datenschutzgesetze zu erlassen und eine Aufsichtsinstanz über das SIS ins Leben zu rufen (A. L. Newman 2008a, 115; Simitis 1995, 453).

Neben der intergouvernementalen Kooperation im Kontext der Schengener Abkommen intensivierte sich auch die Europäische Integration auf Gemeinschaftsebene seit Mitte der 1980er-Jahre. Mit der Unterzeichnung der Einheitlichen Europäischen Akte (EEA) Anfang 1986 wurde ein Prozess der verstärkten Europäischen Integration eingeleitet, der seinen Höhepunkt in der Unterzeichnung des Maastrichter Vertrags Anfang 1992 fand und die Europäische Gemeinschaft von einer Wirtschaftsunion hin zu einer politischen Union transformierte.[89] Das Ziel eines gemeinsamen Binnenmarktes wurde somit um die Abschaffung der Binnengrenzen, den Aufbau einer Wirtschafts- und Währungsunion, die Anerkennung der Unionsbürgerschaft, die Förderung einer gemeinsamen Außen- und Sicherheitspolitik sowie die Entwicklung einer engen Zusammenarbeit in den Bereichen Justiz und Inneres erweitert (Europäische Gemeinschaften 1992, Titel I, Art. B). Die vorherigen Verpflichtungen hinsichtlich der Gewährleistung des

88 Wie Simitis berichtet, sei das Fehlen jeglicher Datenschutzvorkehrungen damit gerechtfertigt worden, dass die Autoren diese schlicht vergessen hätten (Simitis 1995, 453).

89 So äußerten die Vertragsstaaten im Rahmen der EEA erstmals ihre Entschlossenheit, „gemeinsam für die Demokratie einzutreten, wobei sie sich auf die in den Verfassungen und Gesetzen der Mitgliedstaaten, in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und der Europäischen Sozialcharta anerkannten Grundrechte, insbesondere Freiheit, Gleichheit und soziale Gerechtigkeit, stützen“ (Europäische Gemeinschaften 1987, 2). In den vorangegangenen Verträgen äußerten sich die Vertragsstaaten tatsächlich an keiner Stelle zum Thema der Grundrechte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

freien Warenverkehrs, der Freizügigkeit von Arbeitnehmern, von Dienstleistungen sowie von Kapital galten somit zwar immer noch, doch die neuerliche, ausdrückliche Verpflichtung der Gemeinschaft, die Grundrechte ihrer Bürgerinnen und Bürger zu achten, trat fortan in gleichwertiger Weise neben diese.[90] Diese Verschiebung fand zudem vor dem Hintergrund der anhaltend rasanten technologischen Entwicklungen auf dem Gebiet der Datenverarbeitung und den daraus resultierenden individuellen und gesellschaftlichen Gefährdungen statt (Simitis 2001, 104). Wohin diese Entwicklungen führen könnten, falls keine angemessenen Gegenmaßnahmen getroffen würden, hatte das deutsche Bundesverfassungsgericht in seinem Volkszählungsurteil aus dem Jahre 1983 bereits unmissverständlich klargestellt:

> *„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfG 1983 C II 1 a))*

Schließlich ging auch die Kommission dazu über, die vom Europäischen Parlament seit mehr als einem Jahrzehnt und von Datenschutzexperten seit dem ersten hessischen Datenschutzgesetz vertretene Position zu übernehmen, dass die Förderung der EG-weiten wirtschaftlichen Kooperation und der Schutz von Grundrechten nicht als Widerspruch, sondern als zwei Seiten einer Medaille anzusehen seien (Simitis 1995, 447 f.). Daneben setzte selbst der Europäische Rat auf seinem Straßburger Treffen Ende 1989 im Hinblick auf die Verwirklichung der EEA und angesiedelt unter dem Punkt „Freizügigkeit und Europa der Bürger“ erstmals die Zielmarke, dass bei der

90 „Die Union achtet die Grundrechte, wie sie in der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.“ (Europäische Gemeinschaften 1992, Titel I, Artikel F (2))

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

intergouvernementalen „Zusammenarbeit zwischen den Verwaltungen der Persönlichkeitsschutz bei der Benutzung von Datenbanken mit personenbezogenen Angaben sichergestellt wird" (Europäischer Rat 1989, 6).

Zwei Gründe führten somit in Kombination dazu, dass das zuständige Datenschutz-Referat in der Generaldirektion Binnenmarkt und gewerbliche Wirtschaft unter der Aufsicht von Kommissionsvizepräsident und Binnenmarkt-Kommissar Martin Bangemann (FDP) die Arbeiten an Gemeinschaftsregelungen zum Datenschutz aufnahm (Karaboga 2018, 138): Das kontinuierliche Lobbying des Netzwerks nationaler Aufsichtsbehörden und insb. ihre Drohung, den Transfer personenbezogener Daten in jene fünf EG-Mitgliedstaaten zu unterbinden, womit das Binnenmarktprojekt als Ganzes hätte gefährdet werden können, sowie vertragsrechtliche Entwicklungen hin zu einer intensivierten Europäischen Integration auch auf politischen Themenfeldern vor dem Hintergrund der wachsenden Gefährdungslage, denen sich Grundrechte gegenübersahen.

Am 18. Juli 1990 legte die Kommission schließlich ein Bündel an Vorschlägen zum Schutz personenbezogener Daten vor.[91] Als Hauptelement des Schutzes personenbezogener Daten wurde der auch als Rahmenrichtlinie bezeichnete erste Richtlinienvorschlag[92] der Kommission (die spätere DS-RL 95/46/EG) vorgesehen, der sich insbesondere auf die Art. 100a[93]

91 Eine *Mitteilung zum Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten und die Informationssicherheit*, in der die Erwägungsgründe für das Legislativbündel dargelegt wurden, ein *Richtlinienvorschlag zum Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten* (die spätere DS-RL), ein *Richtlinienvorschlag zum Schutz personenbezogener Daten und der Privatheit im Telekommunikationsbereich* (die spätere ISDN-RL), einen *Entwurf einer Ministerratsentschließung zur Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze auch auf jene Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich, die nicht vom Gemeinschaftsbereich abgedeckt sind* (also insb. im Feld Justiz und Inneres), eine *Erklärung zur Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze innerhalb der Gemeinschaftsorgane und –Einrichtungen*, eine *Empfehlung für einen Ministerratsbeschluss zur Aufnahme von Verhandlungen über den Beitritt der Europäischen Gemeinschaft zur Datenschutz-Konvention des Europarats* sowie ein *Vorschlag für einen Ministerratsbeschluss im Bereich der Informationssicherheit* (COM 1990).

92 Sofern im Folgenden vom Richtlinienvorschlag, Richtlinienentwurf oder Kommissionsentwurf die Rede ist, beziehe ich mich damit, sofern nicht anderweitig spezifiziert, auf diesen ersten Rahmenrichtlinienvorschlag der Kommission.

93 Abs. 1 des Art. 100a EWG-Vertrag (in der durch die EEA aktualisierten Fassung) besagt: „Soweit in diesem Vertrag nichts anderes bestimmt ist, gilt abweichend von Artikel 100 für die Verwirklichung der Ziele des Artikels 7a die nachstehende Regelung. Der Rat erläßt gemäß dem Verfahren des Artikels 189b und nach Anhörung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

und 113 des EWG-Vertrags stützte und mit dem das allgemeine Datenschutzniveau festgelegt und im Rahmen der weiteren legislativen Aktivitäten befolgt werden sollte. Gemäß dem Kooperationsverfahren[94] sieht das Prozedere vor, dass der Kommissionsentwurf zunächst an das Europäische Parlament versendet wird. Der Parlamentspräsident überweist den Vorschlag an den federführenden Ausschuss, der (je nach Notwendigkeit unter Einbezug weiterer Ausschüsse) eine Entschließung erarbeitet und dem Plenum des Parlaments vorlegt. Im Falle der Annahme durch das Plenum wird die Entschließung des Parlaments an den Rat überwiesen. Die zuständigen Vorbereitungsgremien des Rats bereiten parallel zur Parlamentsentschließung eine gemeinsame Ratsposition vor. Das Parlament kann den Kommissionsvorschlag bzw. den Gemeinsamen Standpunkt des Rates billigen oder in Form eines aufschiebenden Vetos den Rat in zweiter Lesung zu einem einstimmigen Beschluss zwingen. Die Kommission kann jedoch – auch dann, wenn die Ratsmeinung noch nicht feststeht – unter Verweis auf die Parlamentsmeinung einen geänderten Vorschlag erarbeiten und veröffentlichen (Wessels 2008, 344), wie dies etwa bei der Erarbeitung der DS-RL der Fall sein sollte. Dem Fahrplan der Kommission nach sollten die Verhandlungen bis zur Vollendung des EG-Binnenmarktes am 31. Dezember 1992 abgeschlossen werden. Nach ersten Diskussionen nahm das Europäische Parlament im März 1992 zu dem Richtlinienvorschlag der Kommission Stellung, billigte diesen allerdings nur vorbehaltlich der von ihm vorgeschlagenen, sehr weitgehenden Änderungswünsche, womit sich zugleich abzeichnete, dass eine Verabschiedung bis zur Binnenmarkt-Vollendung nicht mehr möglich sein würde (Hoon 1992). Aufbauend auf der Stellungnahme des Parlaments und weiterer, zwischenzeitlich erfolgter Konsultationen stellte die Kommission Ende November 1992 ihren geänderten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vor (KOM 1992). Nach einer längeren und hitzigen Verhandlungsphase

des Wirtschafts- und Sozialausschusses die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben." (Europäische Gemeinschaften 1987, 8, Art. 18)

94 Bei dem Kooperationsverfahren, das im Zuge der EEA eingeführt wurde, handelt es sich um das erste Verfahren, in dessen Rahmen dem Europäischen Parlament ein eigenständiges Veto-Recht zugesprochen wurde. Insbesondere bot es dem Parlament in Form eines suspensiven Vetos die Möglichkeit, den Rat, sollte er der Position des Parlaments nicht entgegenkommen, in zweiter Lesung zu einem einstimmigen Beschluss zu zwingen (Wessels 2008, 123, 344).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

im Ministerrat verabschiedete dieser seinen Gemeinsamen Standpunkt erst im April 1995 (Rat 1995). Das Parlament sprach dem Ministerrat seine Unterstützung zu und machte nur sieben kleinere Änderungsvorschläge (EP 1995), die alle vom Ministerrat angenommen wurden. Die Datenschutzrichtlinie 95/46/EG wurde schließlich am 24. Oktober 1995 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet und damit erfolgreich verabschiedet (EU 1995).

Die folgende Analyse der DS-RL konzentriert sich – wie auch die vorangegangenen Ausführungen zu den OECD-Richtlinien, der Datenschutz-Konvention und den ersten Bestrebungen auf Gemeinschaftsebene – auf die zentralen datenschutzpolitischen Konfliktlinien. Auf Basis einer Durchsicht der Sekundärliteratur unter Hinzuziehung von Primärdokumenten werden die jeweiligen Konflikte, und, so gut es geht, auch die beteiligten Akteure inkl. ihrer jeweiligen Positionen dargestellt sowie das Zustandekommen der Policy-Ergebnisse erklärt.

3.2.2.4 EG-Richtlinienvorschlag von 1990

3.2.2.4.1 Kontext

In der dem Richtlinienvorschlag vorangestellten Kommissionsmitteilung wurde dargelegt, dass die Kommission die anhaltenden mitgliedstaatlichen Divergenzen im Hinblick auf das datenschutzrechtliche Schutzniveau zum Anlass für die Legislativvorschläge nimmt, weil die Divergenz die weitere Europäische Integration gefährde (Commission of the European Communities 1990, 2, Nr. 1). Damit nahm die Kommission einerseits Bezug auf das Fehlen von Datenschutzregelungen in den genannten fünf Mitgliedstaaten und andererseits auf die bestehenden Unterschiede im Schutzniveau in den sieben Mitgliedstaaten, die bereits Datenschutzregelungen verabschiedet hatten. Zu diesen zählten die aus Kommissionsperspektive weiterhin ungeklärten Fragen im Hinblick auf: Den Anwendungsbereich (1. ob dieser nur automatisierte oder auch manuelle Verarbeitungen umfassen sollte, 2. ob Datenschutzregelungen in gleichem Maße den privaten wie den öffentlichen Sektor umfassen sollten und 3. ob ausschließlich natürliche Personen oder auch juristische Personen umfasst sein sollten), die institutionelle Aufsicht (ob das Model des Datenschutzbeauftragten wie etwa in Deutschland oder das Modell einer Aufsichtsbehörde wie der CNIL in Frankreich praktiziert werden sollte), Informationspflichten bei der Erhebung personenbezogener Daten oder auch im Hinblick auf besondere Kategorien per-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sonenbezogener Daten (Commission of the European Communities 1990a, 2, Nr. 2; Prisclla M. Regan 1993, 259).

Zwar hatte die Kommission bei der Ausgestaltung ihrer Regelungsvorschläge grundsätzlich freie Hand, doch wurde ihr Handlungsspielraum von zwei Faktoren entscheidend eingeengt: Zum einen bedeutete die Verpflichtung der Gemeinschaft auf den Schutz der Grundrechte für die Kommission, dass sie bei der Gestaltung des Schutzniveaus nicht frei, sondern – auch auf Grundlage des Art. 100a Abs. 3 EWG-Vertrag – an die Gewährleistung eines hohen Schutzniveaus gebunden war (S. 5, Nr. 10 und 11). Diese Verpflichtung auf den Schutz der Grundrechte hatte zur Folge, dass der angestrebte Schutz vor dem Hintergrund der Zunahme grenzüberschreitender Datenübertragungen nicht an den Grenzen der Gemeinschaft Halt machen durfte. In anderen Worten musste das anvisierte hohe Schutzniveau nicht nur bei jedem Datentransfer zwischen EG-Mitgliedstaaten, sondern auch bei jedem grenzüberschreitenden Datentransfer in Drittstaaten gewährleistet sein.[95] Zum anderen musste die Kommission bei der Ausgestaltung ihres Richtlinienvorschlags eine ausgewogene Balance zwischen den Rechtselementen aus den existierenden Datenschutzgesetzen der EG-Mitgliedstaaten herstellen. Das mitgliedstaatliche Interesse galt dabei freilich nicht der Erarbeitung von neuen Gemeinschaftsregelungen, sondern dem Erhalt der eigenen Regelungen. D. h., ein Mitgliedstaat war grundsätzlich nur dann mit der Harmonisierung einverstanden, wenn diese das Heben seiner Datenschutzkonzepte auf Unionsebene bedeutete. Allerdings garantierte auch die Inkorporation zentraler Bestandteile der Datenschutzregelungen eines Mitgliedstaates alleine nicht die Unterstützung des jeweiligen Mitgliedstaats, sofern andere, von diesem als ebenso zentral betrachtete Elemente nicht im Richtlinienvorschlag vorzufinden waren.[96] Diese, im politischen Pro-

95 Martin Bangemann verteidigte dieses Vorgehen der Kommission später vor dem Europäischen Parlament gegen die Kritik, dass die Regelungen zu streng und damit impraktikabel seien, folgendermaßen: „Wir haben nicht die bestehenden Vorschriften auf einen gemeinsamen Nenner bringen wollen. […] Die Kommission hätte ganz einfach sagen können: Wir suchen uns ein mittleres Niveau heraus und machen einen Katalog von vielen Ausnahmen, dann haben wir keine Probleme. Wir haben diesen Ansatz bewußt nicht gewählt, sondern wollten zunächst einmal zeigen, was prinzipiell notwendig ist, um die Privatsphäre der einzelnen zu schützen. […] Aber wenn man nicht von klaren Prinzipien ausgegangen wäre, hätte man am Schluß einen ‚Flekkerlteppich' gehabt und im Prinzip gar nichts erreicht. Deswegen haben wir eine, wie ich zugebe, ambitiöse Vorlage gemacht […]." (EP 1992b, 23)

96 Obwohl die Kommission sich in ihrem 1990er-Richtlinienvorschlag stark am deutschen Datenschutzrecht orientierte (was freilich zu heftiger Kritik der anderen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zess der EU angelegte, inhärente Notwendigkeit zur Kompromissfindung erschwerte wiederum die Herstellung eines hohen Schutzniveaus – weil die Kommission auch jenen Staaten mit einem niedrigeren Datenschutzniveau entgegenkommen musste, indem Elemente ihrer Regelungsmodelle übernommen wurden, um sich ihrer Unterstützung sicher zu sein.

3.2.2.4.2 Grundsätzliche Konfliktlinien

Bei der Erarbeitung der Vorschläge hatte die Kommission eine technokratische Strategie verfolgt. Neben den jeweiligen Kommissionsverantwortlichen hatte sie ausschließlich einige wenige Vertreter nationaler – darunter offenbar vor allem deutscher – Aufsichtsbehörden konsultiert. Akteure aus der Zivilgesellschaft[97], der Wirtschaft oder den Regierungen der Mitgliedstaaten wurden dagegen gar nicht involviert. Entsprechend überrascht waren die meisten Beobachter über die Kommissionsvorschläge. Nachdem europäische Wirtschaftsvertreter bereits in der Vergangenheit ihr Desinteresse an harmonisierten Datenschutzregelungen zum Ausdruck gebracht hatten,[98] fühlten sie sich vom Kommissionsvorschlag in besonderem Maße

Mitgliedstaaten führte), wurde der Vorschlag seitens der deutschen Ratsdelegation nicht in besonderem Maße unterstützt. Stattdessen übte die Bundesrepublik Druck auf die Kommission aus, damit im Zuge der Überarbeitung des Vorschlags weitere Bestandteile des deutschen Datenschutzrechts, etwa das Konzept des betrieblichen Datenschutzbeauftragten, in die finale Richtlinie aufgenommen werden (Simitis 1995, 450).

97 Wobei anzumerken ist, dass die im Bereich der Datenschutzpolitik zu dieser Zeit bereits tätigen europäischen NGOs noch vergleichsweise jung waren. Die *Deutsche Vereinigung für Datenschutz e. V.* (DVD) sowie die *Gesellschaft für Datenschutz und Datensicherheit e. V.* (GDD) wurden beide 1977, der *Chaos Computer Club e. V.* (CCC) 1981, das *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.* (FIfF) 1984 und der *Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. FoeBuD* (heute: Digitalcourage e. V.) 1987 gegründet. Andere Organisationen folgten teils deutlich später: das britische *Privacy International* (1990), das niederländische *Bits of Freedom* (2000), das französische *La Quadrature du Net* (2008), Die internationale Vereinigung der nationalen Organisationen *European Digital Rights* (EDRi) wurde 2002 gegründet (vgl. auch Unterabschnitt 3.4.2.3.1).

98 Vgl. diesbezüglich beispielsweise die von Newman zitierten Aussagen des Vorsitzenden des Bundesverbands der Deutschen Industrie (BDI), Friedrich Kretschmer, aus dem Jahr 1989, in denen dieser trotz der durch fehlende Harmonisierung entstehenden Wettbewerbsverzerrungen keine Notwendigkeit für eine Harmonisierung erkennt (A. L. Newman 2008a, 112).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

überrumpelt (A. Newman 2007b, 4 f.). Zudem störten sich gerade Großbritannien und Frankreich am Richtlinienentwurf der Kommission, da sie darin zu wenige ihrer eigenen Datenschutz-Elemente vorfanden und die starke Anlehnung an deutsches Datenschutzrecht bemängelten (Bainbridge 1996, 25). Besonders dem Vereinigten Königreich, Irland, Dänemark und den Niederlanden (der sog. nördliche Block) widerstrebte der Gedanke der supranationalen Regulierung und Harmonisierung ihrer Datenschutzregelungen auf der Ebene der Europäischen Gemeinschaften grundsätzlich. Der nördliche Block vertrat die Auffassung, dass die Ratifizierung der Datenschutz-Konvention des Europarats ein ausreichendes Schutzniveau bieten würde, während es zugleich den Mitgliedstaaten größeren Freiraum bei der Gestaltung der Regelungen überlasse (Bignami 2005, 840 f. Pearce und Platten 1998, 533 f.). Der südliche Block, bestehend aus Italien, Belgien, Spanien, Luxemburg und Frankreich, war dagegen deutlich positiver gegenüber einer Gemeinschaftsregelung zum Datenschutz eingestellt (ebd.). Sie kritisierten einzelne Elemente des Richtlinienvorschlags, jedoch nicht die Notwendigkeit einer Regelung als solche (Bainbridge 1996, 25). Deutschland, das sich in den vorangegangenen Jahren ablehnend gegenüber europäischen Datenschutzregelungen gezeigt hatte (A. L. Newman 2008a, 111), konnte sich – trotz weiterhin geäußerter Kritik – aufgrund des starken Einbezugs deutscher Regelungen[99] mit dem Richtlinienvorschlag immerhin arrangieren (Pearce und Platten 1998, 534). Spanien hingegen schloss sich der Kritik des nördlichen Blocks am Einbezug der manuellen Verarbeitung an (Bignami 2005, 840 f.). Diese und viele weitere Fragen und Probleme waren Gegenstand zahlreicher Auseinandersetzungen, die sich Kommission, Parlament, Rat, Wirtschafts- sowie Aufsichtsbehördenvertreter in den folgenden Jahren liefern sollten. Das Parlament beauftragte den Ausschuss für Recht und Bürgerrechte mit der Erarbeitung einer Stellungnahme. Der Labour-stämmige britische Europaabgeordnete Geoffrey Hoon wurde zum Parlamentsrapporteur gewählt. Der fertige, sog. Hoon-Bericht lag Ende 1991 vor und wurde am 11. März 1992 vom Europäischen Parlament in erster Lesung nahezu einstimmig gebilligt (EP 1992a; Hoon 1992). Schon damals war die Rede von massivem Lobbying (Trubow 1992, 173) von mehr als einhundert Unternehmen und Verbänden (Priscilla M.

99 So etwa die Trennung der Regelungen für den öffentlichen und nicht-öffentlichen Bereich sowie die zentrale Stellung der Einwilligung, insb. dass ihre Einholung konkret und ausdrücklich zu erfolgen habe (Simitis 2001, 129).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Regan 1999, 207), das allerdings seitens Hoon selbst nicht problematisiert, sondern eher sogar positiv aufgenommen wurde (EP 1992b, 16 f.).

Schon bei der Aushandlung der DS-RL zeigte sich, wie stark umstritten das Thema Datenschutz war. Im folgenden Unterabschnitt werden die wichtigsten dieser Auseinandersetzungen und Konfliktlinien vorgestellt.

3.2.2.4.3 Konkrete Konflikte

Zu einer der zentralen Auseinandersetzungen während der Erarbeitung der DS-RL zählt der Konflikt um den Einbezug der manuellen Verarbeitung. Über die 1970er-Jahre hinweg[100] bis hin zur Datenschutz-Konvention des Europarats war die Vorstellung vorherrschend gewesen, dass eine Gefahr des Missbrauchs personenbezogener Daten vor allem im Kontext automatisierter Verarbeitungen bestand und dass automatisierte und manuelle Verarbeitungsweisen klar voneinander getrennt werden könnten. Wie die Verarbeitung personenbezogener Daten im Polizei- oder Beschäftigtenbereich jedoch im Laufe der Jahre verdeutlichten, trafen beide Annahmen nicht (mehr) zu. Manuell gelagerte Daten wurden digitalisiert und digital gespeicherte Daten zugleich auch manuell verarbeitet, sodass eine sinnvolle Grenzziehung zwischen beiden Bereichen zunehmend unrealistischer und schwieriger wurde (Simitis 2001, 125). Daher ging der Richtlinienvorschlag an diesem Punkt über die Datenschutz-Konvention des Europarats und die auf der Konvention basierenden nationalen Datenschutzgesetze der im nördlichen Block vereinigten Mitgliedstaaten hinaus und sah die Anwendung der Richtlinie sowohl auf automatisierte als auch auf manuelle Dateien mit personenbezogenen Daten vor. Die Staaten des nördlichen Blocks beharrten allerdings weiterhin auf der Position, dass Datenschutzregelungen im Kontext der aufkeimenden Informationstechnologien deshalb notwendig wurden, da die automatisierte Verarbeitung spezifische Risiken für die Privatheit von Betroffenen berge und die Regulierung auch der manuellen Verarbeitung die administrative wie wirtschaftliche Effizienz der Mitgliedstaaten zu behindern drohte (Council of the European Communities 1991). Der diesbezügliche Streit im Ministerrat stellte dann auch einen der Gründe dar, weshalb sich die Festlegung des Ministerrats auf

100 So etwa im Rahmen des Hessischen Landesdatenschutzgesetzes aus dem Jahr 1970 oder des schwedischen Datenschutzgesetzes aus dem Jahr 1973 (Simitis u. a. 2019, 161, Rn. 6 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

eine gemeinsame Position enorm verzögerte (Simitis 1995, 465). Das Parlament unterstützte zwar den Vorschlag der Kommission, doch wurde am Richtlinienentwurf bemängelt, dass von Dateien und nicht von Daten die Rede war.[101] Entsprechend war eine der zwei zentralen Forderungen des Parlaments (EP 1992b, 16) die Ersetzung der Bezugnahme auf Dateien durch den schlichten Bezug auf die Verarbeitung personenbezogener Daten (Hoon 1992, siehe z. B. Änderung Nr. 10).

Darüber hinaus erstreckte sich der Richtlinienvorschlag, ebenso wie die OECD-Richtlinien und die Datenschutz-Konvention, zwar sowohl auf den nicht-öffentlichen als auch auf den vergemeinschafteten öffentlichen Bereich und überlies den Mitgliedstaaten in dieser Hinsicht keinen nationalen Freiraum. In Anlehnung an das damalige deutsche Recht wurden allerdings die für beide Bereiche vorgesehenen Regelungen nicht gemeinsam, sondern in unterschiedlichen Artikeln behandelt.[102] Auf Seiten der Mitgliedstaaten wurde die vorgesehene Aufspaltung der Regelungen insbesondere von Frankreich und Luxemburg kritisiert (Council of the European Communities 1991, 9, 16). Die Streichung der Unterscheidung von öffentlichem und privatem Sektor bildete sodann auch die zweite zentrale Forderung des Parlaments (EP 1992b, 16 f.).

Ein weiterer Konflikt entbrannte um die Ausweitung des Anwendungsbereichs der vorgeschlagenen DS-RL auf die nicht vom Gemeinschaftsrecht abgedeckten Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich. Wie schon zuvor im Falle des SIS offenbarten die Mitgliedstaaten keinerlei Interesse an einem hohen Datenschutzniveau bei sicherheitsrelevanten Verarbeitungen (Simitis 2001, 115 f.). Insbesondere Frankreich und Großbritannien wehrten sich vehement gegen den Vorschlag der Kommission (Simitis 1995, 454), der lediglich auf Seiten der Datenschutzaufsichtsbehörden explizite Unterstützung fand (vgl. etwa Deutscher Bundestag 1991, 87 Nr. 28). In der Folge bewirkten die Mitgliedstaaten die Aufnahme von Art. 3 (2) Satz 1 in den Richtlinientext, mit dem die Ausklammerung aller Tätigkeiten aus dem Anwendungsbereich der Richtlinie unmissverständlich klargestellt wird, die nicht in den Anwendungsbe-

101 Diese Einschätzung wurde auch von den Datenschutzaufsichtsbehörden geteilt, da die Beschränkung auf Dateien sowohl „technisch überholt als auch Anlass zu einer Fülle von Interpretationsproblemen [sei]“ (Deutscher Bundestag 1991, 107 IV. Nr. 1).

102 So waren die entsprechenden Regelungen aufgeteilt in ein Kapitel II „Rechtmässigkeit der Verarbeitung im öffentlichen Bereich“ und ein Kapitel III „Zulässigkeit der Verarbeitung im privaten Bereich“ (KOM 1990).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

reich des Gemeinschaftsrechts fallen, also „Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich“ (Art. 3 (2) DS-RL). Aus einer rein formellen Argumentation heraus, konnten die Mitgliedstaaten sich darauf beziehen, dass die DS-RL sich freilich nur auf jene Gemeinschaftsbereiche beziehen konnte, die von ihrer Rechtsgrundlage (Art. 100a und 113 des EWG-Vertrags) auch tatsächlich abgedeckt wurden. Dennoch war diese Ausklammerung höchst problematisch, waren die ersten Datenschutzgesetze doch vor allem ein Instrument zur Einhegung der wachsenden staatlichen Datenmacht. So hätten die Mitgliedstaaten durchaus die Möglichkeit gehabt, die Anwendbarkeit der Gemeinschaftsprinzipien zum Datenschutz auf die nicht-vergemeinschafteten Bereiche im Rahmen einer intergouvernementalen Vereinbarung zu gewährleisten. Später verabschiedete intergouvernementale Regelungen[103] offenbarten schließlich, dass die Mitgliedstaaten mehr Interesse an möglichst großen nationalen Spielräumen hatten als an einem gleichwertigen und hohen Schutz personenbezogener Daten in allen Rechtsbereichen (Simitis 2001, 117 f.). Entsprechend stellte Simitis fest: “In sum, what characterizes once more the Council's debates is not so much the readiness to engage in a racing to the top, in other words in a common effort to strive in the interest of the data subjects for the best possible protection, but rather to favor a racing to the bottom.” (Simitis 1995, 455)

Die Forderung nach mehr nationalen Freiräumen bei der Umsetzung war allerdings eine Forderung die sich nicht allein auf den nicht-vergemeinschafteten öffentlichen Bereich bezog, sondern im Hinblick auf verschiedene Elemente der DS-RL geäußert wurde. So plädierten einzelne Mitgliedstaaten, sofern sie mit einzelnen Regelungen nicht einverstanden waren, häufig für die Ausweitung der nationalen Freiräume bei der Umsetzung der unliebsamen Vorgaben, wie etwa im Falle des Einbezugs der manuellen Verarbeitung (Simitis 1995, 465). Weitere nationale Freiräume wurden allerdings aus unterschiedlichen Gründen auch seitens der Wirtschaft[104] und der nationalen Datenschutzaufsichtsbehörden gefordert. Während die Wirtschaft mittels der Befürwortung nationaler Freiräume

103 Vgl. hier etwa die im Juli 1995 unterzeichnete EUROPOL-Konvention, die u. a. elementare Betroffenenrechte nicht mit einschließt und somit nicht ansatzweise das in der DS-RL festgelegte Datenschutzniveau gewährleistet (H. Busch 1996).

104 Unter den Wirtschaftsvertretern, die sich zur Richtlinienentwurf äußerten, befanden sich bereits mehrere Akteure, die zu festen Größen des EU-Datenschutz-Sub-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Umsetzungskosten der Richtlinie zu senken hoffte, indem der jeweilige Staat zuvor geltende Regelungen so weit wie möglich beibehält (A. L. Newman 2008b, 117), erhofften sich die Aufsichtsbehörden mehr Gestaltungsspielraum in Hinblick auf die Fortentwicklung der Datenschutzregelungen und damit auch die Möglichkeit der Anhebung des Schutzniveaus in ihrem Land (Deutscher Bundestag 1991, 107 II. A. L. Newman 2008b, 117).

Ein Vorschlag der Kommission hätte in dieser Hinsicht Vereinfachungen mit sich gebracht, war allerdings seinerseits hoch umstritten: So hatte die Kommission für sich weitgehende Rechtsetzungsbefugnisse im Hinblick auf die „für die Anwendung dieser Richtlinie auf die Besonderheiten bestimmter Bereiche erforderlichen Maßnahmen" vorgesehen (Art. 29 DS-RL-E). Dabei sollte die Kommission von einem beratenden Ausschuss bestehend aus Vertretern der Mitgliedstaaten unterstützt werden (Art. 30 DS-RL-E). Die Empfehlungen des Ausschusses sollten jedoch nicht bindend sein, sondern von der Kommission lediglich „soweit wie möglich" (ebd.) berücksichtigt werden. Wäre dieser Kommissionsvorschlag erfolgreich gewesen, hätte die Kommission die Befugnis gehabt, jegliche Details der Richtlinie unter Verweis auf ihre Anwendungsrelevanz, also etwa die Harmonisierung der Informations- und Meldepflichten usw. – unter weitgehender Übergehung nationaler Standpunkte – im Alleingang zu regulieren. Wie, angesichts der Zurückhaltung, die die Mitgliedstaaten im Hinblick auf die Harmonisierung ihrer Datenschutzregelungen in den vorangegangenen Jahrzehnten gezeigt hatten, zu erwarten war, zeigten sich die Mitgliedstaaten – in ansonsten ungewohnter Einigkeit – nicht mit dem Vorschlag der Kommission einverstanden. Insbesondere der beratende Charakter des Ausschusses stieß dabei auf Widerstand (Bignami 2005, 838 f.). Schließlich stand das Parlament auch in dieser Frage auf Seiten des Ministerrats und forderte im Hoon-Bericht die vollständige Streichung des betreffenden Artikels (Hoon 1992, 197, Änderung Nr. 94).

Zugleich traten Datenschutzaufsichtsbehörden wie auch das Parlament gemeinsam für eine Stärkung der europäischen Datenschutzinstanz (also der späteren Art. 29-Datenschutzgruppe). Während die Aufsichtsbehörden dafür warben, dass der Vorsitz nicht von einem Kommissionsvertreter,

systems werden sollten und die Jahre später bei den DSGVO-Verhandlungen mitwirkten. Diese sind: Die *Federation of European Direct Marketing* (FEDIM) und *European Direct Marketing Association* (EDMA), die 1997 zur *Federation of European Direct Marketing Association* (*FEDMA*) fusionierten, die *International Chamber of Commerce* (ICC), die *Union of Industrial and Employers' Confederations of Europe* (UNICE), die Im Jahr 2007 in *Businesseurope* umbenannt wurde).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sondern von einem gewählten Mitglied aus dem Kreis der Datenschutzaufsichtsbehörden übernommen wird (Deutscher Bundestag 1991, 108 Nr. 6), ging das Parlament mit seinem Vorschlag deutlich weiter und warb für die Ausstattung der Gruppe mit weitereichenden Vollmachten sowie die Aufnahme von Vertretern aus Gewerkschaften, Arbeitgeberverbänden und Bürgerrechtsgruppen in den Ausschuss (Hoon 1992, 90 und 93, Änderungen Nr. 88 und 128).

Schließlich stieß auch das von der Kommission vorgeschlagene hohe Schutzniveau auf einen breiten Widerstand. Sowohl Ministerrat als auch die Wirtschaft und selbst das Parlament empfanden den Richtlinienvorschlag als zu restriktiv (A. L. Newman 2008b; Pearce und Platten 1998; Priscilla M. Regan 1999; Simitis 2001).[105] Einzig die Aufsichtsbehörden begrüßten – unter Verweis auf die gleichzeitige Beibehaltung nationaler Freiräume – das angestrebte hohe Schutzniveau (Deutscher Bundestag 1991, 107 II.).

Im Zentrum der Kritik der Wirtschaftsvertreter standen die Mehrkosten, die sie bei der Umsetzung der Vorgaben des Richtlinienentwurfs befürchteten (Priscilla M. Regan 1999, 201). Diese Kritik umfasste im Detail insbesondere die Vorgaben betreffend die Weitergabe personenbezogener Daten in Drittländer einerseits und das Erfordernis der Einholung einer ausdrücklichen Einwilligung des Betroffenen andererseits. Bezüglich der Datentransfers in Drittländer wurden – vor allem seitens transnational agierender, darunter vieler US-amerikanischer Unternehmen – die von der Kommission vorgesehenen Bestimmungen als zu restriktiv kritisiert (ebd.).

Obwohl sich seit den 1970er-Jahren für Drittstaatentransfers die Regelung durchgesetzt hatte, dass diese nur in Drittländer erfolgen durften, die ein gleichwertiges Datenschutzniveau garantieren, wich die Kommission in ihrem 1990er-Richtlinienvorschlag von dem Gleichwertigkeitserfordernis ab. Stattdessen sollte bereits ein sog. *angemessenes* Datenschutzniveau im Zielland ausreichend sein. Dieser Wandel hatte laut Simitis zwei Ursachen: Zum einen wollte sich die Europäische Gemeinschaft damit gegen den Vorwurf wehren, man zwinge die eigenen Standards Drittstaaten auf. Zum anderen sollte das Angemessenheitserfordernis die neuerliche Flexibilität der Drittstaatentransfer-Regelungen hinsichtlich der Bewertung der Angemessenheit demonstrieren (Simitis 2001, 118 ff.). Trotz der Erleichterung auf Seiten der Wirtschaft, dass das Gleichwertigkeitserfordernis verworfen

105 Hoon interpretierte den Versuch der Kommission, ein *sehr hohes Schutzniveau* zu etablieren, sogar dahingehend, dass versucht werde, die Gesetze „in praktisch allen Mitgliedstaaten zu revolutionieren" (S. 16).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wurde, wurden die Kommissionsvorschläge – insbesondere seitens transnational agierender, darunter vieler US-amerikanischer Unternehmen – immer noch als zu restriktiv wahrgenommen (Priscilla M. Regan 1999, 201). So sah Art. 24 des Richtlinienvorschlags die rechtmäßige Weitergabe nur dann vor, sofern das Zielland ein *angemessenes* Datenschutzniveau, das diesem zuvor seitens der Kommission bescheinigt wurde, gewährleisten konnte. Während die Aufsichtsbehörden daran bemängelten, dass das Schutzniveau im Zielland gleichwertig und nicht nur angemessen sein sollte (Deutscher Bundestag 1991, 107 IV. Nr. 5), bemängelten Wirtschaftsvertreter das Fehlen von Sonder- bzw. Ausnahmeregelungen fernab der vorgesehenen Kommissionserlaubnis, die sie als zu starr interpretierten (Priscilla M. Regan 1999, 201). Tatsächlich sahen die Ausnahmebestimmungen des Art. 25 DS-RL-E vor, dass ein Mitgliedstaat von den Bestimmungen des Art. 24 abweichen konnte, nachdem dieser zuvor die Kommission und die übrigen Mitgliedstaaten über die geplante Ausnahmeregelung unterrichtet hatte und weder Kommission noch ein anderer Mitgliedstaat innerhalb von zehn Tagen Widerspruch eingelegt hatten, doch wurde auch diese Ausnahmeregelung als zu unflexibel kritisiert. Selbst das Parlament trat für die Erweiterung des Ermessensspielraums bei grenzüberschreitenden Datentransfers ein (EP 1992b, 17), insb. dafür, dass ein Transfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der ausdrücklichen Einwilligung des Betroffenen erfolgen konnte (Hoon 1992, 193, Änderungen Nr. 78 und 127).

Schließlich wurde die Verpflichtung zur Einholung einer ausdrücklichen Einwilligung (gem. Art. 12 und 17 DS-RL-E) seitens der Wirtschaftsvertreter dahingehend kritisiert, dass diese zu bürokratischen Komplikationen, Verzögerungen und Erschwerungen bei vielen Formen der ihrer Meinung nach unproblematischen Verarbeitung personenbezogener Daten führe, für die keine ausdrückliche Einwilligung vonnöten sei (Priscilla M. Regan 1999, 201 f.). Wirtschaftsvertreter aus informationsverarbeitenden Bereichen, insb. dem Direktmarketing sowie der Kreditvergabe (ebd.) einerseits und gemeinnützige und politische Organisationen andererseits teilten dabei die Befürchtung, dass die Erstellung von Listen mit personenbezogenen Daten durch die Einwilligungsverpflichtung praktisch unmöglich würde (EP 1992b, 17 und 19 f.).[106] Gemeinnützige Organisationen befürch-

106 Der Streit drehte sich insbesondere darum, wie die Einholung der Einwilligung zu realisieren sei, wenn selbst das erste Anschreiben zur Einholung der Einwilligung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

teten das Ende der Möglichkeit der Mittelakquise,[107] während beispielsweise der britische Direktmarketingverband auch mit der Verbesserung des Kundenwohls argumentierte, da trotz strengerer Datenschutzregelungen im Heimatland ein Deutscher durchschnittlich mehr Spam-Mails erhalten würde als ein Brite, in dessen Land weniger strenge Datenschutzvorgaben existierten (Priscilla M. Regan 1999, 209). Marktforschungs- und politische Meinungsforschungsunternehmen dagegen führten an, dass angesichts der strengen Vorgaben bezüglich der Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art 17 DS-RL-E selbst die Durchführung von Telefonumfragen nicht mehr möglich sein würde und das Opt-out-Modell daher gegenüber dem Opt-in-Modell zu bevorzugen sei (ebd.). In diesem Zusammenhang wurden auch die strengen Vorgaben hinsichtlich der Weiterverwendung bereits erhobener personenbezogener Daten zu anderen Zwecken als dem ursprünglichen Erhebungszweck, der gem. Art. 8 (2) DS-RL-E vorsah, dass jede Weitergabe mit dem Zweck der Datei vereinbar zu sein habe und andernfalls die ausdrückliche Einwilligung des Betroffenen einzuholen sei. Die Kommission bezweckte mit dieser Vorgabe den entstehenden Handel mit personenbezogenen Daten (vor allem bei Daten-Brokern) zu begrenzen bzw. zumindest eine verbesserte Kontrolle durch die Betroffenen zu gewährleisten. Unterstützt wurden diese Vorschläge der Kommission lediglich seitens der Datenschutzbehörden (Deutscher Bundestag 1991, 88).

Das Parlament (und insb. dessen britische Abgeordnete) vertrat hingegen auch bei dieser Frage die Position, dass eine bessere Balance zwischen den Datenverarbeitungsbedürfnissen öffentlicher und nicht öffentlicher Stellen und dem Schutzbedürfnis der Betroffenen herzustellen notwendig sei, indem vor allem das Opt-out-Modell an die Stelle des Opt-in-Modells tritt (EP 1992b). Vorschläge in Richtung einer Stärkung des Datenschutzes konnten sich im Parlament dagegen nicht durchsetzen. Die Forderung der deutschstämmigen Grünen Hiltrud Breyer etwa, dass der Betroffene das Recht auf den regelmäßigen Erhalt eines kostenlosen sog. Datenkontoauszugs erhalten sollte, in dem Auskunft über die bei einer verantwortlichen Stelle gespeicherten Daten gegeben wird, konnte sich nicht durchsetzen (EP 1992b, 22). Auch ihr Einwand, dass der Richtlinienentwurf nur indivi-

bereits gemäß dem Richtlinienvorschlag auf einer Einwilligung zu basieren habe (EP 1992b, 16 f.).

107 70 gemeinnützige britische Organisationen gründeten die gemeinsame Lobbying-Gruppe CHANGE (Charities and Non-profit Groups in Europe), mit der sie für flexiblere Regelungen eintraten (Priscilla M. Regan 1999, 210).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

duelle Rechte thematisiere und dass auch kollektive Rechte, etwa in Form eines Arbeitnehmer-Datenschutzes, Gegenstand der Richtlinie sein sollten, fand keinen weiteren Zuspruch (ebd.). Daneben fand auch die Forderung des französischstämmigen gaullistisch-konservativen Europaabgeordneten Jacques Vernier, dass nicht nur darüber diskutiert werden müsse, dass „die Datei angelegt und kontrolliert wurde, sondern auch zu welchem Zweck sie genutzt wird" (Parl-Debatte S. 20) nur geringen Widerhall im Parlament, etwa hinsichtlich kosmetischer Verbesserungen der Regelungen zu rechnergestützten Entscheidungen (Hoon-Bericht, vgl. Änderung Nr. 46).

3.2.2.5 Überarbeiteter Richtlinienvorschlag von 1992

Nachdem das Parlament seine Position auf Grundlage des Hoon-Berichts verabschiedet hatte, machte die Kommission von der Möglichkeit Gebrauch, ihren Richtlinienvorschlag zu überarbeiten. Dazu nahm sie in erster Linie auf die Parlamentsposition (COM 1992, 2), daneben aber auch auf die seitens der Mitgliedstaaten, der Wirtschaft und Datenschutzaufsichtsbehörden geäußerten Kritikpunkte Bezug. Zu den angehörten Wirtschaftsvertretern zählten: UNICE (heute bekannt als Businesseurope), the banking federation, CELD, FEWITA, GEDIS, European Federation for Direct Marketing, EAT, CHANGE (non-profit-Organisation), European Society for Opinion and Marketing Research, ACT, EPC, ENPA, CAEJ, EBU und FAEP (ebd., 129). Mit dem Inkrafttreten der Änderungen des Vertrags von Maastricht am 1.11.1993 war die Beschlussfassung gemäß Art. 189 b nunmehr im „Mitentscheidungsverfahren" vorgesehen, was aus dem Parlament und dem Ministerrat gleichberechtigte Mitgesetzgeber machte (EP 1993, 31; Souhrada-Kirchmayer 2010, 509).

3.2.2.5.1 Kontext: Zugeständnisse und Zurückweisungen der Kommission

Mit ihrem überarbeiteten Richtlinienvorschlag verfolgte die Kommission das Ziel, die Anleihen aus französischem, niederländischem und britischem Datenschutzrecht deutlicher sichtbar zu machen, um sich der Unterstützung dieser Länder zu vergewissern.[108] Daneben ordnete die Kommissi-

108 Insbesondere die CNIL war sehr daran interessiert, mehr Einfluss auf die Gestaltung der Richtlinie zu nehmen. Zu diesem Zweck entsandte sie Personal in die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

on die Textstruktur so um, dass die Bezüge auf die Datenschutz-Konvention des Europarats sichtbarer wurden (Pearce und Platten 1998, 533). Indem die Datenschutz-Prinzipien, die im ursprünglichen Richtlinienentwurf noch in der Mitte des Textes in Art. 16 untergebracht waren, nach Art. 6 vorgezogen wurden, machte die Kommission zunächst den Bezug auf die seit den 1970er-Jahren bestehenden und unverändert übernommenen Grundprinzipien des Datenschutzes deutlich (Bainbridge 1996, 25). In Bezug auf die Parlamentsposition wurden dessen zwei zentrale Forderungen erfüllt: Zum einen wurde die Aufspaltung der Regelungen in einen öffentlichen und einen nicht-öffentlichen Bereich aufgegeben und zum anderen wurde an die Stelle der Bezugnahme auf Dateien der Bezug auf die Verarbeitung personenbezogener Daten gesetzt (ebd.). Der französische Einfluss äußerte sich zum einen in der Einfügung der neuen Art. 15 DS-RL-ÜE (Betroffenenrecht auf Widerspruch) und Art. 16 (zu automatisierten Einzelentscheidungen).[109] Zudem erhielten die Aufsichtsbehörden in Art. 18 Abs. 4 die Befugnis, eine Verarbeitung, die hinsichtlich der Rechte und Freiheiten der Betroffenen besondere Risiken birgt, vor ihrer Durchführung prüfen zu können. Diese Verschärfung der Meldepflicht wurde wiederum in Art. 19 durch Vorgaben zur Vereinfachung und Befreiung von der Meldepflicht ergänzt, die seitens der Mitgliedstaaten für bestimmte Kategorien von Verarbeitungen, die die Rechte und Freiheiten der Betroffenen nicht beeinträchtigen, vorgesehen werden können.

Darüber hinaus wurden, in Anlehnung an das niederländische und britische Recht (Bainbridge 1996, 26) und wie zuvor seitens Großbritanniens und der Niederlande gefordert (Pearce und Platten 1998, 533), Elemente der Selbstregulierung in Form weitergehender Vorgaben zu Verhaltensregeln gestärkt. Während in Art. 20 des ursprünglichen Richtlinienentwurfs lediglich sehr abstrakte Aussagen zu europäischen Standes- oder Verhaltensregeln vorzufinden waren, widmete sich im überarbeiteten Entwurf je ein Artikel deutlich detaillierter nationalen (Art. 28) und gemeinschaftlichen Verhaltensregeln (Art. 29). Mit dem Entwurf von Verhaltensregeln durch Interessenverbände und durch deren Anerkennung seitens nationaler Aufsichtsbehörden im Falle mitgliedstaatlicher Verhaltensregeln oder durch die Kommission im Falle gemeinschaftlicher Verhaltensregeln sollte die

Kommission, um an der Überarbeitung des Richtlinienentwurfs unmittelbar mitzuarbeiten (Pearce und Platten 1998, 533).

109 Allerdings sei erwähnt, dass beide Artikel bereits weitgehend übereinstimmend in Art. 14 des ursprünglichen Richtlinienvorschlags unter „Ergänzende Rechte der betroffenen Person" enthalten waren (KOM 1990).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Spezifizierung der Vorgaben der Richtlinie im Hinblick auf die Besonderheiten bestimmter Wirtschaftsbereiche möglich werden, ohne dass weiteres staatliches Eingreifen nötig würde. Im Idealfall hätte die Erarbeitung branchenspezifischer Verhaltensregeln, so die Hoffnung der Kommission, bei neu auftretenden Gefahren für die Privatheit der Betroffenen, die nicht die Grundsätze des Datenschutzes tangieren, sondern lediglich branchenbezogene Spezifizierungen des in der Richtlinie festgelegten Schutzniveaus betreffen, weitere legislative Aktivitäten unnötig gemacht, weil die Unternehmen rechtzeitig freiwillige, angemessene Schutzstandards entwickelt hätten. Zudem wurde durch weitere Ergänzungen in Art. 18 DS-RL-ÜE versucht, dem vergleichsweise umfassenden Meldepflichtsystem des Vereinigten Königreichs mehr entgegenzukommen (Bainbridge 1996, 26).

Das Entgegenkommen gegenüber den Verarbeitern äußerte sich nicht zuletzt in der Änderung des Richtlinientitels. Spiegelte der Titel des ursprünglichen Richtlinienentwurfs noch die Intention der Kommission im Hinblick auf die Erreichung eines hohen Schutzniveaus wider, verdeutlichte der überarbeitete Titel den neuerlichen Drang auf die Bedürfnisse datenverarbeitender Stellen einzugehen und insbesondere deren Wunsch, Datenflüsse durch Datenschutzgesetzte nicht zu erschweren. So erhielt der ursprüngliche Titel, der schlicht den „Schutz bei der Verarbeitung personenbezogener Daten" vorsah, die Ergänzung „[…] Verarbeitung personenbezogener Daten *und zum freien Datenverkehr*" (Hervorhebung durch den Autor) (Simitis u. a. 2019, 194, Rn. 135).

Dem seitens der Aufsichtsbehörden geäußerten Wunsch nach der Erweiterung des aufsichtsbehördlichen Gestaltungsspielraums kam die Kommission nach, indem sowohl nationale Aufsichtsbehörden als auch die Datenschutzgruppe aufgewertet wurden. So wurde der die nationale Aufsichtsbehörde betreffende Art. 30 DS-RL-ÜE dahingehend geändert, dass in Abs. 1 die Unabhängigkeit der Behörde festgeschrieben wurde und in Abs. 2 Ts. 3 die Befugnisse der nationalen Behörden um die Befassung von Justizbehörden bei Verstößen gegen die Bestimmungen der Richtlinie erweitert wurden. Darüber hinaus wurde, dem Wunsch der Aufsichtsbehörden entsprechend, in Art. 31 Abs. 2 vorgesehen, dass der Vorsitz der Datenschutzgruppe nicht von einem Vertreter geführt, sondern mittels einer Wahl unter allen Gruppenmitgliedern ermittelt werden sollte. Außerdem wurde in Art. 32 Abs. 6 klargestellt, dass auch das Europäische Parlament in den Kreis der Adressaten des jährlichen Berichts der Datenschutzgruppe einbezogen sein sollte (Simitis u. a. 2019, 196, Rn. 144).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.2.2.5.2 Weiterhin bestehende und ungelöste grundsätzliche Konfliktlinien

Insgesamt wurde der überarbeitete Entwurf deutlich positiver aufgenommen als der ursprüngliche Entwurf. Gleichwohl konnten aber auch die Zugeständnisse der Kommission in ihrem überarbeiteten Richtlinienvorschlag letztlich nichts an der britischen und irischen Blockadehaltung gegenüber einer Gemeinschaftsregelung zum Datenschutz ändern. Die Ministerratsdelegationen beider Länder vertraten weiterhin die Position, dass die Ratifikation der Europaratskonvention ausreichend sei, um den freien Fluss personenbezogener Daten innerhalb der Gemeinschaft zu gewährleisten. Ähnliche Bedenken wurden auch von Dänemark geäußert. Insbesondere Großbritannien war zudem einerseits grundsätzlich nicht an weiteren Gemeinschaftsmaßnahmen interessiert, die Kosten für die britische Wirtschaft zu verursachen drohten und andererseits teilte man auch nicht dieselben Sorgen über die durch den Missbrauch personenbezogener Daten drohenden Privatheitsgefährdungen wie sie in den übrigen Mitgliedstaaten geäußert wurden (Pearce und Platten 1998, 534). Zwar wurden die neuen Kommissionsvorschläge zum Ausbau der Bedeutung selbstregulatorischer Maßnahmen in Form von Verhaltensregeln begrüßt, doch konnten sie letztlich nur unzureichend sein angesichts der britischen und irischen Maximalforderung nach einer weitgehenden Substitution der meisten verbindlichen Vorschriften des Richtlinienvorschlags durch freiwillige Selbstregulierungsmaßnahmen (Simitis 2001, 120).[110]

In den Niederlanden stieß der überarbeitete Richtlinienvorschlag immerhin auf geteiltes Echo (Pearce und Platten 1998, 535). Die Bundesrepublik hingegen zeigte sich im Ministerrat nur wenig erfreut darüber, dass der überarbeitete Richtlinienvorschlag nicht mehr ganz so deutlich dem deutschen Datenschutzrecht nachempfunden war. Beanstanded wurde die unterschiedslose Anwendung derselben Vorgaben auf den öffentlichen und nicht-öffentlichen Bereich, aber auch das fortdauernde Fehlen der Möglichkeit, unternehmensinterne Datenschutzbeauftragte einberufen zu können und weitere Vorbehalte in Bezug auf die aus deutscher Sicht noch immer nicht ausreichend flexible Meldepflicht und Sonderbehandlung sensibler

110 Zum Teil waren auch absurde Gerüchte über die möglichen Folgen der Richtlinie im Umlauf: Michael Forsyth, britischer Staatsminister im Innenministerium, war beispielsweise selbst nach Vorlage des überarbeiteten Richtlinienvorschlags im Jahr 1994 davon überzeugt, dass die DS-RL verbiete, dass er seiner Großmutter einen Überraschungsblumenstrauß zusende (Battcock 1995, 162).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

personenbezogener Daten sowie verfassungsrechtliche Bedenken im Hinblick auf die für die Aufsichtsbehörden vorgesehene Befugniserweiterung. Entsprechend befürwortete Deutschland weiterhin die Vorgaben des ursprünglichen Richtlinienvorschlags (Bainbridge 1996, 27). Deutschlands möglicher Wechsel in das Lager der Richtliniengegner war von entscheidender Bedeutung für die weiteren Verhandlungen, da das Gegner-Lager dadurch eine Sperrminorität erreicht hätte, mit der es den erfolgreichen Abschluss der Verhandlungen hätte verhindern können.[111]

Trotz des seitens der Kommission grundlegend überarbeiteten Richtlinienvorschlags waren die Staaten des südlichen Blocks, denen an einem erfolgreichen Abschluss der Verhandlungen gelegen war, somit gefordert, den Richtlinien-Gegnern weitere Konzessionen bei einer Reihe von Problemfeldern entgegenzubringen. Diese werden im Folgenden kurz umrissen.

3.2.2.5.3 Konkrete Konflikte und Pattsituation bedrohen erfolgreichen Abschluss der Verhandlungen

Durch die Richtlinie zu erwartende Mehrkosten

Die durch die Richtlinie befürchteten Mehrkosten bildeten einen zentralen, seitens Wirtschaftsvertretern geäußerten, Kritikpunkt. Entsprechend intensiv lobbyierten diese ihre eigenen Regierungen in Richtung der Ablehnung der Richtlinie oder zumindest flexiblerer Datenschutzregelungen, durch die sie sich geringere Implementierungskosten versprachen (vgl. z. B. Priscilla M. Regan 1999). So führte beispielsweise die Deutsche Gesellschaft für Datenschutz und Datensicherheit (GDD) im Jahr 1992 eine Befragung unter 255 Unternehmen (aus verschiedenen Branchen und unterschiedlicher Unternehmensgrößen) durch. Darin äußerten 91 Prozent der befragten Unternehmen ihre Ablehnung gegenüber dem Richtlinienvorschlag der Kommission mit der Begründung, dass dieser die Marktfragmentierung innerhalb Europas verschärfen würde (A. L. Newman 2008a, 112).

Eine vom britischen Innenministerium und eine vom Gesundheitsministerium initiierte Studie bekräftigten 1994 die Befürchtungen hinsichtlich drohender, überproportionaler Kosten. Auf Basis einer Umfrage unter

111 Ohne die 26 Stimmen der Richtlinien-Gegner kamen die Richtlinien-Befürworter nur noch auf 50 der benötigten 54 Stimmen für die Annahme von Legislativ-Vorschlägen der Kommission im Ministerrat, die gemäß dem qualifizierten Mehrheitswahlrecht zur damaligen Zeit nötig waren (vgl.: Tabelle 3-2).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

625 öffentlichen Einrichtungen, Unternehmen und gemeinnützigen Organisationen wurden die Implementierungskosten auf 2 Milliarden britische Pfund geschätzt. Die Kosten für den staatlichen Gesundheitssektor wurden gleichzeitig auf 1 Milliarde britische Pfund geschätzt. Lediglich das britische Oberhaus war grundsätzlich positiv gegenüber der Richtlinie gestimmt, forderte aber dennoch, dass dem Ministerrat vor ihrer endgültigen Abstimmung eine gründliche Kosten-Folgenabschätzung vorgelegt wird (Pearce und Platten 1998, 534).

Während die niederländische Handelskammer die Implementierungskosten der Richtlinie für die heimische Wirtschaft als gering einschätzte und sogar Potential für langfristige Effizienzsteigerungen erkannte, rechnete die Wirtschaftsauskunftei Bureau Krediet Registratie, verantwortlich für die Verarbeitung personenbezogener Daten für Darlehen und Kredite, zu befürchtende, erhebliche administrative und Personal-Mehrkosten im Falle der Verabschiedung der DS-RL aus. Das niederländische Justizministerium schloss sich der gemäßigt positiven Position der Handelskammer an. Das Wirtschaftsministerium initiierte dagegen eine eigene Befragung der heimischen Wirtschaft, deren Ergebnisse die datenschutzkritische Position der Wirtschaftsauskunftei untermauerten (Pearce und Platten 1998, 535).

Zudem kritisierten sowohl der europäische Dachverband EUROCHAMBRES (The Association of European Chambers of Commerce), der zu diesem Zeitpunkt 24 nationale Handelskammern mit insgesamt mehr als 13 Millionen Unternehmen vertrat, als auch die ICC (International Chamber of Commerce – Internationale Handelskammer) beide Richtlinienfassungen im Hinblick auf die bei der Umsetzung befürchteten exzessiven Kosten für die Wirtschaft (Priscilla M. Regan 1999, 211).

Transparenzvorgaben und Informationspflichten des Verantwortlichen

Die Direktmarketingbranche zeigte sich zwar erfreut über die im neuen Vorschlag erfolgte Klarstellung, Werbeansprachen auch ohne die vorherige Einwilligung der Betroffenen gemäß dem Opt-out-Prinzip durchführen zu können, doch beklagte man die als zu restriktiv und umfassend wahrgenommenen Transparenz- und Informationspflichten in jenen Fällen, in denen die personenbezogenen Daten aus öffentlich zugänglichen Quellen stammten (Bainbridge 1996, 28). Der Kritik an den zu restriktiven Transparenz- und Informationspflichten schlossen sich Deutschland, Irland, die Niederlande und das Vereinigte Königreich an (Bignami 2005, 841).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zweckbestimmung und ausdrückliche Einwilligung

Insbesondere die britische Direktmarketingbranche wandte sich sowohl gegen das Prinzip der Zweckbestimmung in Form der als zu eng kritisierten Bestimmungen hinsichtlich der Weiterverwendung zu anderen Zwecken als auch gegen die Verpflichtung, den Betroffenen die Möglichkeit zum Opt-out bieten zu müssen (Priscilla M. Regan 1999, 209). Vergleichbare Kritik kam auch aus dem Bereich der medizinischen, insbesondere der epidemiologischen Forschung. Deren Vertreter befürchteten, dass selbst die Vorgaben der überarbeiteten Richtlinienfassung die Weiterverwendung für andere Zwecke gesammelter personenbezogener Daten für medizinische Forschungszwecke unterbinden könnten. Kritisiert wurde insb. das Erfordernis, personenbezogene Daten nur bei Vorliegen der ausdrücklichen Einwilligung der Betroffenen für andere Zwecke weiterverwenden zu dürfen.[112] Vor allem die dänische Ministerratsdelegation war empfänglich für diese Kritik, sodass entsprechende Nachbesserungen des Richtlinientextes gefordert wurden (Bainbridge 1996, 28).

Vorgaben zum Datentransfer in Drittstaaten

In Reaktion auf die Kritik an den Drittstaatentransfer-Vorgaben des ursprünglichen Richtlinienvorschlags sah der überarbeitete Richtlinienentwurf in Art. 26 (1) nunmehr vor, dass ein Datentransfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der Einwilligung des Betroffenen, bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags und für die Wahrung eines wichtigen öffentlichen Interesses oder lebenswichtiger Interessen des Betroffenen erfolgen können sollte. Zudem wurden die bei der Angemessenheitsprüfung zu berücksichtigenden Faktoren in Art. 26 (2) dahingehend flexibilisiert, dass nicht nur die in dem betreffenden Drittland „geltenden allgemeinen oder sektoriellen gesetzlichen Bestimmungen", sondern auch die „dort beachteten Standesregeln" in Betracht gezogen werden sollten. Weitgehend unverändert blieben die Bestimmungen hinsichtlich Genehmigung eines Transfers seitens eines einzelnen Mitgliedstaates. Diese hingen letztlich immer noch davon ab, dass

112 Die Kritik berief sich unter anderem auf die negativen Erfahrungen, die bei der Einholung der Einwilligung bei Krebspatienten in Deutschland für ein Krebspatientenregister gemacht worden waren. Selbst zwanzig Jahre nach der Verpflichtung zur Einholung der ausdrücklichen Einwilligung gelang dies nur in 70% der Fälle, obwohl ein immenser administrativ-personeller Aufwand betrieben wurde. Für valide Aussagen müsse ein Register dagegen 90–95% aller Fälle umfassen (Vanchieri 1993, 1023).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

weder Kommission noch andere Mitgliedstaaten dem Transfer widersprachen. Im Streitfall wiederum sollte gemäß den ebenfalls weitgehend unveränderten Vorgaben zum beratenden Ausschuss in Art. 34 Abs. 2 DS-RL-ÜE immer noch die Kommission weitgehend autonom über geeignete Maßnahmen entscheiden. Entsprechend vehement wurden die Vorgaben zum Datentransfer in Drittstaaten von den Staaten des nördlichen Blocks (in diesem Fall das Vereinigte Königreich, Dänemark, Irland und Schweden, das aufgrund der bevorstehenden Aufnahme in die Gemeinschaft auch in die Verhandlungen zur DS-RL miteinbezogen wurde) abgelehnt (Bignami 2005, 841). Und auch seitens der Wirtschaft wurden die Konzessionen der Kommission als unzureichend kritisiert (Priscilla M. Regan 1999, 201). Die ICC vertrat zudem die Position, dass unternehmens- bzw. konzerninterne Datentransfers unabhängig vom Datenschutzniveau des Ziellandes möglich sein sollten (Priscilla M. Regan 1999, 211).

Gegen Harmonisierung – Für nationale Freiräume

Zeitgleich sprachen sich sowohl die Mitgliedstaaten als auch die Wirtschaft[113] und selbst die nationalen Datenschutzaufsichtsbehörden (Deutscher Bundestag 1993, 160 Nr. 33.5 b; A. L. Newman 2008b, 112) aus jeweils unterschiedlichen Gründen weiterhin gegen eine weitergehende Harmonisierung aus und traten gemeinsam für mehr nationale Freiräume ein. Die Datenschutzbehörden versprachen sich dadurch, „den Datenschutz auch künftig nicht nur zu erhalten, sondern ihn auch neuen technologischen und gesellschaften [sic] Anforderungen anpassen zu können. Besonders für Länder mit einem weitentwickelten bereichsspezifischen Datenschutz, wie die Bundesrepublik Deutschland, ist dies eine entscheidende Frage." (Deutscher Bundestag 1993, 160 Nr. 33.5 b)) Zudem traten die Aufsichtsbehörden mit der Verlagerung von mehr Macht auf die nationale Ebene dem allseits kritisierten Kompetenzzuwachs, den die Kommission für sich vorgesehen hatte, entgegen.

Die Mitgliedstaaten waren ohnehin der grundsätzlichen Ansicht, dass die Übertragung mitgliedstaatlicher Kompetenzen an die Gemeinschaft sich immer auf das Mindestmaß beschränken sollte und die Wirtschaft hoffte darauf, dass ihre Befürwortung nationaler Freiräume seitens der jeweiligen Mitgliedstaaten für eine möglichst wirtschaftsfreundliche Umsetzung der

113 Hier sei insbesondere EUROCHAMBRES genannt, der die Europäische Kommission im Jahr 1993 dazu aufforderte, den Mitgliedstaaten bei der Umsetzung der Richtlinie mehr Freiraum zu überlassen (Priscilla M. Regan 1999, 211).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Richtlinienvorgaben und der Senkung der Implementierungskosten der Richtlinie sorgen würde (A. L. Newman 2008a, 117 f.).

Ausweitung des Anwendungsbereichs auf manuelle Dateien

In jenen Ländern, in denen manuelle Verarbeitungen nicht vom Anwendungsbereich der nationalen Datenschutzgesetze umfasst waren, wehrten sich Wirtschaftsvertreter weiterhin dagegen, dass die Richtlinie auch diese umfassen sollte. Die Ausweitung des Anwendungsbereichs auch auf manuelle Verarbeitungen bedeutete für viele Unternehmen, dass viele ihrer laufenden und dem Datenschutzrecht nicht entsprechenden manuell geführten Datenbanken und manuellen Verarbeitungen nachträglich und kostenintensiv den Richtlinienvorgaben angepasst werden müssten. Entsprechend ablehnend standen Großbritannien, Irland und Dänemark auch weiterhin gegenüber der vorgesehenen Ausweitung des Anwendungsbereichs gegenüber (Battcock 1995, 164). Der nördliche Block konnte sich mit seinen Forderungen allerdings nicht durchsetzen. Statt der vollständigen Herausnahme der manuellen Verarbeitung aus dem Anwendungsbereich konnten sie im überarbeiteten Richtlinienentwurf allerdings immerhin eine deutliche Verlängerung der Anwendungsfrist auf manuelle Dateien erringen. Während die Umsetzung der übrigen Vorgaben der Richtlinie in nationales Recht binnen drei Jahren abgeschlossen sein sollte, wurde für die Anwendung der Richtlinienvorgaben auf manuelle Dateien zunächst eine Übergangsfrist von zehn Jahren ausgehandelt, um eine kosteneffiziente Durchführung zu ermöglichen (Simitis 1995, 465).

Daneben beschäftigte das vorgesehene Verbot automatisierter Einzelentscheidungen sowohl die Kredit-Scoring- und Werbeversandbranche, die Erschwerungen im Hinblick auf die Erstellung von Kundenprofilen befürchtete (Battcock 1995, 164 f. Priscilla M. Regan 1999, 209) als auch den Großteil des nördlichen Blocks (Dänemark, Irland und demVereinigten Königreich), der die Streichung des entsprechenden Artikels forderte (Bignami 2005, 841).

Ein weiterer Konflikt entbrannte um die Vorgaben zu besonderen Kategorien personenbezogener Daten. Während Belgien, Frankreich, Spanien und Portugal mit dem entsprechenden Artikel grundsätzlich zufrieden waren, beklagten die Staaten des nördlichen Blocks, aber auch die Bundesrepublik, dass nicht die Art eines Datums, sondern der spezifische Verarbeitungskontext im Hinblick auf besondere Schutzmaßnahmen relevant sein sollte. Doch fand diese Perspektive trotz aller Kritik an der mangelnden Flexibilität besonderer Kategorien personenbezogener Daten bei den Staa-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

ten des südlichen Blocks keine Unterstützung (Bignami 2005, 841; Simitis 1995, 450).

Aufgrund der zahlreichen Konfliktfelder gerieten die Verhandlungen im Ministerrat im Laufe des Jahres 1993 zunehmend ins Stocken. Großbritannien, Irland, Dänemark und Deutschland legten schließlich im Oktober 1993 im Ministerrat ein gemeinsames Papier mit Änderungsanträgen für eine deutliche Ausweitung der nationalen Freiräume bei der Umsetzung vor, die das Harmonisierungsziel, aber auch das angestrebte Datenschutzniveau der Richtlinie vollends nichtig gemacht hätten.[114] Interessanterweise bezweckte Deutschland mittels der Forderung nach sehr weitreichenden nationalen Freiräumen die Aufrechterhaltung seiner als überlegen erachteten nationalen Datenschutz-Traditionen, während Großbritannien, Irland und Dänemark mittels der Freiräume vor allem die Absenkung des gemeinschaftlichen Schutzniveaus bei der nationalen Umsetzung anstrebten. An diesem Punkt wiederum war die rote Linie des südlichen Blocks sowie der Kommission erreicht.[115] Eher hätten die Richtlinienbefürworter den grenzüberschreitenden Verkehr personenbezogener Daten ganz gestoppt, als den Vorschlägen des nördlichen Blocks, die den Richtlinienentwurf und insbesondere das Harmonisierungsziel der Gemeinschaft bis zur Unkenntlichkeit verwässert hätten, nachzugeben. Somit lag Ende 1993 bzw. Anfang 1994 im Ministerrat eine Pattsituation vor und die Verhandlungen standen praktisch still (Bainbridge 1996, 28 f. Pearce und Platten 1998, 535 ff.).

Mitgliedstaat	Stimmen
Deutschland	10
Frankreich	10
Italien	10
Vereinigtes Königreich	10
Spanien	8
Belgien	5
Griechenland	5
Niederlande	5
Portugal	5

114 Durch Deutschlands Wechsel in das Lager der Richtliniengegner hatten diese Staaten eine Sperrminorität (26 Stimmen) inne. Die Richtlinienbefürworter verharrten hingegen bei 50 der benötigten 54 Stimmen (vgl. Tabelle 3-2).

115 Die datenschutzfeindliche Haltung des nördlichen Blocks wurde auch seitens der Datenschutzaufsichtsbehörden kritisiert (Der Spiegel 1993, 15).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Mitgliedstaat	Stimmen
Dänemark	3
Irland	3
Luxemburg	2
Insgesamt	76
Benötigt	54

Tabelle 3-2: Qualifiziertes Mehrheitswahlrecht bis Ende 1994, Richtliniengegner Ende 1993/Anfang 1994 in Rot (Council of the European Union 2013, 38)

3.2.2.6 Überwindung der politischen Pattsituation

Die politische Pattsituation auf der Ebene der Ratsarbeitsgruppe bzw. des AStV im Ministerrat konnte letztlich vor allem durch die Entwicklungen auf dem Gebiet der internationalen Informationspolitik und der neuerlichen Selbstverortung der Europäischen Gemeinschaft in diesem Kontext überwunden werden. Bereits 1992 hatte die erfolgreiche Wahlkampagne des zum US-Präsidenten gewählten Bill Clinton und seines Vize-Präsidenten Al Gore die Bedeutung der Informationspolitik für die wirtschaftliche Entwicklung vor Augen geführt und die Förderung von Informations- und Kommunikationstechnologien (IKT) zu einem zentralen Element des Regierungsprogramms ausgebaut. Jacques Delors, der langjährige sozialdemokratische Präsident der Europäischen Kommission, arbeitete zur selben Zeit an einer populären Neuausrichtung der Europäischen Gemeinschaft, die er nach den kritischen Maastrichter Referenden in Frankreich und Dänemark für notwendig erachtete.[116] Die Kommission veröffentlichte ihre neue Vision für die Gemeinschaft schließlich im Juni 1993 in Form des Weißbuchs „Wachstum, Wettbewerbsfähigkeit, Beschäftigung: Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert", das den Wandel

116 Während Mitgliedstaaten wie Deutschland kein Referendum abhielten, fanden im Jahr 1992 in Frankreich, Irland und Dänemark Volksreferenden zum Maastrichter Vertrag statt. Das ablehnende Votum der Dänen im Juni 1992 und das knappe Ja der Franzosen markierten zugleich einen Wendepunkt in der Geschichte der Europäischen Integration. Die langsame, aber technokratische Fortsetzung der Europäischen Integration, die bis dahin als europaweiter gesellschaftlicher Konsens galt, gelangte an ihr Ende, die Politisierung der Europäischen Gemeinschaftspolitiken setzte ein und EU-skeptische Gruppierungen und Parteien erhielten erstmals ernsthaften Auftrieb (Harmsen und Spiering 2004).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

der Gesellschaft hin zu einer Informationsgesellschaft als unaufhaltsam und die Schaffung eines „gemeinsamen Informationsraums" für die weitere Entwicklung der europäischen Wettbewerbsfähigkeit als zentral definierte (Europäische Kommission 1994b, 117, Nr. 5.2). Zur Erreichung dieser Ziele wurde eine Reihe von Maßnahmenvorschlägen formuliert. Einer der Vorschläge sah zur Realisierung des gemeinsamen Informationsraums die „Schaffung der rechtlichen, ordnungspolitischen, normativen und politischen Voraussetzungen" unter Wahrung der Interessen des einzelnen – zu denen Datenschutz hinzugezählt wurde – sowie der Interessen der Gemeinschaft (bestehende Universaldienste und künftige europäische Unternehmen) vor (ebd., 120 lit. b). Zur weiteren Ausarbeitung der erforderlichen Maßnahmen wurde die Gründung einer hochrangigen Arbeitsgruppe, der sog. *Task Force „Europäische Informationsinfrastruktur"* (ebd., 124, Nr. 5.4), bestehend aus einem Mitglied der Kommission, Regierungsangehörigen der Mitgliedstaaten, Vertretern des Europäischen Parlaments sowie hochrangigen Industrievertretern, vorgeschlagen. Von entscheidender Bedeutung war, dass die Task Force dem Europäischen Rat unmittelbar Bericht erstatten und Politik-Empfehlungen unterbreiten sollte (ebd.). Der Europäische Rat billigte die Einsetzung der Task Force auf seiner Sitzung im Dezember 1993, woraufhin diese umgehend mit der Erstellung eines ersten Berichts bis zur nächsten Sitzung des Europäischen Rates am 24. und 25. Juni in Korfu beauftragt wurde (Bangemann 1994, 6). Den Vorsitz der Gruppe übernahm Martin Bangemann, der bereits für die Initiative der Europäischen Kommission zur DS-RL mitverantwortlich gewesen war. Der Bericht der Task-Force, der als Bangemann-Report auch international über die Grenzen der EG hinaus Aufmerksamkeit erzeugen sollte, forderte dem neoliberalen Zeitgeist in der Politik entsprechend und viele der Elemente des Clinton/Gore-Aktionspapiers zur Schaffung einer Nationalen Informations-Infrastruktur übernehmend, die Deregulierung der europäischen IKT-Märkte mit dem Ziel der Stärkung marktbasierter Ansätze zur Erreichung der angestrebten Informationsgesellschaft (Krempl 1997). Der Erlass EG-weiter Datenschutz-Regeln wurde zudem erstmals mit dem Argument verbunden, dass diese ein notwendiges Element zur Herstellung von Vertrauen auf Seiten der Verbraucher für das erfolgreiche Gelingen der Informationsgesellschaft seien:

> *"The Group believes that without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society. Given the importance and sensitiv-*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

> *ity of the privacy issue, a fast decision from Member States is required on the Commission's proposed Directive setting out general principles of data protection." (Bangemann 1994, 22)*

Der Bangemann-Report wurde auf dem Treffen des Europäischen Rates in Korfu von den Regierungschefs der Mitgliedstaaten äußert positiv aufgenommen (Pearce und Platten 1998, 536). Entsprechend deutlich signalisierte der Europäische Rat dann auch seinen Wunsch hinsichtlich der Umsetzung der Kommissionsvorschläge zur Informationsgesellschaft:

> *„Der Europäische Rat ersucht den Rat und das Europäische Parlament, vor Jahresende Maßnahmen […] zu ergreifen, […] indem sie diese Entwicklung durch politische Impulse fördern, einen klaren und stabilen rechtlichen Rahmen (insbesondere in bezug [sic] auf den Marktzugang, die Kompatibilität zwischen Netzen, das geistige Eigentum, den Datenschutz und das Urheberrecht) schaffen und in Bereichen, die unter ihre Zuständigkeit fallen, beispielgebend vorangehen." (Europäischer Rat 1994b I Nr. 4)*

Sowie:

> *„Bei der Ausarbeitung der verschiedenen Rechtsakte zur Schaffung von Informatiksystemen muß dem Datenschutz, insbesondere folgenden Aspekten besondere Aufmerksamkeit gewidmet werden: Recht der Betroffenen auf Zugang zu dem System, Individualbeschwerderecht und Einrichtung einer gemeinsamen Aufsichtsstelle. Der Europäische Rat ersucht die zuständigen Gremien, diesen Fragen weiterhin Vorrang einzuräumen, und hofft, auf seiner Tagung im Dezember 1994 einen Zwischenbericht zu erhalten." (Europäischer Rat 1994b, III Nr. 2)*

Von diesem Zeitpunkt an erhielten die Verhandlungen zur DS-RL wieder Auftrieb. Entsprechend den Vorgaben des Europäischen Rates waren die mitgliedstaatlichen Delegationen, die sich im Ministerrat mit der DS-RL auseinandersetzten, in der Folgezeit gefordert, die politische Pattsituation zu überwinden und die Verhandlungen unter Erzielung eines politischen Kompromisses zu einem erfolgreichen und schnellen Ende zu bringen (Pearce und Platten 1998, 536).

Ein weiteres Schlüsselereignis, das zum erfolgreichen Abschluss der Verhandlungen beigetragen hat, war die Übernahme des Ministerratsvor-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sitzes[117] durch die Bundesrepublik im Juli 1994. Deutschland, das sich zuletzt auf die Seite der Richtliniengegner geschlagen hatte und damit den erfolgreichen Abschluss der Verhandlungen blockierte, auf ihre Seite zu ziehen, war ein zentrales Anliegen der Richtlinienbefürworter. Allerdings erwies sich dies als gar nicht notwendig, da Deutschland seine Haltung aus verschiedenen Gründen änderte. *Erstens* führte der verstärkte Dialog, der traditionell zwischen jedem Ratsvorsitz und der Kommission stattfindet, dazu, dass politische Missverständnisse überwunden werden konnten, indem die Kommission die Gelegenheit erhielt, die deutsche Ratsdelegation davon zu überzeugen, dass ihre nationalen Datenschutz-Traditionen von der Richtlinie nicht gefährdet würden. *Zweitens* war Deutschland, wie jeder andere Ratsvorsitz auch, grundsätzlich darum bemüht, während seines Vorsitzes potentiell prestige-trächtige Politik-Ergebnisse – insb. in Form gemeinsamer Ratspositionen – zu erzielen. Aus diesen taktischen Erwägungsgründen heraus machte die kurz zuvor in Korfu auf höchster europapolitischer Ebene geäußerte Forderung nach einem schnellen Abschluss der Verhandlungen zur DS-RL diese zu einem geeigneten Kandidaten zur Erzielung einer gemeinsamen Position. Schließlich und *drittens* war die Bundesrepublik, weil sie handfeste Fortschritte erzielen wollte, eher dazu geneigt, Konzessionen bei Themen einzugehen, wozu sie zuvor nicht bereit gewesen war (Bainbridge 1996, 30 f. Pearce und Platten 1998, 536 f.).

Zeitgleich wurde in den Mitgliedstaaten und insbesondere im Vereinigten Königreich sowie in den Niederlanden noch immer über die bei der Umsetzung der Richtlinie zu befürchtenden Kosten debattiert. Zur Überprüfung der Ergebnisse der vorherigen Studien und zum Zwecke der Erarbeitung einer eigenen, evidenzbasierten Position unternahm die

117 Der Rolle des Vorsitzes im Ministerrat kommt in der institutionellen Architektur sowohl des Ministerrats als auch der EU eine Schlüsselrolle zu. Der Vorsitz ist u. a. insbesondere verantwortlich für die Einberufung, Vorbereitung und Durchführung aller formellen und informellen Treffen des Ministerrats, für die Kompromisssuche bei Kontroversen und die Vertretung der Ministerratsposition gegenüber anderen EU-Institutionen wie auch Drittstaaten. Über viele Jahrzehnte rotierte der Vorsitz halbjährlich alphabetisch unter allen Mitgliedstaaten. Seit 2007 wurde die alphabetische Rotation zugunsten eines Dreiervorsitzes aufgegeben. Die dabei aufeinanderfolgenden drei Vorsitze setzen sich nach Möglichkeit aus einem größeren Mitgliedstaat, einem kleineren Altmitglied sowie einem neuen Mitgliedstaat zusammen und sollen zum Zwecke der Formulierung langfristigerer politischer Ziele ein gemeinsames Achtzehnmonatsprogramm formulieren, auf dem wiederum der jeweilige Vorsitz sein eigenes detailliertes Halbjahresprogramm aufbauen kann (EU-Ministerrat 2020; Wessels 2008, 214 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommission den für diese Zeit ungewöhnlichen Schritt der Beauftragung einer wissenschaftlichen Studie zur Untersuchung der bei der Umsetzung der Richtlinie in den Niederlanden und dem Vereinigten Königreich zu erwartenden Kosten (Pearce und Platten 1998, 537). Die Studie wurde im Zeitraum Juli 1994 bis Oktober 1994 von unabhängigen britischen und niederländischen Forscherinnen und Forschern durchgeführt. Im Gegensatz zur Mehrheit der anderen Studien verdeutlichten die Ergebnisse, dass die Mehrzahl der von der DS-RL betroffenen öffentlichen wie nicht-öffentlichen Organisationen nur mit sehr geringen finanziellen Mehrkosten während der Umsetzungsphase rechnen mussten, die laufenden Kosten nach Abschluss der Implementierungsphase jedoch wieder auf das Vor-Datenschutz-Richtlinien-Niveau sinken würden. Zwar wurde festgestellt, dass jene Wirtschaftsbereiche, die besonders viele Kundendaten verarbeiten (allen voran der Bankensektor sowie die Direktmarketingbranche) in besonderem Maße von gesteigerten Kosten betroffen sein würden, doch auch diese Zahlen waren deutlich niedriger als jene, die in den vorherigen Studien berechnet worden waren. Zudem stellte die Studie fest, dass die mit der DS-RL notwendig werdende Durchsicht datenverarbeitender Unternehmensprozesse auch zu Effizienzsteigerungen und zu Investitionen in datenverarbeitende Systeme führen könnte. Schließlich propagierte auch diese Studie das neue Argument, dass der angemessene Schutz personenbezogener Daten zu mehr Vertrauen in datenverarbeitende Dienste und zu deren gesteigerter gesellschaftlicher Akzeptanz führen und damit zu nachhaltigem wirtschaftlichen Erfolg beitragen würde (Bainbridge u. a. 1994). Parallel zu den Entwicklungen auf der Ebene des Europäischen Rates und den durch den deutschen Ministerratsvorsitz angestoßenen Entwicklungen, trugen die Ergebnisse dieser Studie ebenfalls dazu bei, dass der Widerstand gegen die Richtlinie in den Mitgliedstaaten zurückgefahren und die Kompromissbereitschaft gesteigert wurde (Pearce und Platten 1998, 537).

3.2.2.6.1 Politische Kompromisse

Aufgrund der genannten externen und internen Rahmenbedingungen wurden in der zweiten Hälfte des Jahres 1994 dann auch zügig Fortschritte im Hinblick auf die Erreichung einer gemeinsamen Position im Ministerrat erzielt.

So wurde die vorgesehene Übergangsfrist bezüglich der Anwendung der Richtlinienvorgaben auf manuelle Dateien von zehn Jahren auf zwölf Jahre

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

erhöht, sodass die irische Ratsdelegation ihren Widerstand gegen die Richtlinie zurückzog. Dänemarks Widerstand konnte aufgebrochen werden, indem eine Reihe von Ausnahmeregelungen bezüglich der Verarbeitung personenbezogener Daten zu wissenschaftlichen bzw. medizinischen Forschungszwecken in die Richtlinie eingebaut wurde. Auch bei dem Streitthema besonderer Kategorien personenbezogener Daten konnte eine Einigung erzielt werden. Die Bundesrepublik, Dänemark, Griechenland, Irland, die Niederlande, Portugal und Großbritannien konnten zur Aufgabe ihrer Ablehnung einer erschöpfenden Liste als sensibel eingestufter personenbezogener Daten bewegt werden, indem in den entsprechenden Artikel weitere Ausnahmebestimmungen hinzugefügt wurden (Bainbridge 1996, 28; Pearce und Platten 1998, 537 ff.).

Die dem deutschen Recht nachempfundene zentrale Stellung der Einwilligung wurde im Laufe der Verhandlungen ebenfalls abgeschwächt. Während im ursprünglichen Richtlinienentwurf noch von einer konkreten und ausdrücklichen Einwilligung und im überarbeiteten Richtlinienentwurf von einer ausdrücklichen Willensbekundung des Betroffenen für jede personenbezogene Datenverarbeitung die Rede war, was vor allem die Einwilligung in Schriftform erforderlich gemacht hätte, sah der finale Ratskompromiss nur noch eine Einwilligung *ohne jeden Zweifel* vor. Die ausdrückliche Einwilligung sollte nur im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten erforderlich sein (Simitis 2001, 129 f.).

Auch der Dauerstreit um die Meldepflicht konnte letztlich überwunden werden. Die Vorabkontrolle riskanter Verarbeitungen personenbezogener Daten wurde zur Ausnahme gemacht, während den Mitgliedstaaten die Möglichkeit eröffnet wurde, die Meldepflicht zu vereinfachen. Dazu bediente man sich in Art. 18 Abs. 2 DS-RL insbesondere des aus dem deutschen Datenschutzrecht stammenden und seitens der deutschen Ministerratsdelegation und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gewünschten (Deutscher Bundestag 1993, 160 Nr. 33.5 c)) Konzepts eines unabhängigen betrieblichen Datenschutzbeauftragten. Für die Bestellung eines betrieblichen Datenschutzbeauftragten, der die unabhängige Überwachung der jeweiligen Verarbeitungen und die Führung eines Verzeichnisses über diese gewährleistet, wurde die Vereinfachung der Meldepflicht bzw. die vollständige Befreiung eines Verantwortlichen von dieser Pflicht vorgesehen (Simitis 2001, 134 f.). Mittels derartiger Konzessionen konnte die Bundesrepublik schließlich dazu bewegt werden, einige ihrer zentralen Forderungen aufzugeben. Dies betraf zum einen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die fortwährend gestellte Forderung nach einer Mindestharmonisierung,[118] die von der Kommission und der Mehrheit der übrigen Mitgliedstaaten abgelehnt wurde und zum anderen die Ablehnung der vorgesehenen Regelungen zum Direktmarketing, das ohne die ausdrückliche Einwilligung der Betroffenen erfolgen dürfen sollte (Pearce und Platten 1998, 536 f.).

Kurz vor Abschluss der Verhandlungen wurden auf Druck Frankreichs hin schließlich auch die letzten verbliebenen Befugnisse der Europäischen Kommission im Hinblick auf die Harmonisierung des europäischen Datenschutzrechts gestrichen. Letztlich war die Kommission nur noch in die Genehmigung von Datentransfers in Drittstaaten eingebunden, verlor aber selbst dort die für sich vorgesehene herausgehobene Stellung (Bignami 2005, 839). Zudem wurde auf Druck Großbritanniens, Dänemarks, Irlands und Schwedens hin auch das Prozedere zur eigenständigen Genehmigung eines Datentransfers in einen Drittstaat seitens eines einzelnen Mitgliedstaates deutlich zugunsten der Mitgliedstaaten vereinfacht (Bignami 2005, 840).

Ende 1994 waren die Mitgliedstaaten schließlich soweit, eine gemeinsame Position zu verabschieden. Auf der Tagung des Binnenmarkt-Rates[119] am 8. Dezember 1994 konnte sodann eine informelle politische Einigung betreffend die DS-RL erzielt werden. Eine formelle Einigung war aus technischen Gründen nicht möglich, da der finale Kompromisstext bis zum Sitzungstermin nicht in allen EG-Sprachen vorlag. Einzig Großbritannien verharrte in Radikalopposition zur Richtlinie und war auch weiterhin gegen den vorgeschlagenen Kompromiss. Die britische Ablehnung ging so weit, dass Angehörige der britischen Ratsdelegation und selbst Minister aus der britischen Regierung noch in den ersten Wochen des Jahres 1995 die übrigen Mitgliedstaaten – letztlich ohne Erfolg – davon zu überzeugen

118 Das Prinzip der Mindestharmonisierung sieht vor, dass einzelne Länder bei der Richtlinienumsetzung höhere Standards festlegen dürfen, während die Maximal- oder Vollharmonisierung keine strengeren Vorschriften als in der Richtlinie erlaubt (EU 2018).

119 Zur Wahrnehmung seiner Aufgaben tagt der Ministerrat in unterschiedlichen Ratsformationen, deren Zuschnitt sich an Politikfeldern orientiert. Die Anzahl der Ratsformationen variierte im Laufe der Geschichte des Ministerrats teils erheblich. Von sieben Formationen im Jahr 1967 stieg ihre Anzahl auf bis zu 22 Formationen im Jahr 1990 und ist wieder auf aktuell zehn Formationen gesunken (EU-Ministerrat 2018b; Wessels 2008, 199). Einen Überblick über die Entwicklung der Zuständigkeitsstrukturen im Ministerrat bietet (Karaboga 2018, 143 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

versuchten, die im Dezember erzielte politische Einigung zu widerrufen.[120] Die übrigen Mitgliedstaaten versuchten währenddessen umgekehrt die britische Ratsdelegation auf den AStV-Sitzungen im Januar und Februar 1995 davon zu überzeugen, ihre ablehnende Haltung zu überdenken. Zwar waren sie bereit, Zugeständnisse gegenüber dem Vereinigten Königreich zu machen, doch war der Spielraum für diese aufgrund der im Dezember bereits erzielten Einigung deutlich geringer als davor. Im Ergebnis führte die vom Vereinigten Königreich jahrelang vertretene Radikalopposition schließlich dazu, dass das Land selbst im Vergleich zu kleineren Staaten wie Dänemark einen nur äußert geringen Einfluss auf die Gestaltung der Richtlinie nehmen konnte, da es während der Verhandlungsphase keine kompromissorientierten Gestaltungsvorschläge machte, die von den Richtlinienbefürwortern ernsthaft hätten in Erwägung gezogen werden können. Zwar konnte Großbritannien trotz vielfacher Bemühungen[121] letztlich nicht zur Zustimmung zur Richtlinie bewegt werden, doch immerhin verwarf das Land seine Ablehnung und entschied sich aufgrund der vielen kleinen Konzessionen der anderen Mitgliedstaaten, die im Land immerhin anerkannt wurden, dazu, sich der Stimme zu enthalten (Bainbridge 1996, 31 f. Pearce und Platten 1998, 537 f. Simitis 1995, 445).

Am 1. Januar 1995 wurde die Europäische Gemeinschaft zudem um drei weitere Mitgliedstaaten – Finnland, Österreich und Schweden – erweitert. Alle drei Staaten waren in der entscheidenden Phase der Verhandlungen des vorangegangenen halben Jahres als Beobachter eingebunden. So waren alle drei Neumitglieder zum Zeitpunkt ihres Beitritts zur Gemeinschaft grundsätzlich mit den Inhalten der Richtlinie einverstanden. Der Gemeinsame Standpunkt des Ministerrates wurde schließlich unter dem neuen französischen Ratsvorsitz formell am 20. Februar 1995 auf der Tagung

120 Dies war auch deshalb unrealistisch, weil der Europäische Rat auf seinem Treffen am 9. und 10. Dezember in Essen sein Ersuchen aus dem Frühjahr an den Rat erneuert hatte, „die noch notwendigen rechtlichen Rahmenbedingungen – in Bereichen wie Marktzugang, Datenschutz und Schutz geistigen Eigentums – zügig zu schaffen." (Europäischer Rat 1994a, Nr. 6)

121 Die Kompromissbereitschaft der Richtlinienbefürworter wurde auch dadurch verstärkt, dass im Ministerrat, obwohl für Legislativvorschläge der Kommission das qualifizierte Mehrheitswahlrecht galt, eine Konsenslösung also technisch gesehen nicht notwendig war, für gewöhnlich die Erreichung eines Konsenses angestrebt wurde. Dementsprechend war es den Befürwortern nicht nur wichtig, die formal erforderliche Mehrheit zu erzielen, sondern möglichst alle Gegner durch weiteres Entgegenkommen zu einer Änderung ihrer Haltung zu bewegen (Bainbridge 1996, 31).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Ratsformation „Allgemeine Angelegenheiten" (General Affairs Council) ohne Gegenstimmen[122] angenommen (Rat 1995). Trotz der Kritik an der vollständigen Streichung der Durchführungsbefugnisse der Kommission, zeigte sich diese einverstanden mit der gemeinsamen Position des Ministerrats (COM 1995, 8). Das Parlament bestätigte die Ministerratsposition in zweiter Lesung ebenfalls grundsätzlich und machte lediglich sieben kleinere Änderungsvorschläge[123] geltend (EP 1995), die sowohl von der Kommission (KOM 1995) als auch vom Ministerrat (Working Party on Economic Questions (Data Protection) 1995) akzeptiert und in der zweiten Lesung des Ministerrats am 24. Juli 1995 von diesem angenommen wurden. Die finale *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* wurde schließlich am 24. Oktober 1995 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet (EU 1995).

122 Mit 77 von 87 Stimmen. Benötigt wurden mindestens 64 Stimmen (Council of the European Union 2013, 39). Vgl. auch Tabelle 3-3.

123 Es wurden zwar rund 60 Änderungsvorschläge eingebracht, doch der neue Rapporteur Medina Ortega (SPE, Spanien) im Parlamentsausschuss für Recht und Bürgerrechte (JURI) befürwortete lediglich die genannten sieben kleineren Änderungsvorschläge (Bainbridge 1996, 32).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Mitgliedstaat	Stimmen
Deutschland	10
Frankreich	10
Italien	10
Vereinigtes Königreich	10
Spanien	8
Belgien	5
Griechenland	5
Niederlande	5
Portugal	5
Österreich	4
Schweden	4
Dänemark	3
Irland	3
Finnland	2
Luxemburg	2
Insgesamt	*87*
Benötigt	*64*
Erhalten	*77*

Tabelle 3-3: Qualifiziertes Mehrheitswahlrecht nach der EU-Erweiterung im Jahr 1995 und Abstimmungsverhalten (Enthaltung des Vereinigten Königreichs) (Council of the European Union 2013, 39)

3.2.2.7 Inhalte der DS-RL

Im Ergebnis des politischen Kompromisses konnte sich in Bezug auf den sachlichen Anwendungsbereich (Art. 3 Abs. 1)[124] durchsetzen, dass kein Unterschied zwischen Regelungen für den öffentlichen und nicht-öffentlichen Bereich gemacht werden und dass allein das Vorhandensein einer Verarbeitung personenbezogener Daten den Ausschlag darüber gibt, ob sie in den Anwendungsbereich fällt oder nicht – unabhängig von der Art (manuell oder automatisiert) der Verarbeitung. Der von Großbritannien und Irland

124 Die Artikel-Angaben dieses Unterabschnitts beziehen sich grundsätzlich auf die finale DS-RL. Sofern der ursprüngliche Richtlinienentwurf von 1990 bzw. der überarbeitete Richtlinienentwurf von 1992 gemeint sind, wird die entsprechende Artikel-Angabe um „DS-RL-UE“ bzw. „DS-RL-ÜE“ ergänzt und spezifiziert.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

favorisierte Versuch, die DS-RL auf den Standard der Datenschutz-Konvention des Europarats „zurückzuschrauben, die Automatisierung also nicht nur als Anlaß, sondern auch als Grenze der regulativen Intervention anzusehen," (Simitis 1997, 283) scheiterte somit endgültig. Allerdings wurde der Einbezug der manuellen Verarbeitung personenbezogener Daten unter den Vorbehalt des Vorhandenseins einer minimalen Organisationsstruktur gestellt. Zu diesem Zweck bedienten sich Kommission und Ministerrat der in deutschen Datenschutzgesetzen verwendeten Formulierung der *Speicherung der verarbeiteten Daten in einer Datei*. Die DS-RL fand, in anderen Worten, auf jede Verarbeitung personenbezogener Daten Anwendung – unabhängig davon, ob es sich dabei um eine automatisierte, teilautomatisierte oder vollständig manuelle Verarbeitung handelt, sofern die dabei verarbeiteten Daten in einer Datei gespeichert sind oder gespeichert werden sollen (Art. 3 Abs. 1) (Simitis 2001, 125 f.).[125] Damit wiederum nicht jede manuelle Verarbeitung personenbezogener Daten (so etwa das Führen eines Tagebuchs oder eines Notizbüchleins) in den Anwendungsbereich der Richtlinie fällt, bediente man sich des sog. Haushaltsprivilegs aus dem britischen und niederländischen Datenschutzrecht, wonach die Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten findet, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (Art. 3 Abs. 2) (Simitis 2001, 126). Die Definition eines personenbezogenen Datums umfasste in der DS-RL „alle Informationen über eine bestimmte oder bestimmbare natürliche Person […], die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer [sic] oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind" (Art. 2 lit. a). Damit spezifizierte die DS-RL einerseits gegenüber den vorherigen internationalen Datenschutz-Instrumenten in deutlichem Maße, was konkret unter einer bestimmten oder bestimmbaren natürlichen Person zu verstehen ist. Andererseits wurde der Anwendungsbereich zugleich auf natürliche Personen eingeengt, während die Datenschutz-Konvention die

125 Etwa die Strukturierung einer manuellen Sammlung personenbezogener Daten nach Namen (Simitis 2001, 126).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Entscheidung darüber, ob auch juristische Personen umfasst sein sollten, noch den Vertragsparteien überlassen hatte.[126]

Der räumliche Anwendungsbereich der DS-RL (Art. 4) gab den Mitgliedstaaten die Anwendung ihres nationalen Datenschutzrechts in drei Fällen vor. Sobald eine Verarbeitung:[127]

- Gemäß Art. 4 Abs. 1 lit. a im Rahmen der Tätigkeiten einer Niederlassung im eigenen Hoheitsgebiet,
- gemäß Art. 4 Abs. 1 lit. b durch Verantwortliche mit Niederlassungen an Orten außerhalb dieses Gebiets, an denen aber das nationale Recht gemäß völkerrechtlichen Regelungen anwendbar ist, sowie
- gemäß Art. 4 Abs. 1 lit. c durch Verantwortliche in Drittländern, wenn diese zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen, die im Hoheitsgebiet des Mitgliedstaats belegen sind, es sei denn, dass dies nur zum Zweck der Durchfuhr erfolgt.

In Art. 6 wurden die Verarbeitungsgrundsätze einschließlich der Grundsätze der Rechtmäßigkeit sowie der Verarbeitung nach Treu und Glauben (lit. a), Zweckbindung (lit. b), Datenminimierung (lit. c), Richtigkeit (lit. d) und Speicherbegrenzung (lit. e) festgelegt. Bis auf eine Einschränkung blieben die Verarbeitungsgrundsätze gegenüber der Datenschutz-Konvention unverändert. So kam auch in der DS-RL, wie schon in den OECD-Richtlinien und der Datenschutz-Konvention zuvor, der Zweckbindung eine zentrale Rolle zu, wonach eine Verarbeitung personenbezogener Daten nur dann als rechtmäßig einzustufen ist, wenn diese einem konkreten und zuvor festgelegten Zweck dient: „Präventive Datensammlungen im Hinblick auf künftige, noch nicht feststehende Aktivitäten scheiden infolgedessen ebenso aus wie Datendepots, die sich jederzeit für neue Ziele reaktivieren lassen." (Simitis 1997, 285) Allerdings wurde der entsprechende Artikel im Ergebnis der Ratsverhandlungen dahingehend abgeändert, dass die Weiterverarbeitung von personenbezogenen Daten *zu historischen, statistischen oder wissenschaftlichen Zwecken im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen sind, sofern die Mitgliedstaaten geeignete Garantien vorsehen.*

126 Zumindest auf EU-Ebene sollte die Nichtanwendung der Datenschutzgesetze auf juristische Personen fortan zum Standard werden und zu keinen weiteren nennenswerten Kontroversen führen.

127 Die folgende Aufzählung ist in gekürzter Form übernommen aus: (Hornung 2019, 267 Rn. 5).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Art. 7 legte die Bedingungen für die Zulässigkeit einer Verarbeitung mit der Einwilligung gemäß Art. 7 lit. a als zentralem Bestandteil dar, die *ohne jeden Zweifel* zu erteilen war. Darüber hinaus konnte eine Verarbeitung auch dann als zulässig gelten, sofern sie gemäß Art. 7 lit. b für die Vertragserfüllung, gemäß lit. c für die Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen, gemäß lit. d für die Wahrung lebenswichtiger Interessen des Betroffenen, gemäß lit. e für die Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt oder gemäß lit. f zur Verwirklichung des berechtigten Interesses des Verantwortlichen erfolgt, sofern dieses nicht das Interesse oder die Grundrechte und Grundfreiheiten des Betroffenen überwiegt. Gegenüber der Datenschutz-Konvention ist an dieser Stelle eine deutliche Spezifizierung der Zulässigkeitsbedingungen sowie eine relative Steigerung der Selbstbestimmungsfähigkeit der von einer Datenverarbeitung betroffenen Individuen festzustellen (Battcock 1995, 162 f.). Die von der Kommission beabsichtigte Einführung einer ausdrücklichen Einwilligung, die ein höheres Schutzniveau geboten hätte, hatte sich in den Verhandlungen allerdings nicht durchsetzen können.

In Art. 8 wurden die Vorgaben zu besonderen Kategorien personenbezogener Daten dargelegt. Demnach wird zunächst gemäß Art. 8 Abs. 1 die Verarbeitung jener personenbezogenen Daten untersagt, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über die Gesundheit oder das Sexualleben.[128] Abweichend von Abs. 1 kann eine Verarbeitung allerdings gemäß Art. 8 Abs. 2 in jenen Fällen erfolgen, in denen (lit. a) der Betroffene in eine Verarbeitung *ausdrücklich* einwilligt, (lit. b) die Verarbeitung erforderlich ist, um den arbeitsrechtlichen Pflichten des Verantwortlichen unter Vorsehung angemessener Garantien Rechnung zu tragen, (lit. c) die Verarbeitung zum Schutz lebenswichtiger Interesse des Betroffenen oder eines Dritten erforderlich ist, (lit. d) die Verarbeitung unter Wahrung angemessener Garantien seitens einer politisch, philosophisch oder gewerkschaftlich ausgerichteten nicht-kommerziellen Organisation erfolgt, oder (lit. e) die Verarbeitung auf Daten bezogen ist, die offenkundig seitens des Betroffenen öffentlich gemacht wurden. Grundsätzlich ausgenommen von den Vorga-

128 Die Auflistung entspricht im Wesentlichen jener der Datenschutz-Konvention. Abweichend ist in der DS-RL zusätzlich die Gewerkschaftszugehörigkeit benannt, während die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, in Art. 8 Abs. 5 DS-RL geregelt wird.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ben des Absatzes 1 waren zum einen (gemäß Art. 8 Abs. 3) Verarbeitungen, die zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erfolgen, und zum anderen (gemäß Art. 8 Abs. 4) Verarbeitungen, die aus Gründen eines wichtigen öffentlichen Interesses erfolgen.

Die Transparenzvorgaben im Falle der Erhebung beim Betroffenen selbst (Art. 10) und in jenen Fällen, in denen die Daten nicht bei dem Betroffenen erhoben wurden (Art. 11) spiegeln den Anspruch der DS-RL wider, die Kontrolle des Betroffenen über die Verarbeitung der ihn betreffenden Daten zu gewährleisten. Hinzu kommen die Betroffenenrechte in Form des Auskunftsrechts (Art. 12 lit. a), des Rechts auf Berichtigung, Löschung oder Sperrung (Art. 12 lit. b) und des Widerspruchsrechts (Art. 14). Das Auskunftsrecht sah vor, dass der Betroffene *in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten*[129] die Existenz einer sie betreffenden Datenverarbeitung, den Zweck der Verarbeitung, die Kategorien verarbeiteter Daten sowie die Empfänger oder Kategorien der Empfänger der Daten in Erfahrung bringen durfte. Art. 12 lit. c sah wiederum abweichend von den vorherigen internationalen Instrumenten vor, dass jede Berichtigung, Löschung oder Sperrung gemäß Art. 12 lit. b den Dritten, denen die Daten seitens des Verantwortlichen übermittelt wurden, mitzuteilen ist, *sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist*. Art. 13 widmete sich den nationalen Freiräumen im Hinblick auf Ausnahmen und die Einschränkung der Transparenzvorgaben in den Artikeln 10 und 11 sowie die Betroffenenrechte in Art. 12.[130]

Art. 15 Abs. 1 sah schließlich das Verbot vollständig automatisierter Entscheidungen vor, die zum Zwecke der Bewertung einzelner Aspekte einer Person, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens erfolgen. Abweichend konnten Betroffene einer der in Art. 15 Abs. 1 genannten Entscheidungen gemäß Art. 15 Abs. 2 lit. a unterworfen werden, wenn diese der

129 Insofern entsprachen die Rahmenbedingungen betreffend die Dauer und Kosten des Auskunftsrechts jenen der Datenschutz-Konvention (vgl. Art. 8 lit. b).

130 Art. 13 Abs. 2 eröffnete den Mitgliedstaaten die Möglichkeit der Einschränkung der Betroffenenrechte sofern die Verarbeitung ausschließlich für Zwecke der wissenschaftlichen Forschung oder zur Erstellung von Statistiken erfolgt. Dieser Absatz war Ergebnis des zuvor genannten Kompromisses, der mit Dänemark erzielt wurde (González Fuster 2014, 138).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Vertragserfüllung dient und auf dem Ersuchen des Betroffenen basiert oder die berechtigten Interessen des Betroffenen, beispielsweise durch die Möglichkeit, seinen Standpunkt geltend zu machen, gewahrt werden. Art. 15 Abs. 2 lit. b sah die Zulässigkeit derartiger Entscheidungen zudem auch im Falle gesetzlicher Bestimmungen vor, sofern darin Garantien zur Wahrung der berechtigten Interessen des Betroffenen festgelegt wurden.

Die Art. 16 und 17 legten die Verarbeiterpflichten in Bezug auf die Vertraulichkeit bzw. die Sicherheit der Verarbeitung nieder. Art. 18 Abs. 1 regelte die Pflicht des Verarbeiters zur Meldung einer Verarbeitung bei der zuständigen Aufsichtsbehörde. Art. 18 Abs. 2 sah die Vereinfachung der bzw. die vollständige Ausnahme von der Meldepflicht seitens einzelner Mitgliedstaaten vor allem dann vor, wenn die verantwortliche Stelle einen unternehmensinternen Datenschutzbeauftragten einbestellt.

Für Verarbeitungen, die gemäß mitgliedstaatlicher Vorgaben spezifische Risiken für die Rechte und Freiheiten der Betroffenen beinhalten, sah Art. 20 die Möglichkeit der Vorabkontrolle seitens der Aufsichtsbehörde oder des unternehmensinternen Datenschutzbeauftragen zum Zwecke der Eindämmung der Risiken vor.

Rechtsbehelfe, Haftung und Sanktionen wurden in den Artikeln 22, 23 respektive 24 behandelt, machten den Mitgliedstaaten außer der Verpflichtung zur Schaffung der entsprechenden Strukturen allerdings keine weitergehenden Vorgaben zu den Details der Umsetzung.

In den Artikeln 25 und 26 wurden die bei der Übermittlung personenbezogener Daten in Drittländer zu beachtenden Grundsätze bzw. Ausnahmen dargelegt. Das im ursprünglichen Richtlinienvorschlag vorgesehene, vor allem auf einer durch die Kommission auszustellenden Genehmigung auf Basis der Evaluierung staatsrechtlicher Garantien basierende Übertragungsprinzip in Drittstaaten musste im Ergebnis des politischen Aushandlungsprozesses einem *flexibleren* Verfahren weichen. Die in den überarbeiteten Richtlinienvorschlag der Kommission integrierten Erleichterungen im Hinblick darauf, dass auch die in einem Drittland geltenden Standesregeln bei der Beurteilung der Angemessenheit berücksichtigt werden können und dass der Datentransfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der Einwilligung des Betroffenen (nunmehr Art. 26 Abs. 1 lit. a), bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags und für die Wahrung eines wichtigen öffentlichen Interesses (nunmehr Art. 26 Abs. 1 lit. d) oder lebenswichtiger Interessen des Betroffenen (Art. 26 Abs. 1 lit. e) erfolgen kann, blieben in der Richtlinie enthalten, wurden allerdings teilweise ausgeweitet. So wurde der Punkt hinsichtlich

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Erfüllung eines Vertrags dahingehend erweitert, dass er gemäß Art. 26 Abs. 1 lit. b die Bedingungen für die Erfüllung eines Vertrags zwischen dem Betroffenen und dem Verantwortlichen und gemäß Art. 26 Abs. 1 lit. c die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse des Betroffenen mit einem Dritten geschlossen wurde, vorsah. Schließlich kam als letzter Punkt hinzu, dass der Datentransfer auch dann stattfinden darf, wenn die Übermittlung aus einem Register erfolgt, dessen Inhalt ohnehin der Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, offen steht. Ebenso bedeutend waren die Entmachtung der Kommission im Rahmen des Ausschussverfahrens gemäß Art. 31 (der beratende Ausschuss gemäß Art. 30 DS-RL-UE) sowie die Ausweitung mitgliedstaatlicher Freiräume bei der Genehmigung eines Transfers seitens eines einzelnen Mitgliedstaates. Während in den nicht-finalen Richtlinienfassungen noch vorgesehen war, dass die Kommission relativ eigenständig und lediglich unter der optionalen Hinzuziehung der Meinung der Mitgliedstaaten über die Angemessenheit von Drittstaaten befinden können sollte, sah die finale DS-RL nunmehr vor, dass die Angemessenheit gemäß dem in Art. 31 geregelten Ausschussverfahren ausschließlich seitens mitgliedstaatlicher Vertreter entschieden werden sollte. In ähnlich radikaler Weise wurden auch die Vorgaben hinsichtlich der Genehmigung eines Transfers in einen Drittstaat seitens eines einzelnen Mitgliedstaates im Laufe des politischen Aushandlungsprozesses abgeändert. Während der ursprüngliche Richtlinienentwurf (Art. 25 DS-RL-UE) noch vorgesehen hatte, dass ein solcher Transfer nur nach Ablauf einer zehntägigen Frist ab dem Moment der Meldung des geplanten Transfers an Kommission und Mitgliedstaaten und sofern diese keinen Widerspruch erheben, erfolgen durfte, wurden die Vorgaben zunächst bereits im überarbeiteten Richtlinienentwurf flexibler gehandhabt. So wich die Zehntagesfrist im überarbeiteten Richtlinienentwurf (Art. 27 DS-RL-ÜE) der Vorgabe, dass die Unterrichtung lediglich *rechtzeitig* vor Wirksamwerden der Genehmigung erfolgen musste, damit die Kommission und Mitgliedstaaten noch vor Wirksamwerden Widerspruch einlegen können. In der DS-RL wurde schließlich nur noch vorgesehen, dass eine Unterrichtung überhaut erfolgen muss, der Zeitpunkt dieser wurde jedoch vollständig dem jeweiligen Mitgliedstaat überlassen, sodass die ursprünglich vorgesehene Interventionsmöglichkeit praktisch nicht mehr vorhanden war. Schließlich hatte auch die Abänderung des Ausschussverfahrens weitreichende Bedeutung für Drittstaatentransfers. Während gemäß den ersten beiden Fassungen der DS-RL (Art. 30 DS-RL-UE bzw. Art. 34 DS-RL-ÜE) auf einen Widerspruch

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Kommission oder der Mitgliedstaaten hin im beratenden Ausschuss die Kommission die Entscheidungsbefugnis innegehabt hätte, sah die finale DS-RL gemäß Art. 31 vor, dass bei strittigen Genehmigungen ausschließlich mitgliedstaatliche Vertreter in Entscheidungsverantwortung waren.

In Art. 27 wurde die Möglichkeit dargelegt, Verhaltensregeln auszuarbeiten. Die im ursprünglichen Entwurf (Art. 20 DS-RL-UE) noch sehr rudimentären und vor allem lediglich auf die Gemeinschaftsebene bezogenen Vorgaben waren bereits im überarbeiteten Richtlinienentwurf (Art. 28 und 29 DS-RL-ÜE) deutlich ausgeweitet worden. Nach Art. 28 sollten nationale Verhaltensregeln durch Interessenverbände ausgearbeitet, durch die zuständige nationale Aufsichtsbehörde auf ihre Verträglichkeit mit der DS-RL hin geprüft und gegebenenfalls genehmigt und durch die nächstzuständige mitgliedstaatliche Stelle amtlich veröffentlicht werden. Art. 29 DS-RL-ÜE sah allerdings abweichend von den vorgenannten Bestimmungen vor, dass die Kommission dazu befugt sein sollte, auch solche gemeinschaftlichen Verhaltensregeln zu veröffentlichen, die von der in Art. 31 DS-RL-ÜE genannten Gruppe (der späteren Art. 29-Datenschutzgruppe) nicht positiv bewertet wurden. In der finalen DS-RL wurde schließlich auch diese Befugnis der Kommission gestrichen und dem mitgliedstaatlichen Verfahren angeglichen. Nach Art. 27 Abs. 3 konnte die Kommission nämlich nur noch jene Verhaltensregeln veröffentlichen, zu denen die Art. 29-Datenschutzgruppe eine positive Stellungnahme abgegeben hatte. Am Ende des politischen Aushandlungsprozesses konnte sich der nördliche Block mit seiner Forderung, die gemeinschaftlichen Datenschutzregelungen grundsätzlich auf dem Prinzip der (regulierten) Selbtsregulierung fußen zu lassen, somit nicht durchsetzen. Verhaltensregeln stellten zwar ein zentrales Element von auf Selbstregulierung fußenden Gesetzen dar, doch kam ihnen in der DS-RL eine lediglich komplementäre und nicht die von den Richtliniengegnern gewünschte staatliche Regulierung substituierende Rolle zu (Simitis 2001, 109 f.).

Dem Regulierungsziel der Richtlinie, die Verarbeitung personenbezogener Daten an Bedingungen und Pflichten (so z. B. insbesondere die Zweckbindung) zu knüpfen und die Einhaltung dieser durch externe Kontrollinstanzen umfassend und konsequent kontrollieren zu lassen, entsprechend (Simitis u. a. 2019, 196 Rn. 142), legten die Art. 28–30 DS-RL jene die Einrichtung der Kontrollinstanzen betreffenden Spezifika nieder. Nachdem bereits der überarbeitete Richtlinienentwurf den Wünschen der Aufsichtsbehörden hinsichtlich der Erweiterung ihrer Befugnisse deutlich entgegengekommen war, wurden die entsprechenden Befugnisse in der finalen DS-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

RL noch weiter ausgebaut. So sah Art. 28 die Überwachung der Umsetzung der DS-RL durch die Aufsichtsbehörden in völliger Unabhängigkeit vor und Art. 28 Abs. 2 sah darüber hinaus auch explizit die Anhörung der Datenschutzbehörden bei der Ausarbeitung datenschutzpolitischer Maßnahmen vor. Art. 28 Abs. 3 eröffnete den Aufsichtsbehörden zudem die Möglichkeit der Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen und ging damit über das beispielsweise in Deutschland geltende Recht, das die Weiterreichung identifizierter Probleme an den Bundestag oder die Landtage bzw. die Mitteilung gegenüber der Öffentlichkeit in Form jährlicher Berichte vorsah, deutlich hinaus. Zudem erhielten Aufsichtsbehörden im Rahmen von Art. 28 Abs. 3 auch das Klagerecht für Verstöße gegen die im nationalen Recht umgesetzten Vorgaben der DS-RL und Verantwortliche im Gegenzug die Möglichkeit des Rechtswegs gegen Entscheidungen der Aufsichtsbehörden.

Die Fähigkeit zur Auslegung der Datenschutzregelungen seitens der einzelnen Aufsichtsbehörden wurde allerdings zugleich durch das Ziel der Harmonisierung der europäischen Datenschutzgelungen beschränkt. Wichtigster Ausdruck dieses Ziels auf dem Gebiet des institutionellen Datenschutzes war die in Art. 29 festgeschriebene Entscheidung zur Gründung einer Datenschutzgruppe[131] – der sog. Art. 29-Datenschutzgruppe, die in den folgenden Jahrzehnten prägend für den europäischen Datenschutz werden sollte. Sie wurde insbesondere damit beauftragt, zu einer einheitlichen Anwendung der Richtlinie beizutragen (Art. 30 Abs. 1 lit. a), die Kommission hinsichtlich des Schutzniveaus in der EU und in Drittländern (Art. 30 Abs. 1 lit. b) sowie bei jedweder Erarbeitung datenschutzpolitischer Maßnahmen (Art. 30 Abs. 1 c) zu beraten. In Art. 30 Abs. 3 wurde zudem ausdrücklich anerkannt, dass die Datenschutzgruppe in eigener Initiative zu allen von ihr als wichtig bewerteten Fragen, die den Schutz personenbezogener Daten in der Gemeinschaft betreffen, Stellung nehmen können sollte.

Neben der Art. 29-Datenschutzgruppe, die sich der Harmonisierung der Datenschutzregeln widmen sollte, wurde im Rahmen von Art. 31 die Gründung eines weiteren Ausschusses zur Verteidigung der Interessen der Mit-

131 Bestehend aus je einem Vertreter der nationalen Aufsichtsbehörden, einem Vertreter der für die Datenschutzaufsicht über die Unionsorgane zuständigen Behörde und einem Vertreter der Europäischen Kommission (Art. 29 (2)).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gliedstaaten, bestehend aus je einem Vertreter eines jeden Mitgliedstaates und einem Vertreter der Europäischen Kommission, vorgesehen.[132]

Für die Umsetzung der Richtlinienvorgaben in nationales Recht wurde in Art. 32 eine Frist von drei Jahren nach ihrer Annahme vereinbart.

In Art. 33 wurde schließlich festgelegt, dass die Kommission dem Europäischen Parlament sowie dem Ministerrat regelmäßig, und erstmals sechs Jahre nach Annahme der Richtlinie einen Bericht über die Durchführung der Richtlinie und gegebenenfalls über notwendige Änderungsvorschläge vorzulegen hat.

3.2.2.8 Fazit: Bewertung der DS-RL

Gemessen an anderen damals in Kraft befindlichen Datenschutzgesetzen bzw. Datenschutz-Instrumenten können sowohl der 1990er-Richtlinienvorschlag als auch die letztendliche DS-RL sicherlich als innovativ gelten. Gemessen am Inhalt der damaligen europäischen Datenschutzgesetze stellten sie dagegen eher eine diffuse Konservierung bestehender Gesetze denn eine ernsthafte Weiterentwicklung dar (Simitis 1995, 451, 2001, 111). Dies hatte zwei Gründe. Zum *einen* war die Kommission sehr darum bemüht, für ihren Richtlinienvorschlag die Zustimmung möglichst vieler Mitgliedstaaten zu gewinnen. Folglich war der bestimmende Faktor der Richtliniengestaltung die Erhöhung der Wahrscheinlichkeit seiner Verabschiedung durch die eklektizistische Inkorporation möglichst vieler mitgliedstaatlicher Rechtselemente und nicht die Erarbeitung eines konsistenten und innovativen Datenschutzgesetzes (Simitis 1995, 2001). Viele unklare Formulierungen in der Richtlinien führten zudem bereits damals zu der Kritik, dass auf die Verabschiedung der Richtlinie *endlose Auslegungskontroversen* folgen würden (Simitis 2001, 130). Zum *anderen* führte aber auch die im politischen Prozess der EG angelegte Notwendigkeit der Erzielung von Kompromissen dazu, dass Möglichkeiten zur Weiterentwicklung und Harmonisierung der Richtlinie verspielt wurden. Letztlich versuchte die

132 Die Befürchtung, dass der Art. 31-Ausschuss die Gewährleistung des Schutzes personenbezogener Daten und die Weiterentwicklung bestehender Datenschutzregelungen in ähnlichem Maße behindern würde, wie der beratende Ausschuss der Datenschutz-Konvention, der seitens der Vertragsstaaten eher zur Rechtfertigung von Divergenzen und der Bekämpfung von Vorschlägen zur Weiterentwicklung der Datenschutzregelungen genutzt wurde, bewahrheitete sich immerhin nicht (Simitis 2001, 141).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommission, jeden Konflikt zu vermeiden, der aus ihrer Sicht die Verabschiedung der Richtlinie gefährdet hätte. Entsprechend wurden selbst in kritischen Fällen nationale Abweichungen von den Richtlinien-Vorgaben toleriert.[133] Die Unklarheit der Regelungen spiegelte somit den schwierigen Gesetzgebungsprozess aufgrund der unterschiedlichen Positionen der mitentscheidenden Instanzen, insb. im Rahmen des Ministerrats, wider (Simitis 2001, 112). Simitis attestierte daher: „Das mühsam zustandegekommene einheitliche Regelwerk droht wieder in seine nationalen Bestandteile zu zerfallen, die angestrebte ‚Harmonisierung' riskiert vollends zur Fiktion zu geraten." (Simitis 1997, 282 f.). Angesichts der sich anbahnenden Probleme hinsichtlich der Erreichung der angestrebten Harmonisierung legte die Kommission ihre Hoffnung schließlich in die Implementierung der Richtlinie (Simitis 2001, 111).

Das am Ende dominierende Verständnis zum Datenschutz war somit keines, das Datenschutz als Grundrecht betrachtete, sondern ein wirtschaftspolitischer Blick auf das Thema: Die DS-RL konnte nur verabschiedet werden, weil ansonsten der freie Verkehr personenbezogener Daten in der Gemeinschaft, oder besser, im gemeinsamen Binnenmarkt, gefährdet worden wäre (Simitis 1997, 282).

Die entscheidenden Akteure während der Aushandlung der Richtlinie waren die Mitgliedstaaten und letztlich waren es die unter den Mitgliedstaaten ausgefochtenen Konflikte, die entscheidenden Einfluss auf die Ausgestaltung der Richtlinie nehmen sollten. Unterstützt wurden die datenschutzkritischen Mitgliedstaaten sowohl von der europäischen als auch US-amerikanischen Wirtschaft. Während die Ablehnung auf Seiten von Mitgliedstaaten und Privatwirtschaft angesichts des Desinteresses, das diese Akteure in vorangegangenen Jahrzhenten an Gemeinschaftsregelungen zum Datenschutz gezeigt hatten, nicht verwunderte, tat es die Kritik am *zu hohen* Schutzniveau des ursprünglichen Richtlinienvorschlags, die von Seiten des Europäischen Parlaments kam, umso mehr. Als konsequente Vertreter eines hohen Datenschutzniveaus traten einzig die europäischen Datenschutzaufsichtsbehörden auf. Die Kommission war im Dilemma gefangen, einerseits ein hohes Schutzniveau zu befürworten und andererseits

133 Beispielhaft sei an dieser Stelle die Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 8 DS-RL genannt. Dieser verbietet im Rahmen des ersten Absatzes zunächst die Verarbeitung, schafft im zweiten Absatz allerdings dermaßen weitreichende nationale Ausnahmeregelungen, dass vom zuvor formulierten Verbot kaum etwas übrig bleibt (Simitis 2001, 112).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Verabschiedung der Richtlinie durch Zugeständnisse gegenüber den Mitgliedstaaten und dem Parlament nicht zu gefährden.

Trotz der im Aushandlungsprozess vorgenommenen zahlreichen Senkungen des Schutzniveaus stellte die DS-RL 95/46/EG zum Zeitpunkt ihrer Verabschiedung das weitreichendste Datenschutzinstrument der Welt dar. Schließlich sollte die Richtlinie im Laufe der Jahre auch die Rolle der Datenschutz-Konvention ablösen und zum weltweit einflussreichsten Datenschutzinstrument aufsteigen (Greenleaf 2012; Raab und Bennett 2003).

Zu den markantesten Unterschieden der Richtlinie gegenüber der Konvention zählen die Stärkung der informationellen Selbstbestimmung der Betroffenen, die Einführung spezifischer Regelungen für Datentransfers in Drittstaaten, die Schaffung von Beschwerde- und Klagemöglichkeiten für Betroffene, die Einführung von Meldepflichten und gegebenenfalls der Vorabkontrolle von Verarbeitungen sowie die Beschränkung der automatisierten Verarbeitung personenbezogener Daten. Insbesondere mit der Verpflichtung der Mitgliedstaaten auf die Einrichtung einer Datenschutzaufsichtsbehörde und der Art. 29-Datenschutzgruppe ging der Richtlinienvorschlag weit über die Datenschutz-Konvention hinaus.

3.2.2.9 Implementierung der DS-RL in den Mitgliedstaaten

Der folgende Unterabschnitt widmet sich der Umsetzung der Vorgaben der Datenschutzrichtlinie 95/46/EG in nationales Recht. Fokussiert wird dabei vor allem die Einhaltung des zur Umsetzung vorgegebenen Zeitrahmens. Im Anschluss wird am Beispiel der Umsetzung in der BRD verdeutlicht, wie gering das Interesse an einer harmonisierten Umsetzung der DS-RL in einigen Mitgliedstaaten gewesen ist. Darauf, inwiefern sich diese Divergenz im Detail äußerte, wird an späterer Stelle (vgl. 3.3.3) eingegangen.

Die in der DS-RL vereinbarte Dreijahresfrist sah die Umsetzung der Richtlinienvorgaben in nationales Recht innerhalb von drei Jahren nach ihrer Annahme, also bis zum 24. Oktober 1998 vor. Doch sollte sich die EU-weite Implementierung der Richtlinie deutlich verzögern. Lediglich Italien, Griechenland, Großbritannien, Portugal und Schweden setzten die Richtlinienvorgaben innerhalb der vorgegebenen Frist um (vgl. grün markierte Mitgliedstaaten in Tabelle 3-4).[134] Belgien und Finnland folgten mit kurzer Verspätung im Dezember 1998 bzw. Mitte 1999. Österreich und Spanien

134 Von den fünf Mitgliedstaaten, die zu Beginn des politischen Aushandlungsprozesses der DS-RL noch über keine Datenschutzgesetze verfügten, hatten drei – Belgien,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

setzten die Revision ihrer Datenschutzregelungen zum Jahresbeginn 2000 um, Dänemark Mitte 2000 (vgl. graumarkierte Mitgliedstaaten in Tabelle 3-4).

EG-Mitglieder (Stand: 2001)	Fristgemäße Umsetzung der Richtlinie	(Verabschiedung bzw.) Inkrafttreten der Implementierung	Notifikation an die Kommission
Belgien	Verzögert	11.12.1998	
BRD	Deutl. verzögert	23.05.2001	2001
Dänemark	Verzögert	01.07.2000	
Finnland	Verzögert	02.06.1999	
Frankreich	Deutl. verzögert	20.10.2005	2001
Griechenland	Fristgemäß	10.04.1997	
Irland	Deutl. verzögert	01.07.2003	2001
Italien	Fristgemäß	08.05.1997	
Luxemburg	Deutl. verzögert	01.12.2002	
Niederlande	Deutl. verzögert	01.09.2001	2001
Österreich	Verzögert	01.01.2000	
Portugal	Fristgemäß	27.10.1998	
Schweden	Fristgemäß	24.10.1998	
Spanien	Verzögert	14.01.2000	
Verein. Königreich	Fristgemäß	(16.07.1998) 01.03.2000[135]	

Tabelle 3-4: Implementierung der DS-RL in den Mitgliedstaaten (Commission of the European Communities 2003, 3; European Commission 2005; Korff 2002, 1)

Schwieriger gestaltete sich die Umsetzung hingegen in Deutschland, Frankreich, Irland, Luxemburg sowie in den Niederlanden (vgl. dunkelgraumarkierte Mitgliedstaaten in Tabelle 3-4). Nachdem diese fünf Mitgliedstaaten auf die von der Kommission zuvor versandte Aufforderung nicht reagiert

Portugal und Spanien – bereits im Laufe der Verhandlungszeit entsprechende Gesetze erlassen. Lediglich Italien und Griechenland hatten zum Zeitpunkt der Verabschiedung der DS-RL noch immer überhaupt keine Datenschutzgesetze in Kraft. Die zum 1. Januar 1995 der Gemeinschaft beigetretenen Mitgliedstaaten Österreich und Schweden hatten bereits lange vor ihrem Beitritt Datenschutzgesetze erlassen. Das dritte Neumitglied Finnland erlies 1992 ein Datenschutzgesetz (vgl. auch Tabelle 3-1).

135 Die Novelle des Data Protection Act wurde zwar Mitte 1998 verabschiedet, die meisten Änderungen traten allerdings zum 1. März 2000 in Kraft.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

hatten, beschloss die Kommission Ende 1999 die Initiierung von Vertragsverletzungsverfahren vor dem EuGH gemäß Art. 226 EG-Vertrag (Europäische Kommission 2000a) und leitete diese schließlich am 1. Dezember 2000 ein (Europäische Union 2001). Als Deutschland, Frankreich, die Niederlande und Irland daraufhin schließlich konkrete Schritte zur Richtlinienumsetzung ankündigten, zog die Kommission ihre gegen diese Staaten gerichtete Klage wieder zurück (Commission of the European Communities 2003, 3). Einzig Luxemburg wurde am 4. Oktober 2001 vom EuGH aufgrund der Nichtumsetzung der DS-RL verurteilt (ECJ 2001).

Gerade der Implementierungsprozess in Deutschland und Frankreich war sinnbildlich für die Ablehnung harmonisierter Richtlinienvorgaben. Beide Länder hatten ein großes Interesse daran, den mitgliedstaatlichen Entscheidungsspielraum dahingehend zu nutzen, ihre nationalen Regelungen so weit es geht beizubehalten. Am Beispiel der Richtlinienumsetzung in Deutschland soll dies im Folgenden verdeutlicht werden: So hatte die Regierungskoalition aus CDU/CSU und der FDP (schwarz-gelbe Koalition) bereits die BDSG-Novelle des Jahres 1990 nicht dazu genutzt, ein effektives und modernes Datenschutzrecht zu entwickeln. Weder überzeugte die 1990er-Novelle im Hinblick auf die Harmonisierung von BDSG und den LDSG, noch nahm sie Rücksicht auf die informations- und kommunikationstechnologischen Veränderungen, die seit der vorherigen BDSG-Novelle im Jahr 1976 eine Anpassung der Regelungen erforderlich gemacht hatten (Simitis u. a. 2019, 173 ff.). Im Falle der Umsetzung der DS-RL wiederholte sich dieses Desinteresse. Nachdem die schwarz-gelbe Koalition weitgehend untätig geblieben war, beharrte das für die Novellierung des BDSG zuständige Bundesministerium des Innern (BMI) auch nach der im Jahr 1998 erfolgten Regierungsübernahme durch die rot-grüne Koalition bestehend aus SPD und Grünen auf der Position, dass geringfügige Änderungen des BDSG der Implementationsvorgabe bereits ausreichend Rechnung tragen würden. In der folgenden Debatte auf Grundlage des BDSG-Entwurfs vom 11. März 1999 waren vor allem sicherheitspolitische Bedenken im Hinblick auf die vorgesehenen Regelungen zur Videoüberwachung, die Kritik der Datenschutzbeauftragten am vorgeschlagenen Datenschutzaudit sowie die Kritik der Länder an der Übertragung der Überwachungsaufgaben an eine einzige, unabhängige Instanz dominant. Nachdem die Kommission das Vertragsverletzungsverfahren gegen Deutschland und die übrigen Staaten initiiert hatte, entschied sich das BMI für einen Strategiewechsel: „Auf eine erste mehr oder weniger ausschließlich der Anpassung an die EG-Vorga-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ben gewidmete Novellierungsstufe sollte möglichst bald eine zweite Phase folgen, deren Ziel eine konsequente Modernisierung des Datenschutzes sein müsste" (Simitis u. a. 2019, 177 Rn. 64). Dem in der Folge mit der Stimmenmehrheit von SPD und Grünen (CDU/CSU sowie FDP enthielten sich, während die PDS dagegen stimmte) unter Zeitdruck am 6. April 2001 verabschiedeten „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze", das am 22. Mai 2001 in Kraft trat, fehlte es an einem Mindestmaß an Verständlichkeit, Lesbarkeit und Normenklarheit. Positiv gegenüber der 1990er-Novelle war lediglich etwa die Verbesserung der Rechte des BfDI hervorzuheben, doch wurde die Gewährleistung von dessen Unabhängigkeit entgegen den Richtlinienvorgaben nicht angegangen.[136]

3.2.3 Drittstaatentransfers und Safe Harbor-Vereinbarung

Nachdem die Datenschutzrichtlinie 95/46/EG verabschiedet worden war und während noch die ersten Umsetzungen in nationales Recht erfolgten, richtete sich das Augenmerk in der zweiten Hälfte der 1990er wieder auf das Thema der Drittstaatentransfers. Dieses war mit der Richtlinienverabschiedung der nationalen Datenschutzpolitik weitgehend enthoben worden. Stattdessen sollten Transfers in Drittstaaten fortan ausschließlich auf Basis der Art. 25 und 26 DS-RL erfolgen.

Ursprünglich hatten die Kommission und die Datenschutzbeauftragten intendiert, dass ein solcher Transfer grundsätzlich nur auf Basis eines Angemessenheitsbefundes der Kommission (Art. 25) erfolgen darf. Am Ende der Verhandlungen zur DS-RL erfuhr diese Regel jedoch eine Erweiterung um zahlreiche Alternativen, z. B. die Übertragung auf Basis der Einwilligung des Betroffenen, bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags, für die Wahrung eines wichtigen öffentlichen Interesses oder lebenswichtiger Interessen oder im Falle der Übermittlung aus einem öffentlichen Register (Art. 26 Abs. 1 lit. a bis f). Daneben sah Art. 26 Abs. 2 die Möglichkeit eines Datentransfers in einen Drittstaat, der kein angemessenes Schutzniveau im Sinne von Art. 25 gewährleistet, auf Basis der Genehmigung eines Mitgliedstaates vor, sofern der für eine Verarbeitung Verantwortliche, trotz des Fehlens staatlicher Datenschutzvorgaben, selbst ausreichende Datenschutzgarantien einräumt. Gerade die Datenschutzauf-

136 Für eine umfassendere Diskussion von Verbesserungen und Schwachstellen, siehe: (Simitis u. a. 2019, 177 Rn. 66)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sichtsbehörden bestanden bei der Umsetzung jedoch darauf, dass die *Ausnahme*regelungen tatsächlich als solche interpretiert und nicht zum Regelfall würden (Simitis 2001, 120). Der damalige stellvertretende Berliner Datenschutzbeauftragte Alexander Dix äußerte beispielsweise im Zusammenhang mit dem auf Basis einer Vertragslösung erfolgenden Datentransfer zwischen der Deutschen Bahn und der US-amerikanischen Citibank, dass die Festlegung vertraglicher Normen seitens privater Unternehmen die nationale Gesetzgebung in einem Drittstaat lediglich ergänzen und unterstützen, aber nicht ersetzen könnte (Dix 1996). Nach der Verabschiedung der DS-RL waren daher Drittstaaten, die ein Handelsinteresse mit der Europäischen Gemeinschaft hatten, das die Verarbeitung personenbezogener Daten tangierte, gefordert, ein angemessenes Datenschutzniveau zu garantieren oder in Kauf zu nehmen, dass die EG Datentransfers in diese Staaten blockierte. Verschiedene Staaten unternahmen in der Folge Anstrengungen, um ihre Datenschutzregelungen an die DS-RL anzupassen. Insofern wirkte die DS-RL, wie schon zuvor die Datenschutz-Konvention des Europarats, durchaus als internationale Normgeberin.[137]

Als besonders kompliziert sollte sich die Feststellung der Angemessenheit in Bezug auf die Vereinigten Staaten, den Haupthandelspartner der Europäischen Gemeinschaft bzw. seiner Mitgliedstaaten, erweisen. Die Regulierung des Schutzes personenbezogener Daten basierte in den Vereinigten Staaten Ende der 1990er-Jahre noch immer auf sektoralen Datenschutzgesetzen. Für die Mehrheit der Sektoren, in denen personenbezogene Daten verarbeitet werden, so insbesondere im Bereich des für grenzüberschreitende Datentransfers relevanten E-Commerce, galt hingegen ein auf Selbstregulierung gestützter Regulierungsansatz.[138] So sollte der individuelle Datenschutz vor allem durch das Vertrauen auf Zertifizierungsstellen

137 So passten sich etwa die im Jahr 2000 verabschiedeten Neufassungen der norwegischen und isländischen Datenschutzgesetze der DS-RL an. Auch der Europarat bemühte sich bei seinen Beratungen über neue Empfehlungen, der DS-RL Rechnung zu tragen. Schließlich trug auch die Prüfung und Feststellung der Angemessenheit des Datenschutzes in Drittstaaten zur internationalen Durchsetzung der europäischen Datenschutzstandards bei. Folgende Angemessenheitsbefunde stellte die Kommission aus: Schweiz 2000, Kanada 2002, Argentinien 2003, Israel 2011, Uruguay 2012, Neuseeland 2013 (Simitis u. a. 2019, 183 Rn. 89 und Fn. 231).

138 Zuletzt hatte das 1997 veröffentlichte *Framework for Global Electronic Commerce* der Clinton-Administration diesem Ansatz zusätzlich Nachdruck verliehen und dazu beigetragen, Privatheit als Sache des Individuums aufzufassen, die als vertrauensbildende Maßnahme den Erfolg von E-Commerce garantieren sollte (Clinton und Gore Jr. 1997).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

gewährleistet werden, indem Webseiten-Betreiber die Zertifizierung ihrer Webseite beantragen und Gütesiegel-Agenturen wie TRUSTe oder BBBOnline diese dann ausstellten. In strittigen Fällen sollten, ebenfalls auf Selbstregulierung fußende, alternative Streitschlichtungsverfahren (alternative dispute resolution mechanism – ADR) Abhilfe schaffen (A. Busch 2012a, 413–15; Farrell 2003, 277). Klar war, dass das Fehlen eines US-weit einheitlichen Datenschutzgesetzes und die mangelnde Bereitschaft auf Seiten der zuständigen US-Stellen in Bezug auf die Verabschiedung einheitlicher Datenschutzregelungen zu einem Problem im Zusammenhang mit Datentransfers in die Vereinigten Staaten werden würden. Die Situation erinnerte an die Anfangszeit der Verhandlungen zur DS-RL. Zu Beginn der Verhandlungen hatten US-amerikanische Datenschutzbefürworter darauf gedrängt, ein einheitliches Datenschutzgesetz in den USA auszuarbeiten, damit der transatlantische Datenverkehr weiterhin reibungslos stattfinden könnte. Insbesondere bestand die Hoffnung, dass die US-amerikanische datenverarbeitende Wirtschaft die Verabschiedung von US-Datenschutzgesetzen aus ihrem wirtschaftlichen Eigeninteresse heraus fördern würde, damit Datentransfers aus der EG auch weiterhin erfolgen könnten (Prisclla M. Regan 1993). Anstatt bei der eigenen Regierung zu lobbyieren, übten US-amerikanische Wirtschaftsvertreter allerdings gemeinsam mit ihren europäischen Verbündeten Druck auf die Europäischen Entscheider aus, um eine Lockerung der europäischen Vorgaben zu Drittstaatentransfers zu erreichen. Ihre Strategie hatte Erfolg und statt des strengeren Gleichwertigkeitserfordernisses hatte sich in den Verhandlungen das flexiblere Angemessenheitserfordernis durchgesetzt (Priscilla M. Regan 1999). In ähnlicher Weise stand in der Zeit nach der Verabschiedung der DS-RL die Frage im Raum, ob die Vereinigten Staaten zum Zwecke ungehinderter Wirtschaftsflüsse einheitliche Datenschutzregelungen in Erwägung ziehen würden (C. J. Bennett und Raab 1997). Doch wieder sollten sich Wirtschaftsinteressen gegenüber Datenschutzinteressen durchsetzen. Die zuständigen US-Regierungsstellen gingen noch bis in die erste Hälfte des Jahres 1998 hinein zunächst wie selbstverständlich davon aus, dass transatlantische Datentransfers auf Basis der in Art. 26 DS-RL festgelegten Ausnahmebedingungen möglich und einheitliche, gesetzliche Datenschutzvorschriften nicht nötig sein würden (A. Busch 2012a, 414). Ira Magaziner, in der Clinton-Administration zuständig für den Bereich E-Commerce, ging sogar so weit, die drohende Blockade von Datentransfers in die Vereinigten Staaten vor die Welthandelsorganisation zu bringen, mit der Begründung, dass diese ein nichttarifäres Handelshemmnis darstellen würden (Farrell 2004, 5 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Europäische Kommission hatte zur selben Zeit zunächst zwei mögliche Szenarien zur Hand, mit denen ihr Ziel einer möglichst geringfügigen Beeinträchtigung des transatlantischen Datenverkehrs erreicht werden könnte. Erstens stand die Frage im Raum, ob der sektorspezifische Datenschutz in der Vereinigten Staaten als angemessen nach Art. 25 DS-RL bewertet werden könnte. Eine von der Europäischen Kommission beauftragte und von den beiden US-amerikanischen Datenschutz-Professoren Paul Schwartz und Joel Reidenberg erstellte Studie lieferte zwar keine klaren Antworten auf diese Frage, doch bestanden die zuständigen Kommissionsstellen trotzdem darauf, dass formelle gesetzliche Regelungen im Rahmen eines allgemeinen Datenschutzgesetzes erforderlich seien (A. Busch 2012a, 415; Priscilla M. Regan 2003, 272). Zweitens bestand gemäß Art. 25 DS-RL grundsätzlich die Möglichkeit, bei der Berücksichtigung der Angemessenheit eines Drittstaates auch die im jeweiligen Staat geltenden Standesregeln, also auf Selbstregulierung fußende Maßnahmen, zu berücksichtigen. Doch auch diese Möglichkeit musste ausgeschlossen werden, da die Datenschutzbehörden diese Möglichkeit, wie bereits erwähnt, vehement ablehnten (vgl. Dix 1996). Insofern waren beide Seiten gefordert, Verhandlungen aufzunehmen.

Die ersten informellen Gespräche wurden Ende 1997, also etwa ein Jahr vor Inkrafttreten der DS-RL aufgenommen. Während die Zuständigkeit für die Verhandlungen auf europäischer Seite bereits klar war,[139] kristallisierte ssie ich für die US-Seite erst nach einiger Verzögerung heraus. Schließlich übernahm David Aaron, Staatssekretär für internationalen Handel im US-Handelsministerium, die Verhandlungsführung (Farrell 2004, 6 f.). Zu Beginn der eigentlichen Verhandlungen Anfang 1998 verhärteten sich die Fronten zunächst noch weiter. Die EG-Seite verwies auf die geltenden Gemeinschaftsgesetze und beharrte folglich auf der Position, dass die Vereinigten Staaten entsprechende staatliche Regulierungen erlassen müssten, um einen Angemessenheitsbefund ausgestellt bekommen zu können. Die US-Seite dagegen zeigte keinerlei Interesse am Erlass umfassender Datenschutzregulierungen. Einerseits widersprach dies dem US-amerikanischen (Selbst-)Regulierungsansatz und andererseits wurden die Forderungen der Europäischen Gemeinschaft in der US-Regierung im Sinne einer interna-

139 Geführt wurden die Beratungen von dem britisch-stämmigen Leiter der Generaldirektion Binnenmarkt und Dienstleistungen (GD Markt), John Mogg, unter Hinzuziehung weiterer GDs, insbesondere der Generaldirektion Auswärtige Beziehungen (González Fuster 2014, 139).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

tionalen Machtfrage als ein *Herumschubsen* wahrgenommen, dem man keinesfalls nachgeben würde. Stattdessen verlangten die US-amerikanischen Verhandlungsführer, dass die in den Vereinigten Staaten geltenden sektoriellen Datenschutzregulierungen und Selbstregulierungsmaßnahmen als angemessen beurteilt würden. In der Folge gerieten die Verhandlungen schließlich in einen Stillstand (Farrell 2003, 292, 2004, 7). Die Verhandlungsposition der Vereinigten Staaten litt zeitgleich unter der nur sehr schleppend verlaufenden Umsetzung selbstregulierter Zertifizierungsmaßnahmen. Selbst das erste, von TRUSTe unter Beteiligung großer Unternehmen initiierte, Gütesiegel-Programm, das deutlich laxere Datenschutz-Vorgaben für Webseiten enthielt, zu denen sich teilnehmende Unternehmen freiwillig verpflichten sollten, als die DS-RL sie in der EG vorschrieb, wurde nur von wenigen Unternehmen in Anspruch genommen. Dies gab der europäischen Position Auftrieb und untermauerte den Anspruch der EG, dass für einen wirksamen Schutz personenbezogener Daten verbindliche Regelungen vonnöten waren. Zugleich übten Datenschutzbefürworter in den USA Druck auf Regierungsstellen aus, um den Datenschutz bei E-Commerce-Transaktionen zu gewährleisten. Die Drohkulisse der DS-RL wurde von diesen Datenschutzbefürwortern zur Untermauerung ihres Arguments genutzt. Erst als zu Beginn des Jahres 1998 zunehmend klarer wurde, dass mit dem Inkrafttreten der DS-RL ernsthafte Konsequenzen für die Geschäftspraktiken US-amerikanischer Unternehmen drohten, regte sich die zuständige US-Administration. Unter Androhung des Erlasses verbindlicher staatlicher Regulierungen erhöhten Politiker wie Ira Magaziner den Druck auf Unternehmen zur Inanspruchnahme von E-Commerce-Gütesiegeln. In der Folge nahm die Mitgliederzahl von TRUSTe bis Mitte 1998 rapide zu. Da die US-Administration befürchtete, dass diese Maßnahme nicht ausreichend sein würde, bewegte sie gemeinsam mit Unternehmensvertretern die anerkannte Selbstregulierungsorganisation Better Business Bureau (BBB) dazu, ein Datenschutz-Gütesiegel-Programm aufzusetzen. Nach anfänglichem Widerstand bei der BBB wurde nach der Zusicherung finanzieller Mittel das auf Online-Streitschlichtungen spezialisierte BBBOnline ins Leben gerufen (Farrell 2003, 291). Diese Fortschritte wirkten auf Seiten der EU nur wenig überzeugend. In der Folge blieben beide Seiten bei ihrer jeweiligen Maximalforderung der Anerkennung ihres Regulierungsmodells, sodass der Verhandlungsstillstand zunächst erhalten blieb (ebd.).

Eine Überwindung bahnte sich erst mit dem von David Aaron eingebrachten Vorschlag für einen sog. *Safe Harbor* an. Demnach sollten

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zwischen der EG und den USA eine Reihe von Prinzipien ausgehandelt werden, zu deren Einhaltung sich US-Unternehmen, die ein Interesse an transatlantischen Datentransfers haben, verpflichten können sollten. Diese im Rahmen des Safe Harbor-Abkommens festgelegten Prinzipien sollten schließlich seitens der Europäischen Kommission als angemessen im Sinne der DS-RL anerkannt werden. Der grundlegenden Idee nach würden weder die Vereinigten Staaten ihr auf Selbstregulierung fußendes Regime ändern müssen, noch müsste die Europäische Gemeinschaft auf zentrale datenschutzrechtliche Bestandteile verzichten (A. Busch 2012a, 416 f. Farrell 2003, 291–93). Am 4. November 1998 legte Aaron schließlich einen ersten Entwurf für Safe Harbor-Prinzipien vor und rief US-Wirtschaftsvertreter dazu auf, diesen zu kommentieren. Die vorgeschlagenen Prinzipien waren Ausfluss der in den Vereinigten Staaten unter dem Namen *Fair Information Practices* bekannten Datenschutzprinzipien, die im Grundsatz auch in den von den Vereinigten Staaten angenommenen OECD-Richtlinien enthalten waren. Die sieben Prinzipien umfassten: Informationspflichten der Verarbeiter, Wahlmöglichkeiten der Betroffenen, Weitergabe verarbeiteter personenbezogener Daten, Datensicherheit, Datenintegrität/Zweckbindung, Auskunftsrechte der Betroffenen und schließlich das Thema der Durchsetzung. Der anderthalb Jahre andauernde und vier Phasen umfassende Konsultationsprozess auf US-Seite war insbesondere in den ersten zwei Phasen klar von Wirtschaftsinteressen dominiert, die für die Absenkung des in den Safe Harbor-Prinzipien vorgesehenen Schutzniveaus eintraten. Bürgerrechtliche Akteure brachten sich erst in den letzten beiden Phasen ein, konnten jedoch die Abschwächung der Vorgaben zu diesem späten Zeitpunkt nicht mehr verhindern (Priscilla M. Regan 2003, 273).

Während eine Einigung zwischen den Verhandlungsführern auf US- und EG-Seite im Hinblick auf die ersten sechs Themen im Laufe des Jahres 1999 noch vergleichsweise einfach möglich war, gestalteten sich die Diskussionen um das Thema der Durchsetzung als mühevoll. Insbesondere die mitgliedstaatlichen Vertreter der sozialdemokratischen Regierungen Deutschlands und Frankreichs lehnten die Idee eines Safe Harbor-Abkommens bzw. einer auf Selbstregulierung fußenden Lösung grundsätzlich ab. Ein Durchbruch bei den Verhandlungen konnte schließlich erst erzielt werden, als die europäische Verhandlungsdelegation im Januar 2000 nach Washington, D. C. eingeladen wurde und dort im Rahmen eines dreitägigen Workshops die Möglichkeit erhielt, mit den Vertretern der Selbstregulierungsstellen in einen direkten Dialog zu treten. Beobachtern zufolge habe dieser Diskurs

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

schließlich auch die letzten Skeptiker in den Mitgliedstaatsdelegationen davon überzeugen können, dass ein wirksamer Datenschutz auch auf Basis von Selbstregulierung gewährleistet werden könnte. In der Folge konnten die Verhandlungsparteien eine erste informelle Übereinkunft im März 2000 treffen. Am 9. Juni 2000 übermittelte das US-Handelsministerium schließlich die ausgehandelten Safe Harbor-Prinzipien an die Europäische Kommission. Wie üblich, begann das Europäische Parlament nach Erhalt des Kommissionsentwurfs eine Stellungnahme zu erarbeiten und überstellte den Entwurf des Safe Harbor-Abkommens zu diesem Zweck an den LIBE-Ausschuss. Der Bericht der italienisch-stämmigen sozialdemokratischen Europaabgeordneten Elena Ornella Paciotti (SPE, DS) wurde am 21. Juni zunächst vom Ausschuss mit 21 Stimmen (bei 0 Gegenstimmen und 16 Enthaltungen) angenommen und am darauffolgenden Tag schließlich auch vom Parlamentsplenum verabschiedet (Paciotti 2000, 4). Das Parlament bemängelte dabei jedoch nicht nur die konkreten Inhalte des Abkommens (etwa die unzureichende Ausgestaltung der Wahrnehmung von Betroffenenrechten) (ebd., 10, Nr. 7), sondern verwies auch auf folgende drei Aspekte: *Erstens* wurde in Bezug auf die Umsetzung des Safe Harbor-Abkommens in den Vereinigten Staaten grundsätzlich bemängelt, dass bislang lediglich Versprechungen gemacht worden seien, das im Safe Harbor-Abkommen versprochene System allerdings in der Realität nicht ansatzweise praktiziert werde. Insofern sei es fraglich, wie die EG-Verhandlungsführer realistischerweise davon ausgehen könnten, dass in einem Staat bzw. Unternehmen parallel zwei Datenschutzsysteme nebeneinander existieren könnten. Schließlich sollten sich US-amerikanische Unternehmen gemäß Safe Harbor dazu verpflichten, Bürgerinnen und Bürger der Europäischen Union anders zu behandeln als Menschen US-amerikanischer oder sonstiger Nationalität, was eine parallele Datenbankstruktur und viele weitere Maßnahmen erforderlich gemacht hätte (ebd., 9 f., Nr. 2 und 7). *Zweitens* wurde unter Verweis auf die in den Vereinigten Staaten geführten Konsultationen bemängelt, dass die Kommission während der Verhandlungen keine europäischen Unternehmen und Nichtregierungsorganisationen konsultiert hatte (ebd., 10, Nr. 4 und 5). Und *drittens* wurde in Bezug auf die europäischen Unternehmen festgestellt, dass der Abschluss des Safe Harbor-Abkommens zu einem offensichtlichen Wettbewerbsnachteil für diese führe, da somit US-amerikanische datenverarbeitende Unternehmen die Daten europäischer Bürgerinnen und Bürger auf Grundlage weniger

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

strenger Datenschutzregeln verarbeiten dürften als es den europäischen Unternehmen erlaubt war (ebd., 10, Nr. 4).[140]

Trotz der weitreichenden Kritik entschied die Art. 31-Gruppe letztlich einstimmig über die Angemessenheit des Safe Harbor-Abkommens (Farrell 2003, 294). Am 26. Juli 2000 befand die Kommission schließlich über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" gewährleisteten Schutzes, sodass das Safe Harbor-Abkommen am 1. November 2000 in Kraft trat (EU-Kommission 2000a).

Die Beurteilung des Abkommens war in den Folgejahren gespalten. So betonten einige Beobachter, dass die Safe Harbor-Einigung demonstriert hätte, dass auf Grundlage von Deliberation und geteilten sozialen Normen die Überwindung einer zwischenzeitlich als ausweglos geltenden Situation möglich geworden war, ohne dass eine Seite ihre Interessen einseitig durchsetzen konnte oder es zu einer Blockade oder einem Handelskonflikt kam. Darauf aufbauend wurde sogar gemutmaßt, dass Safe Harbor als neues Regulierungsmodell auf die in den USA und der EU geltenden Regulierungssysteme rückwirken, diese also verändern würde und dass Safe Harbor als Modelllösung für künftige transatlantische Dispute im Bereich des Datenaustausch dienen würde (Farrell 2003; vgl. Long und Quek 2002). Andere Autoren waren dagegen deutlich skeptischer und verwiesen einerseits darauf, dass Safe Harbor nicht einfach eine Kompromisslösung gewesen sei, die beiden Seiten in gleichem Maße entgegenkommt, sondern vor allem der Wirtschaft weiterhin weitgehend freien Handlungsraum überlasse und die US-Perspektive sich letztlich durchgesetzt habe. Zudem wurde selbst angesichts der schwachen Safe Harbor-Vorgaben infrage gestellt, in welchem Maße sich die US-amerikanische Datenwirtschaft an diese halten würde (vgl. insb. Priscilla M. Regan 2003).[141]

140 In den Vereinigten Staaten erntete das Abkommen sowohl vonseiten der Wirtschaft als auch vonseiten der Bürgerrechtler Kritik. Vor allem die National Business Coalition on E-Commerce and Privacy, zu deren Mitgliedern General Electric, Home Depot und VISA USA zählten, veröffentlichte eine vernichtende Kritik an den Inhalten des Abkommens auf Grundlage der im März 2000 erfolgten informellen Einigung (National Business Coalition 2000). Die bürgerrechtlichen Kritiker dagegen verwiesen auf das Scheitern das Selbstregulierungsmodells in den Vereinigten Staaten und vertraten konsequenterweise die Ansicht, dass es auch im Falle des Safe Harbor keinen wirksamen Datenschutz gewährleisten würde (TACD 2000).

141 Die letztgenannte Perspektive sollte Recht behalten: Das Abkommen wurde 2015 vom EuGH gekippt (vgl. auch Fn. 405).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.2.4 ISDN-RL 97/66/EG

Gemeinsam mit dem Legislativvorschlag für die DS-RL hatte die Kommission 1990 auch einen *Richtlinienvorschlag zum Schutz personenbezogener Daten und der Privatheit im Telekommunikationsbereich* auf Grundlage des Kooperationsverfahrens veröffentlicht, der aufgrund der hitzigen Debatten um die DS-RL nur wenig Beachtung fand.

Die Erarbeitung der Richtlinie fand im Kontext der seit den 1980er-Jahren laufenden, gemeinschaftlichen Digitalisierungs- und Harmonisierungsbestrebungen sowie der Deregulierungspolitik im europäischen Telekommunikationsbereich statt, die zum 1. Januar 1998 wirksam wurde. Unter Bezugnahme auf die Hervorhebung der Bedeutung angemessener Maßnahmen zum Schutz personenbezogener Daten und der Privatheit im Lichte der technologischen Entwicklungen auf dem Gebiet der Telekommunikation seitens des Europäischen Parlaments und des Ministerrats sowie seitens der Datenschutzbehörden auf der Berliner Konferenz internationaler Datenschutzbeauftragter (Commission of the European Communities 1990, 8, Nr. 18), verfolgte der Richtlinienvorschlag zunächst das Ziel *der Harmonisierung der Vorschriften, die erforderlich sind, um einen gleichmäßigen Schutz der Privatsphäre in der gesamten Gemeinschaft zu gewährleisten und sowohl innerhalb der Mitgliedstaaten als auch grenzüberschreitend den freien Verkehr von Telekommunikationsgeräten und -diensten sicherzustellen* (Art. 1 Abs. 1 ISDN-RL UE). Mittels der Ausweitung bzw. Spezifizierung der in der Rahmenrichtlinie festzulegenden allgemeinen Datenschutz-Grundsätze im Sinne einer sektoralen Regulierung auf den Telekommunikationsbereich sollte auch im Zusammenhang mit der ISDN-RL „the fullest possible protection" (Commission of the European Communities 1990, 6, Nr. 13) erzielt werden. Dazu sollte in allen Mitgliedstaaten die Sicherheit[142] bzw. Vertraulichkeit von Telefongesprächen sichergestellt werden, das ungenehmigte Mithören bzw. die Speicherung von Telefongesprächen sowie neue

142 Die Regelung in Artikels 8 Abs. 1 des ursprünglichen Richtlinienentwurfs der Kommission sah die Gewährleistung eines dem Stand der Technik entsprechenden, angemessenen Schutzes personenbezogener Daten gegen unbefugten Zugriff und unbefugte Verwendung vor. Art. 8 Abs. 2 sah zudem die Benachrichtigung der Betroffenen seitens der Telekommunikationsorganisation im Falle eines besonderen Risikos der Verletzung der Netzsicherheit vor. Diese in Art. 4 der finalen ISDN-RL geregelte Vorschrift sollte später im Rahmen der Aushandlungen zur Novellierung der Nachfolgerrichtlinie der ISDN-RL, der ePrivacy-Richtlinie 2002/58/EG, zur Benachrichtigung im Falle einer Verletzung des Schutzes personenbezogener Daten ausgebaut werden (vgl. Unterabschnitt 3.3.2).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Techniken wie die Rufnummernübermittlung oder die Aufnahme in elektronische Verzeichnisse geregelt werden (Europäische Kommission 1990).

Gemeinsam mit seiner Stellungnahme zur DS-RL bewertete der Wirtschafts- und Sozialausschuss auch die für den Telekommunikationsbereich vorgesehene Richtlinie (WSA 1991, 45–47). Ebenso war auch die – ebenfalls unter Geoffrey Hoon ausgearbeitete – Parlamentsposition zur Telekommunikationsrichtlinie am 11. März 1992 gemeinsam mit Parlamentsposition zur DS-RL verabschiedet worden (Europäisches Parlament 1992).

Wie im Falle der DS-RL, unterbreitete die Kommission auch im Falle dieser Richtlinie bereits vor Beschluss des Gemeinsamen Standpunkts im Ministerrat einen geänderten Richtlinienvorschlag am 23. Juni 1994 *zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere in diensteintegrierenden digitalen Telekommunikationsnetzen (ISDN) und in digitalen Mobilfunknetzen* (Europäische Kommission 1994a).

Der Gemeinsame Standpunkt des Ministerrats in erster Lesung wurde am 12. September 1996 verabschiedet (Ministerrat 1996). Dem üblichen Mitentscheidungsverfahren gemäß verfolgten Ministerrat und Parlament das Ziel, am Ende der zweiten Lesung eine politische Übereinkunft zu erzielen. Zu dieser sollte es aber zunächst nicht kommen. Das Parlament bestätigte die Position des Ministerrats in seiner zweiten Lesung am 16. Januar 1997 nämlich nicht uneingeschränkt, sondern machte elf unter dem Rapporteur Medina Ortega ausgearbeitete Änderungsvorschläge geltend (Europäisches Parlament 1997a). Gefordert wurde zum einen eine bessere Gewährleistung der gemeinschaftsweiten Harmonisierung im Bereich der Telekommunikation bzw. störte sich das Parlament an den seitens des Ministerrats geforderten nationalen Freiräumen (vgl. Änd. 3 betreffend EG 7 des Gemeinsamen Standpunkts des Rats). Daneben plädierte das Parlament für die Wiedereinfügung des Rechts der Betroffenen, die Nichtaufnahme in ein Teilnehmerverzeichnis (z. B. Telefonbuch) kostenfrei beantragen zu können (vgl. Änd. 9 betreffend Art. 11 Abs. 2 des Gemeinsamen Standpunkts des Rats). Dieses war im überarbeiteten Entwurf der Kommission aus dem Jahr 1994 bereits enthalten gewesen, vom Ministerrat in seinem Gemeinsamen Standpunkt allerdings wieder gestrichen worden, indem den Betreibern von Telekommunikationsdiensten die Möglichkeit eröffnet wurde, dafür eine Gebühr zu verlangen. Zudem hatte das Parlament für die Ausweitung der Richtlinienregelungen auf juristische Personen plädiert, um „vor allem die KMU in bezug [sic] auf ihre Aufnahme

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

in öffentliche Verzeichnisse sowie in bezug [sic] auf unerbetene Anrufe" (Marlies Mosiek-Urbahn in: Europäisches Parlament 1997c, 236) zu schützen. Nachdem die Kommission zunächst ihrer weitgehenden Unterstützung für die Änderungen des Parlaments Ausdruck verliehen hatte (Europäische Kommission 1997), machte die Weigerung des Ministerrats, die Änderungswünsche des Parlaments anzunehmen, die Einsetzung eines Vermittlungsausschusses[143] erforderlich. Im Ergebnis konnte sich das Parlament vor allem mit seiner Forderung nach Einbezug auch juristischer Personen in den Anwendungsbereich der Richtlinie durchsetzen, während sich bezüglich der kostenfreien Nichtaufnahme in Verzeichnisse der Ministerrat – bis auf kleinere Konzessionen – weitgehend durchsetzen konnte und beim Thema Harmonisierung ein Kompromiss erzielt wurde (Europäisches Parlament 1997c).

Der vom Vermittlungsausschuss gebilligte gemeinsame Entwurf des Parlaments und des Rates wurde in dritter Lesung am 20. November 1997 vom Parlament (Europäisches Parlament 1997b) und am 1. Dezember 1997 vom Ministerrat angenommen. Die finale ISDN-RL wurde schließlich am 15. Dezember 1997 von den Präsidenten des Europäischen Parlaments und des Ministerrats unterzeichnet (Das Europäische Parlament und der Rat der Europäischen Union 1997).

Auch im Falle der ISDN-RL verzögerte sich die Umsetzung in den Mitgliedstaaten. Die Kommission leitete in der Folge Vertragsverletzungsverfahren gegen Frankreich, Irland und Luxemburg ein (EU-Kommission 2001a). Der EuGH sanktionierte schließlich Frankreich für die Versäumung der fristgemäßen Umsetzung der Richtlinie (EuGH 2001).

3.2.5 DS-VO 45/2001

Vom Anwendungsbereich der DS-RL ausgeschlossen war die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft. Bereits im Rahmen ihres 1990er-Legislativbündels hatte die

143 Für den Fall, dass der Rat die Vorschläge des Parlaments nicht annimmt, sehen die europäischen Verträge die Einberufung eines *Vermittlungsausschusses* binnen sechs Wochen vor. Dieser wird paritätisch aus Mitgliedern des Parlaments und des Ministerrats besetzt, während der Kommission die Moderationsrolle zukommt. Nach Einberufung muss der Vermittlungsausschuss innerhalb von sechs Wochen eine Einigung erzielen, da der Rechtsakt ansonsten als gescheitert gilt (Wessels 2008, 346).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommission daher auch eine Erklärung verabschiedet, in der für die Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze auf die Gemeinschaftsorgane und -einrichtungen geworben wurde. Zudem kündigte die Kommission an, zum frühestmöglichen Zeitpunkt (legislative) Maßnahmen folgen zu lassen, bis dahin allerdings zunächst die in der Rahmenrichtlinie festzulegenden Grundsätze auf die in ihrem Verantwortungsbereich erfolgende Verarbeitungen personenbezogener Daten anzuwenden. Daneben ermutigte die Kommission die übrigen Gemeinschaftsinstitutionen dazu, selbiges zu tun (Commission of the European Communities 1990, 74). Die Vorlage eines diesbezüglichen Rechtsaktes sollte allerdings noch einige Jahre auf sich warten lassen. Trotz fehlender Regulierung verarbeiteten die Gemeinschaftsorgane und -einrichtungen freilich weiterhin personenbezogene Daten, was wiederum zu Kritik vonseiten der Datenschutzaufsichtsbehörden führte (Deutscher Bundestag 1991, 60, 1993, 126–27; Simitis 1995, 468 f.). Allerdings konnte ein entsprechender Rechtsakt von der Kommission formell nicht vorgeschlagen werden, da der Schutz personenbezogener Daten bei der Verarbeitung durch die Gemeinschaftsorgane und -einrichtungen in den Europäischen Verträgen nicht vorgesehen war.

Die Situation änderte sich schließlich mit der Unterzeichnung des Vertrags von Amsterdam am 2. Oktober 1997.[144] Der neue Art. 286 im EWG-Vertrag besagte, dass ab dem 1. Januar 1999 „die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch diesen Vertrag oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung [zu finden haben]" (Europäische Union 2002). Zudem forderte der zweite Absatz des entsprechenden EWG-Artikels (Art. 286 Abs. 2) die im Ministerrat versammelten Mitgliedstaaten dazu auf, unabhängig vom Erlass eines Rechtsaktes, die Errichtung einer unabhängigen Kontrollinstanz auf EU-Ebene noch vor dem 1. Januar 1999 zu fördern und gegebenenfalls entsprechende Bestimmungen zu verabschieden (ebd.).[145]

144 Mit dem am 1. Mai 1999 in Kraft getretenen Amsterdamer Vertrag wurden kleinere Ergänzungen und Anpassungen an der mit dem Maastrichter Vertrag grundlegend reformierten institutionellen Architektur vorgenommen (Wessels 2008, 94 f.).

145 Aufgrund des Widerstands der Kommission scheiterte dieses Anliegen jedoch. Offenbar war die Kommission über potentielle Überschneidungen des Tätigkeitsbereichs des Europäischen Ombudsmanns besorgt (González Fuster 2014, 144).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Zum Zwecke der Umsetzung der Bestimmungen des aktualisierten EWG-Vertrags legte die Kommission im Rahmen des Mitentscheidungsverfahrens dem Parlament sowie dem Ministerrat schließlich am 17. September 1999 ihren *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr* vor (Europäische Kommission 1999b). Der Wirtschafts- und Sozialausschuss gab seine Stellungnahme nur wenig später am 8. Dezember 1999 ab. Die Stellungnahme des Parlaments folgte mehr als ein Jahr später am 11. Oktober 2000 (Annahme des Rapporteur-Berichts im zuständigen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) bzw. am 14. November 2000 (Annahme des Berichts im Parlamentsplenum). Der Ministerrat nahm den Standpunkt des Parlaments am 30. November an, sodass die Verordnung schließlich am 18. Dezember 2000 von den Präsidenten des Parlaments sowie des Rats unterzeichnet wurde und Ende Januar 2001 als *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr* in Kraft getreten ist (Das Europäische Parlament und der Rat der Europäischen Union 2001).

Die auffälligste Änderung der finalen Verordnung gegenüber dem ursprünglichen Entwurf bestand in der Abänderung des Gegenstands der Verordnung in Art. 1. Der erste Satz des Artikels, der den *Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre* im Rahmen der Organe und Einrichtungen der Gemeinschaft als Gegenstand der Verordnung festlegt, wurde auf Vorschlag des Parlaments um die Aussage erweitert, dass die gemäß diesem Artikel erlassenen Bestimmungen *den freien Verkehr personenbezogener Daten untereinander oder mit Empfängern, die dem in Anwendung der Richtlinie 95/46/EG erlassenen einzelstaatlichen Recht der Mitgliedstaaten unterliegen, weder beschränken noch untersagen* dürfen. Da sich die Inhalte der Verordnung lediglich auf den Datenschutz bei der Datenverarbeitung in den Gemeinschaftsorganen und -einrichtungen bezogen, dabei zugleich das Schutzniveau der DS-RL wiederholten und keine umstrittenen neuen Elemente einbrachten, kam es zu keinen nennenswerten politischen Konflikten (Hijmans 2006).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3 Die Datenschutzpolitik der Europäischen Gemeinschaft nach der Jahrtausendwende

Mit der Jahrtausendwende ging die Datenschutzpolitik in der Europäischen Gemeinschaft in eine neue und konfliktreiche Phase über. Datenschützer, die für die Stärkung der datenschutzrechtlichen Regelungen im allgemeinen Datenschutzrecht wie auch im Sicherheitsbereich eintraten, konnten ihre Forderungen aufgrund der wirtschafts- und sicherheitspolitischen Bedeutungssteigerung, die die Datenverarbeitung erfahren hatte, nicht durchsetzen. In der Folge stagnierte die Entwicklung des Datenschutzrechts fast ein Jahrzehnt lang. Der vorliegende Unterabschnitt widmet sich der Analyse dieser Entwicklungen.

3.3.1 Hintergrund und Kontext: Wirtschafts- und sicherheitspolitisch bedingte Legitimationskrise des Datenschutzes

Das gesellschaftliche und politische Klima, das die Verabschiedung der Datenschutzgesetze der 1970er-Jahre bis hin zur DS-RL begünstigt hatte, wandelte sich im Laufe der 1990er-Jahre und stellte die Befürworter von Datenschutzregelungen zu Beginn der 2000er- bis insb. in die Mitte der 2000er-Jahre vor große neue Herausforderungen. Anders als zuvor waren nicht die strukturellen Regelungsdefizite deren Ursache, sondern eine sich in dieser Zeit zunehmend verschärfende, Subsystem-extern bedingte Legitimationskrise. Zwei Entwicklungen trugen dazu entscheidend bei: Zum einen wirtschaftspolitische und zum anderen sicherheitspolitische Effekte. Diese Faktoren werden in den folgenden Unterabschnitten herausgearbeitet.

3.3.1.1 Kommerzialisierung von (personenbezogenen) Daten und IuK-Technologien als Wirtschaftsmotor

Bereits in der ersten Hälfte der 1980er-Jahre versuchte die Europäische Kommission auf die im Jahr 1982 erfolgte Entflechtung des US-amerikanischen Telefonmonopolisten AT&T und die stärker wettbewerbliche Neuorganisation des dortigen Telekommunikationssektors mit dem Versuch zu reagieren, die Mitgliedstaaten von einer engeren Kooperation auf Gemeinschaftsebene im Hinblick auf die Telekommunikationspolitik und

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

von begleitenden Deregulierungsmaßnahmen nach US-amerikanischem Vorbild zu überzeugen. Allerdings konnte sich die Kommission anfangs nur teilweise durchsetzen. Während europaweit die ersten Deregulierungsmaßnahmen umgesetzt wurden, nahmen die Mitgliedstaaten auch weiterhin Rücksicht auf die Interessen der nationalen Telekommunikationsriesen (vor allem Deutschland und Frankreich), indem als Kerntechnologie auf ISDN und auf europäische Netz-Standards gesetzt wurde (vgl. z. B. die Empfehlungen des Bangemann-Berichts: Bangemann 1994).[146] Nachdem ab der zweiten Hälfte der 1990er endgültig klar geworden war, dass sich das Internet weltweit als Netzwerktechnologie durchgesetzt hatte und die nationalen Computernetz-Politiken gescheitert waren (Werle 2005), konnte sich die Europäische Kommission schließlich Ende der 1990er-Jahre als die führende europäische Institution auf dem Gebiet der europäischen Telekommunikationspolitik etablieren und eine Reihe von Gemeinschaftsmaßnahmen auf diesem Gebiet durchsetzen, die das Ziel der wirtschaftlichen Stärkung der Europäischen Gemeinschaft hatten (V. Schneider und Werle 2007, 271 ff.). Aufbauend auf der Unterteilung des Internets in eine Infrastrukturebene und eine Dienstleistungsebene sowie auf der Einsicht, dass die Gemeinschaft bei der Auseinandersetzung um die Infrastrukturebene bereits in einen uneinholbaren Rückstand geraten war, wurde der Fokus seit Anfang der 2000er-Jahre auf die Förderung der europäischen Industrie auf der Dienstleistungsebene in Gestalt von E-Commerce-Anwendungen gelegt. In der Zwischenzeit hatte sich wiederum die Verarbeitung personenbezogener Daten bereits zu einem Kernelement der Wertschöpfung auf der Dienstleistungsebene des Internets entwickelt. Die zunehmende Konzentration aller Kommunikationsmittel auf der Ebene des Computers bot dieser Kommerzialisierung von Daten Vorschub: „Mit steigendem Um-

146 Angesichts der sich ankündigenden Liberalisierung der Telekommunikationsmärkte bauten die staatlichen Telekommunikationsunternehmen, die ihre eigenen Standards durchsetzen wollten, auf die OSI-nahen ISDN-Standards mit dem Ziel, verschiedene Sprach- und Datendienste auf digitaler Basis in integrierter Form in einem Netz anbieten zu können und damit auch ihre Monopole zu verteidigen. Noch 1994 hieß es in den Empfehlungen „Europa und die globale Informationsgesellschaft" der Bangemann-Kommission für den Europäischen Rat, dass ISDN als Baustein der Informationsgesellschaft gefördert werden müsse, während das Internet nur am Rande erwähnt wurde (Werle 2005, 25). Demgegenüber hatten die skandinavischen Länder, die Niederlande und bis zu einem gewissen Grade auch das Vereinigte Königreich ihre Telekommunikationsmärkte früher liberalisiert bzw. nicht auf ISDN gesetzt, weshalb sich das Internet und entsprechende wirtschaftliche Gewinne in diesen Ländern früher und effizienter durchsetzen konnten (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

fang und fortschreitender Differenzierung wächst auch der Eigenwert der Datenbestände. Die Daten lösen sich mehr und mehr aus ihrem ursprünglichen Verarbeitungszusammenhang und fügen sich zu einem Informationskapital zusammen. Die Verwertungsmöglichkeiten reichen von einer weit reichenden Revision der Absatzstrategien bis hin zu einer konsequenten Vermarktung. Der Datenberg wandelt sich so zur Datenmine. Je tiefer die Stollen getrieben werden, desto größer der Nutzen." (Simitis 2000, 312) Dabei wurde zugleich in zunehmendem Maße auf die Kooperation der Betroffenen gesetzt: Indem diesen Dienste im Austausch für ihre personenbezogenen Daten angeboten wurden, konnten Datenverarbeiter ganz legitim auf Basis der individuellen Einwilligung Zugriff auf enorme personenbezogene Datenmengen erhalten und diese zu Zwecken des Data Mining und der personalisierten Werbung nutzen (ebd., 312). Die Vereinigten Staaten, die noch bis in die Mitte der 1990er-Jahre in einer Rezession steckten, konnten ihrer Wirtschaft mittels der gezielten Unterstützung der Verbreitung von IuK-Technologien zu massiven Wachstumsgewinnen verhelfen, sodass IuK-Technologien als *bahnbrechende Basis- und Schlüsseltechnologie* bezeichnet wurden (vgl. Grupp, Legler, und Breitschopf 2003).[147] So wurde 1999 ein enormes Wachstum des elektronischen Handels allein in Deutschland von 3 Milliarden D-Mark auf über 25 Milliarden D-Mark bis 2002 prognostiziert (Persson 1999). Letztlich konnte beispielsweise im ersten Quartal 2004 eine Wachstumsrate von 28,1 Prozent verzeichnet werden, während der konventionelle Handel lediglich mit 8,8 Prozent gewachsen war. Der elektronische Handel in Europa betrug 86 Mrd. Dollar im Jahr 2001 und in den Vereinigten Staaten wurde 2004 ein E-Commerce-Handelsvolumen von 120 Mrd. Dollar erzielt. Unter Einbezug des B2B-Bereichs betrug das E-Commerce-Handelsvolumen im Jahr 2001 in der Europäischen Gemeinschaft 430. Mrd. Dollar und in den Vereinigten Staaten bereits 1,08 Bio Dollar (The Economist 2004; UNCTAD 2004).

Waren in Zeiten der Großcomputer nur wenige private Akteure imstande gewesen, die entsprechende Infrastruktur zu finanzieren, konnten seit den 1980er-Jahren auch kleinere Betriebe Daten mittels der einfacher finanzierbaren Personal Computer verarbeiten und für Produktionssteige-

147 „Nicht unbedingt einzelne etablierte Firmen der Branche, sondern insgesamt die amerikanische informationstechnische Industrie und die Anbieter Internet basierter Dienstleistungen profitierten von dem ‚First Mover Advantage' der USA, der gegenüber Deutschland wegen der einseitigen Technologiepolitik besonders groß war." (Werle 2005, 29)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

rungen nutzen. Ende der 1990er war der Personal Computer schließlich zu einem Haushaltsprodukt avanciert, das als Terminal zur Nutzung des Internets diente (Bendrath 2007b, 17). Damit durchlebte die Datenverarbeitung einen grundlegenden Bedeutungswandel: Waren Datenschutzvorkehrungen in den 1970er- und 1980er-Jahren noch vor allem aus der Angst vor einem Big-Brother-Szenario heraus gerechtfertigt worden, das den Staat als Hauptgefahr in den Mittelpunkt der Betrachtung rückte, war seit den 1980er-Jahren in zunehmendem Maße die Privatwirtschaft an die Stelle staatlicher Stellen als Hauptakteur der Datenverarbeitung getreten. Wurde zuvor befürchtet, dass die massenhafte Verarbeitung personenbezogener Daten die Kommunikations- und Partizipationsfähigkeit des Einzelnen einschränken würde, so schien sich mit dem Zugriff auf das Internet trotz der gleichzeitig zunehmenden Verarbeitung personenbezogener Daten eben jener Kommunikations- und Partizipationsraum des Einzelnen in ungekanntem Maße auszuweiten (Simitis 2000, 314 f.). Verstärkt wurde dieser Effekt durch die später als Netzeuphorie bezeichneten Hoffnungen, dass mit der Verbreitung des Internets die unausweichliche Lösung beliebiger Menschheitsprobleme, allen voran die Erreichung einer echten, globalen, demokratischen Öffentlichkeit, möglich werde.[148] Dass dieses Erfolgsmedium, das Internet, das massives wirtschaftliches Wachstum und gesellschaftliche Entwicklung versprach, in weiten Teilen der Gesellschaft und Politik als weitgehend unregulierter Ort[149] wahrgenommen wurde,

148 Sinnbildlich für diese Perspektive sei auf John Perry Barlows „A Declaration of the Independence of Cyberspace" (1996) verwiesen. Für frühe Kritiken, siehe: (Horvath 1996; Lovink und Schultz 1996). Für eine spätere, umfassende Kritik, siehe: (Morozov 2011).

149 In Bezug auf die Selbstverwaltung des technischen Internets (etwa die Verwaltung der technischen Standards und Protokolle) ist dies zwar eine durchaus treffende Feststellung. So hatte das US-Verteidigungsministerium in der Frühphase der Entwicklung des Internets einen sehr weitgehenden Einfluss auf die Gestaltung des Internets, der jedoch mit der Abkoppelung des zivilen Internets vom militärischen MILNET im Jahr 1983 ein Ende fand. Fortan erfolgte die Weiterentwicklung des Internet auf Basis der sog. Multi-Stakeholder-Governance (Abbate 1999, 43 ff. Warnke 2011, 45 f.). In Bezug auf den wirtschaftlichen Erfolg US-amerikanischer Unternehmen auf der Dienstleistungsebene des Internets kann dieser Perspektive jedoch entgegnet werden, dass die Clinton-Administration Mitte der 1990er, angesichts der wirtschaftlichen Wachstumspotentiale dieses Sektors, enorme Anstrengungen unternommen hatte, den Erfolg US-amerikanischer Unternehmen durch regulative Maßnahmen (Stichwort: *Regulierte Selbstregulierung*, so etwa mit den 1997 verabschiedeten E-Commerce-Gesetzen) abzusichern (Holznagel und Werle 2004, 27; U.S. Government Working Group on Electronic Commerce 1998).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

verstärkte in Verbindung mit dem zu dieser Zeit große Anziehungskraft ausstrahlenden politischen Fokus auf Soft-Governance-Maßnahmen (EU-Kommission 2001c; vgl. z. B. Tömmel 2008), die Bereitschaft auf Seiten der politischen Entscheider, zum einen grundsätzlich weniger intensiv – sei es auch im Hinblick auf die Verhinderung negativer Effekte neuer Technologien mittels Datenschutzmaßnahmen – regulieren zu wollen, und zum anderen Regulierung noch stärker als zuvor eher als Katalysator für wirtschaftliches Wachstum zu nutzen. Die Verabschiedung der Signaturrichtlinie 1999/93/EG sowie der E-Commerce-Richtlinie 2000/31/EG sind in diesem Zusammenhang als derartige Katalysator-Maßnahmen zu bewerten, die den unbedingt notwendigen rechtlichen Rahmen abstecken, innerhalb dessen sich der E-Commerce-Markt ansonsten weitgehend unreguliert ausbreiten können sollte (Holznagel und Werle 2004, 26 f.). Mahnungen zur Wahrung des Datenschutzes konnten sich in diesem gesellschaftlichen und politischen Klima kaum mehr Gehör verschaffen (Simitis 2000, 312).

Stattdessen wurde seit Mitte der 1990er-Jahre eine andere – im Kontext des Bangemann-Reports bereits kurz angesprochene (vgl. Unterkapitel 3.2.2.6) – Perspektive auf den Umgang mit personenbezogenen Daten dominant. Datenschutzmaßnahmen sollten nicht mehr nur Individuum und Gesellschaft vor staatlichen Übergriffen schützen, sie sollten vielmehr im Sinne einer vertrauensbildenden Maßnahme zwischen Anbietern und Kunden in der virtuellen Welt, in der es keinen physischen Kontakt der Kunden mit Verkäufern oder Produkten gibt, wirken und somit zu einer gesteigerten gesellschaftlichen Akzeptanz neuer Technologien beisteuern und das auf neuen IuK-Technologien basierende Gelingen wirtschaftlichen Wachstums flankieren (Priscilla M. Regan 1999). Während einige Unternehmen bereits die Existenz von staatlichen Datenschutzregelungen als Behinderung des wirtschaftlichen Potentials des neuen E-Commerce-Marktes kritisierten, gingen andere Unternehmen erfolgreich dazu über, nationale und europäische Entscheider von der Notwendigkeit einer zu schaffenden Balance zwischen dem rechtlichen Schutz personenbezogener Daten und der wirtschaftlichen Verwendung ebenjener Daten zu überzeugen. Datenschutz galt, diesem aktualisierten Verständnis nach, zunehmend als individualistisch verstandener Verbraucherschutz, während das angestrebte Wirtschaftswachstum als gesellschaftliches Ziel bzw. Förderung des Allgemeinwohls definiert wurde. Der technologische Rückstand der Europäischen Gemeinschaft erhöhte dabei die Bereitschaft der Politik, Konzessionen zugunsten wirtschaftspolitischer Versprechungen einzugehen. In anderen Worten setzt sich zu dieser Zeit in zunehmendem Maße die Perspektive

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

durch, dass der Schutz personenbezogener Daten in erster Linie nur insoweit aufrechterhalten werden sollte als dieser zu mehr Vertrauen in digitale Technologien und dadurch zu mehr Wirtschaftswachstum führte (Bendrath 2007a).

Diese wirtschaftspolitisch ausgelöste Legitimationskrise des Datenschutzes wurde sodann um eine sicherheitspolitisch motivierte Legitimationskrise ergänzt, die deren Effekte verstärken sollte. Die nähere Betrachtung dieser zweiten Legitimationskrise ist Gegenstand des folgenden Kapitels.

3.3.1.2 Von 9/11 bis London 2005: Der Einfluss von Terroranschlägen

Am 11. September 2001 entführten mehrere, dem islamistischen Terrornetzwerk al-Qaida zugehörige, Selbstmordattentäter zeitgleich vier Passagierflugzeuge und verursachten mittels der auf das World Trade Center in New York sowie auf das Pentagon in Arlington verübten Selbstmordanschläge den Tod von knapp 3.000 Menschen. Dieser historisch beispiellose Angriff auf die Vereinigten Staaten hatte nicht nur weitreichende außenpolitische, sondern auch innenpolitische Folgen, von denen viele gesellschaftliche und staatliche Bereiche betroffen waren. Von enormer politischer Bedeutung war insbesondere die zunehmende Versicherheitlichung der Innenpolitik. Diese betraf nicht nur die Vereinigten Staaten, sondern auch ihre Verbündeten, von denen die größtmögliche Kooperation im Hinblick auf die Eindämmung als terroristisch eingestufter Gefahren abverlangt wurde (Fey 2012, 38). Von Bedeutung für die vorliegende Arbeit ist insbesondere die im Nachgang der Anschläge erfolgte massive Ausweitung von geheim- und nachrichtendienstlichen[150] Überwachungsmaßnahmen – zunächst in den Vereinigten Staaten und in der Folgezeit auch in der EU und ihren Mitgliedstaaten. Angetrieben vom Übergang „vom Rechtsstaat zum Präventionsstaat“ (Denninger 2002) war bzw. ist das Leitziel jener sich mit diesem Staatstypus identifizierenden sicherheitspolitischen Akteure die Ab-

150 Die begriffliche Differenzierung sei wie folgt zu verstehen: „Geheimdienste bezeichnen in den meisten Staaten eigene, von den regulären Polizeibehörden mehr oder weniger verselbstständigte Dienststellen zur Aufklärung und Bekämpfung vergangener oder zukünftiger Bestrebungen gegen Bestand, Sicherheit oder Grundelemente der politischen Ordnung eines Staates. Nachrichtendienste hingegen beschränken sich darauf, solche Bestrebungen aufzuklären, überlassen deren Bekämpfung aber anderen Stellen. Sie sind also ausschließlich auf Beschaffung und Verarbeitung von Informationen gerichtet.“ (Gusy 2014, 9)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wehr und Verhinderung von Anschlägen sowie die Gewährleistung von Sicherheit als oberstem Ziel: „Während der Rechtsstaat normenverletzendes Verhalten lediglich sanktioniert, ist der Präventionsstaat bemüht, die Normenverletzung an sich zu verhindern. Zu diesem Zweck muss er umfangreiches Wissen über jeden einzelnen Bürger sammeln und in der Exekutive Kapazitäten aufbauen, um jeder plausiblen Art von aus Normverletzung erwachsender Bedrohung wirksam entgegentreten zu können." (A. Busch 2012b, 865) In anderen Worten setzte sich zu Beginn der 2000er-Jahre die Überzeugung durch, dass eine möglichst große Informationsbasis eine Schlüsselvoraussetzung für die erfolgreiche Bekämpfung des Terrorismus darstelle. Meinungsverschiedenheiten existierten lediglich hinsichtlich der für eine wirksame Bekämpfung benötigten konkreten Datenmenge, der Speicherdauer erhobener Daten, der Betroffenenrechte sowie der Spezifika des Zugriffs auf die Daten seitens Sicherheitsbehörden. So forderten sicherheitspolitisch motivierte Akteure im Nachgang der Anschläge vom 11. September auch innerhalb der EU die Ausweitung des Informationsaustauschs zwischen den zuständigen Behörden der Mitgliedstaaten sowie den entsprechenden europäischen Institutionen. Datenschutzrechtliche Vorgaben wurden von diesen Akteuren dabei regelmäßig als Behinderung der behördlichen Pflichten wahrgenommen und gegenüber der Öffentlichkeit auch in dieser Weise kommuniziert. Eine beliebte wiederkehrende Rhetorik in diesem Kontext war die Gleichstellung von Datenschutz mit „Täterschutz" (Wetzel 2012, 559 f.).[151] Bürgerrechtlich motivierte Akteure erwiderten, dass Datenschutz die Verarbeitung personenbezogener Daten nicht verhindere und auch „keine Marotte von Gespenstersehern [sei], sondern […] den Staat, und nicht nur ihn [dazu zwinge], bestimmte Regeln bei der Verarbeitung personenbezogener Informationen einzuhalten – [sic] und zwar zum Schutz der Bürger." (Simitis, zit. nach: Klingst 2001)

Den Höhepunkt erreichte die innereuropäische Debatte mit den Anschlägen von Madrid am 11. März 2004 und London am 7. Juli 2005. Die bis dahin auf dem Felde der Terrorismusbekämpfung vor allem auf

151 So hatte sich etwa der damalige von der SPD gestellte Bundesinnenminister Otto Schily im Nachgang von 9/11 dahingehend geäußert, dass ein überzogenes Maß an Datenschutz zu den Anschlägen beigetragen habe. Belege lieferte Schily keine (Sanders 2001). Wie sich später herausstellen sollte, war das Problem nicht das Fehlen einer ausreichend großen Datenbasis, sondern im Gegenteil der Mangel an zielführenden Auswertungsmethoden der bestehenden, enormen Datenbestände (Matheou 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Solidarität gegenüber den Vereinigten Staaten gerichteten EU-Aktivitäten[152] kondensierten sich erst im Nachgang der Madrider Anschläge, zunächst im Rahmen der *Erklärung zum Kampf gegen Terrorismus* der Staatschefs der EU (Europäischer Rat 2004) und der darin beschlossenen Einrichtung der Position einer unionsweiten Koordination für die Terrorismusbekämpfung und schließlich in Folge der Londoner Anschläge zu einer *EU-Strategie zur Terrorismusbekämpfung* (EU-Ministerrat 2005b; MacKenzie, Kaunert, und Léonard 2015, 96 f.). Die Folge war eine massive Versicherheitlichungspolitik (Buzan, Waever, und Wilde 1998, 24 ff.), die zum Erlass dutzender weitreichender Regelungen führte, die den Handlungsspielraum von Überwachungs- und Polizeibehörden ausdehnten. So wurden zwischen 2001 und 2013 allein seitens der EU insgesamt 238 Maßnahmen – darunter 88 rechtsverbindliche Maßnahmen wie Verordnungen, Richtlinien und Beschlüsse – zur Bekämpfung von Terrorismus verabschiedet (Hayes und Jones 2013, 25).

Die folgenden Unterabschnitte beschreiben, wie es den Befürwortern von Datenschutzregelungen unter diesen veränderten Kontextbedingungen zunehmend schwerer fiel, öffentliches Gehör zu finden und sich in den datenschutzpolitischen Aushandlungsprozessen durchzusetzen.

3.3.2 ePrivacy-Richtlinie 2002/58/EG

Der erste datenschutzpolitische Aushandlungsprozess, bei dem Wirtschafts- und Sicherheitsinteressen sich in relevantem Maße gegenüber Datenschutzinteressen durchsetzen konnten, stellt die Aushandlung der ePrivacy-Richtlinie dar. Die Analyse des Aushandlungsprozesses zeigt insbesondere, wie in der Anfangsphase der Verhandlungen im Vorfeld von 9/11 zunächst noch wirtschaftspolitische Argumente dominant waren und wie diese nach den Terroranschlägen von sicherheitspolitischen Argumenten abgelöst wurden.

3.3.2.1 Vorgeschichte zur ePrivacy-Richtlinie

Noch vor Inkrafttreten der Bestimmungen des Rechtsrahmens für Telekommunikation zum 1. Januar 1998, initiierte die Kommission mit der

152 So etwa die Ende 2003 angenommene EU-außenpolitisch motivierte *Europäische Sicherheitsstrategie* (Europäischer Rat 2003).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Veröffentlichung eines Grünbuchs Anfang Dezember 1997 einen ersten öffentlichen Evaluations- und Konsultationsprozess[153] zur Identifikation und zum Abbau weiterer Barrieren auf dem Weg zu einer wettbewerbsfähigeren Europäischen Gemeinschaft auf dem Gebiet der Telekommunikation. Das Grünbuch der Kommission rahmte das Thema Datenschutz lediglich als nebensächliche Maßnahme, die im Hinblick auf das übergeordnete Ziel der Förderung der Systemkonvergenz und der Förderung eines EU-weiten Telekommunikationssektors nur insofern bedeutsam sei, dass durch Datenschutz das für die erfolgreiche Verbreitung und Nutzung konvergenter Systeme benötigte Vertrauen aufgebaut werde (European Commission 1997, 29). Die Grundrechtsperspektive auf Datenschutz fand erst später in den Konsultationsergebnissen Erwähnung. Interessanterweise ordnete die Kommission das Thema Datenschutz und Privatheit dabei einerseits dem Themenfeld Verbraucherschutz bzw. -Interessen (European Commission 1998, 30) und andererseits dem Themenfeld „Securing Public Interest Objectives in the Light of Convergence" zu und rahmte es somit auch als ein öffentliches Interesse (ebd., 31). Die Mehrheit der am Konsultationsprozess teilnehmenden Akteure befürworteten zwar die regulatorische Festlegung eines Mindest-Datenschutzniveaus (ebd., 32). Allerdings stellten einige Akteure aus der Wirtschaft die Notwendigkeit weiterer Verbraucherschutzmaßnahmen auch grundsätzlich infrage (ebd., 31).[154]

Nachdem die Kommission ihre Strategie zur weiteren Entwicklung elektronischer Kommunikationsinfrastrukturen und zugehöriger Dienste ausgearbeitet hatte, veröffentlichte sie Anfang November 1999 den sog.

153 Der Konsultationsprozess fand zwischen Dezember 1997 und Mai 1998 statt. In einer ersten Runde gingen schriftliche Stellungnahmen von insgesamt 270 Akteuren bei der Kommission ein. In einem weiteren Schritt setzten sich die Ratsformationen *Verkehr und Telekommunikation* sowie *Kultur und Audiovisuelle Medien* mit der Materie auseinander. Außerdem gab der WSA eine Stellungnahme ab. Schließlich wurden im dritten Schritt zwischen März und April 1998 Anhörungen mit ausgewählten Akteuren durchgeführt. Folgende Akteure, die an diesem Konsultationsprozess partizipierten, nahmen später auch am politischen Aushandlungsprozess der DSGVO teil: ACT. AmCham EU, BEUC, ENPA, EPC, ETNO, FAEP, FEDMA, ICC, UNICE (später umbenannt in: Businesseurope), VDZ, WFA, Intel, Nokia, Telefónica (European Commission 1998, 1 und 42 ff.).

154 Mit der Veröffentlichung der Konsultationsergebnisse folgte auf den ersten öffentlichen Konsultationsprozess ein zweiter, weniger umfangreicher, der zwischen Ende Juli und November 1998 lief, doch wurden im Rahmen dieser Konsultation keine datenschutzpolitisch relevanten Themen diskutiert, weswegen diese nicht näher betrachtet wird (European Commission 1999).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommunikationsbericht 1999, mit dem ein weiterer Konsultationsprozess[155] initiiert wurde (Europäische Kommission 1999a). Darin wurde zum einen über die bis dahin umgesetzten Liberalisierungsbestrebungen im Telekommunikationsbereich reflektiert und zum anderen *Vorschläge für die Hauptkomponenten eines neuen Rahmens für Kommunikationsinfrastrukturen und zugehörige Dienste* unterbreitet (ebd., ii). Die auf dem Europäischen Ratstreffen vom März 2000 verabschiedete Lissabonner Strategie bettete die geplanten Maßnahmen schließlich in den Gesamtkontext gemeinschaftlicher Deregulierungsmaßnahmen im Telekommunikationssektor ein, deren übergeordnetes Ziel im Aufbau eines wettbewerbsfähigen europäischen Binnenmarktes lag. Die Strategie betonte das Potential für Wachstum, Wettbewerbsfähigkeit und die Schaffung von Arbeitsplätzen durch den Übergang zu einer digitalen und wissensbasierten Gesellschaft, indem eine günstige und qualitativ hochwertige Kommunikationsinfrastruktur aufgebaut wird (Europäischer Rat 2000b). Dazu sah die Kommission die Verabschiedung einer Rahmenrichtlinie vor, mit der die allgemeinen und spezifischen politischen Ziele festgelegt werden sollten, sowie vier spezifischer Richtlinien zu den Themenbereichen *Erteilung von Genehmigungen*, *Zugang und Zusammenschaltung*, *Universaldienst*, und eine Richtlinie zum *Schutz der Privatsphäre und Datenschutz* (ebd.).[156] Da bereits die ISDN-RL 97/66/EG einige Aspekte des Themas abdeckte, sollte diese im Rahmen des Gesetzesbündels aktualisiert werden. Dabei verwies die Kommission einerseits auf die unzureichende Harmonisierung aufgrund von Unterschieden bei der Umsetzung der Richtlinie und andererseits auf die Notwendigkeit der Überarbeitung der – bereits zum Zeitpunkt ihrer Verabschiedung als veraltet bewerteten (Debusseré 2005, 72) – Richtlinienvorgaben, damit sichergestellt würde, dass die Regelungen für einen konvergierenden Telekommunikationsmarkt, der neben der Festnetztelefonie auch jegliche mobile, satelliten- oder kabelbasierte Technologie umfasst, geeignet wären (Europäische Kommission 1999a, 54 und 73). Im Rahmen des öffentlichen Konsultati-

155 Hauptverantwortlich für diesen Konsultationsprozess war die Generaldirektion Informationsgesellschaft bzw. deren Referat Rechtsrahmen A/1 (Europäische Kommission 1999a, xii).

156 Das Gesetzesbündel hatte neben der Aktualisierung bestehender Regelungen insb. die Vereinfachung der geltenden Regelungen zum Ziel, indem die geltenden zwanzig Rechtsvorschriften auf sechs reduziert werden sollten (Europäische Kommission 1999a, 21).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

onsprozesses gingen mehr als 200 Antworten bei der Kommission ein.[157] In ihrer Mitteilung zu den Ergebnissen der Konsultation resümierte die Kommission, dass sich die Mehrheit der Einsendungen und vor allem die partizipierenden Regulierungsbehörden wie die Art. 29-Datenschutzgruppe für die Überarbeitung der ISDN-RL aussprachen, damit die Technologieneutralität der Regelungen und damit ihre Wirksamkeit weiterhin gewährleistet werden könnten. Allerdings vertraten Wirtschaftsvertreter – ähnlich zu ihrer während der ersten Konsultation zur Konvergenz vertretenen Position – auch während dieser Konsultation die Position, dass die Notwendigkeit einer sektorspezifischen Regulierung grundsätzlich infrage zu stellen sei. Seitens der Wirtschaftsvertreter wurden die bestehenden horizontalen Rechtsvorschriften in Gestalt der DS-RL 95/46/EG als ausreichend bewertet. Sektorspezifische Präzisierung der Richtlinienvorgaben seien erforderlichenfalls mit einem flexiblen Instrument wie Verhaltensregeln besser zu erreichen statt mit staatlicher Regulierung (Europäische Kommission 2000b, 5 und 18).

3.3.2.2 Veröffentlichung des Kommissionsvorschlags

Die Europäische Kommission veröffentlichte schließlich am 12. Juli 2000 im Rahmen des Mitentscheidungsverfahrens ihren *Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation* (EU-Kommission 2000b). Der Vorschlag sah überwiegend kleinere Anpassungen an den Stand der Technik sowie die Aufrechterhaltung des in der Vorgängerrichtlinie festgelegten Datenschutzniveaus vor. Lediglich im Zusammenhang mit zwei Richtlinienelementen sollte es zu Konflikten kommen. In Bezug auf die Debatte, ob an Betroffene gerichtete Werbung nur nach der vorherigen Einwilligung dieser erfolgen dürfte (Opt-in) oder Betroffene nach dem Erhalt der Werbung das Recht auf Widerruf (Opt-out) erhalten sollten, vertrat

157 Der Konsultationsprozess fand zwischen Mitte November 1999 und Mitte Februar 2000 statt. Neben schriftlichen Einsendungen berücksichtigte die Kommission dabei auch die Beiträge von mehr als 500 Personen, die bei einem zweitägigen öffentlichen Hearing am 25. und 26. Januar 2000 teilnahmen. Auch an diesem Konsultationsprozess waren viele Akteure beteiligt, die später während des Aushandlungsprozesses der DSGVO eine wichtige Rolle spielen sollten: AmCham EU, Association of Commercial Television in Europe ACT, BEUC, ENPA, Euro-ISPA, European Public Telecommunications Network Operators' Association (ETNO), GSM Europe, Intel, Microsoft, Nokia, Telefónica, UNICE/Businesseurope (Europäische Kommission 2000b, 32 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Kommission zwar die Position, dass ein Opt-in-Verfahren zu bevorzugen sei. Aus Rücksichtnahme auf die diesbezüglichen unterschiedlichen Positionen in den Mitgliedstaaten und anhaltende Kritik aus der Wirtschaft hin, schlug die Kommission allerdings die Regelung dieser Materie im mitgliedstaatlichen Recht statt auf Gemeinschaftsebene vor (Art. 13 Abs. 2). In einem weiteren zentralen Aspekt, nämlich der seitens einiger Mitgliedstaaten geforderten anlasslosen Aufbewahrung von Verkehrsdaten für einen längeren Zeitraum und der Zurverfügungstellung dieser Daten an staatliche Exekutivbehörden, hatte sich die Kommission unnachgiebig gezeigt und war bei der bereits in der ISDN-RL verwendeten Formulierung geblieben. Demnach sollten Verkehrsdaten gelöscht werden, sobald sie nicht länger für die Erbringung des Dienstes bzw. für die Gebührenabrechnung benötigt würden (EG 15). Art. 15 Abs. 1 wiederum sah mitgliedstaatliche Ausnahmen im Zusammenhang mit der Sicherheit des Staates, der Landesverteidigung und der Ermittlung und Verfolgung von Straftaten vor. Da diese Regelung lediglich anlassbezogene Speicherungen erlaubte, stieß sie auf Seiten der mitgliedstaatlichen Exekutivbehörden auf vehemente Ablehnung, da die Regelung als eine inakzeptable Einschränkung der Ermittlungstätigkeiten bewertet wurde. Spätestens seit dem Jahr 1997 forderten europaweit zahlreiche Exekutivbehörden den Aufbau der Möglichkeit einer Vorratsdatenspeicherung, mittels derer sie sich Erleichterungen in ihrer Ermittlungstätigkeit erhofften (Bunyan 2002; Statewatch 2001).

3.3.2.3 Formierung des Gemeinsamen Standpunktes im Ministerrat

Nachdem die Kommission den Gesetzgebungsprozess initiiert hatte und der Legislativvorschlag an den Ministerrat übersandt worden war, erhielt nicht die Ratsarbeitsgruppe *Datenschutz*,[158] die bereits für die Beratungen zur DS-RL, zur ISDN-RL sowie zur DS-VO die Zuständigkeit inne hatte, sondern die Arbeitsgruppe *Telekommunikation* unter der Leitung der Ratskonfiguration „Verkehr/Telekommunikation" (Karaboga 2018, 145–48). Auf der Sitzung der Arbeitsgruppe am 29 Mai 2001 brachte die schwedische Ratspräsidentschaft gemeinsam mit der belgischen und britischen Delegation den Vorschlag ein, die in Art. 6 Abs. 1 des Richtlinienentwurfs enthal-

158 Bis zu ihrer Umbenennung im Sinne einer klareren Zuordnung im Jahr 1999 firmierte die Arbeitsgruppe unter dem Namen „Wirtschaftsfragen (Datenschutz)" bzw. „Economic Questions – Data Protection" (Presidency of the Council of the European Union 2006, 1).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tene Löschungspflicht für Verkehrsdaten herauszunehmen, da diese den Erfordernissen der Exekutivbehörden nicht entspräche. Die griechische, italienische sowie die niederländische Ratsdelegation gemeinsam mit der Kommission lehnten den Vorschlag unter Verweis auf die menschen- und grundrechtliche Bedeutung der Thematik allerdings ab. Ausgehend von einem britischen Vorschlag, schlug die schwedische Ratspräsidentschaft zudem eine Änderung von Art. 15 vor. Demnach sollte in Art. 15 Abs. 1 eine Ausnahme für die Mitgliedstaaten vorgesehen werden, Verkehrsdaten für eine bestimmte Zeit speichern zu dürfen. In der letzten Version des Diskussionsstandes der Arbeitsgruppe setzte sich schließlich ein Vorschlag Belgiens (der folgenden Ratspräsidentschaft) durch, wonach Art. 6 Abs. 1 dahingehend abgeändert werden sollte, dass die zu löschenden Daten gemäß dem nationalen Recht für rechtmäßige Zwecke weiterverarbeitet werden dürfen sollten. Die Art. 29-Datenschutzgruppe bzw. dessen Vorsitzender Stefano Rodotà wandte sich daraufhin am 7. Juni 2001 mit einem Brief an Göran Persson, den amtierenden schwedischen, sozialdemokratischen Vorsitzenden des Ministerrates, und forderte diesen dazu auf, den *bestehenden, ausgewogenen Ansatz* beizubehalten und den Vorschlag der Kommission zu unterstützen (Article 29 WP 2001).

Die am 27. Juni 2001 auf der Tagung des Ministerrats (Telekommunikation) erzielte Einigung zwischen den Mitgliedstaaten blendete diese und weitere bürgerrechtliche Zwischenrufe allerdings aus, indem die vom AStV erfolgte Ergänzung von Art. 15 Abs. 1 gestrichen bzw. in den Erwägungsgrund 10 verschoben wurde (Statewatch 2001).

Währenddessen übten die Ministerratsvertreter nicht nur Druck auf die Gegner der Vorratsdatenspeicherung im Ministerrat aus, sondern auch auf das Parlament und die Kommission. Diese blieben jedoch zunächst bei ihrer ursprünglichen Position und traten für eine Beibehaltung des Datenschutzniveaus (Kommisison) der Vorgängerrichtlinie (97/66/EG) bzw. eine Erhöhung (Parlament) ein. Erst die Terroranschläge vom 11. September sollten die Kommissions- und Parlamentsmeinung nachhaltig verändern.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.2.4 Formierung der Parlamentsposition in erster Lesung: Erster Cappato-Bericht

Die Parlamentspräsidentin beauftragte am 8. September 2000 zunächst den LIBE-Ausschuss[159] damit, die Stellungnahme des Parlaments vorzubereiten. Dieser wählte den italienisch-stämmigen, linksliberalen Marco Cappato (zu dieser Zeit: Technische Fraktion der Unabhängigen Abgeordneten – TGI / Lista Emma Bonino)[160] zum Berichterstatter. Bald darauf, am 6. Oktober 2000, legte die Parlamentspräsidentin gemäß Hughes-Verfahren (heute: Verfahren mit assoziierten Ausschüssen)[161] fest, dass der Parlamentsbericht vom LIBE-Ausschuss gemeinsam mit dem ITRE-Ausschuss (Berichterstatterin: Ilka Schröder von den Grünen bzw. der Europäischen Freien Allianz/EFA) ausgearbeitet werden sollte (Cappato und Schröder 2001, 4). Am 2. November 2000 verabschiedete zunächst die Art. 29-Datenschutzgruppe ihre Stellungnahme, in der sie die mit dem Legislativvorschlag verfolgte Absicht der Kommission, ein hohes Datenschutzniveau aufrechtzuerhalten, ausdrücklich unterstützte (Artikel 29-Datenschutzgruppe 2000). Anfang 2001 gab auch der Wirtschafts- und Sozialausschuss seine den Kommissionsvorschlag unterstützende Stellungnahme ab (WSA 2001). Der letztlich aufgrund von Komplikationen doch nicht im Hughes-Verfahren verfasste LIBE-Bericht wurde schließlich am 5. September 2001 im Plenum des Europäischen Parlament debattiert. Berichterstatter Cappato unterstützte die Kommission darin, enge Grenzen für die Speicherung von Verkehrsdaten vorzusehen, mit der klassisch liberalen Begründung, dass „die größte Gefahr für die Privatsphäre der Bürger gerade in der Allmacht des Staates beim Zugang zu personenbezogenen Daten besteht“ (Vgl. Cappato, in: Europäisches Parlament 2001b). Der Parlamentsbericht ging in diesem Bereich daher viel weiter als die Kommission und trat für eine weitere Be-

159 Als mitberatende Ausschüsse waren der Ausschuss für Industrie, Außenhandel, Forschung und Energie (ITRE), JURI, der Ausschuss für Umweltfragen, Volksgesundheit und Verbraucherpolitik (ENVI) sowie der Haushaltsausschuss beteiligt. Der Haushaltsausschuss entschied sich allerdings dazu, keine Stellungnahme abzugeben (Karaboga 2018, 152).

160 Zwischen 2001 und 2004 hatte Cappato keine Fraktionszugehörigkeit im EU-Parlament. In der sechsten Wahlperiode gehörte er der ALDE-Fraktion an (EP 2020b).

161 Da Ausschüsse dazu neigen ihr Kern-Themenportfolio zu begünstigen, findet dieses Verfahren gem. Art. 47 der Geschäftsordnung des EP Anwendung, um die Gefahr der Erarbeitung einseitiger Ergebnisse zu vermeiden, sofern die Zuordnung eines zu beratenden Legislativvorschlags nicht klar zugunsten eines einzelnen Ausschusses möglich ist (Kluger Dionigi 2017, 156 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schränkung der Speicherung von Verkehrsdaten ein: Diese sollte nur dann zulässig sein, soweit sie „in einer demokratischen Gesellschaft angemessen, verhältnismäßig und zeitlich begrenzt ist. Diese Maßnahmen müssen ganz und gar die Ausnahme darstellen, sich auf eine allgemein verständliche spezifische Rechtsvorschrift stützen und von gerichtlichen oder zuständigen Behörden für Einzelfälle genehmigt sein. Im Rahmen der Europäischen Menschenrechtskonvention und gemäß den Entscheidungen des Menschrechtsgerichtshofs ist jede Form einer großangelegten elektronischen Überwachung verboten." (vgl. Änderungsantrag 50, in: Cappato und Schröder 2001, 37) Bezüglich der Opt-in/Opt-out-Thematik schlug Cappato jedoch im Gegensatz zum Kommissionsvorschlag eine einheitliche Kompromissregelung vor, die aufgrund der von Cappato bemängelten Unwirksamkeit des Opt-in-Prinzips bei der Bekämpfung von Spam auf das Opt-out-Prinzip unter Einbeziehung der betroffenen Wirtschaftssektoren setzen und auf Selbstregulierungsmechanismen (Filter und Technologien) basieren sollte (vgl. bspw. die Änderungsanträge 38 und 43, in: Cappato und Schröder 2001).[162]

Den Cappato-Bericht nahm zunächst der LIBE-Ausschuss am 11. Juli 2001 mit 22 Stimmen (bei 12 Gegenstimmen und 5 Enthaltungen) an (Cappato und Schröder 2001, 4). Daraufhin wurde der Entwurf am 5. September 2001 im Europäischen Parlament debattiert und darüber am darauffolgenden Tag abgestimmt. Nachdem zuvor im Plenum vor allem länger über die Opt-in/Opt-out-Frage gestritten worden war (Europäisches Parlament 2001b, 2001c), lehnte eine aus PSE, Grünen und Linken bestehende Mehrheit den Bericht mit 204 Stimmen ab, während lediglich 129 Abgeordnete (aus der liberalen Fraktion (ELDR) sowie TDI (Technische Fraktion der Unabhängigen Abgeordneten) gemeinsam mit etwas mehr als 40 Abgeordneten der EVP-ED) dafür stimmten. 155 vor allem der EVP-ED zugehörige Abgeordnete enthielten sich (Europäisches Parlament 2002a, 261 f.). Um ein Scheitern des Legislativvorschlags zu verhindern, beantragte Cappato schließlich die Rücküberweisung des Berichts an den LIBE-Ausschuss. Das Parlament gab dem statt und der LIBE-Ausschuss setzte sich in zwei weiteren Sitzungen (am 10. und 22. Oktober) mit der Überarbeitung des Berichts auseinander (Cappato 2001, 5).

162 Diese Haltung Cappatos, einerseits Datenschutz im Hinblick auf Sicherheitsfragen den Vorzug zu geben und andererseits Einschränkungen des Schutzniveaus dann in Kauf zu nehmen, wenn dieses mit wirtschaftspolitischen Zielen konfligiert, deckt sich mit der Analyse der Haltung liberaler Parteien zum Datenschutz (Baumann 2013; Schütz und Karaboga 2015, 18).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.2.5 Post 9/11: Formierung der Parlamentsposition in erster Lesung: Zweiter Cappato-Bericht

Wenige Tage nach den Terroranschlägen vom 11. September traten die EU-Justiz- und Innenminister zusammen, um „die erforderlichen Maßnahmen zur Wahrung eines höchstmöglichen Sicherheitsniveaus sowie jede andere angezeigte Maßnahme zur Bekämpfung des Terrorismus zu ergreifen." (EU-Ministerrat 2001, 1) Zudem ersuchte der Ministerrat die EU-Kommission, „Vorschläge zu unterbreiten, mit denen dafür Sorge getragen wird, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden, und Maßnahmen gegen die Urheber zu ergreifen." (EU-Ministerrat 2001, 3, Nr. 4) Ergänzt wurde diese Forderung um den Hinweis, dass der Rat besonders darauf achten werde, „dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten *für strafrechtliche Ermittlungszwecke* gewährleistet wird." (ebd., Hervorhebung durch den Autor) Doch machte dieser wohl aus Rücksicht auf Datenschutzbedenken integrierte Passus zugleich die sehr weitgehende Intention des Ministerrats deutlich: Die anfallenden Daten sollten eben nicht nur für Zwecke der Terrorismusbekämpfung, sondern für jedweden strafrechtlichen Ermittlungszweck verwendet werden können (ebd.).

Zusätzlicher Druck auf die EU-Organe wurde auch aus dem EU-Ausland geübt. Nachdem die Europäischen Institutionen und Mitgliedstaaten im unmittelbaren Nachgang der Anschläge ihre Solidarität und Hilfsbereitschaft gegenüber den Vereinigten Staaten bekundet hatten, sandte die US-Regierung im Namen von Präsident George W. Bush einen Brief an die EU-Kommission bzw. Kommissionspräsident Romano Prodi, in dem die Organe der EU zur Verabschiedung einer Reihe von Sicherheitsmaßnahmen aufgefordert wurden. So wurde die EU u. a. dazu aufgerufen, Datenschutzfragen im Zusammenhang mit den Erfordernissen der Strafverfolgung und der Terrorismusbekämpfung zu berücksichtigen und die bestehenden Rechtsvorschriften im Datenschutzbereich dahingehend zu lockern, dass die *Speicherung kritischer Daten für einen angemessenen Zeitraum* ermöglicht würde (US Mission to the EU 2001). Interessanterweise verfügten nicht einmal die Vereinigten Staaten unter dem PATRIOT Act

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zu diesem Zeitpunkt selbst über eine der Öffentlichkeit bekannte Vorratsdatenspeicherung (Bunyan 2002).[163]

Nach Abschluss der Diskussionen im Ausschuss wurde der Entwurf für den zweiten Cappato-Bericht nur kurze Zeit nach dem Anschlägen in den USA am 22. Oktober 2001 vom LIBE-Ausschuss mit 23 Stimmen (bei 14 Gegenstimmen) angenommen und an das Parlamentsplenum überwiesen (Cappato 2001, 5). Dieses setzte sich am 12. November 2001 mit dem Bericht auseinander. Darin bestätigte der Ausschuss – entgegen den Forderungen des Ministerrats und der US-Administration – seine bereits zuvor festgelegte und das Datenschutzniveau stärkende Position hinsichtlich des Umgangs mit Verkehrsdaten. Außerdem kam Berichterstatter Cappato den Bedenken der Sozialdemokraten insofern entgegen, als für SMS-Werbung die Opt-in-Regel festgelegt werden sollte. Dagegen sah der zweite Bericht die Ausweitung der Opt-out-Regel – entgegen dem Parlamentsstandpunkt im ersten Bericht – auf öffentliche Verzeichnisse (also Telefonbücher) vor und auch in Bezug auf den Erhalt von unerbetenen Mails wurde am Opt-out-Prinzip festgehalten. Die Gründe dafür lassen sich besonders gut dem Redebeitrag des LIBE-Ausschussmitglieds Ulrik von Boetticher (EVP-ED, CDU) entnehmen: „Sollte das Parlament Werbung im Bereich business to customer zunächst generell verbieten, wie es der Vorschlag von Frau Paciotti nun vorsieht, werden Unternehmen eben ihre Werbung von den USA oder anderen Drittstaaten aus in die Europäische Union versenden. Nichts, aber auch gar nichts wäre damit für den europäischen Verbraucher gewonnen, einzig der europäische Markt im elektronischen Handel wäre geschwächt. Wir wollen darum den Staaten, die heute ein Opt out-System haben, dieses auch belassen, die Entwicklung beobachten und nach zwei Jahren neu entscheiden. […] Einzig dieser Vorschlag unterstützt die Interessen der Verbraucher, ohne massiv Arbeitsplätze in Europa zu vernichten." (Europäisches Parlament 2001d) Cappato verwies zudem darauf, dass nicht der Versand von E-Mail-Werbung die größte Gefahr für den Datenschutz darstellte, sondern der staatliche Zugriff: „Ich möchte jedoch nicht, dass, nachdem wir unsere große und verständliche Sorge wegen der durch unerbetene Werbe-E-Mails verursachten Belästigung bewiesen haben, wir ande-

163 So hatten nicht nur die Snowden-Enthüllungen die auf Basis des PATRIOT Act erfolgte massenhafte Speicherung von Verbindungsdaten im Rahmen des Überwachungsprogramms PRISMS zu Tage gebracht (Appelbaum und Poitras 2013). Schon vor der NSA praktizierte bereits die Drug Enforcement Agency (DEA) zwischen 1992 und 2013 eine umfassende geheime und keiner demokratischen Kontrolle unterworfene Vorratsdatenspeicherung (Beuth 2015b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

rerseits den nationalen Polizeibehörden demnächst die uneingeschränkte Befugnis erteilen, nach Gutdünken über unsere personenbezogenen Daten zu verfügen. Das ist kein Problem, das einzig und im engeren Sinne nur diese Richtlinie betrifft, sondern ein allgemeineres politisches Problem, dessen bin ich mir bewusst. Ich fürchte, dass wir genau diese Richtung einschlagen; ich fürchte, die größten Gefahren für den Schutz der Privatsphäre gehen nicht von einer mehr oder weniger erbetenen E-Mail-Werbung aus." (ebd.) Zudem verwies Cappato, dem liberalen Verständnis nach individueller Selbstbestimmung entsprechend, darauf, dass es bereits technische Möglichkeiten gäbe, die Absender-Adressen von Spam oder unerbetener Werbung zu blockieren, um fortan keine E-Mails mehr von diesen zu erhalten (ebd.).

Gekontert wurde dieses Argument seitens der sozialdemokratischen Paciotti damit, dass es „neben Leuten wie unserem Berichterstatter, der sich mit der Benutzung elektronischer Instrumente sehr gut auskennt, […] es noch viele [gibt], sehr viele Bürgerinnen und Bürger wie mich, denen der Umgang damit noch wenig vertraut ist und die sich deshalb Sorgen machen." (ebd.) Zudem verknüpfte Paciotti ihre Kritik am Opt-out-Prinzip schließlich mit der Frage nach Nutzer-Vertrauen: „Solange ich also nicht geschützt werde - [sic] und ich spreche für mich persönlich, obwohl es viele andere, vorwiegend ältere Bürgerinnen und Bürger wie mich gibt, die sich weniger auskennen als viele junge Leute - [sic], werde ich keinen Gebrauch vom elektronischen Geschäftsverkehr machen, weil ich kein Vertrauen dazu habe. Die Vorstellung, in einem durch das ganze Internet geisternden Verzeichnis zu stehen, Nachrichten zu erhalten, dann ihre Löschung zu verlangen, sie vorher öffnen zu müssen und zu versuchen, diese Instrumente zu verstehen, ist wenig vertrauenerweckend. Es kann ja sein, dass die Entwicklung der Elektronik einen besseren Schutz ermöglicht, doch zunächst einmal muss diese Entwicklung stattfinden; vorher müssen wir die Möglichkeiten für die Entwicklung des e-Commerce schaffen, wofür es Vertrauen braucht, was mit diesem Vorschlag nicht geschaffen wird." (ebd.)

Der finisch-stämmige sozialdemokratische EU-Kommissar für Industrie und Informationsgesellschaft Erkki Antero Liikanen lehnte die Vorschläge des Berichterstatters mit derselben Begründung ab[164] und ergänzte dies

164 „Wenn wir also positive Rahmenbedingungen für die Entwicklung des elektronischen Geschäftsverkehrs und der Mobildienste der dritten Generation schaffen wollen, müssen wir jetzt dafür zu sorgen, dass die Akzeptanz der drahtlosen Internetdienste nicht durch riesige Mengen von ‚Müll' in der elektronischen Post, für die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mit dem wirtschaftspolitischen Argument, dass das „Ausfiltern dieser unerwünschten Massenwerbung […] schätzungsweise über 8,2 Mio. US-Dollar kosten [werde]." (ebd.)

Lediglich die Abgeordnete und Verfasserin der Stellungnahme des mitberatenden ITRE-Ausschusses, Ilka Schröder (GUE/NGL)[165], vertrat unter Absehung wirtschaftspolitischer Argumente die Position, dass es bei der bevorstehenden Entscheidung um die Selbstbestimmung des Individuums ginge und dem Cappato-Bericht deshalb nicht zugestimmt werden sollte (ebd.).

Der Cappato-Bericht wurde schließlich am 13. November 2001 mit einer großen Mehrheit von 339 Stimmen angenommen. Vor allem die EDD, EL-DR (ALDE), EVP-ED, UEN sowie die parteilosen Abgeordneten stimmten weitgehend geschlossen für den Cappato-Bericht. Unterstützung erhielten die Befürworter zudem von etwas weniger als der Hälfte der SPE-Abgeordneten. Die 92 Gegenstimmen setzen sich vor allem aus den Stimmen der Grünen/EFA und der GUE/NGL zusammen.[166] Hinzukamen einige sozialdemokratische und liberale Abweichler. Die 89 Enthaltungen setzten sich hingegen vor allem aus Sozialdemokraten zusammen. Etwa die halbe Fraktion enthielt sich und fand Unterstützung von einem liberalen, vier parteilosen, zwei konservativen, zwei nationalkonservativen/europaskeptischen (UEN) sowie einem grünen Abgeordneten (Europäisches Parlament 2002b, 38 f.).

3.3.2.6 Interinstitutionelle Auseinandersetzungen und ein schaler Kompromiss

Kurz nach Verabschiedung der Parlamentsposition trat der Ministerrat (Telekommunikation) am 6. und 7. Dezember 2001 zusammen und nahm in Art. 15 Abs. 1 erneut die Formulierung auf, dass Verbindungsdaten „während einer begrenzten Zeit gemäß den allgemeinen Grundsätzen des Gemeinschaftsrechts aufbewahrt werden" dürfen sollen. Zugleich demons-

der Verbraucher gegen seinen Willen zahlen soll, erschwert wird." (vgl. Liikanen, in: Europäisches Parlament 2001d)

165 Schröder war Abgeordnete der Grünen auf Bundes- und Europaebene, verließ jedoch aufgrund ihrer Unzufriedenheit mit dem flüchtlings- und militärpolitischen Kurs der Partei (Schröder 2001) die grüne Europafraktion am 27. September 2001 und schloss sich am 28. September 2001 der GUE/NGL an (EP 2020a).

166 Je ein Abgeordneter der Grünen/EFA stimmte für den Vorschlag bzw. enthielt sich. Die GUE/NGL war die einzige Fraktion die ausnahmslos dagegen stimmte (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

trierte der Ministerrat auf dieser Sitzung seine Enschlossenheit, keine Kompromisse bei der Frage der Speicherung von Verkehrsdaten elektronischer Kommunikation eingehen zu wollen und intensivierte auf diese Weise den Druck auf Kommission und Parlament. Seine Änderungen begründete der Ministerrat später mit den „erheblichen Gefahren, die durch die Ereignisse am 11. September 2001 sichtbar geworden sind," (vgl. Begründung des Rates, Nr. III, in: EU-Ministerrat 2002, 51) Die Kommission signalisierte daraufhin erstmals auf der Ratstagung am 6. Dezember die Bereitschaft, ihren Widerstand gegen die Änderungen in Art. 6 und Art. 15 Abs. 1 aufzugeben, woraufhin die Art. 29-Datenschutzgruppe gegen die Reduktion demokratischer Standards zugunsten von Anti-Terror-Maßnahmen Einspruch erhob und die „zunehmende Tendenz, den Schutz der Privatsphäre als Hindernis eines effizienten Kampfs gegen den Terrorismus darzustellen" mit Nachdruck kritisierte (Bunyan 2002).

Schließlich verabschiedete der Ministerrat seinen zuvor festgelegten Gemeinsamen Standpunkt am 28. Januar 2002 unter der konservativen spanischen Ratspräsidentschaft offiziell (EU-Ministerrat 2002), sodass gemäß dem Mitentscheidungsverfahren das Parlament an der Reihe war, eine zweite Lesung abzuhalten, in der es auf die Ministerratsposition reagiert. Bereits zwei Tage nach Bekanntgabe der Ministerratsposition wandte sich die Kommission in einer Mitteilung an das Parlament, in der sie ihre Unterstützung der Ministerratsposition zum Ausdruck brachte und dem Parlament die Annahme der Ministerratsposition empfiehl (EU-Kommission 2002). Ihren Meinungswechsel begründete die Kommission mit dem Argument, dass die Änderungen des Ministerrats hinsichtlich Art. 15 Abs. 1 aus datenschutzrechtlicher Perspektive unbedenklich seien, da mit ihnen keine generelle Verpflichtung der Mitgliedstaaten zur Speicherung von Verkehrsdaten bzw. zur Abweichung vom Grundsatz der Löschung vorgesehen würde und somit „der erste Satz des Artikels 15 dem Wesen nach rechtlich nicht verändert und [„„] ihm nichts hinzugefügt" (ebd.) werde. Dabei handelte es sich freilich um den Versuch der Kommission, angesichts ihres bedingungslosen Einknickens gegenüber den Forderungen der Mitgliedstaaten mithilfe eines rhetorischen Tricks den Anschein von Integrität zu wahren. Denn dass eine Reihe von Mitgliedstaaten bereits spätestens seit dem Jahr 1998 die Einführung einer gemeinschaftsweiten Vorratsdatenspeicherung befürwortete, wird den Kommissionsverantwortlichen hinlänglich bekannt gewesen sein (Statewatch 2001). Insofern konnte der Änderungsvorschlag des Ministerrats – entgegen der Interpretation der Kommission – nur so gedeutet werden, dass mit ihm Tür und Tor für

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

eine generelle Aufbewahrung von Verkehrsdaten geöffnet würde. Fraglich ist, ob die Kommission zu diesem Zeitpunkt überhaupt noch ernsthaft gegen die Einführung einer unionsweiten Vorratsdatenspeicherung war, oder ob der als Gegnerschaft interpretierte Passus nicht lediglich ein Verweis auf einen primärrechtlichen und zu diesem Zeitpunkt noch ungeklärten Zuständigkeitskonflikt hinsichtlich der Speicherung von Verkehrsdaten zu Zwecken der Strafverfolgung gewesen ist (Bunyan 2002). So begründete die Kommission ihre Ablehnung damit, dass die ePrivacy-Richtlinie, „die sich auf Artikel 95 EG-Vertrag stützt, keine wesentlichen Bestimmungen über Maßnahmen des Gesetzesvollzugs enthalten" dürfe. Dementsprechend sollte sie „keinerlei konkrete Maßnahmen, die die Mitgliedstaaten für notwendig halten mögen, verbieten oder billigen." (ebd.). Die Gegnerschaft der Kommission lässt sich auf Basis dieser Zitate m. E. daher lediglich als ein Verweis auf die ungeklärte Frage, ob derartige Maßnahmen Gegenstand einer Regulierung im Rahmen der ersten oder der dritten Säule zu sein hätten, verstehen.

Am 6. Februar 2002 überwies der Parlamentspräsident den Gemeinsamen Standpunkt des Rates schließlich erneut an den LIBE-Ausschuss. Auf Grundlage des LIBE-Beschlusses vom 29. August 2000 war weiterhin Marco Cappato der zuständige Berichterstatter. Auf drei weiteren LIBE-Sitzungen im Februar, März und April wurde über die Änderungsanträge des Ministerrats beraten und schließlich am 18. April 2002 der Entwurf für eine Stellungnahme des Parlaments für die zweite Lesung mit 36 Stimmen bei 6 Gegenstimmen und 0 Enthaltungen angenommen (Cappato 2002, 4). Der finalen Abstimmung des Ausschusses über den Entwurf als Ganzes war allerdings eine Kampfabstimmung über einen Änderungsantrag der spanischen LIBE-Ausschussvorsitzenden Ana Palacio (EVP-ED, PP) vorangegangen. Palacio hatte im Rahmen eines informellen Trilogs am 16. April, also zwei Tage vor der LIBE-Abstimmung mit Vertretern der Kommission und des Rates verhandelt und dem Schattenberichterstatter der EVP-DE-Fraktion sowie dem britisch stämmigen LIBE-Ausschussmitglied Michael Cashman (SPE, Labour) einen Änderungsantrag vorgelegt, der den Standpunkt des Rates akzeptiert und damit dem Druck der spanischen Ratspräsidentschaft nachgab. Mit diesem Schritt brüskierte Palacio zudem die Ausschuss-Tradition gemäß der nicht noch einmal über Fragen abgestimmt wird, über die bereits zuvor einstimmig entschieden worden war. Palacios Änderungsantrag wurde schließlich mit 25 gegen 19 Stimmen abgelehnt. Die Mehrheit kam dadurch zustande, dass die sozialdemokratischen Ausschussmitglieder gemeinsam mit liberalen, grünen und

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

linken Ausschussmitgliedern gegen Palacios Vorschlag votierten. Befürwortet wurde dieser dagegen von den Ausschussmitgliedern der konservativen Fraktion, unterstützt von den nationalkonservativen/euroskeptischen sowie europakritischen Fraktionen (Statewatch 2002c).

Nachdem Palacios Vorstoß gescheitert war und die Position des LIBE-Ausschusses angenommen wurde, intensivierte die spanische Ratspräsidentschaft ihre Bemühungen dahingehend, einzelne Abgeordnete unmittelbar zu kontaktieren, um diese von der Annahme eines *Kompromissantrages* bei der für den 15. Mai 2002 angesetzten Abstimmung im Parlamentsplenum zu überzeugen. Ein Blick auf die Größe der Fraktionen zeigt, dass dies aus Ratsperspektive eine vielversprechende Strategie war. So bestand das Parlament zu diesem Zeitpunkt aus insgesamt 626 Abgeordneten. Für die Beschlussfassung wurden 314 Stimmen benötigt, von denen allein 233 durch die konservative EVP-DE-Fraktion beigesteuert werden konnten. Unterstützt wurde sie von den übrigen rechtsgerichteten Fraktionen, der UEN mit 22 Abgeordneten sowie der EDD bestehend aus 18 Abgeordneten, sodass insgesamt bereits 273 der erforderlichen Stimmen erreicht wurden. Dadurch musste die Ratspräsidentschaft *nur* 41 weitere Abgeordnete zur Unterstützung ihres Vorschlags motivieren, um die Verabschiedung ihres Vorschlags abzusichern. Daneben saßen im Parlament insgesamt 32 fraktionslose Abgeordnete, von denen wiederum 18 ehemalige Mitglieder der rechtskonservativ bis rechtsextremen Fraktion[167] der Technischen Fraktion der Unabhängigen Abgeordneten (TDI) waren, die Ende 2001 aufgelöst worden war. Die übrigen, gegenüber der Vorratsdatenspeicherung kritisch eingestellten Fraktionen kamen allerdings gemeinsam auf 321 Stimmen (PSE 179, ELDR 53, Grüne/EFA 45, GUE/NGL 44), sodass für die Ratspräsidentschaft von zentraler Bedeutung war, mögliche Abweichler aus deren Reihen zur Unterstützung der Ratsposition zu bewegen (Statewatch 2002d, 2002e). Um mehr Zeit für ihre Intervention zu haben, erreichte die Ratspräsidentschaft, dass der Abstimmungstermin im Parlament vom 15. Mai auf den 30. Mai verschoben wurde. Währenddessen arbeitete die zuständige Ratsarbeitsgruppe auf ihren Sitzungen am 3. und 13. Mai an der Formulierung eines Kompromissvorschlags, den man dem Parlament unterbreiten würde. Ohne Rücksprache mit dem Berichterstatter Cappato

167 Eine Ausnahme war die Mitgliedschaft der linksliberal-radikalen *Lista Emma Bonino*. Abgesehen davon war die Fraktion Heimat für rechtsextreme Parteien wie *Lega Nord*, *Front National* (der heutigen *Rassemblement National*) und *Vlaams Blok* (der heutigen Vlaams Belang) (European Parliament 1999).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zu halten, initiierte Ana Palacio schließlich am 15. Mai die Übersendung eines Kompromissvorschlags im Namen des Parlaments an den Ministerrat. Der sogenannte Kompromissvorschlag war praktisch derselbe Vorschlag, über den der Ausschuss etwa einen Monat zuvor bereits ablehnend abgestimmt hatte. Als Cappato von dem Vorgang erfuhr, konnte er die offizielle Übersendung verhindern. Allerdings griff die spanische Ratspräsidentschaft nur einen Tag später Palacios Vorschlag trotzdem auf und bewarb diesen beim AStV als grundsätzlich akzeptablen Kompromiss.[168] Während der Ministerrat einerseits auf Seiten des Parlaments auf Kompromissbereitschaft drängte, war er selbst nicht gewillt, Kompromisse einzugehen. Von den 23 Änderungsvorschlägen, die der Cappato-Bericht in Bezug auf die Ratsposition formulierte, war der Rat lediglich bereit, zwei kleinere anzunehmen, während alle anderen abgelehnt wurden (Statewatch 2002d).

Nachdem diese Bemühungen des Ministerrats und der Ausschutzvorsitzenden zum Kippen der Parlamentsabstimmung bekannt geworden waren, wandte sich die Global Internet Liberty Campaign (GILC), eine internationale Koalition bestehend aus 40 Bürgerrechtsorganisation aus 15 Staaten[169] an alle Europaabgeordneten, in der sie diese dazu aufforderten, für die vom LIBE-Ausschuss vorgelegte Empfehlung zu votieren. Interessanterweise wurde diese Forderung zudem nicht nur mit dem Verweis auf individuelle Privatheit, sondern auch mit Gemeinwohlargumenten begründet: „Neue Speicherungserfordernisse, wie sie in der gemeinsamen Position des Rates befürwortet wurden, würden neue Risiken für die persönliche Privatsphäre, die politische Freiheit, die Meinungsfreiheit und die öffentliche Sicherheit bedeuten." (GILC 2002) Daneben wurde eine internationale Unterschriftenkampagne der 2001 gegründeten, überwachungskritischen Bürgerinitiative *STOP1984* innerhalb kurzer Zeit von mehr als 17.000 Menschen in 48 Staaten unterzeichnet (Europäisches Parlament 2002c; Statewatch 2002a). Kritik kam auch von Seiten der Wirtschaft. Die von einer Vorratsdatenspeicherung betroffenen europäischen Internet Service Provider bzw. deren Verbände wandten sich in einer gemeinsamen Stellungnahme im April 2002 gegen die Einführung der Vorratsdatenspeicherung. Diese verwiesen einerseits auf die Grundrechtseingriffe infolge einer Vorratsdatenspeicherung und andererseits auf die im Zusammenhang mit

168 Für einen Überblick über die konkreten Änderungsvorschläge zu Art. 15 Abs. 1, siehe: (Statewatch 2002d).

169 Darunter ACLU, Bits of Freedom, CDT, DVD, EFF, EPIC, PI, Statewatch, quintessenz (GILC 2002).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

der Einrichtung und dem Betrieb einer Vorratsdatenspeicherung zusammenhängenden Kosten (ETNO, EuroISPA, und ECTA 2002).

Währenddessen hatte auch der Ministerrat seinen Druck auf das Parlament weiter intensiviert. Nachdem die konservative LIBE-Ausschussvorsitzende Palacio bereits zuvor auf den Kurs des spanischen Ratsvorsitzes umgeschwenkt war, gelang es kurz vor der Abstimmung des Parlaments auch Elena Paciotti, das führende SPE-Mitglied im LIBE-Ausschuss davon zu überzeugen, der Ratsposition zuzustimmen. Der Meinungsumschwung der Konservativen und Sozialdemokraten wurde von diesen auf der folgenden Plenardiskussion des Parlaments am 29. Mai 2002, an der Ana Palacio[170] übrigens nicht teilnahm, damit begründet, dass die Mitgliedstaaten die entsprechenden Regelungen zur Vorratsdatenspeicherung selbst im Falle eines Parlamentsvetos, bei dem zudem das gesamte ePrivacy-Richtlinienvorhaben scheitern würde, ohnehin auf Basis mitgliedstaatlicher und/oder intergouvernementaler Maßnahmen durchsetzen würden.[171] Dies wiederum würde das Parlament jeglicher Mitgestaltung berauben, weshalb ein zugegebenermaßen unzureichender Kompromiss im Falle der ePrivacy-Richtlinie zu akzeptieren wäre (vgl. hierzu insb. die Ausführungen von Boettichers, Paciottis und Cederschiölds, in: Europäisches Parlament 2002c).[172] Dem

170 Die Verdienste Ana Palacios sollten schließlich nicht unbelohnt bleiben. Am 9. Juli schied die spanische Europaabgeordnete aus dem Parlament aus und trat ihre neue Stelle als erste spanische Außenministerin in der konservativen Regierung José María Aznars an und behielt diese Position bis zur Abwahl der Regierung am 16. April 2004 (Wikipedia 2019a).

171 Dies ist allerdings als eine leere Behauptung zu bewerten, da für einen intergouvernementalen Rahmenbeschluss die Einstimmigkeit im Rat erforderlich gewesen wäre, die es aber weder zu diesem Zeitpunkt noch später gegeben hat. Die Behauptung, dass der Erlass entsprechender Maßnahmen seitens einzelner Mitgliedstaaten schwerer wiege als eine Unionsmaßnahme kann jedoch nur von Relevanz sein, sofern die Unionsmaßnahme deutlich bürgerrechtsfreundlicher gestaltet wäre als die nationalen Maßnahmen. Wie sich im politischen Entscheidungsprozess der EG-Richtlinie zur Vorratsdatenspeicherung wenig später zeigen sollte, konnte das Parlament keinen nennenswerten Einfluss auf die Ausgestaltung der Unionsmaßnahme nehmen (vgl. 3.3.4.2 zur Richtlinie 2006/24/EG).

172 So etwa die konservative Cederschiöld, die für den *Kompromiss* stimmte: „Leider ist es schwer, Befriedigung angesichts des Ergebnisses zu empfinden, aber nationale Vorschriften würden noch größere Unterschiede und umfassendere Probleme schaffen." (Europäisches Parlament 2002c) Paciotti verteidigte ihr Vorgehen folgendermaßen: „Wie jede Lösung, die einen Ausgleich zwischen verschiedenen Interessen herstellen soll, muss auch diese hier im Ganzen beurteilt werden. Mir erscheint sie vernünftig und unterstützenswert, da es gewiss nicht in der Macht des Europäischen Parlaments steht, vom Rat zu erreichen, dass er den Mitgliedstaaten die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ministerrat spielte zudem der Umstand in die Hände, dass die übrigen fünf Richtlinien des neuen Rahmens für die elektronische Kommunikation bereits zum 24. April 2002 in Kraft getreten waren und alle beteiligten Akteure daher möglichst bemüht darum waren, die bereits zu diesem Zeitpunkt verspätete Verabschiedung der ePrivacy-Richtlinie durch die Initiierung eines Vermittlungsverfahrens nicht noch weiter zu verzögern oder gar die Verabschiedung grundsätzlich zu gefährden.[173] Daneben war der Ministerrat Paciotti im Hinblick auf die von den Sozialdemokraten favorisierte und von Berichterstatter Cappato abgelehnte Opt-in-Regelung entgegenkommen und trat im Rahmen der Einigung gegen die im Cappato-Bericht vorgeschlagene europaweite Opt-out-Regelung ein und überlies die Entscheidung den Mitgliedstaaten, sodass Paciotti bei dieser ihr wichtigen Frage durchaus auch einen Teilerfolg verzeichnen konnte. Darüber hinaus war insbesondere Paciotti darum bemüht, die mit dem Ministerrat erzielte Einigung als Kompromiss darzustellen. Sowohl in ihrer Antwort an die Bürgerrechtskoalition als auch während der Plenardebatte vertrat sie die Ansicht, dass die mit dem Ministerrat erzielte Einigung deshalb als Kompromiss zu bezeichnen wäre, weil sie es geschafft hätte, in den zur Debatte stehenden Artikeln explizite Verweise auf die Vereinbarkeit der zu verabschiedenden Maßnahmen mit der EMRK, Art. 6 EUV und der Rechtsprechung des EGMR unterzubringen, die andernfalls keine Erwähnung gefunden hätten (Europäisches Parlament 2002c; Statewatch 2002b). Der Ministerrat dagegen hatte keine Probleme mit den entsprechenden Verweisen, da sie ohnehin auf jede Gemeinschaftsmaßnahme Anwendung fanden und damit als keine zusätzliche Maßregelung der von den Strafverfolgungsbehörden geforderten Maßnahmen zu verstehen waren. Aufgrund dessen wurde Paciotti dann auch berechtigterweise Augenwischerei vorgeworfen (Statewatch 2002b) – fraglich ist allein, ob sie persönlich tatsächlich der Ansicht war, einen wirklichen Kompromiss erzielt zu haben oder dies aus anderen Gründen lediglich behauptete. Deutlich klarer artikulierte ihr britischer Parteikollege Michael Cashman seine Befürwortung der Ministerratsposition: „Vielleicht darf ich Sie daran erinnern, dass die bürgerlichen

Aufbewahrung von Verkehrsdaten aus Gründen der nationalen Sicherheit untersagt. Wir können das nicht verbieten; wir können einen Rahmen der Garantien, der Sicherheiten und des Schutzes der Grundrechte abstecken, damit diese durch die künftige Gesetzgebung gewahrt werden müssen." (ebd.)

173 Wie den Äußerungen von Kommissar Liikanen zu entnehmen ist, war dies offenbar einer der ausschlaggebenden Gründe für den Positionswechsel der Kommission (Europäisches Parlament 2002c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Freiheiten vor international operierenden Terroristen geschützt werden müssen, vor Drogenhändlern, internationalen Verbrechern, Frauen- und Kinderhändlern. Das sind die bürgerlichen Freiheiten, die wir mit den angemessenen und ausgewogenen Bestimmungen zur Datenspeicherung in den dem Parlament vorliegenden Vorschlägen schützen wollen." (Europäisches Parlament 2002c) Hervorzuheben ist zudem, dass in der Kritik der ELDR und der EVP-DE neben bürgerrechtlichen Erwägungen die für die Wirtschaft drohenden Kosten einer Vorratsdatenspeicherung thematisiert wurden.[174] Lediglich die Vertreterin der Linken, Ilka Schröder, verwies auf die potentiellen gesellschaftlichen Folgen einer durch die Vorratsdatenspeicherung ermöglichten Massenüberwachung (ebd.).

Bei der finalen Abstimmung im Parlament am 30. Mai 2002 votierte schließlich eine aus EVP-DE und SPE geformte Mehrheit der Europaparlamentarier gegen die Empfehlungen des Cappato-Berichts und für den *Kompromiss*, der die Ministerratsposition bestätigte. So wurde der umstrittene zweite Teil des Änderungsantrags 46 mit 351 Stimmen (bei 133 Gegenstimmen und 13 Enthaltungen) angenommen. Während es bei den Konservativen und Sozialdemokraten kaum Abweichler gab, erhielten sie von der Mehrheit der EDD- und der UEN-Fraktion, von einigen liberalen und fraktionslosen sowie seitens eines grünen Abgeordneten Unterstützung. Dagegen stimmten die vollständige GUE/NGL-Fraktion, die Mehrheit der ELDR, der Grünen/EFA und fraktionslosen Abgeordneten sowie einzelne Abgeordnete der übrigen Fraktionen (Europäisches Parlament 2003, 54 f.). Der Ministerrat bestätigte die in zweiter Lesung des Parlaments angenommenen Änderungsanträge am 25. Juni, sodass die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG am 12. Juli 2002 vom Präsidenten des Parlaments und der Ratspräsidentschaft unterzeichnet wurde und am darauffolgenden Tag in Kraft trat (Das Europäische Parlament und der Rat der Europäischen Union 2002).

Wie schon zuvor im Falle der DS-RL und der ISDN-RL erfolgte auch die Umsetzung der ePrivacy-Richtlinie teils mit erheblicher Verzögerung. Die ePrivacy-Richtlinie musste in den alten Mitgliedstaaten bis zum 30. Oktober 2003 und in den zehn neuen Mitgliedstaaten bis zum 1. Mai 2004 umgesetzt werden. Dieser Verpflichtung kam nur ein Teil der Mitgliedstaaten nach, sodass die Kommission Ende 2004 Vertragsverletzungsverfahren gegen die fünf Mitgliedstaaten Belgien, die tschechische Republik, Estland,

174 Vgl. hierzu die Ausführungen der Liberalen Plooij-van Gorsel und der Konservativen Charlotte Cederschiöld (Europäisches Parlament 2002c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Griechenland und Luxemburg initiierte (EU Commission 2004, 6 f. EU-Kommission 2004, 9). Die Richtlinie wurde schließlich in Estland Ende 2004 (EU-Kommission 2005, 30), in Belgien, in Tschechien und in Luxemburg im Laufe des Jahres 2005 (EU-Kommission 2006, 19, 26, 78) sowie in Griechenland erst 2006 (Europäische Kommission 2008a, 57) in nationales Recht umgesetzt.

3.3.2.7 Zwischenfazit

Der politische Aushandlungsprozess der ePrivacy-Richtlinie war aus mehreren Gründen wichtig für die EU-Datenschutzpolitik. *Erstens* zeichneten sich hier erstmals in aller Deutlichkeit die Fronten zwischen den parteipolitischen Akteuren ab, die fortan relativ stabil bleiben sollten. Während das Europäische Parlament in den 1970er- und 1980er-Jahren noch als Datenschutzbefürworter aufgetreten und für den Erlass von Datenschutzregelungen eingetreten war, hatte es während der Aushandlung der DS-RL eine eher ambivalente Rolle eingenommen. An den Konflikten bei der Aushandlung der ePrivacy-Richtlinie differenzierte sich diese Rolle nun aus: Es zeigte sich erstmals in offensichtlicher Weise auf EU-Ebene, dass es vier Fronten gab: Eine *liberale Perspektive* auf Datenschutz, die unter Verweis auf die Selbstbestimmungsfähigkeit des Einzelnen und unter Absehung der Verwirklichungsbedingungen dieser für weniger Einschränkungen gegenüber privatwirtschaftlichen Datenverarbeitern eintrat, aber zugleich eine stärkere Rolle des Staates strikt ablehnt. Privatwirtschaftliche Datenverarbeiter standen dieser Perspektive am nächsten. Daneben eine *konservative Perspektive*, die einen möglichst weitreichenden Verarbeitungsspielraum sowohl für privatwirtschaftliche als auch für staatliche Akteure einfordert. Eine *grundrechtsorientierte Perspektive* auf Datenschutz, die einen möglichst umfassenden Schutz personenbezogener Daten vor privatwirtschaftlichen sowie staatlichen Akteuren fordert. Dieser Perspektive standen sowohl Datenschutzaufsichtsbehörden als auch zivilgesellschaftliche Datenschützer nahe. Und schließlich eine *sozialdemokratische Perspektive* auf Datenschutz, die einer grundrechtsorientierten Perspektive zwar nahestand und für Einschränkungen gegenüber privatwirtschaftlichen Akteuren eintrat, aus Gründen der Staatsraison allerdings letztlich einer weitgehenden staatlichen Datenverarbeitung zustimmte. Die politische Einigung, die letztlich erzielt wurde, spiegelt einen Kompromiss zwischen konservativer und sozialdemokratischer Perspektive wider.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zweitens bildete der Aushandlungsprozess der ePrivacy-Richtlinie den ersten politischen Konflikt auf EU-Ebene, bei dem sich eine transnationale Koalition aus Bürgerrechtsorganisationen[175] auf die Seite der parlamentarischen Vertreter der grundrechtsorientierten Perspektive schlug und damit den ersten Grundstein zur Bildung einer längerfristigen Advocacy-Koalition der Datenschutzbefürworter legte.[176]

Schließlich und *drittens* bildete der Erfolg der Überwachungsbefürworter den Anfangspunkt einer Reihe von politischen Niederlagen, denen sich Datenschutzbefürworter in den Folgejahren gegenübersahen. Diese politischen Niederlagen bzw. der dabei erreichte Ausbau der Überwachungsmöglichkeiten sollte später wesentlich dazu beitragen, dass die EU-Datenschutzreform als eine Reaktion auf diese Prozesse eingeleitet und letztlich auch erfolgreich zu Ende gebracht wurde.

3.3.3 Berichte der Kommission über die Durchführung der DS-RL

In Art. 33 der DS-RL 95/46/EG wurde geregelt, dass die Kommission dem Europäischen Parlament und dem Ministerrat regelmäßig einen Bericht über die Durchführung der Richtlinie vorlegen und gegebenenfalls geeignete Änderungsvorschläge machen sollte. Art. 33 sah die Veröffentlichung des ersten Berichts drei Jahre nach Ablauf der in Art. 32 Abs. 1 vorgesehenen dreijährigen Umsetzungsfrist (1998), also im Jahr 2001 vor. Aufgrund der verzögerten Umsetzung der DS-RL in den Mitgliedstaaten (vgl. 3.2.2.9) verschob sich die Veröffentlichung des Berichts allerdings um 18 Monate, sodass die Kommission diesen erst am 15. Mai 2003 vorlegte (KOM 2003, 3). Bei der Erarbeitung des Berichts stützte sich die Kommission auf ihre neue, insb. im Kommissionsweißbuch vom Juli 2001 für das Europäische Regieren niedergelegte, Governance-Strategie (EU-Kommission 2001b), mit der eine breite Beteiligung verschiedener gesellschaftlicher Gruppen

175 So insb. die GILC, zu deren Mitgliedern zu diesem Zeitpunk ACLU, Bits of Freedom, CDT, DVD, EFF, EPIC, Privacy International, Statewatch, quintessenz zählten (GILC 2002).

176 Die Ausweitung von Überwachungsmaßnahmen auf EU-Ebene war dann auch ein wesentlicher Grund, der zur Entstehung der European Digital Rights Initiative (EDRi) im Sommer 2002 führte (Ziegler 2002). EDRi sollte schließlich die GILC, die ihre Aktivitäten seit 2003 einstellte, ablösen und zum zentralen zivilgesellschaftlichen Akteur der Community der Datenschutzbefürworter aufsteigen (vgl. 3.4.2.3.1).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gewährleistet werden sollte (KOM 2003, 3). Zu diesem Zweck stellte die Kommission im Jahr 2002 „Fragen an die Regierungen der Mitgliedstaaten und getrennt an die Datenschutzbehörden […]; [gab] zwei wissenschaftliche Studien in Auftrag […]; [veröffentlichte] im Amtsblatt und auf der Kommissionswebsite eine Aufforderung zur Abgabe von Stellungnahmen […]; [stellte] zwei Fragebogen über zwei Monate lang auf ihre Website […], einen, der sich an für die Verarbeitung Verantwortliche richtete, und einen für von der Verarbeitung Betroffene; [und veranstaltete] eine internationale Konferenz […], auf der in sechs verschiedenen Workshops ein umfangreiches Themenspektrum erörtert wurde." (ebd., 7)[177] Während Wirtschaftsvertreter und Behörden der Aufforderung zur Abgabe von Stellungnahmen folgten, beteiligte sich aus den Reihen jener Organisationen, die Bürgerrechtsinteressen vertraten, lediglich BEUC[178] am schriftlichen Konsultationsprozess (ebd.).

3.3.3.1 Die Ergebnisse des Berichts: Kritikpunkte

Im Hinblick auf den *Hauptzweck* der Richtlinie in Gestalt der Gewährleistung des freien Datenverkehrs stellte die Kommission fest, dass trotz des Vorhandenseins subtilerer Behinderungen des freien Datenverkehrs[179] keine Aussetzung oder Ablehnung eines grenzüberschreitenden Datentransfers zwischen Mitgliedstaaten stattgefunden habe, der Hauptzweck der

177 An der internationalen Konferenz nahmen neben Kommissions-, Parlaments und Ministerratsangehörigen insb. Vertreter aus den nationalen Datenschutzaufsichtsbehörden, der Industrie und Verbraucher- bzw. Datenschutzorganisationen teil. Folgende Akteure, die später am Aushandlungsprozess der DSGVO beteiligt waren, partizipierten auch an dieser Konsultation: GDV, Yahoo, UNICE/Businesseurope und FEDMA auf Seiten der Industrie. Vonseiten der Zivilgesellschaft waren BEUC, EPIC und Privacy International beteiligt. Darüber hinaus beteiligten sich auch Vertreter der US Federal Trade Commission, der OECD und des EGMR an der Konferenz (European Commission 2002). An der schriftlichen Konsultation nahmen die folgenden Akteure teil: ACCIS, AmCham EU, BITKOM, EMOTA, ENPA, EPC, ETNO, Eurofinas, BEUC, FEDMA, GDD, IAB, ICC, Telefónica, UNIC/Businesseurope, ZAW (EU-Kommission 2003).

178 BEUC ist ein 1962 gegründeter europäischer Zusammenschluss nationaler Verbraucherschutzorganisationen. Ihm gehören mehrere Dutzend nationale Verbände an (BEUC 2013).

179 Etwa der Erlass unterschiedlich strenger Vorschriften in verschiedenen Mitgliedstaaten, die „zunächst die interne Verarbeitung personenbezogener Daten in diesem Mitgliedstaat und in der Folge auch den Export dieser Daten in andere Mitgliedstaaten einschränken." (ebd., 11)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Richtlinie daher als erfüllt zu bewerten sei. Auch das Ziel der Gewährleistung eines hohen Datenschutzniveaus sah die Kommission – trotz anderslautender Ergebnisse der Online-Befragung, in der die teilnehmenden EU-Bürgerinnen und -Bürger sowohl das Schutzniveau als auch den Informationsstand über den Datenschutz kritisierten – als weitgehend erfüllt an (ebd., 10 f.). Vertreter multinationaler Unternehmen bemängelten derweilen insbesondere die abweichende Umsetzung der Richtlinienvorgaben (beispielsweise Schwierigkeiten beim anwendbaren einzelstaatlichen Recht, die unterschiedliche Umsetzung der Meldepflicht sowie abweichende Bedingungen für grenzüberschreitende Datentransfers) in verschiedenen Mitgliedstaaten. Die von einigen dieser Unternehmen vorgeschlagene Harmonisierung der nationalen Divergenzen auf dem Wege einer Änderung der Richtlinie lehnte die Kommission unter Verweis darauf, dass mit der Richtlinie eine Annäherung und nicht vollständige Vereinheitlichung angestrebt werde, nationale Divergenzen also zu verkraften sein sollten, ab (ebd., 12). Zugleich sah die Kommission aber durchaus ein, dass selbst in Bereichen, für die eine weitgehende Harmonisierung vorgesehen war, inakzeptable Divergenzen entstanden seien: „z. B. bei den ‚Begriffsbestimmungen' oder den abschließenden Aufzählungen in der Richtlinie wie in Artikel 7 (Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung), 8 Abs. 1 (sensible Daten), 10 (Informationen der Betroffenen), 13 (Ausnahmen, 26 (Ausnahmen bezüglich der Übermittlung in Drittländer usw.)." (ebd.)

Eine der am häufigsten kritisierten Bestimmungen war jene des *Art. 4 zum anwendbaren einzelstaatlichen Recht*. In diesem Zusammenhang forderten einige der betroffenen Verantwortlichen die Einführung des Herkunftslandprinzips, da dieses den „internationalen Organisationen ermöglichen würde, innerhalb der EU mit einem einzigen Regelwerk arbeiten zu können." (ebd., 18) Zudem wurde die Regel kritisiert, dass EU-Recht lediglich auf außerhalb der EU niedergelassene für die Verarbeitung Verantwortliche anwendbar war, sofern diese zum Zwecke der Verarbeitung personenbezogener Daten auf Mittel (i. S. v. Gerätschaften zur Verarbeitung) zurückgriffen, die im Hoheitsgebiet eines Mitgliedstaates belegen waren.

Eine weitere sehr häufig kritisierte Bestimmung war die in den Art. 18 und 19 geregelte *Meldepflicht*. Unternehmensvertreter forderten die Vereinfachung der Regelungen und ihre gemeinschaftsweite Harmonisierung (ebd., 19).

Schließlich stellte die Kommission im Zusammenhang mit der *Übermittlung personenbezogener Daten in Drittländer* fest, dass einige Mitgliedstaaten die Beurteilung der Angemessenheit des vom Empfänger garantierten

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Schutzniveaus auf unzulässige Weise dem für die Verarbeitung Verantwortlichen übertrugen, während andere Mitgliedstaaten alle Übermittlungen in Drittländer auch dann von einer Genehmigung abhängig zu machen versuchten, wenn für das entsprechende Drittland bereits ein Angemessenheitsbefund vorlag. Im Zusammenhang mit dem zu nachsichtigen Umgang mit grenzüberschreitenden Datenübermittlungen wies die Kommission auf die Gefahr hin, „dass der Schutz in der gesamten EU geschwächt wird, weil aufgrund des durch die Richtlinie garantierten freien Datenverkehrs die Datenströme wahrscheinlich über die ‚am wenigsten aufwändigen' Ausfuhrwege geleitet werden." (ebd., 20) Andererseits betonte die Kommission, dass ein zu strenger Ansatz „die legitimen Erfordernisse des internationalen Warenverkehrs und die Realität der globalen Telekommunikationsnetze ignorieren und die Gefahr bergen [würde], dass sich eine Kluft zwischen Gesetz und Praxis [auftue], die der Glaubwürdigkeit der Richtlinie und der Rechtsvorschriften der Gemeinschaft generell [schade] […]." (ebd.)

Neben diesen Punkten wurden Mängel auch bei der Umsetzung von Art. 6 (Abs. 1 lit. b hinsichtlich der Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken) und von Art. 7 festgestellt. Die Liste der Gründe für eine rechtmäßige Verarbeitung sei auf unzulässige Weise von einigen Mitgliedstaaten erweitert und von anderen Mitgliedstaaten gekürzt worden. Zudem seien Divergenzen im Hinblick auf die Interpretation der Einwilligung ohne jeden Zweifel (Art. 7 lit. a) und der ausdrücklichen Einwilligung (Art. 8) festzustellen, die zu klären seien. Die Kommission stellte zudem fest, dass die Information der Betroffenen gemäß den Art. 10 und 11 eine Reihe von Abweichungen aufgewiesen habe, die auf divergierende Umsetzungen in den Mitgliedstaaten und auf abweichende Auslegungen und Praktiken der Datenschutzaufsichtsbehörden zurückzuführen seien, in deren Ergebnis die Verantwortlichen mit unterschiedlichen Anforderungen konfrontiert seien und ihre Informationspflichten nicht im Sinne des zu erreichenden Schutzniveaus wahrnehmen könnten (ebd., 19).

Neben diesen von den konsultierten Akteuren benannten Punkten machte die Kommission auch selbst auf drei miteinander verflochtene Phänomene aus den Bereichen der Rechtsdurchsetzung, Rechtsbefolgung und Sensibilisierung aufmerksam: So seien die auf Seiten der Datenschutzaufsichtsbehörden vorhandenen Ressourcen zur Erfüllung ihres breiten Aufgabenspektrums unzureichend, sodass zu selten auf Durchsetzungsmaßnahmen zurückgegriffen werde. Verantwortliche, die die Datenschutzvorschriften nicht befolgten, würden sich in der Folge nur einem sehr geringen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Risiko ausgesetzt sehen, weshalb sie wiederum ein geringes Interesse an der Änderung ihrer Verarbeitungspraktiken zeigten. Aufgrund des geringen Kenntnisstands der Betroffenen über ihre Betroffenenrechte würden zudem nur wenige Betroffene die ihnen zustehenden Rechte wahrnehmen, sodass die von den Datenschutzaufsichtsbehörden nicht aufgedeckte mangelnde Vorschriftenbefolgung der Verantwortlichen auch seitens der Betroffenen nicht wahrgenommen bzw. angegangen werde (ebd., 13 f.).

3.3.3.2 Die Ergebnisse des Berichts: Lösungsvorschläge und Arbeitsprogramm der Kommission

Nach Ende der Konsultation lagen mehrere Maßnahmenvorschläge zum Umgang mit den identifizierten Defiziten vor. Seitens einiger Wirtschaftsvertreter sowie Österreichs, Schwedens, Finnlands und des Vereinigten Königreichs wurden detaillierte Vorschläge zur Änderung der DS-RL vorgelegt, die zum Ziel hatten, den bürokratischen Aufwand der für die Verarbeitung Verantwortlichen bei der Befolgung der Richtlinie zu senken und die Richtlinie besser an die neuen Erfordernisse der Online-Umgebung anzupassen (ebd., 7 f.).[180] Lediglich BEUC machte im Gegensatz zu dieser Position geltend, dass „es die Online-Umgebung sei, die angepasst werden müsse, um sicherzustellen, dass die Grundsätze der Richtlinie uneingeschränkt beachtet werden." (ebd., 7)

Die Kommission selbst vertrat die Position, dass eine Änderung der Richtlinie *in nächster Zukunft* aufgrund mehrerer Faktoren nicht sinnvoll wäre. Zunächst sei aufgrund der verspäteten Umsetzung der Richtlinie in den Mitgliedstaaten keine ausreichende Erfahrungsgrundlage gegeben, eine Änderung zu dem Zeitpunkt also noch verfrüht. Daneben konstatierte die Kommission, dass viele der im Konsultationsprozess benannten Schwierigkeiten ohne eine Änderung der Richtlinie behoben werden könnten (vgl. das von der Kommission verabschiedete Arbeitsprogramm weiter unten): Nicht die Richtlinie, sondern die divergierende Umsetzung von deren Vorgaben im mitliedstaatlichen Recht seien das Problem, das adressiert werden müsse. Schließlich sprach sich die Kommission auch deshalb gegen die

180 Während Wirtschaftsvertreter in der Vergangenheit europäische Datenschutzregelungen mehrheitlich prinzipiell abgelehnt hatten (vgl. Unterabschnitt 3.2.2), vertrat nunmehr eine Mehrheit von 69,1% der Antwortenden die Ansicht, dass Datenschutzvorschriften notwendig seien. Lediglich 2,64% forderten die vollständige Abschaffung von Datenschutzregelungen (ebd., 10).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Änderung der Richtlinie aus, da viele der vorgeschlagenen Änderungen zugleich die Senkung des Datenschutzniveaus nach sich gezogen hätten. Stattdessen hob die Kommission hervor, dass alle potentiellen Änderungen „auf die Aufrechterhaltung des Datenschutzniveaus zielen und mit dem Gesamtrahmen in Einklang stehen [sollten], der durch die bestehenden internationalen Instrumente [gemeint sind die OECD-Richtlinien und die Datenschutz-Konvention des Europarats, M. K.] vorgegeben ist." (ebd., 8). Daher setzte die Kommission insbesondere auf freiwillige Harmonisierungsmaßnahmen der Mitgliedstaaten sowie auf die engere Zusammenarbeit zwischen den Kontrollstellen unter der Anleitung der Kommission bzw. der Art. 29-Datenschutzgruppe und in einzelnen Fällen auch unter Beteiligung der Verantwortlichen (ebd., 13 und 24).

Das für die Jahre 2003 und 2004 vorgesehene Arbeitsprogramm der Kommission für eine bessere Durchführung der DS-RL sah zehn Maßnahmen vor, mit denen die identifizierten Kritikpunkte angegangen werden sollten und die im Folgenden kurz vorgestellt werden. Maßnahme 1 sah die Erörterung erforderlicher Änderungen mit den Mitgliedstaaten und gegebenenfalls auch mit den zuständigen Datenschutzaufsichtsbehörden sowie im Rahmen der Art. 29-Datenschutzgruppe vor (ebd., 24). Maßnahme 2 sah die intensivierte Einbeziehung der EU-Beitrittsländer[181] in die Bemühungen um eine bessere und einheitliche Durchführung der DS-RL vor, um die bestmögliche Harmonisierung der Rechtsvorschriften der neuen Mitgliedstaaten an die Richtlinienvorschriften zu erreichen (ebd., 25). Maßnahme 3 beinhaltete organisatorische und kommunikative Maßnahmen, mit denen zum einen weitere Daten über die Durchführung der Richtlinie erhoben werden sollten, indem die nationalen Datenschutzaufsichtsbehörden und die Mitgliedstaaten zu mehr Kooperation und Kommunikation angehalten würden. Daneben sah die Maßnahme die Veröffentlichung zentraler Informationen auf der Webseite der Kommission vor (ebd.). Mit Maßnahme 4 wurde die Art. 29-Datenschutzgruppe damit beauftragt, ihre Anstrengungen auf dem Gebiet der Durchsetzung zu intensivieren, indem sie sektorale Untersuchungen auf EU-Ebene durchführt und auf Basis der gewonnenen Daten den betroffenen Sektoren gemeinsame Empfehlungen und praktische Hinweise an die Hand gibt, die eine harmonisierte Umsetzung der Richtlinienvorgaben gewährleisten (ebd., 26). Im Hinblick auf die

181 Estland, Lettland, Litauen, Polen, Tschechien, Slowenien, Slowakei, Ungarn, Malta sowie Zypern traten am 1. Mai 2004 der EU bei.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kritik im Zusammenhang mit der uneinheitlichen Umsetzung der Meldepflicht sah Maßnahme 5 vor, dass die Art. 29-Datenschutzgruppe Vorschläge – inklusive Vorschläge zur Änderung einzelstaatlicher Rechtsvorschriften – für „eine wesentliche Vereinfachung der Meldeanforderungen in den Mitgliedstaaten und für Zusammenarbeitsmechanismen zur Vereinfachung der Meldungen internationaler Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten unterbreitet" (ebd.). Im Hinblick auf das Problem der divergierenden Bestimmungen zu Informationspflichten kündigte die Kommission im Rahmen der Maßnahme 6 einen Dialog mit den Mitgliedstaaten an, an dessen Ende korrigierende rechtliche Maßnahmen stehen sollten. Zudem rief die Kommission die Datenschutzgruppe dazu auf, bei der Suche nach einer Harmonisierung der Informationspflichten mitzuwirken (ebd., 26 f.). Mit Maßnahme 7 bezweckte die Kommission die Vereinfachung der Anforderungen für internationale Übermittlungen. In Zusammenarbeit mit der Art. 29-Datenschutzgruppe und dem Artikel-31-Ausschuss sah die Maßnahme Fortschritte in vier Bereichen vor: Von einer Ausweitung der Angemessenheitsentscheidungen über die Genehmigung von mehr Standardvertragsklauseln und mehr unternehmensinternen Vorschriften auf Basis von Selbstregulierung bis hin zur einheitlichen Auslegung der Ausnahmeregelungen (ebd., 27). Maßnahme 8 sah die Förderung von Technologien zur Verbesserung des Datenschutzes vor: „Die Idee, die hinter den PETs steht, ist die von Informations- und Kommunikationssystemen und -technologien, die so ausgelegt sind, dass die Erhebung und Nutzung personenbezogener Daten minimiert wird und unzulässige Verarbeitungsformen verhindert werden. *Die Kommission hält den Einsatz geeigneter technologischer Maßnahmen für eine unverzichtbare Ergänzung rechtlicher Maßnahme und ist der Auffassung, dass sie integraler Bestandteil jeglicher Bemühungen um einen [sic] ausreichendes Datenschutzniveau sein sollten*." (ebd., 17, Hervorhebung M. K.) Dabei unterschied die Kommission zwischen solchen Produkten, die (1) voll und ganz den Anforderungen der Richtlinie entsprechen, die (2) einen Schritt weitergehen und bestimmte Aspekte des Datenschutzes für Benutzende besser zugänglich machen, bspw. durch Benutzerfreundlichkeit und die (3) einen maximalen Datenschutz unter Rückgriff auf Anonymisierungstechniken gewährleisten (ebd.). Die Kommission kündigte an, einen Fach-Workshop zum Thema PETs zu veranstalten, auf dem auch mögliche Implementierungsmaßnahmen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wie Gütesiegel, Zertifizierungssysteme[182] oder PIAs[183] diskutiert werden sollten. Die Datenschutzgruppe wurde dazu angehalten, die Frage der PETs weiter zu erörtern und über Möglichkeiten der Förderung von PETs auf nationaler Ebene nachzudenken. Zudem wies die Kommission darauf hin, „dass Regierungen und Einrichtungen des öffentlichen Sektors ermutigt werden müssen, mit gutem Beispiel voranzugehen und PETs bei ihren Verarbeitungen, z.B. [sic] in den E-Government-Anwendungen, zu benutzen." (ebd., 28) Mit der Maßnahme 9 drückte die Kommission zunächst ihre Enttäuschung darüber aus, dass die Möglichkeit der Vorlage sektoraler Verhaltenskodizes nur von sehr wenigen Einrichtungen wahrgenommen worden war, forderte aber Branchen und Interessengruppen dennoch ein weiteres Mal dazu auf, „eine viel aktivere Rolle zu übernehmen, da sie glaubt, dass die Selbstregulierung und insbesondere Verhaltenskodizes eine wichtige Rolle bei der zukünftigen Entwicklung des Datenschutzes innerhalb und außerhalb der EU spielen sollten, nicht zuletzt, um zu detaillierte Rechtsvorschriften zu vermeiden." (ebd., 28) Maßnahme 10 sah schließlich die verstärkte Thematisierung von Datenschutzfragen in der Öffentlichkeit vor. Dazu kündigte die Kommission zum einen die Durchführung einer Eurobarometer-Umfrage unter der europäischen Bevölkerung an und forderte zum anderen die Mitgliedstaaten dazu auf, mehr Ressourcen für die Sensibilisierung der Öffentlichkeit insbesondere in den Haushalten der nationalen Datenschutzaufsichtsbehörden bereitzustellen (ebd., 29).

182 Dass die Kommission bereits zu diesem Zeitpunkt ernsthaft über die Ausweitung von Zertifizierungssystemen und Gütesiegeln nachdachte, verdeutlichen die beiden folgenden Zitate: „Die Kernfrage ist daher nicht nur, wie Technologien entwickelt werden können, die tatsächlich den Datenschutz verbessern, sondern wie dafür gesorgt werden soll, dass diese Technologien ordnungsgemäß als solche gekennzeichnet und von den Nutzern erkannt werden. Zertifizierungssysteme spielen hier eine entscheidende Rolle […]." (ebd., 17) Und: „Die Kommission ist der Meinung, dass solche Systeme gefördert und weiterentwickelt werden sollten, […] ferner sollten diejenigen, die in die Gewährleistung und sogar die Verbesserung des Datenschutzes investieren Gelegenheit gegeben werden, ihre Leistung auf diesem Gebiet darzustellen und Wettbewerbsvorteile daraus zu ziehen." (ebd., 17 f.)

183 Als Beispiel für Privacy Impact Assessments nannte die Kommission Kanada, „dessen Bundesregierung die erste Zentralregierung war, die obligatorische Datenschutz-Folgenabschätzungen für alle Bundesministerien und -agenturen vorgeschrieben hat, bei allen Programmen und Diensten, bei denen der Datenschutz berührt werden könnte. Die Agenturen müssen in der Frühphase der Konzeption oder Überarbeitung eines Programms oder eines Dienstes eine solche Folgenabschätzung vornehmen, damit der Entwicklungsprozess entsprechend gesteuert und dafür gesorgt wird, dass der Datenschutz eines der Hauptkriterien ist." (ebd., 17)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Kommission bezeichnete ihren Bericht als einen ersten Schritt zur Auswertung der Durchführung der DS-RL und kündigte an, den weiteren Verlauf der Umsetzung zu verfolgen und weiterhin (gegen Ende 2004) Bericht über den Stand der Umsetzung zu erstatten (ebd., 30).

3.3.3.3 Stellungnahme des Europäischen Parlaments

Nach Erhalt des Kommissionsberichts über die Durchführung der DS-RL am 15. Mai 2003 wurde der LIBE-Ausschuss am 4. September 2003 mit der Ausarbeitung eines Initiativberichts beauftragt. Der JURI-Ausschuss und der ITRE-Ausschuss wurden als mitberatende Ausschüsse am Verfahren beteiligt. In seiner Sitzung vom 8. September 2003 benannte der LIBE-Ausschuss Marco Cappato als Berichterstatter. Dessen Berichtsentwurf wurde auf den LIBE-Ausschusssitzungen vom 22. Januar 2004 und vom 19. Februar 2004 geprüft und auf der letztgenannten Sitzung einstimmig angenommen (Cappato 2004, 4). Der Bericht wurde am 24. Februar an das Parlamentsplenum überwiesen und auf der Plenarsitzung vom 9. März 2004 mit 439 Stimmen (bei 39 Gegenstimmen und 28 Enthaltungen) angenommen. Gegen die Entschließung des Parlaments stimmten lediglich einige konservative Europaparlamentarier vor allem der EVP-ED sowie drei Abgeordnete der EDU (Europa der Demokratien und der Unterschiede, engl. Europe of Democracies and Diversities EDD). Die Enthaltungen setzten sich aus einigen Abgeordneten der EDU, der Mehrzahl der UEN-Angehörigen, fraktionslosen Abgeordneten sowie einem Abgeordneten der EVP-ED zusammen (Europäisches Parlament 2004, 62 f.).

Inhaltlich fokussierte der Cappato-Bericht vor allem den Schutz der europäischen Bürgerinnen und Bürger vor sicherheitspolitisch motivierten Datenzugriffen. Während der *formelle Schutz des Rechts auf Achtung des Privatlebens* zumindest im Bereich der ersten Säule als im Wesentlichen recht zufriedenstellend zu bewerten sei, müsse der Aushöhlungsprozess des *inhaltlichen Schutzes dieses Rechts* mit Sorge betrachtet werden, da zahlreiche Staaten *so genannte Vorschriften zur Terrorismusbekämpfung* verabschiedet hätten, die jene Grundrechte und Grundfreiheiten gefährdeten, auf denen die Demokratie und Rechtsstaatlichkeit aufbauen: „Das Recht auf Privatsphäre ist eines der ersten Opfer dieses legislativen Notstandsaktivismus, der die delikaten Grenzen zwischen Grundrechten und rechtmäßigen und notwendigen Eingriffen in eine demokratische Gesellschaft zu Zwecken der ‚öffentlichen Ordnung' neu festlegen soll." (Cappato 2004, 14)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Im Hinblick auf den eigentlichen Inhalt des Kommissionsberichts über die Durchführung der DS-RL teilte der Cappato-Bericht die Auffassung der Kommission, dass die Richtlinie wegen der Langsamkeit und des noch begrenzten Umfangs ihrer Umsetzung „vorläufig […] nicht geändert werden sollte und dass derzeitige Mängel in der Anwendung der Richtlinie durch [die von der Kommission vorgeschlagenen] Maßnahmen überwunden werden sollten" (ebd., 8). Für den Fall, dass nach Ende eines angemessenen Zeitraums von einem Jahr noch immer einige hartnäckige Mitgliedstaaten *gegen den Buchstaben und den Geist der Richtlinie* verstoßen, forderte das Parlament eine entschlossene Vorgehensweise inkl. der Wahrnehmung der Möglichkeit der Einleitung von Vertragsverletzungsverfahren (ebd., 8 f. und 15 f.).

Der Rest der Parlamentsentschließung widmete sich dagegen den verschiedenen zu diesem Zeitpunkt akuten Streitpunkten hinsichtlich sicherheitspolitisch motivierter Datenverarbeitungen: der Zugriff amerikanischer Behörden auf Fluggastdaten europäischer Bürgerinnen und Bürger; die Übermittlung von Daten, die bei Europol, Eurojust, SIS usw. gespeichert sind, an Drittstaaten; und die in Art. 15 der ePrivacy-Richtlinie eingeführte Möglichkeit einer Vorratsdatenspeicherung. Im Besonderen bemängelte das Parlament in diesem Zusammenhang das anhaltende Fehlen einer der DS-RL vergleichbaren Regelung für die dritte Säule, während zugleich im Rahmen der ersten Säule erhobene personenbezogene Daten für Aktivitäten, die in den Bereich der dritten Säule fallen, genutzt würden (Zugriff auf Fluggastdaten) bzw. werden sollten (Vorratsdatenspeicherung) (ebd., 9 f. und 16 f.).

Daher forderte das Parlament die Kommission dazu auf, im ersten Halbjahr 2004 ein Rechtsinstrument zum Schutz der Privatsphäre im Rahmen der dritten Säule vorzuschlagen, das verbindlich sein sollte und welches das für die erste Säule geltende Schutzniveau auf die Aktivitäten der dritten Säule ausweite und eine Harmonisierung herbeiführe (ebd., 7). Zugleich machte das Parlament klar, dass es auf lange Sicht – und insbesondere mit Blick auf die angekündigte Aufhebung der Säulen in der EU durch die Europäische Verfassung – die Anwendung der DS-RL inkl. der zu diesem Zeitpunkt nötigen Anpassungen auf alle dann ehemaligen Säulen fordere (ebd., 7 und 15). In diesem Zusammenhang verlangte das Parlament zudem, dass es „künftig zu jedem Vorschlag, der sich auf den Schutz der Privatsphäre in der EU bezieht oder auswirkt, beispielsweise internationale Vereinbarungen ihrer Institutionen, Angemessenheitsentscheidungen usw., mit Entscheidungsbefugnissen konsultiert wird" (ebd., 8).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.3.4 Folgebericht

Über den Stand des Arbeitsprogramms für eine bessere Durchführung der DS-RL resümierte die Kommission doch deutlich später als angekündigt. Statt *gegen Ende 2004* wurde die entsprechende Mitteilung der Kommission mehr als zwei Jahre später erst Anfang März 2007 veröffentlicht (KOM 2007). Im Gegensatz zum ersten Bericht ging der 2007er-Bericht deutlich oberflächlicher auf viele der diskutierten Punkte ein, wie sich insbesondere am Umgang mit den drei im Vorläuferbericht als zentral bezeichneten Punkten zeigte.[184] Aufgrund dessen, dass die Potentiale bei der Umsetzung der Richtlinie noch immer nicht vollständig ausgeschöpft worden seien und weil die bestehenden Abweichungen keine Gefahr für das Funktionieren des Binnenmarktes oder für die Gewährleistung eines hohen Schutzniveaus darstellten, sah die Kommission trotz einzelner Kritikpunkte[185] keine Notwendigkeit für eine Änderung der Richtlinie (ebd., 10). Ebenso wurden die Grundsätze der Richtlinie für weiterhin gültig und nicht änderungsbedürftig erklärt (ebd., 11).

Trotz der auch erfolgten Erwähnung des durch die Richtlinie garantierten hohen Schutzniveaus hob die Kommission an mehreren Stellen interessanterweise vor allem die wirtschaftliche Bedeutung der Richtlinie hervor. In den Schilderungen der bestehenden Divergenzen bei der Umsetzung der Richtlinie im Kapitel zur aktuellen Situation hob der Text vor allem auf die Auswirkungen für den Binnenmarkt ab, während das Schutzniveau lediglich in einem Nebensatz Erwähnung fand. Noch augenfälliger äußerte sich der Fokus auf die wirtschaftliche Bedeutung der Richtlinie, als die Kommission die Bedeutung des Grundrechts auf den Schutz personenbezogener Daten mit der folgenden Argumentation herausstellte: „Der Einzelne soll so Vertrauen in die Art und Weise der Verwendung seiner Daten gewinnen, denn ohne dieses Vertrauen wäre eine Ausweitung des elektronischen Geschäftsverkehrs nicht denkbar." (ebd., 10) Wie zu erwarten war, nahm der EDSB in seiner Stellungnahme im Hinblick auf die Bewertung der Grundrechts- bzw. Binnenmarktdimension der Richtlinie eine der Kommissionsmitteilung entgegengesetzte Position ein (EDSB 2007b): So kritisierte der EDSB den Wortlaut der Kommission und hob hervor, dass die Richtlinie in erster Linie ein Grundrecht darstelle. Die Förderung des freien Datenver-

184 So aber auch am Seitenumfang: Während der 2003er-Bericht noch 30 Seiten umfasste, war der neue Bericht nur 12 Seiten lang.

185 Darunter insb. die lückenhafte bzw. divergierende Umsetzung in einigen Mitgliedstaaten (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

kehrs im Binnenmarkt sei zwar ebenfalls wichtig, aber letztlich zweitrangig (ebd., 3, Nr. IV. A. 15-19).

Über die Kommissionsmitteilung hinausgehend schlug der EDSB zudem folgende Instrumente vor, die „für eine künftige Änderung der Richtlinie in Erwägung gezogen oder in andere horizontale Rechtsvorschriften aufgenommen werden könnten" (ebd., 10, Nr. VI. F. 67): *Sammel- bzw. Verbandsklagen*,[186] *Meldung von Datenschutzverletzungen* sowie *grenzüberschreitende Bestimmungen zu Datenschutzgütesiegeln oder Datenschutz-Audits durch Dritte*.

Schließlich begrüßte der EDSB auch die möglicherweise bevorstehende Aufhebung der Säulenstruktur der EU und das Rechtswirksamwerden der EU-Grundrechtecharta infolge des potentiellen Inkrafttretens des EU-Reformvertrags (ebd., 8, Nr. V. E.). Aufgrund der sich zu diesem Zeitpunkt noch in der Schwebe befindenden Debatte über den weiteren Umgang mit dem EU-Reformvertrag (siehe 3.4.1.2) äußerte sich die Kommission nur auf sehr defensive Weise zu den möglichen neuen Kompetenzen im Bereich des Datenschutzes. So erwähnte die Kommission zwar die geplante Ausweitung ihrer Gesetzgebungskompetenz auf nahezu alle Politikbereiche infolge der vorgesehenen Auflösung der Säulenstruktur. Bis allerdings „geklärt ist, wie es mit dem Ratifizierungsprozess des Verfassungsvertrags weitergeht," (ebd., 9) kündigte die Kommission an, sich weiterhin an die im Rahmen der Umsetzung des Haager Programms vereinbarten Maßnahmen zu halten (ebd.).

3.3.3.5 Zwischenfazit

Die Berichterstattung der Kommission über die Durchführung der DS-RL war ein wichtiger Zwischenschritt auf dem Weg zur Datenschutzreform, da durch diesen klar wurde, in welchen inhaltlichen Bereichen noch immer Defizite anzutreffen waren.

186 Mit seiner Forderung nach kollektiven Rechtsbehelfen knüpfte der EDSB an eine seit dem Jahr 2005 auf EU-Ebene stattfindende Diskussion an, die ihren Anfang mit der Veröffentlichung eines Grünbuchs der Kommission im selben Jahr genommen hatte und schließlich in der Ankündigung der Schaffung von Mechanismen des kollektiven Rechtsschutzes im Rahmen der verbraucherpolitischen EU-Strategie 2007–2013 kulminierte (Dawidowicz 2014, 239–41).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.4 Datenschutz-Bestimmungen im Sicherheitsbereich

Wie bereits in Unterabschnitt 3.3.1.2 erwähnt, wurde das Subsystem der Europäischen Datenschutzpolitik in den 2000er-Jahren in entscheidendem Maße von den Entwicklungen im Bereich der Sicherheitspolitik beeinflusst. Die dabei ausgefochtenen Konflikte und insbesondere die politischen Niederlagen, die Datenschutzbefürworter in dieser Zeit erlitten, sollten später ausschlaggebend für die Initiierung und den erfolgreichen Abschluss der Datenschutzreform sein.

Der vorliegende Unterabschnitt widmet sich der Untersuchung der politischen Auseinandersetzungen beim Zustandekommen der Datenschutz-Bestimmungen im Sicherheitsbereich. Angefangen mit den ersten Gemeinschaftsaktivitäten auf diesem Gebiet (3.3.4.1), wird außerdem das Zustandekommen der wichtigsten und umstrittensten politischen Ergebnisse dieser Phase untersucht: der Richtlinie zur Vorratsdatenspeicherung (3.3.4.2), des Zugriffs auf Fluggastdaten (3.3.4.3) sowie des JI-Rahmenbeschlusses (3.3.4.4).

3.3.4.1 Erste Aktivitäten auf dem Gebiet

Bereits im Rahmen ihres 1990er-Legislativbündels hatte die Kommission die Mitgliedstaaten dazu eingeladen, die für den Gemeinschaftsbereich vorgesehenen Datenschutz-Grundsätze (der späteren DS-RL) mittels einer Ministerratsentschließung auch auf jene Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich anzuwenden, die nicht von Gemeinschaftsbereich abgedeckt sind (COM 1990, 73 f.). Zu diesem Zeitpunkt umfasste der vom Gemeinschaftsrecht abgedeckte Politikbereich vor allem wirtschaftliche und seit Mitte der 1980er-Jahre auch einige wenige soziale Fragen. Die Initiative der Kommission hatte zum Ziel, die Anwendung der Datenschutz-Grundsätze auch auf den Justiz- und Inneres-Bereich sicherzustellen, um ein EG-weit einheitliches und hohes Datenschutzniveau auf allen von der Verarbeitung personenbezogener Daten betroffenen Politikbereichen zu gewährleisten (ebd.).[187] Wie bereits in Unterabschnitt 3.2.2.4.3 dargelegt, konnte diese Initiative der Kommission trotz ihrer Befürwortung seitens der Datenschutzaufsichtsbehörden keine Unterstützung bei den

187 Die von der Kommission 1990 vorgeschlagene Ministerratsentschließung hätte eine freiwillige Bindung seitens der Mitgliedstaaten dargestellt, die keine eigenständige Grundlage in den Gemeinschaftsverträgen gehabt hätte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Mitgliedstaaten generieren, sodass der Vorschlag bis auf Weiteres fallen gelassen wurde.

Erst eine Kette von Ereignissen sollte später wieder Bewegung in die Thematik bringen und zum Abschluss des Justiz und Inneres-Rahmenbeschlusses 2008/977/JHA führen. Den Anfang markierte das Inkrafttreten des Maastrichter Vertrags Ende 1993. Dieser weitete die intergouvernementale Zusammenarbeit der EG über die Wirtschaftskooperation (nunmehr als erste Säule bezeichnet) hinaus auf die teil-vergemeinschafteten Politikbereiche der gemeinsamen Außen- und Sicherheitspolitik (GASP) (zweite Säule) sowie die Justiz- und Innenpolitik (JI)[188] (dritte Säule) aus, sodass der Erlass von Gemeinschaftsmaßnahmen im Bereich der JI-Politik prinzipiell ermöglicht wurde (Europäische Gemeinschaften 1992). Im Maastrichter Vertrag wurde auch erstmals im Rahmen eines Gemeinschaftsvertrags die Idee einer gemeinschaftlichen Polizeibehörde erwähnt, die für grenzüberschreitende Verbrechen wie Terrorismus und Drogenschmuggel zuständig sein sollte. Das sog. Europol-Übereinkommen zur Gründung der Europol (European Police Office), wurde am 26. Juli 1995 unterzeichnet und trat zum 1. Oktober 1998 in Kraft. Schon die Präambel des Übereinkommens unterstrich *die besondere Aufmerksamkeit*, die dem Schutz der Rechte des Einzelnen und insbesondere dem Schutz personenbezogener Daten zuteilwerden sollte. Letztlich orientierte sich das Übereinkommen hinsichtlich des Datenschutzniveaus allerdings lediglich an der Datenschutz-Konvention des Europarats.[189] Das Problem beim Datenschutz im Bereich der dritten EU-Säule war, dass kein gemeinschaftlich festgelegter Datenschutzrahmen existierte, der die Standards für sektorspezifische Regelungen (Europol, Eurojust und SIS) vorgab. Stattdessen waren in Umkehrung der gewöhnlichen Regulierungslogik noch vor einer Rahmenrichtlinie die sektorspezifischen Regelungen mit eigeständigen Datenschutzvorgaben erlassen worden, die sich mehr oder weniger an der Datenschutz-Konvention des Europarats orientierten. Die für die dritte Säule bestehenden Re-

188 Nachdem die justizielle Zusammenarbeit in Zivilsachen und die flankierenden Maßnahmen zum freien Personenverkehr mit dem Vertrag von Amsterdam 1997 in die erste Säule verschoben worden waren, verblieb die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) in der dritten Säule, die fortan entsprechend bezeichnet wurde (Wessels 2008, 94).

189 Bzw. an der Empfehlung Nr. R (87) 15 des Ministerkomitees des Europarats über die Nutzung personenbezogener Daten im Polizeibereich, die zwischenzeitlich am 17. September 1987 verabschiedet worden war (vgl. auch Boehm 2012, 96 ff. Council of Europe 1987).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gelungen waren also einerseits zersplittert und uneinheitlich und wurden von Datenschutzexperten andererseits als unzureichend im Hinblick auf das Schutzniveau bewertet. Schließlich lag ein entscheidender Grund für die Erarbeitung der DS-RL darin, dass das Schutz-Niveau der Datenschutz-Konvention als unzureichend bewertet wurde (P. de Hert und Papakonstantinou 2009, 405 f.).

Den ersten konkreten politischen Schritt in Richtung der Festlegung eines gemeinschaftlichen Datenschutzrahmens in der dritten Säule unternahm im Jahr 1998 die italienische Ministerratsdelegation (JAI 15 8321/98), die von den Datenschutzbeauftragten der EU-Mitgliedstaaten Unterstützung in Form einer Resolution erhielt (JAI 16 8563/98). Die italienische Initiative regte vor dem Hintergrund der Befürchtung einer Zersplitterung der Datenschutzregelungen für verschiedene komplexe Informationssysteme wie SIS, Europol oder ZIS (Zollinformationssystem) sowie für den Abschluss bi- oder multilateraler Abkommen die Herausbildung einheitlicher Standards und Datenschutzkontrollen an – während die Resolution der Europäischen Datenschutzbeauftragten auf Harmonisierung sowie ein hohes Schutzniveau drängte (Vorsitz - Rat der Europäischen Union 1999). Zeitgleich erhielt das im Rahmen des Vertrags von Amsterdam beschlossene Ziel des *Aufbaus eines gemeinsamen Raumes der Sicherheit, der Freiheit und des Rechts* mit dem Inkrafttreten des Vertrags am 1. Mai 1999 Geltung (Europäische Union 1997). Ende 1998 nahm der Europäische Rat schließlich den sog. Wiener Aktionsplan an.[190] In diesem wurde beschlossen, innerhalb von zwei Jahren nach Inkrafttreten des Amsterdamer Vertrags die Harmonisierung der Datenschutzvorschriften in der PJZS zu prüfen (Rat der Europäischen Union 1998, 24; Vorsitz - Rat der Europäischen Union 1999, 2). Die Annahme einer zu diesem Zweck ausgearbeiteten Ministerratsentschließung scheiterte jedoch im April 2001 – offenbar am Widerstand jener während der Verhandlungen der DS-RL als nördlicher Block bezeichneten Mitgliedstaaten (P. de Hert und Papakonstantinou 2009, 405, Fn. 15; Ministerrat 2001).

Als das von den Vereinigten Staaten und dem Vereinigten Königreich unter Zuarbeit Australiens, Neuseelands und Kanadas betriebene weltweite

190 Der *Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags* (Rat der Europäischen Union 1998).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Spionagenetzwerk Echelon[191] zu einem öffentlichen Thema wurde, eröffnete sich kurzzeitig ein politisches Gelegenheitsfenster für Europäische Reaktionen (Dix 2000). Doch wirkten die Terroranschläge vom 11. September 2001 als externer Schock, der jegliche Reaktionen in Richtung der Verschärfung datenschutzrechtlicher Standards verhinderte und dafür sorgte, dass stattdessen die weitere Ausdehnung von Überwachungsmaßnahmen die politischen Agenden dominierte (H. Busch 2002).

Im Juni 2003 unternahm schließlich der griechische Ratsvorsitz einen erneuten Anlauf und unterbreitete auf der Ministerratssitzung der Justiz- und Innenminister einen Vorschlag zur Erarbeitung gemeinsamer Regeln für den Schutz personenbezogener Daten im Rahmen der dritten Säule, die sich am Schutzniveau der DS-RL und der EU-GRCh, die in der Zwischenzeit verabschiedet worden war (vgl. 3.4.1.1), orientieren sollten. Doch scheiterte auch dieser Vorstoß an der mangelnden Bereitschaft der Mehrheit der Mitgliedstaaten (Ministerrat 2003, 32).

Schließlich erhielt die Debatte um die Verbesserung des Informationsaustauschs zwischen den Mitliedstaaten vor allem nach den Anschlägen vom 11. März 2004 in Madrid weiteren Auftrieb. Im Rahmen ihres neuen mehrjährigen Programms, dem Haager Programm,[192] einigten sich die EU-Organe auf den sog. Verfügbarkeitsgrundsatz, der ab dem 1. Januar 2008 inkrafttreten sollte und mittels dessen mitgliedstaatliche Strafverfolgungsbehörden zur gegenseitigen Bereitstellung ihrer Datenbestände verpflichtet wurden. Zugleich legte das Haager Programm zur Verwirklichung des Verfügbarkeitsgrundsatzes die strenge Einhaltung mehrerer Hauptbedingungen fest, zu denen auch die Gewährleistung von Datenschutzrechten zählte (Europäischer Rat 2005a, 7 f.). Die Befürwortung der Erarbeitung von strengen Bedingungen[193] im Rahmen des Haager Programms stieß dann auch auf die ausdrückliche Unterstützung der europäischen Datenschutzbeauftragten. In der sog. Erklärung von Krakau forderten die Datenschutzbeauftragten der Mitgliedstaaten sowie der EDSB Ende April 2005 dann auch die Erarbeitung eines eigenständigen Instruments für den Datenschutz in der dritten Säule. Mehr noch, wurde gefordert, „dass, sobald der Euro-

191 Siehe insb. den Echelon-Bericht des Sonderausschusses des Europäischen Parlaments (Europäisches Parlament 2001a). Für eine kurze Chronologie der Ereignisse, siehe: (Campbell 2001).

192 Der bereits im Tampere-Programm vorhandene Fokus auf innere Sicherheit wurde im Rahmen des für den Zeitraum 2005 bis 2010 gültigen Haager Programms weiter verstärkt (Pütter 2006).

193 Als *streng* galt in diesem Zusammenhang das Schutzniveau der DS-RL.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

päische Verfassungsvertrag in Kraft tritt, ein umfassendes Europäisches Datenschutzgesetz gelten sollte, das sämtliche Bereiche [also sowohl die dann ehemalige erste als auch dritte Säule, M. K.] der Verarbeitung personenbezogener Daten abdeckt." (Frühjahrskonferenz der Europäischen Datenschutzbeauftragten 2005) Am 7. Juni 2005 nahm auch das Europäische Parlament eine Empfehlung an, in der es den Europäischen Rat und den Ministerrat dazu aufforderte, die bestehenden Datenschutz-Regeln bei den Instrumenten der dritten Säule zu harmonisieren, indem diese in ein eigenständiges Datenschutz-Instrument überführt würden, und dabei zugleich das Datenschutzniveau, das im Rahmen der ersten Säule bestand, aufrecht zu erhalten (Europäisches Parlament 2005, 260 vgl. Nr. 1. h)).

Zwischenzeitlich unterzeichneten Belgien, Deutschland, Frankreich, Luxemburg, die Niederlande, Österreich und Spanien auf eine Initiative von Bundesinnenminister Schily (SPD, BRD) aus dem Jahr 2003 hin, am 27. Mai 2005 den Prümer Vertrag. Dieses zwischenstaatliche Abkommen sah unter Einhaltung datenschutzrechtlicher Garantien den automatischen und direkten Zugriff der Strafverfolgungsbehörden eines Vertragsstaates auf die von einem anderen Vertragsstaat gespeicherten personenbezogenen Daten (z. B. DNA-Daten oder Fingerabdrücke) vor (Prümer Vertrag 2005).[194] Doch noch bevor es zur Verabschiedung eines Datenschutz-Rahmeninstruments im Bereich der dritten Säule kam, wurde der Zugriff auf personenbezogene Daten zu Sicherheitszwecken zunächst auf mehreren Gebieten weiter ausgedehnt. Dies betraf vor allem die EG-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, daneben aber auch die Übertragung von Fluggastdaten an Regierungsstellen in den Vereinigten Staaten. Diese Maßnahmen werden im Folgenden näher betrachtet und dabei einerseits im Hinblick auf ihre Bedeutung für die EG-Rahmenrichtlinie im Bereich der dritten Säule im Besonderen und andererseits auf ihre Bedeutung für die Datenschutzpolitik der Europäischen Union im Allgemeinen analysiert.

3.3.4.2 Richtlinie 2006/24/EG zur Vorratsdatenspeicherung

Die Idee einer EU-weiten, einheitlichen Vorratsdatenspeicherung wurde erstmals formell von der rechtskonservativen dänischen Regierung im Rahmen ihrer EU-Ratspräsidentschaft im August 2002 vorgebracht, konnte bei

194 Der Ministerratsbeschluss 2008/615/JI überführte die Vorgaben des Prümer Vertrags, das außerhalb des Gemeinschaftsrechts abgeschlossen worden war, im Juni 2008 in das Gemeinschaftsrecht (EU-Ministerrat 2008a).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

den übrigen Mitgliedstaaten allerdings keine ausreichende Unterstützung finden. Im Sinne eines Minimalkompromisses konnten sich die Regierungen der Mitgliedstaaten jedoch im Rahmen der Verhandlungen zur ePrivacy-Richtlinie darauf einigen, dass denjenigen Mitgliedstaaten, die ein Interesse an der Vorratsdatenspeicherung hatten, der Erlass entsprechender Regelungen nicht erschwert werden sollte, sodass die im Kommissionsvorschlag und in den Parlamentspositionen zur ePrivacy-Richtlinie vorgesehenen Beschränkungen auf Druck des Ministerrats aus dem finalen Richtlinientext entfernt wurden (vgl. 3.3.2). In der Folge verfolgten mehrere EU-Mitgliedstaaten nationale Pläne zur Einführung einer Vorratsdatenspeicherung. Allerdings vertraten insb. die Strafverfolgungsbehörden die Ansicht, dass eine Vorratsdatenspeicherung nur dann wirksam sein könne, wenn diese in der gesamten EU entlang harmonisierter Gemeinschaftsvorgaben eingeführt werde. Da nicht alle Regierungen in gleichem Maße von dieser Ansicht überzeugt waren, konnte dieser Vorschlag zunächst allerdings noch keine Mehrheit finden (Hayes, Peers, und Bunyan 2004).

Erst mit den Anschlägen von Madrid im März 2004 und den Londoner Anschlägen vom 7. Juli 2005 wandelte sich die Debatte zugunsten der Vorratsdatenspeicherungsbefürworter. Im Nachgang der Madrider Anschläge veröffentlichte der Europäische Rat eine Erklärung zum Kampf gegen Terrorismus, in der der Ministerrat u. a. vorrangig mit der Beratung von *Vorschlägen für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter* und mit der Annahme der entsprechenden Vorschläge bis Juni 2005 beauftragt wurde (Europäischer Rat 2004, 4 f.). Daraufhin legten Frankreich, Großbritannien, Irland und Schweden bereits Ende April 2004 einen Entwurf für einen Rahmenbeschluss zur Vorratsdatenspeicherung im Ministerrat vor (EU-Ministerrat 2004a). Der Vorschlag sah eine Mindestspeicherfrist von 12 Monaten und eine Höchstspeicherdauer von 36 Monaten vor. Während der dänische Vorschlag aus dem Jahr 2002 die Vorratsdatenspeicherung noch lediglich zur Aufklärung bereits erfolgter Straftaten und eine Beschränkung auf besonders schwere Straftaten und Terrorismus vorgesehen hatte, sollte die Vorratsdatenspeicherung zudem nunmehr auch zur Straftatenprävention dienen dürfen und auch bei leichteren Delikte wie Urheberrechtsverletzungen greifen (EU-Ministerrat 2004b).

Doch auch dieser neue Vorschlag konnte sich zunächst nicht durchsetzen. Da der Vorschlag auf Grundlage der Art. 31 Abs. 1 lit. c sowie Art. 34

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Abs. 2 lit. b gestützt wurde, d. h. als Rahmenbeschluss[195] zur Harmonisierung im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vorgeschlagen wurde, musste über diesen im Ministerrat einstimmig entschieden werden. Allerdings konnte zu keinem Zeitpunkt ein Konsens unter allen Mitgliedstaaten gefunden werden, da die Vorratsdatenspeicherung vor allem von Deutschland, Österreich und den Niederlanden abgelehnt wurde (EDRi 2005a). Aufgrund des gewählten Konsultationsverfahrens musste der Ministerrat das Parlament zudem zwar anhören, aber formell keine Rücksicht auf dessen Position nehmen. Diese Vorgehensweise des Ministerrats führte wiederum zu massiver Kritik vonseiten des Europäischen Parlaments. Die von Berichterstatter Alexander Alvaro im LIBE-Ausschuss ausgearbeitete Parlamentsposition zum Rahmenbeschluss hob auf drei Kritikpunkte ab: *Erstens* wurde, aufgrund dessen, dass die im Vorschlag benannten, auf Vorrat zu speichernden Datenkategorien teilweise in den Bereich der ersten Säule fielen, die Rechtsgrundlage des Vorhabens angezweifelt. *Zweitens* wurde, aufgrund der im Vorschlag vorgesehenen weitreichenden Zugriffsmöglichkeiten, die Verhältnismäßigkeit bzw. Notwendigkeit der Maßnahme angezweifelt und schließlich, *drittens*, wurde auf die Möglichkeit einer Verletzung des Art. 8 der Europäischen Menschenrechtskonvention hingewiesen (A. N. Alvaro 2005, 6 ff.). Entsprechend sprach sich das Parlamentsplenum am 27. September 2005 gegen den Vorschlag aus und forderte Frankreich, Großbritannien, Irland und Schweden dazu auf, ihre Initiative zurückzuziehen. In der Zwischenzeit schlossen sich der Juristische Dienst des Ministerrats sowie die Kommission der Parlamentsposition hinsichtlich der Kritik an der Rechtsgrundlage an (A. N. Alvaro 2015, 33). Die Kommission legte Anfang 2005 einen diesbezüglichen Prüfungsvorbehalt ein und rief den Ministerrat unter Verweis auf ein noch von der Kommission auszuarbeitendes Rechtsinstrument im Bereich der ersten Säule ebenfalls zur Aufgabe der Initiative auf (EDRi 2005c).

195 Ein Rahmenbeschluss konnte bis zum Inkrafttreten des Lissabon-Vertrags (am 1. Dezember 2009) vom Ministerrat ohne Zustimmung des Parlaments für Angelegenheiten im Rahmen der dritten Säule der EU erlassen werden. Darin wurden lediglich die zu erreichenden Ziele und nicht die Art und Weise der Zielerreichung festgelegt. Damit sind Rahmenbeschlüsse das Gegenstück zu Richtlinien, die im Rahmen der ehemaligen ersten Säule erlassen wurden. Seit Inkrafttreten des Lissabon-Vertrags und der damit einhergehenden Aufhebung der Säulenstruktur müssen die ehemals im Rahmen der dritten Säule behandelten Angelegenheiten nunmehr im ordentlichen Gesetzgebungsverfahren und mit der Zustimmung des Parlaments verhandelt werden (Schönberger 2007).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Der Verlauf der Verhandlungen sollte sich allerdings schon bald darauf infolge der Anfang Juli 2005 in London verübten Terroranschläge drastisch ändern. Am 21. September 2005 veröffentlichte die Kommission schließlich, gestützt auf Art. 96 des EG-Vertrags und unter dem noch sehr frischen Eindruck der jüngsten Terroranschläge und aufgrund des politischen Drucks der britischen Ratspräsidentschaft,[196] die auf der Verabschiedung eines EG-Instruments zur Vorratsdatenspeicherung unbedingt beharrte, ihren Vorschlag für eine im Rahmen des Mitentscheidungsverfahrens auszuarbeitende Richtlinie des Parlaments und des Rates (Europäische Kommission 2005b). Dieser Vorschlag war zwar als Kompromiss gedacht, griff allerdings nur wenige der inhaltlichen Bedenken des Parlaments auf, während die Position des Ministerrats weitgehend übernommen wurde (A. N. Alvaro 2015, 33; Ripoll Servent 2015, 77). Die britische Ratspräsidentschaft übte daraufhin massiven Druck auf das Europäische Parlament aus, damit die Verhandlungen während ihrer Präsidentschaft und somit noch vor Ende des Jahres abgeschlossen werden konnten. Dahinter lag die Befürchtung der britischen Regierung, dass die auf sie nachfolgende österreichische Ratspräsidentschaft, die zu den erklärten Gegnern der Vorratsdatenspeicherung zählte, die Verhandlungen nicht oder nicht in ihrem Sinne abschließen würde (Maras 2011, 6).

Charles Clarke, sozialdemokratischer britischer Innenminister von Dezember 2004 bis Mai 2006 in der Regierung Blair, der sich im Rahmen der britischen Ratspräsidentschaft innerhalb der Ministerratskonfiguration Justiz und Inneres für die Verhandlungen zu den Instrumenten zur Vorratsdatenspeicherung verantwortlich zeichnete, setzte alle Hebel in Gang, um jegliche nennenswerte datenschutzrechtliche Ausbesserungen an der Vorratsdatenspeicherung zu verhindern. Dazu setzte Clarke die Mitglieder des LIBE-Ausschusses zunächst dahingehend unter Druck, dass, sollte das Parlament die von der britischen Ratspräsidentschaft gewünschte Vorratsdatenspeicherung nicht akzeptieren, die Vorratsdatenspeicherung als Rahmenbeschluss unter Ausschluss des Parlaments beschlossen würde. Außerdem hatte Clarke dem Parlament im Falle des Scheiterns der britischen Initiative damit gedroht, dass er dafür sorgen werde, dass das Europäische Parlament künftig an keiner einzigen Justiz und Inneres-Maßnahme mehr beteiligt würde (EDRi 2005a). Diese Drohung wurde im LIBE-Ausschuss, der mit den technischen Details des Verfahrens und den mitgliedstaatli-

196 Das Vereinigte Königreich hatte die EU-Ratspräsidentschaft Anfang Juli 2005 übernommen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

chen Positionen im Ministerrat gut vertraut war, als Bluff wahrgenommen. Schließlich hatte sich zuvor kein Konsens hinsichtlich der britischen Position im Ministerrat abgezeichnet, der zur Verabschiedung eines Rahmenbeschlusses jedoch nötig war. Außerdem schätzte der LIBE-Ausschuss das Zurückrudern des Ministerrats zu einem Rahmenbeschluss im Falle eines Parlamentsvetos im Rahmen des Mitentscheidungsverfahrens als eine politische Niederlage ein, welche die Ratspräsidentschaft einzugehen nicht bereit sein würde.

Dennoch kam der LIBE-Ausschuss bzw. Rapporteur Alvaro Clarkes Forderungen insofern entgegen, als der Parlamentsbericht innerhalb kürzester Zeit erarbeitet und im Rahmen informeller Trilog-Gespräche mit der Kommission und dem Ministerrat abgestimmt wurde. Allerdings beugte sich der LIBE-Ausschuss nicht den Maximalforderungen Clarkes und sah im Ausschussbericht Verbesserungsvorschläge hinsichtlich des Datenschutzniveaus vor. Dieser Bericht wurde am 24. November 2005 im LIBE-Ausschuss mit 33 Stimmen (bei 8 Gegenstimmen und 5 Enthaltungen) angenommen (Ripoll Servent 2015, 72). Auf Ablehnung stieß der Ministerratsvorstoß erneut insbesondere bei den Datenschutzaufsichtsbehörden, aber auch die europäische Wirtschaft erneuerte ihre Kritik – wenn auch in abgeschwächter Weise und vor allem mit Blick auf die entstehenden Kosten einer Vorratsdatenspeicherung.[197]

Nachdem der LIBE-Ausschuss sich gegen Clarkes Forderungen gestellt hatte, eskalierte letzterer den Konflikt und wandte sich an die Vorsitzenden der Parlamentsfraktionen. Insbesondere die Vorsitzenden der beiden größten Fraktionen (die *Europäische Volkspartei* EVP und die *Sozialdemokratische Partei Europas* SPE) reagierten im Gegensatz zu den LIBE-Ausschussmitgliedern deutlich hellhöriger auf Clarkes Drohungen und befürchteten auch eine Beeinträchtigung der anstehenden Verhandlungen des Lissabon-Vertrags, in deren Ergebnis sie sich eine allgemeine Stärkung der Mitwirkungsrechte des Parlaments erhofften. Im Sinne einer Zuckerbrot-und-Peitsche-Strategie eröffnete Clarke den Fraktionsvorsitzenden zugleich zwei Zugeständnisse: Zum einen versprach er, dass der Ministerrat im Falle der Unterstützung durch das Parlament das seit 1990 zur Debatte stehende aber nie erfolgreich zu Ende verhandelte Rahmeninstrument zum

197 So etwa seitens des BDI, bitkom, eco, UNICE (Businesseurope), ISPA und ETNO (EDRi 2005b; ETNO 2005; Hermida 2006; Scheffel 2016, 106)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutz in der dritten Säule endlich verabschieden würde.[198] Zum anderen versprach er die (bei den Mitgliedstaaten durchaus umstrittene) Ausweitung der Mitentscheidungsbefugnisse des Parlaments mittels der sog. Passerelle-Regelung auf weitere Maßnahmen im Bereich der dritten Säule (Ripoll Servent 2013, 978). Auf diese Weise schaffte es die britische Ratspräsidentschaft, die Haltung des Parlaments zur Vorratsdatenspeicherung als eine Entscheidung von besonderer Tragweite für die weitere Kooperation der EU-Organe darzustellen. Die Debatte wurde somit von den Details des Legislativvorschlags (Aufbewahrungsfristen, Verfassungsverträglichkeit, Regelungen zum Zugriff, Verwendungszwecke) erfolgreich losgelöst und als eine Meta-Debatte über verantwortungsbewusstes institutionelles Handeln (in dem Sinne, ob der Ministerrat bei einem ihm besonders wichtigen Thema auf die kompromisslose Unterstützung des Parlaments bauen konnte oder nicht) dargestellt. Bis auf die Forderung des Parlaments nach strafrechtlichen Sanktionen im Falle der Verletzung der datenschutzrechtlichen Pflichten konnte sich letztlich keine seiner übrigen Forderungen durchsetzen (vgl. dazu den Überblick über die verschiedenen Positionen und das Verhandlungsergebnis in: Ripoll Servent 2013, 975). Das Parlament verabschiedete den Kompromissvorschlag am 14. Dezember 2005 mit der Stimmenmehrheit (378 Stimmen dafür, 197 dagegen und 30 Enthaltungen) der *sozialistischen Fraktion im Europaparlament* (PES), der christdemokratisch-konservativen *Fraktion der Europäischen Volkspartei und europäischen Demokraten* (EVP-ED), etwa der Hälfte der *Fraktion der Allianz der Liberalen und Demokraten für Europa* (ALDE)[199] und der Mitglieder der nationalkonservativen und europaskeptischen *Union für das Europa der Nationen* (UEN) (European Union 2005; Ripoll Servent 2013, 977). Gegen den Kompromissvorschlag stimmten die vollständige *Konföderale Fraktion der Vereinten Europäischen Linken/Nordischen Grünen* (GUE/NGL) und bis auf eine Enthaltung auch die vollständige *Fraktion der Grünen/Europäischen Freien Allianz* (Grüne/EFA), etwa die Hälfte von ALDE, die fast vollständige europaskeptische *Fraktion Unabhängigkeit/Demokratie* (IND/DEM) sowie einige wenige Abweichler der EVP-ED, der PES und der UEN (Ripoll Servent 2015, 73).

198 Die Kommission hatte am 4. Oktober 2005 einen Vorschlag für einen Rahmenbeschluss zum Datenschutz in der dritten Säule vorgelegt (vgl. Unterabschnitt 3.3.4.4).

199 Darunter vor allem MEPs aus Italien, Belgien, Frankreich und Litauen (Ripoll Servent 2015, 72).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nach Annahme des Kompromisstextes durch das Parlament in erster Lesung Ende 2005, nahm auch der Ministerrat den Text in erster Lesung Ende Februar 2006 an.[200] Die *Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG* wurde schließlich am 15. März 2006 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet und trat am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der EU, also am 3. Mai 2006 in Kraft und sah die Umsetzung der Richtlinien-Vorgaben in nationales Recht bis zum 15. September 2007 vor (Europäische Union 2006).

3.3.4.3 Der Zugriff auf Fluggastdaten zu Sicherheitszwecken

Eine Folge der Anschläge vom 11. September war das Interesse der Vereinigten Staaten am Zugriff auf personenbezogene Daten von Menschen, die in die Vereinigten Staaten einreisen. Zu diesem Zweck verabschiedete der US-Kongress bereits am 19. November 2001 den *Aviation and Transportation Security Act* (US Congress 2001), um Zugriff auf möglichst umfassende personenbezogene Daten der in die Vereinigten Staaten einreisenden Fluggäste zu erhalten. Dazu verpflichtete das Gesetz alle Fluggesellschaften, die Flüge in, aus oder durch die USA anboten, dazu, Zugang zu ihren Fluggastdaten – dem sogenannten *Passenger Name Record* (PNR)[201] – zu gewähren. Jenen Fluggesellschaften, die das Gesetz nicht befolgten, wurde mit einem Landeverbot gedroht. Entsprechend befanden sich die betroffenen Fluggesellschaften in dem Dilemma, entweder durch die Nicht-Herausgabe der geforderten Informationen US-Recht oder durch die Herausgabe personenbezogener Daten EU-Recht zu verletzen. Zur Lösung des Konflikts nahm die Generaldirektion Binnenmarkt der Europäischen Kommission (die grundsätzlich am Erhalt des in der DS-RL festgelegten Schutzniveaus

200 Lediglich Irland und die Slowakei stimmten aufgrund der Verortung der Regelung in der ersten Säule gegen die Richtlinie zur Vorratsdatenspeicherung (Ripoll Servent 2013, 978).

201 Ein PNR wird bei jeder Buchung und Durchführung einer Flugreise erstellt und beinhaltet ein Datenset, bestehend aus über dreißig personenbezogenen Merkmalen. Darunter befinden sich neben dem Namen, Kreditkarteninformationen, der Anschrift und ggf. IP-Adresse auch Details über Speisewünsche (die Rückschlüsse auf die Religionszugehörigkeit erlauben können) und den gesundheitlichen Zustand des Reisenden (A. Busch 2012a, 420).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

interessiert war) Verhandlungen mit dem zuständigen US-Heimatschutzministerium auf. Dieses drängte ohne Kompromissbereitschaft auf einen vollständigen Zugriff auf die geforderten Daten bei einem weitgehend unkontrollierten Zugang und konnte den anfänglichen Widerstand der EU insb. aufgrund der Androhung eines Landeverbots letztlich brechen. Daraufhin schloss der EU-Ministerrat 2004 ein erstes Fluggastdatenabkommen mit den Vereinigten Staaten, das von der EU-Kommission für angemessen im Hinblick auf die in der DS-RL verbrieften Drittstaatentransferregelungen befunden wurde. Diese Vereinbarung bzw. Entscheidung wurde vonseiten der europäischen Datenschutzbeauftragten sowie des Parlaments allerdings als mit Datenschutz-Vorgaben unverträglich scharf kritisiert. Das Europäische Parlament brachte den Fall schließlich vor den EuGH, der das Abkommen 2006 annullierte. Ausschlaggebend für die EuGH-Entscheidung waren allerdings weniger inhaltliche als vielmehr prozedurale Gründe: Demzufolge verfüge der Ministerrat nicht über die Befugnis zum Abschluss des Abkommens und die Kommission nicht über die Kompetenz der Formulierung eines Angemessenheitsbefundes im Rahmen der DS-RL, da der zur Debatte stehende Sachverhalt nicht der ersten, sondern dritten Säule der EU zuzuordnen sei. Aufgrund dieses *forum shift* war nicht mehr die Binnenmarkt-Generaldirektion, sondern die im Ministerrat versammelten nationalen Innen- und Justizminister sowie der EU-Justizkommissar für die weiteren Verhandlungen zuständig (A. Busch 2012a, 428 ff. Hummer 2011, 238 ff.). Der seinerzeitige EU-Justizkommissar Franco Frattini handelte in der Folge gemeinsam mit dem damaligen deutschen Bundesinnenminister Wolfgang Schäuble, die beide deutlich offener gegenüber weitreichenden Sicherheitsregelungen eingestellt waren, unter Umgehung des Europäischen Parlaments 2007 ein neues Abkommen mit den Vereinigten Staaten aus, das u. a. aufgrund der Verlängerung der Vorhaltungsdauer der PNR-Daten von 3,5 auf 15 Jahre als ein weiteres Zugeständnis gegenüber den Wünschen des transatlantischen Verhandlungspartners gewertet wurde (Rötzer 2007). Nachdem der *forum shift* durch die Verlagerung der Zuständigkeit an sicherheitspolitisch motivierte Akteure zunächst die Schwächung der Parlamentsposition zur Folge hatte, führte das Inkrafttreten des Lissabon-Vertrags Anfang Januar 2009 zu einer Aufwertung der Mitentscheidungsbefugnisse des Parlaments. Sachverhalte, die zuvor der dritten Säule zugeordnet waren, wurden durch die Abschaffung der Säulenstruktur dem in Art. 14 des EU-Vertrags geregelten ordentlichen Gesetzgebungsverfahren zugeordnet, wodurch das Parlament eine faktische Vetomacht erhielt. Auf Grundlage seiner erweiterten Kompetenzen und unter Verweis

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

auf die Einhaltung bestimmter, durch das Parlament definierter Mindeststandards, lehnte das Parlament im Mai 2010 die Kommissionsinitiative vom Dezember 2009 zur endgültigen Regelung des Sachverhalts nach den Regeln des Lissabon-Vertrags ab (A. Busch 2012a, 430). In Kooperation mit dem Parlament wurde in der Folgezeit ein neues transatlantisches Abkommen zum Transfer von Flugpassagierdaten ausgehandelt und 2012 vom Ministerrat und Parlament verabschiedet (VoteWatch Europe 2012). Für den vom rumänischen konservativen Traian Ungureanu ausgearbeiteten Bericht stimmten im Parlamentsplenum 409 Abgeordnete, darunter praktisch die gesamte EVP- und EKR-Fraktion, zwei Drittel der S&D-Abgeordneten, die halbe EFD-Fraktion, ein Viertel der ALDE-Fraktion sowie einige unabhängige Abgeordnete. Die 226 Gegenstimmen setzten sich aus der vollständigen GUE/NGL und Grünen/EFA, knapp drei Viertel der ALDE-Fraktion, einem Drittel der S&D-Fraktion sowie einigen EFD- und unabhängigen Abgeordneten zusammen. Die 33 Enthaltungen verteilten sich vor allem auf einige wenige ALDE-, EVP- und S&D-Abgeordnete (EU-Parlament 2012f, 19 f.).

3.3.4.3.1 Zwischenfazit

Auch am Beispiel der Fluggastdatentransfers wiederholte sich das Muster, das bereits mit dem Kompromiss bei der ePrivacy-Richtlinie seinen Anfang genommen hatte. Sobald die Staatsräson in den Vordergrund rückte, verließ die S&D ihren datenschutzbefürwortenden bzw. überwachungskritischen Standpunkt und unterstützte die EVP und die übrigen konservativen Akteure in ihren Bestrebungen zur Ausweitung der Überwachung. Im Vergleich zu den vorherigen datenschutzpolitischen Auseinandersetzungen war am Beispiel des Fluggastdatentransfers zusätzlich problematisch, dass die Inhalte des Abkommens im Laufe der Jahre zunehmend überwachungsfreundlicher geworden waren. Nicht nur erlaubte das Abkommen auch weiterhin die Speicherung der PNR-Daten für 15 Jahre, im Falle der Anonymisierung der Daten wurde eine unbegrenzte Aufbewahrungsfrist vorgesehen. Weder eine unabhängige Aufsicht, noch die elementaren Betroffenenrechte in Form der Rechte auf Auskunft, Berichtung und Löschung oder Rechtsschutz wurde den europäischen Bürgerinnen und Bürgern zuerkannt (A. Busch 2012a).

Sowohl der EDSB als auch die in der Art. 29-Datenschutzgruppe versammelten EU-Datenschutzbeauftragten kritisierten das Verhandlungsergebnis

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

im Hinblick darauf, dass es den europäischen Grundrechten nicht gerecht werde (Krempl 2012c). Während zu Beginn der 2000er-Jahre der Zugriff auf Fluggastdaten zu sicherheitspolitischen Zwecken noch als weitgehender Eingriff in Freiheits- und Datenschutzrechte gewertet wurde, hatte sich die Debatte im Laufe der Jahre dermaßen verschoben, dass nicht nur weitere PNR-Abkommen mit Kanada und Australien abgeschlossen wurden, sondern die EU-Kommission 2007 sogar eine Initiative für die Sammlung von Fluggastdaten in der EU selbst startete (EU-Kommission 2011).

3.3.4.4 Die Erarbeitung des JI-Rahmenbeschlusses 2008/977/JHA

Nachdem mehrere seit den 1990er-Jahren betriebene Initiativen zur Festlegung gemeinsamer Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS) aufgrund des Widerstands einiger Mitgliedstaaten[202] gescheitert waren, hatte sich im Laufe des Jahres 2005 ein Gelegenheitsfenster geöffnet, in dessen Ergebnis die Verabschiedung des JI-Rahmenbeschlusses erfolgen sollte. So hatten sich die EU-Organe im Rahmen des Haager Programms auch zur Festlegung von Datenschutzstandards auf dem Schutzniveau der DS-RL für den Bereich der Politiken der dritten Säule entschlossen. Zudem erneuerten die europäischen Datenschutzbeauftragten sowie das Europäische Parlament ihren Wunsch nach Datenschutzregelungen für die dritte Säule Mitte 2005 und ermutigten die Kommission und den Ministerrat zur Verabschiedung entsprechender Regeln (vgl. die vorangegangenen Unterabschnitte).

Schließlich wurde im Rahmen des Maßnahmenpakets, das nach den Londoner Anschlägen von den EU-Justiz- und Innenminister auf einer Sondersitzung des Ministerrats verabschiedet wurde, die Kommission zur Vorlage eines entsprechenden Legislativvorschlags bis Oktober 2005 aufgefordert (EU-Ministerrat 2005a, 7). Dieser Aufforderung kam die Kommission nach und veröffentlichte am 4. Oktober 2005 ihren *Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden* (Europäische Kommission 2005c).

Der Veröffentlichung war ein Prozess der Konsultation unter den EU-Organen und -Institutionen vorangegangen. Dabei wurden Vertreter

202 Der Widerstand einzelner Mitgliedstaaten im Bereich der Politiken der dritten Säule war insofern von herausgehobener Bedeutung, als Beschlüsse im Rahmen der dritten EU-Säule grundsätzlich einstimmig gefasst wurden (Wessels 2008, 201 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

der Mitgliedstaaten (am 22. November 2004 und am 21. Juni 2005), der nationalen Datenschutzaufsichtsbehörden, des EDSB, von Europol und Eurojust (am 11. Januar 2005) und die erwähnte Resolution der Europäischen Datenschutzbeauftragen bzw. des Europäischen Parlaments berücksichtigt. Außerdem partizipierten Kommissionsvertreter an Treffen der von der Frühjahreskonferenz der Europäischen Datenschutzaufsichtsbehörden mandatierten *Arbeitsgruppe Polizei* (am 12. April und 21. Juni 2005) sowie an einer einschlägigen Veranstaltung des LIBE-Ausschusses (EU Commission 2005, 6). Die Kommission stellte fest, dass die Datenschutzaufsichtsbehörden und das EP dabei ihre vollständige Unterstützung für das Gesetzesvorhaben der Kommission zum Ausdruck gebracht hätten, während die Vertreter der Mitgliedstaaten und von Europol und Eurojust keine einheitliche Position vertreten hätten. Klar sei geworden, dass die Mitgliedstaaten Interesse an einem Datenschutzinstrument nur dann hätten, sofern es unter Wahrung von Datenschutz-Grundsätzen dem von den Polizei- und Justizbehörden anvisierten Ziel der europaweiten Verfügbarkeit dienlich wäre (ebd., 6 f.).

Obwohl die Erarbeitung des Kommissionsvorschlags nicht mehr unter der Verantwortung des in der Binnenmarkt-GD angesiedelten Datenschutz-Referats, sondern unter dem in der Direktion D „Innere Sicherheit und Strafjustiz" der Generaldirektion „Justiz, Freiheit und Sicherheit" angesiedelten Referat „Bekämpfung von Terrorismus, Sicherheit und Strafjustiz" erfolgte (Zerdick 2008, 3),[203] sah der Vorschlag der Kommission entgegen zivilgesellschaftlichen Befürchtungen (Statewatch 2005) ein hohes, entlang der Vorgaben der DS-RL erarbeitetes Datenschutzniveau vor. Begründet wurde dieser Schritt damit, dass die „Grundprinzipien des Datenschutzes […] für den Datenschutz sowohl im Rahmen des ersten als auch im Rahmen des dritten Pfeilers [gelten]." (Europäische Kommission 2005c, 5) Entsprechend waren vergleichbare Betroffenenrechte wie in der DS-RL vorgesehen (Informationsrechte in Art. 19 und 20 sowie die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten in Art. 21 JI-Rahmenbeschluss-E). Auch die Datenschutz-Grundsätze (Art. 4 JI-Rahmenbeschluss-E) waren den Grundsätzen der DS-RL ähnlich. Darüber hinaus sah der Vorschlag besondere Regeln für Drittstaatentransfers (Art. 15),

203 Im Zuge des Kommissionsaktionsplans zur Umsetzung des Haager Programms war das bis dahin in der GD-Binnenmarkt angesiedelte Datenschutz-Referat im Laufe der ersten Hälfte des Jahres 2005 *im Interesse eines kohärenten Konzepts* in die Direktion C „Ziviljustiz, Grundrechte und Unionsbürgerschaft" der GD Justiz, Freiheit und Sicherheit übertragen worden (Europäische Kommission 2005a, 10),

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Einrichtung unabhängiger Aufsichtsbehörden bzw. die Übertragung dieser Aufgabe an die bestehenden Datenschutzaufsichtsbehörden (Art. 30) sowie die Einrichtung einer EU-weiten Arbeitsgruppe – ähnlich der Art. 29-Datenschutzgruppe – vor (Art. 31). Der Anwendungsbereich des Vorschlags umfasste sowohl den Datenaustausch zwischen den EU-Mitgliedstaaten als auch Verarbeitungen in den Mitgliedstaaten selbst. Ausgenommen vom Anwendungsbereich waren jedoch Europol, Eurojust und ZIS (Art. 3).

3.3.4.4.1 Stellungnahmen der Datenschutzaufsichtsbehörden

Nach der Veröffentlichung des Kommissionsentwurfs setzten sich das Parlament und der Ministerrat sowie die europäischen Datenschutzbehörden mit diesem auseinander. Zunächst veröffentlichte der EDSB im Dezember 2005 eine erste Stellungnahme. Ausgehend von der ausdrücklichen Unterstützung des Kommissionsentwurfs machte die EDSB-Stellungnahme zahlreiche Vorschläge hinsichtlich der Verbesserung des Schutzniveaus, etwa im Hinblick darauf, dass die Verarbeitung von Daten über unterschiedliche Personengruppen (Verdächtige, Verurteilte, Opfer, Zeugen, Kontaktpersonen, Nicht-Verdächtige) nach unterschiedlichen, angemessenen Bedingungen und Schutzbestimmungen erfolgen, dass in Bezug auf automatisierte Einzelentscheidungen besondere Schutzbestimmungen eingeführt werden und schließlich, dass der Austausch personenbezogener Daten mit Drittländern auf Basis angemessener Datenschutzgarantien erfolgen sollte (EDSB 2005, 45–47). Der EDSB kam den Forderungen der Strafverfolgungsbehörden aber auch in mehreren Punkten entgegen, so wurde der Ausschluss geheim- und nachrichtendienstlicher Datenverarbeitung aus dem Anwendungsbereich des Rahmenbeschlusses nicht infrage gestellt, sondern lediglich darauf verwiesen, dass die einzelstaatlichen Rechtsvorschriften für diesen Bereich einen angemessenen Schutz für die Betroffenen vorsehen müssten (EDSB 2005, 31, Nr. 33). Zudem verwies der EDSB zwar auf die Bedeutung der Zweckbindung im europäischen Datenschutzrecht, vertrat jedoch zugleich die Ansicht, „dass hinsichtlich der Weiterverwendung eine gewisse Flexibilität möglich sein" (EDSB 2005, 34, Nr. 62), d. h. eine Ausnahmeregelung vorhanden sein müsse, auf deren Grundlage die Weiterverarbeitung für Zwecke, die mit dem ursprünglichen Zweck unvereinbar seien, möglich werde, während zugleich Datenschutzgarantien berücksichtigt würden (EDSB 2005, 34, Nr. 60-65). Auf die Stellungnahme des Europäischen Datenschutzbeauftragten folgte Ende Januar 2006

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

eine erste Stellungnahme der Konferenz der europäischen Datenschutzbeauftragten. In dieser wurden das dem Entwurf zugrundeliegende hohe, an der DS-RL 95/46/EG orientierte, Schutzniveau sowie die Anwendbarkeit der Regeln sowohl auf den Datenaustausch zwischen EU-Mitgliedstaaten als auch auf Datenverarbeitungen in den Mitgliedstaaten selbst, gelobt (Conference of European Data Protection Authorities 2006, 6). Zudem wiesen auch die mitgliedstaatlichen Datenschutzbeauftragten auf zahlreiche Mängel in Bezug etwa auf die Betroffenenrechte, die Weiterverwendung von Daten zu anderen Zwecken und die vorgesehenen Regelungen zu automatisierten Einzelentscheidungen hin. Auf ihrer jährlichen Frühjahreskonferenz verabschiedeten die mitgliedstaatlichen Datenschutzbeauftragten zudem die sog. Erklärung von Budapest (*Budapest declaration*), in der zum einen ihre vorgenannten Forderungen bekräftigt wurden, aber insbesondere das Europäische Parlament und die Parlamente der Mitgliedstaaten dazu aufgerufen wurden, auf die Regierungen der Mitgliedstaaten dahingehend einzuwirken, dass für den Rahmenbeschluss ein hohes Datenschutzniveau realisiert werden könne. An die Regierungen der Mitgliedstaaten wurde lediglich appelliert, die bürgerlichen Freiheiten der in der EU lebenden Bürger zu achten und zu stärken, wenn sie die Möglichkeiten für den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten erweiterten (European Data Protection Authorities 2006a).

3.3.4.4.2 Positionierung des Parlaments

Gemäß dem Konsultationsverfahren bat der Ministerrat das Europäische Parlament am 13. Dezember 2005, zu dem Kommissionsentwurf Stellung zu nehmen. Das Parlamentspräsidium übergab den Richtlinienentwurf im Januar 2006 an den LIBE-Ausschuss, der sich mit diesem auf drei Sitzungen auseinandersetzte und schließlich am 15. Mai 2006 den Berichtsentwurf der Berichterstatterin Martine Roure (SPE, PS, Frankreich) einstimmig annahm (Roure 2006, 47). Der Roure-Bericht, der viele der Änderungsanträge und Vorschläge des Europäischen Datenschutzbeauftragten aufgriff, wurde schließlich am 13. Juni 2006 im Parlamentsplenum debattiert. Während der Sitzung wurde die Intention des Parlaments bekräftigt, die innerstaatliche polizeiliche und justizielle Verarbeitung von Daten im Anwendungsbereich des Rahmenbeschlusses zu belassen und für die dritte Säule insgesamt ein Schutzniveau zu etablieren, das dem der ersten Säule

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

entsprach. Begründet wurde die Haltung des Parlaments nicht nur mit dem Schutz personenbezogener Daten, sondern auch mit der Verbesserung der Interoperabilität der nationalen Datenbanken, also der Effizienzsteigerung strafverfolgungsbehördlicher Tätigkeiten. Interessanterweise vermied es das Parlament, den gesellschaftlichen Sicherheitsinteressen der Strafverfolgungsbehörden nur individuelle Datenschutzinteressen entgegenzustellen, wie es der folgende Kommentar des Abgeordneten Alexander Alvaro gut auf den Punkt bringt: „Das Problem ist aber, dass Leute, die Daten schützen wollen, oft in eine Ecke gestellt werden, als wären sie irgendwelche Knallschoten, die nicht in der Lage sind, Grundrechte und Sicherheitsrechte in irgendeiner Weise vernünftig gegeneinander abzuwägen. Gott sei Dank hat sich dieses Parlament in diesem Fall nicht in diese Ecke treiben lassen, dass wir Grundrechte gegen Sicherheitsrechte ausspielen würden, *denn das Weniger an Grundrechten gefährdet definitiv die Sicherheit der Bevölkerung*." (Alexander Alvaro, in: Europäisches Parlament 2006c, Hervorhebung M.K.) Zudem erinnerte Martine Roure an die *moralische Verpflichtung* hinsichtlich der raschen Verabschiedung von Datenschutzregelungen im Bereich der dritten Säule *unter Einhaltung einer fairen Zusammenarbeit zwischen den europäischen Organen*, die der Ministerrat im Rahmen der Verabschiedung der Richtlinie über die Vorratsdatenspeicherung gegenüber dem Parlament eingegangen war (vgl. die entsprechenden Ausführungen des britischen Ratsvorsitzes in 3.3.4.2). Da sich die Einigung im Rat erheblich verzögert hatte und die für Ende 2006 vorgesehene Verabschiedung des Rahmenbeschlusses zunehmend schwieriger zu realisieren schien, forderte Roure die an der Plenardebatte teilnehmenden Vertreter des Ministerrats dazu auf, noch am selben Tag *eindeutige Zusagen zu den für das Europäische Parlament wesentlichen Punkten* zu machen und dem Parlament einen *Zeitplan für die Verabschiedung des Rahmenbeschlusses* vorzulegen. Roure gab zu verstehen, dass sie bereits stark enttäuscht vom Rat sei und, sollte der Rat den geäußerten Wünschen nicht nachkommen, das Parlament sich hintergangen fühlen und dies das Vertrauen des Parlaments künftig ernsthaft beeinträchtigen würde (Martine Roure, in: Europäisches Parlament 2006c). Tatsächlich hatte das Parlament durchaus ein Druckmittel in der Hand, da es im Rahmen des Mitentscheidungsverfahrens an der Aktualisierung des Schengener Informationssystems (SIS)[204] beteiligt war und somit

204 Am sog. Schengener Informationssystem der zweiten Generation (SIS II) (EU 2007).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

über ein Veto-Recht verfügte. Zwar zeigten sich die Fraktionen der Linken und Grünen bereit, dieses Druckmittel auch zu nutzen, doch die konservative Fraktion weigerte sich und Berichterstatterin Roure übte lediglich dahingehenden Druck auf den Ministerrat aus, den Rahmenbeschluss gemeinsam mit SIS II zu verabschieden (Europäisches Parlament 2006c; Roure 2006, 44 f.). Auf die Forderungen, die Roure gegenüber dem Ministerrat geäußert hatte, erhielt sie allerdings keine Antwort, da keine Ratsvertreter während des Plenums anwesend waren. Nachdem der Roure-Bericht am 14. Juni 2006 vom Parlamentsplenum mit überwältigender Mehrheit angenommen wurde, wurde auf den Antrag von Berichterstatterin Roure hin die Vertagung der Abstimmung über die Legislativentschließung des Parlaments bis zur Stellungnahme des Ministerrats beschlossen (Europäisches Parlament 2006e). Schließlich nahm die finnische Ratspräsidentschaft am 27. September im Rahmen der Parlamentsdebatte über die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts Stellung zu den Forderungen des Parlaments. Der sozialdemokratische Ratspräsident Kari Rajamäki (finnischer Innenminister von 2003–2007) erklärte, dass die Präsidentschaft beabsichtige, den Rahmenbeschluss schnellstmöglich anzunehmen und „die erste Lesung des Vorschlags noch während der laufenden Sechsmonatsperiode abzuschließen." (Europäisches Parlament 2006f)[205] Nachdem die moralische Verpflichtung des vorangegangenen britischen Ratsvorsitzes von der finnischen Ratspräsidentschaft bekräftigt

205 Zudem hatte sich das Parlament zwischenzeitlich endgültig gegen die Blockade von SIS II und der vom Ministerrat im Alleingang verhandelten VIS entschieden und damit ein weiteres Mal sein äußerstes Entgegenkommen gegenüber den Wünschen des Ministerrats demonstriert, was die Ratspräsidentschaft durchaus zur Kenntnis nahm: „Der Vorsitz ist sich des Charakters des Vorschlags für einen Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der dritten Säule – ich beziehe mich jetzt auf den Vorschlag von Frau Roure – und seiner Bedeutung für die Bürger Europas sehr wohl bewusst, ebenso auch der Tatsache, das sich das Europäische Parlament für die Vorschläge über Rahmenbeschlüsse zu den Informationssystemen VIS und SIS II ausgesprochen hat. In diesem Zusammenhang und im Namen des Ratsvorsitzes möchte ich dem Europäischen Parlament für seine Arbeit danken und sagen, dass wir alles in unseren Möglichkeiten Stehende tun werden, um noch vor Ablauf unserer Präsidentschaft eine Einigung über den Vorschlag für den Rahmenbeschluss zu erzielen. Soweit möglich, werden wir bei unserer weiteren Arbeit die Stellungnahme und die Auffassungen des Europäischen Parlaments im Kontext der Bestimmungen des EG-Vertrags berücksichtigen, um letztlich mit einem brauchbaren legislativen Instrument ein hohes Maß an Schutz der persönlichen Daten durch die Schaffung gemeinsamer Regeln für den Datenschutz im Rahmen der dritten Säule zu gewährleisten." (Kari Rajamäki, in: Europäisches Parlament 2006f)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

und konkretisiert worden war, stimmte das Parlament noch am selben Tag für die Legislativentschließung, in der es den Ministerrat dazu aufforderte, das Parlament zu unterrichten, sofern die Parlamentsänderungen nicht angenommen würden und im Falle einer weitergehenden Änderung des Kommissionsentwurfs das Parlament erneut zu konsultieren (Europäisches Parlament 2006b).

3.3.4.4.3 Verhandlungen im Ministerrat

Auf Seiten des Ministerrats übernahm keine mit Datenschutz befasste Ratsarbeitsgruppe die Verantwortung für die Beratungen und Verhandlungen zum JI-Rahmenbeschluss, sondern die sog. MDG, multidisziplinäre Gruppe „Organisierte Kriminalität" (Working Group for Organized Crime and other Horizontal Issues) (Vorsitz - EU-Ministerrat 2006).[206] Die seit ihrer Einsetzung am 21. Februar 1991 für die Verhandlungen zur DS-RL, ISDN-RL sowie DS-VO zuständige Ratsarbeitsgruppe Datenschutz[207] war zwischenzeitlich unter Verweis auf ihre Inaktivität seit April 2001 am 24. Januar 2002 aufgelöst (General Secretariat of the Council of the European Union 2002) und erst unter der österreichischen Ratspräsidentschaft Anfang 2006 wieder reaktiviert worden. Die wiedereingerichtete Gruppe *Datenschutz* wurde zwar mit zahlreichen Aufgaben betraut, doch die Verantwortung der Beratungen zum Rahmenbeschluss verblieb – trotz der Einbindung der Gruppe Datenschutz in den Prozess – weiterhin bei der MDG (Statewatch 2006).

Die MDG, die sich aus Beamten der mitgliedstaatlichen Strafverfolgungsbehörden zusammensetzte (P. de Hert und Papakonstantinou 2009, 407), hatte allerdings zu keinem Zeitpunkt Interesse an einem ernsthaf-

206 Für die Datenschutzfragen im JI-Bereich im Kontext der dritten Säule war die Ratsarbeitsgruppe „Informationssysteme und Datenschutz" („Working Party on Information Systems and Data Protection") zuständig, die von ihrer ersten Sitzung am 11 Februar 1999 bis zum Juni desselben Jahres zunächst unter dem Namen „Informatik" als horizontale Gruppe tagte (Rat der Europäischen Union 1999). Die Funktionen der Ratsarbeitsgruppe „Informationssysteme und Datenschutz" wurden Anfang 2002 schließlich parallel zur Auflösung der Datenschutz-Ratsarbeitsgruppe in den Verantwortungsbereich der MDG übertragen (Swedish Delegation 2002, 5),

207 Bis zu ihrer Umbenennung im Sinne einer klareren Zuordnung im Jahr 1999 firmierte die Arbeitsgruppe unter dem Namen „Wirtschaftsfragen (Datenschutz)" bzw. „Economic Questions – Data Protection" (Presidency of the Council of the European Union 2006, 1).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

ten inhaltlichen Austausch mit dem Europäischen Parlament oder den europäischen Datenschutzbeauftragten.[208] Stattdessen war die MDG von dem Ziel angetrieben, einen möglichst reibungslosen und weitgehenden Datenaustausch zwischen den Mitgliedstaaten zu gewährleisten. Mehrere Faktoren strukturierten das Handeln der Arbeitsgruppe und sollten die Verabschiedung eines hohen Datenschutzniveaus deutlich erschweren: *Erstens* war die für eine wirksame Ausgestaltung der Datenschutzregelungen erforderliche und EU-weit einheitliche Differenzierung zwischen Polizei- und Justizbehörden schwierig zu leisten, wie z. B. mit polizeilichen Daten umgegangen werden sollte, die auf Hörensagen beruhen, während die Unabhängigkeit des Justizbereichs deren Kontrolle erschwerte. *Zweitens* waren die existierenden Unterschiede zwischen den Polizei- und Justizsystemen enorm: Während z. B. die Polizei in einigen Mitgliedstaaten Strafmaßnahmen anordnen durfte, war dies in anderen Staaten einem Staatsanwalt vorbehalten. *Drittens* erschwerten nationale politische Sensibilitäten den Einigungsprozess in der Ratsarbeitsgruppe bzw. im Ministerrat generell: Einige Delegationen hatten ein außerordentlich einseitiges Interesse an der weitest möglichen Verfügbarkeit aller Daten und betrachteten Datenschutzvorkehrungen als Beeinträchtigung und nicht als elementaren Bestandteil ihrer täglichen Arbeit. *Viertens* hatten alle Mitgliedstaaten im Laufe der Jahre Pfadabhängigkeiten geschaffen, die nur schwer umzukehren waren. Viele Mitgliedstaaten hatten bilaterale Abkommen mit anderen, auch Nicht-EU-Staaten zum Datenaustausch abgeschlossen, deren Fortbestand von dem im Rahmenbeschluss festzulegenden Datenschutzniveau abhing. Schließlich und *fünftens* musste der Ministerrat über den Rahmenbeschluss einstimmig entscheiden, sodass jeder Mitgliedstaat das Vorhaben verhindern konnte. Da zudem die Gegner von Datenschutzregelungen im Bereich der dritten Säule mit dem Status Quo zufrieden waren, im Falle eines Scheiterns des Legislativvorhabens also nichts zu verlieren, aber viel zu gewinnen hatten, mussten sie keinerlei Kompromisse mit den Datenschutzbefürwortern eingehen. Dadurch gerieten die Verhandlungen im Ministerrat zu einem Wettlauf nach unten (P. D. Hert, Papakonstantinou, und Riehle 2008, 165 f.).

Die erste, von der MDG im November 2005 begonnene Lesung des Kommissionsentwurfs konnte aufgrund dieser Schwierigkeiten erst verspätet im September 2006 abgeschlossen werden. Kurz vor dem Ende ihrer

208 Ein Beobachter machte die Feststellung, dass ihr *"primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects"* (Lord Avebury 2006).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Amtszeit legte die finnische Ratspräsidentschaft schließlich noch im November 2006 einen ersten Entwurf für eine gemeinsame Position des Rats vor. Dieser erste Ratsentwurf änderte den Kommissionsentwurf allerdings dermaßen stark, dass kaum ein Datenschutzelement übrig blieb, das nicht durch sehr weit und zugleich unklar gefasste Ausnahmeregelungen außer Kraft gesetzt werden konnte. So sah der November-Ratsentwurf, obwohl der Juristische Dienst des Rates, die Kommission, das Parlament, die Europäischen Datenschutzbeauftragten sowie auch die Mehrheit der EU-Mitgliedstaaten für den Einbezug innerstaatlicher Datenverarbeitung votierten, aufgrund des Widerstands einiger Mitgliedstaaten, angeführt vom Vereinigten Königreich, eine Abschwächung des Anwendungsbereichs vor.[209] Die Anforderung, dass Drittländer, in die personenbezogene Daten aus der EU übertragen werden sollten, ein angemessenes Datenschutzniveau garantieren müssten, wurde zwar von der Tschechischen Republik, der Schweiz, Finnland, Griechenland und Portugal befürwortet, doch von Deutschland, Dänemark, Spanien, Irland, Norwegen, Schweden und dem Vereinigten Königreich abgelehnt, sodass die Regelung dahingehend aufgeweicht wurde, dass bestehende bi- bzw. multilaterale Abkommen unberührt von der Regel, eine Angemessenheitsprüfung durchzuführen, sein sollten (Bunyan 2006, 10 f.).[210] Aufgeweicht wurden auch die Bestimmungen zur Weiterverarbeitung von personenbezogenen Daten zu anderen Zwecken als dem ursprünglichen Verarbeitungszweck und auch die Bestimmungen zur Verarbeitung besonderer Kategorien personenbezogener Daten (ebd.,

209 In diesem Zusammenhang wurde darauf hingewiesen, dass die Polizei- und Justizbehörden der Mitgliedstaaten dann zwei Datenbanken (eine für die nationale Datenverarbeitung und eine weitere für den unionsweiten Datenaustausch) führen müssten, woraufhin sich eine Reihe von praktischen und theoretischen Fragen stellen lässt: Wie kann die Polizei zuvor wissen, welche Daten in der Zukunft von den anderen Mitgliedstaaten angefragt werden? Und welche Arten von möglicherweise problematischen Verarbeitungen führen die Mitgliedstaaten durch, dass sie nicht gewillt sind, elementare Datenschutzgrundsätze auf diese Verarbeitungen anzuwenden? (P. D. Hert, Papakonstantinou, und Riehle 2008, 166) Letztere Frage wurde einige Jahre später, zumindest in Bezug auf das Vereinigte Königreich mit dem Bekanntwerden des Überwachungsprogramms Tempora teilweise recht eindeutig beantwortet.

210 In Bezug auf den Datentransfer in Drittstaaten berichtete beispielsweise die grüne niederländische Europaabgeordnete Kathalijne Maria Buitenweg später von einer *lustigen Begebenheit* während des deutschen Ratsvorsitzes, „als ein Vertreter des Rates ausführte, es sei manchmal tatsächlich notwendig, sehr schnell Daten in den Iran zu übermitteln. Das ganze Haus war sprachlos; das konnte nicht sein Ernst sein – Datentransfers in den Iran!“ (EP 2008c)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

12–14). Gegen die in den Art. 19 und 20 des Kommissionsentwurfs vorgesehenen Informationsrechte der Betroffenen bzw. Informationspflichten der Verarbeiter votierten Belgien, die Tschechische Republik, Deutschland, Spanien, Griechenland, Italien, die Niederlande, Norwegen, Portugal, Schweden und das Vereinigte Königreich (ebd., 14). Zudem erfolgten auf den Wunsch Dänemarks, der Niederlande und des Vereinigten Königreichs hin auch Streichungen beim Betroffenenrecht auf Auskunft (ebd., 15) und auf den Wunsch Dänemarks, Frankreichs, Griechenlands, der Niederlande und Schwedens hin auch die Einschränkung der Vorgabe, rechtmäßige Berichtigungs- und Löschungswünsche an Dritte, denen die Daten zuvor übermittelt worden waren, weiterzureichen (ebd., 16).

3.3.4.4.4 Stillstand der Verhandlungen

Nachdem der erste Entwurf der gemeinsamen Ratsposition, die eine Einschränkung des Datenschutzniveaus vorsah, bekannt geworden war, veröffentlichten die Europäischen Datenschutzbehörden die Londoner Erklärung (*London declaration*), in der sie ihre Forderung nach einem hohen und harmonisierten Datenschutzniveau für den Bereich der dritten Säule ein weiteres Mal bekräftigten (European Data Protection Authorities 2006b). Am 29. November 2006 veröffentlichte der Europäische Datenschutzbeauftragte seine zweite Stellungnahme zum Rahmenbeschluss. Darin stellte der EDSB zunächst fest, dass die zirkulierenden Ratspositionen weder die vom Europäischen Parlament vorgeschlagenen Abänderungen noch jene des EDSB oder die der Konferenz der europäischen Datenschutzbehörden berücksichtigten und stattdessen sogar das Schutzniveau des Kommissionsentwurfs reduzierten: „Infolgedessen besteht die Gefahr, dass das Schutzniveau niedriger als dem [sic] Schutzniveau der Richtlinie 95/46/EG oder gar des allgemeiner gefassten Übereinkommens Nr. 108 des Europarates, das für die Mitgliedstaaten bindend ist [sic] sein wird." (EDSB 2006, 9, Nr. 4) Neben einer Reihe von Änderungsvorschlägen empfahl der EDSB dem Rat schließlich, aufgrund des Ziels einer zügigen Entscheidungsfindung nicht die Absenkung des Schutzniveaus in Kauf zu nehmen und sich lieber mehr Zeit für die Verhandlungen zu nehmen, damit im Ergebnis ein ausreichender Schutz geboten werde (ebd., 10, Nr. 8).

Am 13. Dezember fand die erste Aussprache zum Thema nach Bekanntwerden der Ratspositionen im Europäischen Parlament statt. Die liberale finnische Vertreterin des noch amtierenden Ratsvorsitzes, Paula Lehtomäki

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(Zentrumspartei, finnische Ministerin für Außenhandel, Entwicklung und Europaangelegenheiten zwischen 2003 und 2007) gab während der Plenardebatte bekannt, dass es trotz der Bemühungen der finnischen Ratspräsidentschaft wohl nicht mehr in ihrer Amtszeit zu einer Einigung im Ministerrat kommen werde. Als Hauptgrund nannte Lehtomäki den Konflikt um den Anwendungsbereich des Rahmenbeschlusses, dessen Beschränkung auf grenzüberschreitende Datentransfers weiterhin von einigen Mitgliedstaaten gefordert werde (Europäisches Parlament 2006d). Parlamentsberichterstatterin Roure dankte dem finnischen Ratsvorsitz für seine Bemühungen, machte allerdings angesichts der beunruhigenden Entwicklungen der Ratsverhandlungen in Richtung einer Einigung auf dem kleinsten gemeinsamen Nenner, die hinter dem Schutzniveau der DS-RL und der Europaratskonvention deutlich zurückbleibe, auch deutlich, dass das Parlament das Visainformationssystem (VIS) nicht einführen werde, „ohne über Garantien zu verfügen, dass ein Rahmenbeschluss über den Datenschutz angenommen werden soll." (Europäisches Parlament 2006d) Am Tag darauf, dem 14. Dezember 2006, verabschiedete das Parlament schließlich eine an den Rat gerichtete Empfehlung, in der es diese Sorgen zum Ausdruck brachte (Europäisches Parlament 2006a).

3.3.4.4.5 Überwindung der politischen Pattsituation

Mit dem Jahresbeginn 2007 übernahm Deutschland die Ratspräsidentschaft und damit auch die Verantwortung über die Weiterführung der Verhandlungen zum Rahmenbeschluss, musste aber bereits im Januar feststellen, dass die Verhandlungen in eine Sackgasse geraten waren und aufgrund der Frage nach dem Anwendungsbereich zu scheitern drohten. Daraufhin bat der deutsche Ratsvorsitz die Kommission zunächst um die Erstellung eines überarbeiteten Kommissionsentwurfs, veröffentlichte im März 2007 dann aber einen eigenen überarbeiteten Entwurf. Zudem beschloss der Ratsvorsitz, das Parlament aufgrund der weitgehenden Änderungen ein weiteres Mal zu konsultieren (P. de Hert und Papakonstantinou 2009, 408; Roure 2007, 45). Der Vorschlag des deutschen Vorsitzes sah für den Kernkonflikt um den Anwendungsbereich des Rahmenbeschlusses die Einigung auf dem kleinsten gemeinsamen Nenner vor, mit dem Hinweis darauf, dass eine Erhöhung des Schutzniveaus für einzelne Bereiche seitens der Mitgliedstaaten explizit möglich sein sollte. Und auch im Hinblick auf die anderen Streitthemen (Datentransfers in Drittländer, Weiterverarbeitung,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Betroffenenrechte) stellte der Vorschlag eine Verschlechterung dar. Mehr noch, wurde die im Kommissionsentwurf (Art. 31) vorgesehene Einrichtung einer EU-weiten und sich aus Vertretern der nationalen Datenschutzbehörden zusammensetzenden Arbeitsgruppe weitgehend verworfen (Peers 2007, 2–5).

In der Folge bekräftigten der EDSB im Rahmen seiner dritten Stellungnahme (EDSB 2007a), die Konferenz der europäischen Datenbehörden im Rahmen ihrer Erklärung von Zypern (European Data Protection Authorities 2007) sowie das Parlament (Roure 2007) ein weiteres Mal ihren Wunsch nach einem hohen Datenschutzniveau, wiesen darauf hin, dass der vom deutschen Ratsvorsitz vorgelegte Text eine weitere Verschlechterung des Schutzniveaus darstelle, und zeigten sich erneut enttäuscht über die anhaltende Ignoranz des Ministerrats gegenüber ihren Änderungswünschen.

Nach weiteren mühevollen Verhandlungen konnte unter portugiesischer Ratspräsidentschaft auf der Tagung des gemischten Ausschusses auf Ebene der Justiz- und Innenminister am 8. November eine erste politische Einigung und am 30. November 2007 schließlich die endgültige Einigung auf Arbeitsgruppenebene erzielt werden (EU-Ministerrat 2007). Auf Grundlage dieser Einigung konsultierte der Ministerrat das Parlament schließlich Anfang 2008 zum dritten Mal und das Parlament verabschiedete am 23. September 2008 seine Position auf Grundlage des von Martine Roure ausgearbeiteten LIBE-Ausschuss-Berichts (Roure 2008). Am 27. November 2008 verabschiedete der Ministerrat schließlich den *Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*, dessen Vorgaben bis zum 27. November 2010 in nationales Recht umzusetzen waren (EU-Ministerrat 2008c).

Bemerkenswerterweise gaben die im Ministerrat versammelten Regierungsvertreter die Verabschiedung des Rahmenbeschlusses weder in der Pressekonferenz nach ihrer Tagung, auf der das Dokument verabschiedet wurde, noch in einer eigenen Pressemeldung bekannt (Krempl 2008a). Von allen sonstigen beteiligten Akteuren und Beobachtern wurde der Text, auf den sich der Ministerrat geeinigt hatte, hingegen rege kommentiert und als eine weitere Aushöhlung des ursprünglichen Kommissionsentwurfs wahrgenommen. So kommentierte etwa Berichterstatterin Roure: „Das Datenschutzniveau dieses Textes ist minimal und weist auch sehr erhebliche Defizite auf. In einigen Fällen könnte man sich sogar fragen, ob es die im Übereinkommen 108 festgesetzten Standards, insbesondere im Hinblick auf das Prinzip der Verhältnismäßigkeit einhält, das ein grundlegendes Daten-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schutzprinzip ist." (Roure 2008, 26) Etwas diplomatischer bezeichnete der Europäische Datenschutzbeauftragte Peter Hustinx den Rahmenbeschluss als ersten wichtigen Schritt auf dem Weg zu einem angemessenen Schutz personenbezogener Daten im Bereich der Polizei und Strafverfolgung, auf den allerdings noch weitere folgen müssten (EDPS 2008). Sowohl Parlament als auch EDSB bemängelten weiterhin insbesondere die Begrenzung des Anwendungsbereichs des Beschlusses auf die zwischen Mitgliedstaaten und EU-Behörden bzw. anderen Mitgliedstaaten ausgetauschten Daten. Daneben wurde aber auch die weiterhin fehlende Differenzierung zwischen Daten von unterschiedlichen Personengruppen (Verdächtige, Verurteilte, Opfer, Zeugen, Kontaktpersonen, Nicht-Verdächtige), das Fehlen gemeinsamer Standards beim Datentransfer in Drittstaaten, die Aushöhlung der Zweckbindung, die Untergrabung von Betroffenenrechten sowie die vollständige Streichung der sich aus den nationalen Kontrollstellen zusammensetzenden Arbeitsgruppe kritisiert (EDPS 2008; Roure 2008). Die wissenschaftlichen Analysen zum Rahmenbeschluss kritisierten die genannten Punkte ebenfalls, hoben aber zugleich hervor, dass der Text immerhin einen ersten, wichtigen Schritt auf dem Weg zu einem angemessenen Datenschutzrahmen im Bereich der dritten Säule darstelle (Belfiore 2013; Bigo u. a. 2011; Boehm 2012, 114 f. González Fuster 2014, 220–22; P. de Hert und Papakonstantinou 2009; Hijmans und Scirocco 2009).

3.3.4.4.6 Zwischenfazit

Zunächst lässt sich festhalten, dass der JI-Rahmenbeschluss einen Minimalkonsens zu den vielen offenen Datenschutzfragen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen darstellt (P. de Hert und Papakonstantinou 2009). Vielmehr aber noch führte der schwierige Aushandlungsprozess den Datenschutzbefürwortern verschiedene kritische Punkte vor Augen.

So hatte die britische Ratspräsidentschaft das bei der Verabschiedung der Richtlinie zur Vorratsdatenspeicherung gegebene Versprechen bezüglich der Zusammenarbeit im Hinblick auf die Verabschiedung eines Rahmeninstruments zum Datenschutz in der dritten Säule unter Beachtung der Parlamentsposition schlicht gebrochen. Der bereits aus den Verhandlungen zur DS-RL bekannte nördliche Block opponierte auch bei diesem Vorhaben gegen fast jeden Vorschlag, der die Gewährleistung eines der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

DS-RL entsprechenden Schutzniveaus vorsah. Der nördliche Block setzte sich – je nach Frage auch variierend – zusammen aus Schweden, Norwegen, den Niederlanden, Dänemark und Irland und wurde vom Vereinigten Königreich angeführt. Das Parlament hatte auf diesen bevorstehenden Vertrauensbruch des Ministerrats während der Verhandlungsjahre mehrfach in der Hoffnung, dass die Datenschutzgegner zur Räson kommen und ihre Opposition beenden würden, hingewiesen, war jedoch letzten Endes durch den getroffenen Minimalkonsens im Rat massiv enttäuscht worden (EP 2008c; vgl. z. B. Roure 2006, 2007, 2008). In anderen Worten hatte der Aushandlungsprozess zum JI-Rahmenbeschluss endgültig vor Augen geführt, dass auf Grundlage der Einstimmigkeitsregel keine angemessenen Datenschutzgesetze in der EU zu machen waren.

Der Hauptkritikpunkt der Datenschutzbefürworter am Rahmenbeschluss in Form des Ausschlusses der innerstaatlichen Datenverarbeitung aus dessen Anwendungsbereich sollte allerdings mittelfristig zu einer deutlichen Stärkung der datenschutzrechtlichen Regelungen in diesem Bereich führen. So hatten bereits jene Mitgliedstaaten, die etwas offener gegenüber einem höheren Datenschutzniveau eingestellt waren (z. B. Frankreich, Finnland und stellenweise auch die Tschechische Republik, die Schweiz, Griechenland, Portugal und Deutschland), in Reaktion auf die vonseiten der Datenschutzbefürworter geäußerte Kritik am unzureichenden Anwendungsbereich hin, den Rahmenbeschluss dahingehend ergänzt, dass im Erwägungsgrund 8 die Absicht der Mitgliedstaaten, den Datenschutzstandard des Rahmenbeschlusses auch bei innerstaatlichen Datenverarbeitungen zu gewährleisten, festgehalten wurde. Art. 27 sah zudem die Prüfung der Auswirkungen der Bestimmungen auf den Anwendungsbereich nach einem Zeitraum von fünf Jahren vor und eröffnete der Kommission die Möglichkeit, diesbezügliche Änderungsvorschläge vorzulegen. Deutlich bedeutsamer war allerdings das geplante Inkrafttreten des Lissabon-Vertrags zum 1. Januar 2009. Je wahrscheinlicher die Verabschiedung von Datenschutzbestimmungen auf lediglich dem kleinsten gemeinsamen Nenner während der Verhandlungen wurde, umso mehr begannen die Europaparlamentarier in der Konsequenz ihre Hoffnungen auf das Inkrafttreten des Lissabon-Vertrags zu legen und umso selbstbewusster forderten sie die Einbeziehung des Parlaments in Entscheidungen über Gesetzesvorlagen im Bereich

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der dritten Säule auf Augenhöhe.[211] So stellte Berichterstatterin Roure in ihrem dritten Bericht klar, dass es notwendig sei, „eine Überarbeitung des Rahmenbeschlusses innerhalb von sechs Monaten nach Inkrafttreten des Vertrags von Lissabon insbesondere im Hinblick auf die Ausdehnung des Anwendungsbereichs vorzunehmen." (Roure 2008, 26) Während der Parlamentsaussprache verwies zudem selbst der Vertreter des Ministerrats, Jean-Pierre Jouyet (parteiloser französischer Staatssekretär für europäische Angelegenheiten im Bereich des französischen Außenministeriums, der während der Plenardebatte die Justizministerin Rachida Dati vertrat), dass der JI-Rahmenbeschluss lediglich einen ersten wichtigen Schritt darstelle, auf den weitere Folgen müssten (EP 2008c).

Schließlich sprach sich insbesondere der neue konservativ-republikanische Kommissar für Justiz, Freiheit und Sicherheit, Jacques Barrot[212] (UMP, Frankreich), klar für die Stärkung des europäischen Datenschutzrahmens aus: „Wie ich bereits sagte, und ich möchte dies nicht überstrapazieren, wäre natürlich auch die Kommission beim Datenschutz wie auch das Parlament gerne weitergegangen. Der Minister, Herr Jouyet, hat erwähnt, dass sich der französische Ratsvorsitz danach richten musste, ob ein Kompromiss erzielt werden konnte, obwohl er dasselbe wollte. Ich kann nur sagen, dass die Kommission versuchen wird, die Evaluierungsklausel und die Erwägung 6a gut umzusetzen. Daher hören wir auf den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres und versuchen, ihrem Wunsch nach einer gründlichen Revision des Rahmenbeschlusses nachzukommen, um eine Erweiterung seines Geltungsbereichs zu beurteilen. Das ist es, was die Kommission tun kann und was ich persönlich zu tun versuchen werde. Ich weiß, dass das Europäische Parlament eine baldige Revision anstrebt. Ich hoffe nur, der Rat wird einer Revision innerhalb eines Zeitrahmens zustimmen, der es ermöglicht, schon bald eine europäische Maßnahme zu entwickeln." (EP 2008c)

211 Siehe die Ausführungen von Ludford (Europäisches Parlament 2007). Siehe auch die Wortbeiträge von Alvaro, Dührkop, Ludford. Leichtfried und Lefrançois (EP 2008c).

212 Der amtierende Kommissar für Justiz, Freiheit und Sicherheit, Franco Frattini hatte im April 2008 bei den italienischen Parlamentswahlen kandidiert und trat Anfang Mai schließlich den Posten des Außenministers im Kabinett Berlusconi IV an, sodass der Kommissarsposten im selben Monat an Jacques Barrot überging, nachdem dieser den Posten zwei Monate lang bereits vertretungsweise ausgefüllt hatte (Barrot 2008, 2).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Diese Revision sollte schon weniger als ein Jahr später im Rahmen der Reform der EU-Vorschriften für den Schutz personenbezogener Daten erfolgen, an deren Ende wiederum die Verabschiedung der DSGVO und der JI-Richtlinie stehen sollte.

3.3.5 Novellierung der ePrivacy-RL zur Cookie-Richtlinie 2009/136/EG

Den Anfangspunkt der Debatten, die zur Novellierung der ePrivacy-RL führen sollten, bildete die Überprüfung der Lissabonner Strategie seitens des Europäischen Rates im März 2005. In diesem Rahmen wurde schließlich die Neubelebung der Strategie mit dem unabdingbaren Ziel der Priorisierung der Themen Wachstum und Beschäftigung entschieden. Angesichts der „Kluft zwischen dem Wachstumspotenzial Europas und dem seiner Wirtschaftspartner" (Europäischer Rat 2005b, 2) müsse Europa die „Grundlagen seiner Wettbewerbsfähigkeit erneuern, sein Wachstumspotenzial sowie seine Produktivität erhöhen und den sozialen Zusammenhalt stärken, indem es vor allem auf Wissen, Innovation und Erschließung des Humankapitals setzt." (ebd.) Als Kernpunkte der erneuerten Strategie wurden die Verbesserung der Politikgestaltung, die Reduzierung des Verwaltungsaufwands für die Wirtschaft und die Vollendung des Binnenmarktes identifiziert und die Europäische Kommission, der Ministerrat und die Mitgliedstaaten darum gebeten, die Neubelebung der Strategie in Gang zu setzen (ebd., 2 f.).

Der konkrete politische Prozess, der auch zur Überarbeitung der ePrivacy-Richtlinie führte, startete am 25. November 2005 (EC 2006b, 5). Die politische Verantwortung für den Gesamtprozess der Novellierung der EU-Telekommunikationspolitik hatte die EU-Kommissarin für Informationsgesellschaft und Medien, Viviane Reding (Luxemburg, CSV/EVP) und damit die Generaldirektion Informationsgesellschaft inne.[213] Im Rahmen einer ersten Konsultationsphase forderte die Kommission Stakeholder zur Einrei-

213 Bereits Anfang 2006 hatte die konservative Kommissarin Reding mit ihrem Vorstoß gegen die hohen internationalen Roaming-Gebühren der Telekommunikationsdienstleister und ihrer dabei vertretenen Überzeugung, einen bürgerfreundlichen Telekommunikationsmarkt zu schaffen, erfolgreich Aufmerksamkeit auf sich gezogen und sich als bürgernahe EU-Politikerin profiliert (Europäisches Parlament 2017; Reding 2006b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

chung von Stellungnahmen auf.[214] Im Ergebnis der knapp 160 schriftlichen Stellungnahmen, die eingingen, offenbarte sich, dass eine Überarbeitung des geltenden Rechtsrahmens von einer breiten Mehrheit der Stakeholder als erforderlich angesehen wurde. Die beiden auf Grundlage des Stakeholder-Inputs entwickelten Hauptvorschläge der Kommission waren die *Verwirklichung des strategischen Frequenzverwaltungskonzepts der Kommission* und die *Verringerung des Verwaltungsaufwands im Zuge der Vereinfachung der Verfahren im Zusammenhang mit der Überprüfung der Märkte, die für eine Vorabregulierung in Betracht kommen* (EC 2006c, 7). Daneben wurden die *Konsolidierung des Binnenmarktes*, die *bessere Wahrung der Verbraucher- und Nutzerinteressen*, die *Erhöhung der Sicherheit* und die *Aufhebung veralteter Vorschriften* vorgeschlagen (ebd.).

Die Kommission erachtete insbesondere eine größere Produkt- und Anbieterauswahl, innovative Dienste und ein besseres Preis-Leistungsverhältnis als zentrale Ziele im Rahmen der Verwirklichung echter Vorteile für die Verbraucher. Daneben wurden aber auch rechtliche Verpflichtungen für Bereiche wie Datenschutz als weitere Ziele definiert. Anders als in der früheren Telekommunikationsstrategie wurde zudem das Thema IT-Sicherheit als zentral erachtet. So begrüßte die Kommission die im Rahmen der Deregulierungspolitiken vollzogene Öffnung der Telekommunikationsmärkte als eine begrüßenswerte Entwicklung, die zu einer Steigerung des anbieterseitigen Wettbewerbs und dem Umstieg vieler Nutzerinnen und Nutzer auf IP-basierte Technologien geführt habe. In diesem Zusammenhang rechnete die Kommission den Themen Vertrauenswürdigkeit, Sicherheit und Zuverlässigkeit von Informations- und Kommunikationstechnologien eine zentrale Rolle im Hinblick auf ihre gesellschaftliche Akzeptanz und weitere Verbreitung zu. Des Weiteren stellte die Kommission fest, dass der Markt darin versagt habe, die Sicherheitsprobleme zur Zufriedenheit der Nutzerinnen und Nutzer zu lösen und die Zunahme von Spam, Viren,

214 Diese erste Konsultationsphase fand zwischen dem 25. November 2005 und dem 31. Januar 2006 statt. Auf diese folgte eine öffentliche Anhörung mit mehr als 440 Teilnehmern. Die Federführung hatte die GD Informationsgesellschaft bzw. das Referat B 1 „Politikentwicklung" inne (EC 2005, 2007c, 4). Wie schon bei den Konsultationen zur ePrivacy-Richtlinie partizipierten auch an dieser Konsultation zahlreiche Akteure, die später auch im Rahmen des Aushandlungsprozesses zur DSGVO eine wichtige Rolle spielen sollten: Aea Europe/TechAmerica, AmCham, BEUC, Bitkom, BSA, BT, ECTA, ETNO, EuroISPA, EPC, Google, Intel, Liberty Global Europe, GSM Europe, Microsoft, Nokia, Telefónica, UK Information Commissioner's Office (ICO), UNICE/Businesseurope (European Commission DG InfSo 2006).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Spyware und anderen Formen von Malware das Vertrauen der Nutzerinnen und Nutzer in elektronische Kommunikationsdienste verringere.

Ausgehend von Art. 4 der ePrivacy-Richtlinie, der Vorgaben zu den seitens des Verantwortlichen vorzunehmenden *geeigneten technischen und organisatorischen Maßnahmen* formulierte, wurde daher die Ausweitung und Stärkung der Sicherheitsvorgaben vorgeschlagen. Insbesondere ging es dabei darum, den konkreten Gehalt der seitens eines Verantwortlichen zu treffenden *geeigneten technischen und organisatorischen Maßnahmen* zu spezifizieren. Daneben unterbreitete die Kommission auch erstmals Vorschläge zum Umgang mit Verstößen gegen die (Netz-)Sicherheit: Sofern im Zuge eines Verstoßes gegen die Netzsicherheit der Verlust personenbezogener Daten die Folgen wäre, sollte der Verantwortliche dazu verpflichtet werden, die zuständige nationale Aufsichtsbehörde wie auch die Nutzerinnen und Nutzer über den Vorfall zu informieren. Sofern die Aufsichtsbehörde der Ansicht sei, dass der Vorfall das öffentliche Interesse berühre, solle sie zudem die Öffentlichkeit über die Sicherheitsverletzung informieren dürfen (EC 2006a, 28–30). Daneben identifizierten die Berichte der Kommission ein massives Problem im Bereich der Rechtsdurchsetzung: So führe der rechtliche Status Quo dazu, dass eine Sanktionierung selbst größerer Sicherheitsversäumnisse durch die zuständigen Aufsichtsbehörden regelmäßig aufgrund verschiedener Faktoren nicht möglich gewesen sei, da die Betreiber nach der Genehmigungsrichtlinie die Möglichkeit hätten, Verstöße zu beheben, bevor Sanktionen verhängt würden. Selbst wenn eine Aufsichtsbehörde bereits im Vorfeld einer konkreten Sicherheitsverletzung Versäumnisse festgestellt und den Betreiber darauf hingewiesen habe, der Betreiber die Hinweise jedoch ignorierte, sei es der Aufsichtsbehörde – aufgrund von Bestimmungen zu unlauteren kommerziellen oder wettbewerbswidrigen Praktiken – nicht möglich gewesen, den entsprechenden Betreiber für die Nicht-Einhaltung zu sanktionieren (ebd., 22). Infolge der Nicht-Sanktionierung und des sehr niedrigen Strafmaßes im seltenen Falle einer Sanktionierung hätten die Betreiber wiederum keinen ausreichenden Anreiz für die Einhaltung von Sicherheitsvorgaben gehabt, was in manchen Fällen zu einem ineffektiven oder unzureichenden Schutz personenbezogener Daten und der Privatsphäre geführt habe. Daher befürwortete die Kommission die Erweiterung der Befugnisse der Aufsichtsbehörden, Betreiber zur Umsetzung spezifischer, grundlegender Sicherheitsmaßnahmen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

verpflichten und sie ggf. auch sanktionieren zu können (ebd.).[215] Erstmals wurde seitens der Kommission im Kontext der Regelungen zum Datenschutz in der EU auch der Vorschlag eingebracht, die Strafhöhe ins Verhältnis zum Umsatz des jeweiligen Betreibers zu setzen und zu erwartende Strafen bei Verstößen im entsprechenden Gesetz bereits zu definieren. Daneben wurde auch erstmals ein Vorschlag eingebracht, der in Richtung eines Sammel- bzw. Verbandsklagerechts ging (ebd., 23).[216]

Mit der Veröffentlichung der Dokumente, in denen die oben skizzierte Strategie der Kommission bekanntgegeben wurde, leitete die Kommission zugleich die zweite Konsultationsphase ein, während der die Stakeholder dazu eingeladen wurden, die vorgenannten Vorschläge der Kommission zu kommentieren (EC 2007a, 4).[217] Die Art. 29-Datenschutzgruppe etwa begrüßte die Initiative der Kommission grundsätzlich, sah allerdings Verbesserungspotenzial in Bezug auf verschiedene Aspekte: Unter Verweis auf die Bedeutungszunahme privater Netzwerke im täglichen Leben und die Vermischung von privaten und öffentlichen Diensten plädierte die Datenschutzgruppe für die Überprüfung und ggf. Ausweitung des Geltungsbereichs der Richtlinie (Artikel 29-Datenschutzgruppe 2006, 3). In Bezug auf die angekündigte Verbesserung der Durchsetzungsmöglichkeiten

215 Die in diesem Zusammenhang für einzelne Unternehmen drohenden Kosten relativierte die Kommission unter Verweis auf den Gesamtnutzen für die Branche (EC 2006a, 34) Zudem machte die zuständige Kommissarin Viviane Reding auch deutlich, dass die Regulierung auch und gerade der Telekommunikationsmonopolisten fortgesetzt werde und steigende Kosten auf Unternehmensseite nicht als Grund für eine Deregulierung akzeptiert würden: „I firmly believe that the response to these challenges must be new and more successful business models, and certainly not protection, by regulators, from competition. I simply do not buy the argument that investment will only happen if we stop regulating monopolies." (Reding 2006a, 8)

216 „As regards the implementation of the e-Privacy Directive, new rules could be established providing for specific remedies (e.g. an explicit right of action against spammers, *possibly on behalf of consumers*)" (EC 2006a, 23, Hervorhebung in kursiv, M. K.).

217 Die zweite Konsultationsphase fand zwischen dem 29. Juni und dem 27. Oktober 2006 statt. Im Oktober 2006 wurde zudem ein öffentlicher Workshop unter Einbezug von Stakeholdern und Interessierten durchgeführt. Insgesamt 224 Antworten aus EU-Mitgliedstaaten und Drittländern gingen bei der Kommission ein (EC 2007c, 4). Auch diese Konsultation wurde von den Stellungnahmen privatwirtschaftlicher Akteure dominiert. Aus den Reihen der im Aushandlungsprozess zur DSGVO relevanten Akteure beteiligten sich: Aea Europe/TechAmerica, ACT, AmCham, BEUC, Bitkom, BSA, BT, ECTA, ETNO, EuroISPA, EPC, Google, GSM/GSMA Europe, Intel, Microsoft, Nokia, Telefónica, UK Information Commissioner's Office (ICO), UNICE/Businesseurope (EC 2007b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

seitens der Datenschutzaufsichtsbehörden verwies die Datenschutzgruppe vor allem auf die uneinheitliche Umsetzung der Richtlinie. Im Ergebnis verfügten einige der mitgliedstaatlichen Aufsichtsbehörden über unzureichende Ermittlungsbefugnisse, die „ihnen zum Beispiel keinen Zugriff auf die Kommunikationsdaten ermöglichen, die zum Nachweis eines Verstoßes gegen die Richtlinie erforderlich sind." (ebd., 4) Im Hinblick auf die mögliche Befugniserweiterung der Aufsichtsbehörden um die Verpflichtung von Diensteanbietern zur Ergreifung spezifischer Sicherheitsmaßnahmen äußerte sich die Datenschutzgruppe skeptisch. So seien die Anbieter bereits unter den geltenden Bestimmungen zur Umsetzung von Sicherheitsmaßnahmen verpflichtet bzw. stelle die Missachtung der Leitlinien der Aufsichtsbehörden längst einen Verstoß gegen die Richtlinie dar. Schließlich sei der Sektor „so beschaffen, dass den Datenschutzbehörden nicht möglich ist, Sicherheitsbestimmungen in Form verbindlicher Anweisungen festzulegen" (ebd., 6), da die Behörden nicht die Kapazitäten innehätten, den gesamten Sektor zu überwachen und Leitlinien zu sektorspezifischen Sicherheitsmaßnahmen zu veröffentlichen. Daher begrüße die Datenschutzgruppe stattdessen die Einführung der Meldepflicht von Sicherheitsverstößen, da dieses ein geeignetes Instrument dafür sei, die Anbieter zur Verabschiedung angemessener Schutzmaßnahmen zu motivieren. Jene Anbieter, die regelmäßig mit Sicherheitsvorfällen Negativschlagzeilen produzierten, würden von den Kundinnen und Kunden eher gemieden und an deren Stelle sichere Dienste eher genutzt. Insofern stelle die Meldepflicht ein *echtes marktgesteuertes Abschreckungsmittel* für diejenigen dar, die Sicherheitsvorschriften umgehen wollen (ebd.). Allerdings bemängelte die Datenschutzgruppe drei Aspekte der Kommissionsüberlegungen: *Erstens* müsse es den Aufsichtsbehörden ermöglicht werden, die Nichtanwendung der Meldepflicht zu sanktionieren. *Zweitens* stellten die vor allem aus den USA gemeldeten Sicherheitsverstöße (hier werden Choicepoint, LexisNexis, Bank of America und Time Warner genannt) kein Problem öffentlicher Internetdiensteanbieter, sondern privater Akteure wie Datenmakler, Banken und anderer Anbieter von Onlinediensten dar. Für eine wirksame Regelung sei es daher erforderlich, dass die Regelung nicht nur für die Betreiber öffentlicher Telekommunikationsdienste, sondern auch für private Diensteanbieter greife. Schließlich, *drittens*, müsse die Kommission in ihrem Legislativvorschlag Regeln für die Einteilung der Verstöße in Schweregrade und abgestufte Informationsverpflichtungen festlegen (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.5.1 Kommissionsentwurf

Die Kommission gab an, dass ihre datenschutzpolitischen Vorschläge vor allem seitens der Verbraucherorganisationen unterstützt wurden. Während die Datenschutzbehörden weitergehende Maßnahmen gefordert hätten, seien *einige Netzbetreiber und Dienstleister* vor allem aufgrund möglicher Folgekosten besorgt gewesen. Die Mitgliedstaaten hätten dagegen eine vorsichtige Unterstützung zum Ausdruck gebracht (ebd., 13). Im Ergebnis der Konsultation reduzierte die Kommission ihre datenschutzpolitischen Maßnahmenvorschläge etwas in ihrer Intensität, blieb aber grundsätzlich bei ihrer vorherigen Position, dass das Datenschutz- und Datensicherheitsniveau nicht in erster Linie durch Maßnahmen seitens des Individuums, sondern durch legislative und betreiberseitige Maßnahmen angehoben werden sollte. So sah der aktualisierte Maßnahmenkatalog auch weiterhin „mehr Verantwortung der Betreiber und NRB [nationalen Regulierungsbehörden, M. K.] für die Sicherheit und Integrität aller elektronischen Kommunikationsnetze und -dienste" (EC 2007a, 14) vor. Zwar wurde die angekündigte Erweiterung der Sanktionsbefugnisse der zuständigen Aufsichtsbehörden (und damit auch die Idee der Setzung der Strafhöhe ins Verhältnis zum Umsatz des Betreibers) gestrichen, doch wurden immer noch „größere Umsetzungs- und Durchsetzungsbefugnisse der zuständigen Behörden, insbesondere im Kampf gegen ‚Spam'" (ebd.) angekündigt. Schließlich bildete den Kern der datenschutzpolitischen Kommissionsvorschläge die Einführung einer Meldepflicht, wonach die Betreiber im Falle einer Schutzverletzung personenbezogener Daten infolge eines Verstoßes gegen die Netzsicherheit die Nutzer(-innen) über den Vorfall informieren sollten (ebd.). Gestrichen wurde jedoch die Pflicht zur Benachrichtigung der zuständigen Aufsichtsbehörde bzw. der Öffentlichkeit durch die Aufsichtsbehörde. Ihre Maßnahmenvorschläge begründete die Kommission damit, Verbraucherinteressen in der EU zu wahren: „Dazu ist unter anderem ein umfassender Schutz der personenbezogenen Daten und der Privatsphäre sicherzustellen und die Integrität und Sicherheit der öffentlichen Kommunikationsnetze zu gewährleisten. Angesichts der wachsenden Zahl elektronischer Bedrohungen in den letzten Jahren, etwa durch Viren, unerbetene Werbung (‚*Spam*'), Spähsoftware (‚*Spyware*') und das Ausspionieren persönlicher Zugangsdaten (‚*Phishing*'), sind diese Ziele heute wichtiger denn je." (ebd., 13, Hervorhebungen im Original)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zeitgleich mit der Bekanntgabe der Konsultationsergebnisse veröffentlichte die Kommission am 13. November 2007 auch ihren Richtlinienvorschlag,[218] der unter anderem die Änderung der ePrivacy-Richtlinie 2002/58/EG vorsah (EC 2007c). Darin wurden die folgenden fünf zentralen Änderungen an der ePrivacy-Richtlinie vorgeschlagen (ebd., 6):

(1) Im Rahmen der Änderung von Art. 3 Abs. 1 wurde intendiert, dass öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte (z. B. kontaktlos arbeitende RFID-Geräte) unterstützen, ebenfalls in den Anwendungsbereich der Richtlinie fallen.
(2) *Die Einführung einer Meldepflicht für Sicherheitsverletzungen, die zum Verlust oder zur Preisgabe personenbezogener Daten der Nutzer führen.* In Art. 4 Abs. 3 wurde vorgeschlagen, dass der *Teilnehmer* und die nationale Regulierungsbehörde unverzüglich benachrichtigt werden und dass die Benachrichtigung des Teilnehmers *zumindest eine Darlegung der Art der Verletzung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten* müssten. In der Meldung an die zuständige Aufsichtsinstanz sollte der Betreiber *zusätzlich die Folgen der Verletzung und die vom Betreiber nach der Verletzung ergriffenen Maßnahmen* darlegen. die Festlegung der Details *in Bezug auf die Umstände, Form und Verfahren der in diesem Artikel vorgeschriebenen Informationen und Benachrichtigungen* sollte dagegen nicht in der Richtlinie selbst, sondern auf Basis eines Ausschussverfahrens nach Konsultation der sog. Europäischen Behörde für die Märkte der elektronischen Kommunikation und des EDSB mittels technischer Durchführungsmaßnahmen erfolgen.
(3) Mit der Änderung von Art. 5 Abs. 3 wurden die Bedingungen festgelegt, die gölten, wenn ein Zugriff auf Informationen oder die Speicherung von Informationen im Endgerät des Nutzers (u. a. mittels Cookies) erfolgt. Demnach sollten die Nutzer gemäß der DS-RL klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhalten und die Möglichkeit haben, einer derartigen Verarbeitung umstandslos widersprechen zu können.

218 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(4) Mit der Ergänzung von Art. 13 um den Abs. 6 wurde insbesondere Internet-Diensteanbietern die Möglichkeit eingeräumt, gegen Spam-Versender wegen Missbrauchs ihrer Netze oder gegen Stellen, die Sender-Adressen fälschten oder Server hackten, um sie als Spam-Relays zu missbrauchen, rechtlich vorzugehen.
(5) Während die ePrivacy-Richtlinie 2002/58/EG selbst keine ausdrücklichen Bestimmungen zur Durchsetzung enthielt, sondern stattdessen lediglich auf den Abschnitt zur Durchsetzung in der DS-RL verwies, wurde mit der Hinzufügung von Art. 15a die ausdrückliche Regelung der Materie im Rahmen der ePrivacy-Richtlinie vorgeschlagen.

3.3.5.2 Stellungnahmen des EDSB und der Art. 29-Datenschutzgruppe

Der Europäische Datenschutzbeauftragte veröffentlichte seine Stellungnahme am 10. April 2008 (EDSB 2008) und die Art. 29-Datenschutzgruppe ihre Stellungnahme am 15. Mai 2008 (Artikel 29-Datenschutzgruppe 2008). Beide Institutionen begrüßten den Kommissionvorschlag zur Änderung der ePrivacy-Richtlinie grundsätzlich: Besonders die mit der Änderung von Art. 3 vorgeschlagene Ausweitung des Anwendungsbereichs auf RFID, die Cookie-/Spyware-Regelungen mit der Änderung von Art. 5 Abs. 3 sowie die im Rahmen von Art. 15a vorgeschlagenen Änderungen im Hinblick auf die Verbesserung der Durchsetzung (Artikel 29-Datenschutzgruppe 2008; EDSB 2008, 13). Zudem begrüßten beide Institutionen die von der Kommission vorgeschlagene Klärung der Details bzgl. der Umstände, der Form und Verfahren der Meldung von Verletzungen des Schutzes personenbezogener Daten im Rahmen des Ausschussverfahrens (Artikel 29-Datenschutzgruppe 2008, 4; EDSB 2008, 13). Die Art. 29-Datenschutzgruppe kritisierte lediglich, dass sie nicht unter den zu konsultierenden Akteuren aufgelistet worden war und hob die Notwendigkeit ihres Einbezugs hervor (Artikel 29-Datenschutzgruppe 2008, 4). Trotz der Begrüßung der Einführung der Meldepflicht bei Datenschutzverletzungen bemängelten beide Institutionen, dass die vorgesehenen Regelungen ausschließlich für die Anbieter öffentlicher elektronischer Kommunikationsdienste gelten würden, nicht aber für die Anbieter von Diensten der Informationsgesellschaft (wie Online-Banken, Daten-Broker, Online-Unternehmen, Online-Anbieter von Gesundheitsdiensten usw.). Entsprechend vertraten beide Institutionen die Position, dass Art. 4 Abs. 3 dahingehend abzuändern sei, dass die Meldepflicht auch bei Diensten der Informationsgesellschaft greife

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(Artikel 29-Datenschutzgruppe 2008, 3; EDSB 2008, 12).[219] In ähnlicher Weise begrüßte der EDSB zwar die Ergänzung der ePrivacy-Richtlinie um das in Art. 13 Abs. 6 vorgeschlagene Recht, das juristische Personen, und damit vor allem die Anbieter elektronischer Kommunikationsdienste, aber auch Verbraucherverbände und Gewerkschaften, die die Interessen Spam-geschädigter Verbraucher verträten, in die Lage versetzen würde, gerichtlich gegen Spam-Versender vorzugehen. Doch wurde das Fehlen der Möglichkeit von Sammelklagen kritisiert, mittels derer eine Gruppe von von Spam betroffener Nutzerinnen und Nutzer gemeinsam gegen den Spam-Versender hätten vorgehen können. Schließlich begrüßten beide Institutionen die Ausweitung des Anwendungsbereichs auf RFID-fähige Geräte, doch bedauerten sie zugleich, dass der Kommissionsvorschlag die Problematik der sich in zunehmendem Maße verwischenden Unterscheidung zwischen privaten und öffentlichen Netzen unberücksichtigt ließ. Aufgrund der wachsenden Bedeutung gemischter (privater/öffentlicher) und privater Netze im täglichen Leben und aufgrund des dabei entstehenden Risikos für personenbezogene Daten forderten die Institutionen die Ausweitung des Anwendungsbereichs der ePrivacy-Richtlinie auch auf jene Anbieter. Bemängelt wurde seitens sowohl des EDSB als auch der Datenschutzgruppe zudem, dass sich das in Art. 13 vorgesehene Verbandsklagerecht lediglich auf Situationen beschränkte, in denen die in Art. 13 festgelegten Bestimmungen hinsichtlich unerbetener E-Mails verletzt würden, Verstöße gegen andere Bestimmungen der ePrivacy-Richtlinie jedoch unberücksichtigt blieben (Artikel 29-Datenschutzgruppe 2008, 6; EDSB 2008, 10 f.). Darüber hinaus betonte die Datenschutzgruppe im Hinblick auf ihre Befürwortung eines standardmäßig hohen Datenschutzniveaus die Bedeutung des Prinzips der Datensparsamkeit und des Einsatzes datenschutzfreundlicher Technologien und forderte die Festlegung dieser Prinzipien in Art. 1 der Richtlinie (Artikel 29-Datenschutzgruppe 2008, 6). Schließlich vertrat die Datenschutzgruppe unter Bezugnahme auf eine ihrer Stellungnahmen (Artikel 29-Datenschutzgruppe 2007) die Position, dass IP-Adressen im Zweifel als personenbezogene Daten zu behandeln seien (ebd., 6 f.).

219 Unterstützt wurde der Vorschlag auch seitens Privacy International (PI 2011, 6).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.5.3 Position des Europäischen Parlaments

Das Europäische Parlament entschied über das Verfahren zur Erarbeitung der Parlamentsposition Ende 2007. Zum federführenden Ausschuss wurde der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO-Ausschuss) unter Berichterstatter Malcolm Harbour (Vereinigtes Königreich, Conservative Party/EVP bzw. EKR)[220] benannt.[221] Für die Datenschutzaspekte des Richtlinienvorschlags war der LIBE-Ausschuss (seit dem 13. März 2008 auch als assoziierter Ausschuss) zuständig. Die Aufgabe des Berichterstatters übernahm erneut Alvaro. Überdies waren am Verfahren die Ausschüsse ECON, ITRE, CULT und JURI mitberatend tätig (Harbour und Alvaro 2008, 251). Der LIBE-Ausschuss nahm seine Stellungnahme am 26. Juni 2008 an und der Entwurf der Parlamentsstellungnahme wurde schließlich am 18. Juli 2008 angenommen (ebd.). Der Harbour-Bericht fand im Europäischen Parlament eine breite Mehrheit. Nachdem einige der Änderungswünsche der Sozialdemokraten (vgl. hierzu die Plenardebatte in: EP 2008b, 67 ff.) berücksichtigt worden waren und diese dem Bericht zugestimmt hatten, wurde der geänderte Berichtsvorschlag am 24. September 2008 mit den Stimmen der Fraktionen ALDE, EVP-DE, SPE und UEN, die praktisch geschlossen für den Bericht stimmten, mit 561 Für-Stimmen angenommen. Die 99 Gegenstimmen setzten sich vor allem aus den Stimmen der GUE/NGL, der Grünen/EFA und IND/DEM sowie einiger fraktionsloser Europaabgeordneter zusammen, während sich die 13 Enthaltungen auf verschiedene Fraktionen verteilten (EP 2008a, 123 f.). Die Grüne Fraktion bemängelte insbesondere einige der die Richtlinie 2002/22/EG betreffenden Vorschläge (etwa hinsichtlich urheberrechtspolitischer Änderungen, die mit einer Filterung des Internets einhergehen sollten) des Berichterstatters Harbour (vgl. z. B. die Äußerungen Staes' in: EP 2008d). Im Hinblick auf den Alvaro-Bericht kritisierten die Grünen (z. B. Rebecca Harms) den Nicht-Einbezug von IP-Adressen. Die GUE/NGL teilte die Kritik an den urheberrechtspolitischen Maßnahmen, kritisierte aber darüber hinaus auch

220 Harbour war bereits beim ursprünglichen Universaldienste-Richtlinienvorschlag 2001 Berichterstatter (Harbour und Alvaro 2008, 114). Bis zur Europawahl 2009 gehörte Harbour der EVP an, schloss sich nach der Wahl jedoch der neu gegründeten nationalkonservativen bzw. EU-skeptischen Fraktion EKR an (EP 2020d).

221 Der größere Teil der Änderungen betraf die Richtlinie über den Universaldienst und die Nutzerrechte. Die ePrivacy-Richtlinie war dagegen von einer vergleichsweise kleinen Zahl von Änderungen betroffen. Daher wurde der für Verbraucherschutzfragen zuständige IMCO-Ausschuss mit der Hauptverantwortung der Berichterstellung betreut (Harbour und Alvaro 2008, 114 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die aus ihrer Perspektive generelle Fokussierung der Parlamentsposition auf die Wünsche der Wirtschaft (vgl. die Äußerungen Svenssons und de Brúns in: EP 2008a, 84 und 98; vgl. auch die Äußerungen Droutsas' in: 2008d).

3.3.5.3.1 Inhalt der Parlamentsposition

Folgende Änderungsvorschläge finden sich in der verabschiedeten Parlamentsposition: So sollten beispielsweise jüngste Entwicklungen im Verfassungsrecht der Mitgliedstaaten – durch einen Verweis auf das *Recht auf Vertraulichkeit und Sicherheit der Systeme der Informationstechnologie* gemäß der Änderungsanträge 1 und 16 – berücksichtigt werden. Das Parlament befürwortete zudem die Ergänzung des EG 34 um eine Passage hinsichtlich der Ermutigung der Endnutzer zu Selbstdatenschutzmaßnahmen (ebd., 229 f., Änderungsantrag 37).

Unter Bezugnahme auf die Stellungnahmen der Art. 29-Datenschutzgruppe und des EDSB trat das Parlament zudem für die Ausweitung des Anwendungsbereichs der ePrivacy-Richtlinie auf private Kommunikationsnetze sowie auf öffentlich zugängliche private Netze ein (vgl. Änderungsantrag 18). In diesem Zusammenhang forderte das Parlament auch die Ausweitung der Klagemöglichkeiten juristischer Personen, nicht nur bei Verstößen gegen Art. 13, also im Falle unerbetener Nachrichten, sondern bei jeglichen Verstößen gegen die Bestimmungen der ePrivacy-Richtlinie gerichtlich vorgehen zu können. Nicht übernommen wurde jedoch die Forderung der Datenschutzgruppe nach Einführung eines Sammelklagerechts (vgl. Änderungsantrag 31). Im Hinblick auf die Meldepflicht bei Datenschutzverletzungen folgte das Parlament ebenfalls der Position der Datenschützer und forderte die Ausweitung des Umfangs der Verpflichtung auf Dienste der Informationsgesellschaft (vgl. Änderungsantrag 20). Dagegen rückte das Parlament von der Spezifizierung der Details bzgl. der Umstände, der Form und Verfahren der Meldung im Rahmen des Ausschussverfahrens, die von der Kommission vorgeschlagen worden war, ab und trat für eine unmittelbare Spezifizierung der entsprechenden Punkte in der Richtlinie ein. Im Gegensatz zur Kommission plädierte das Parlament dabei für eine Zwei-Stufen-Meldepflicht: Damit es nicht zu einer Überforderung der Nutzerinnen und Nutzer aufgrund zu häufiger Meldungen komme, sollte die Meldung nicht mehr zeitgleich an die zuständige Aufsichtsbehörde und die Betroffenen erfolgen. Stattdessen sollte eine Verletzung zunächst unverzüglich an die zuständige Aufsichtsbehörde gemeldet

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

werden, die daraufhin auf Grundlage der Ernsthaftigkeit der entstandenen Verletzung die Notwendigkeit der Benachrichtigung der Betroffenen prüfen und den Verantwortlichen zu einer Meldung auffordern können sollte (vgl. Änderungsantrag 21). Gemäß des Änderungsantrags 22 sollte der Ernst einer Verletzung, die eine Benachrichtigung erforderlich mache, nach „den Umständen der Verletzung bestimmt [werden], z. B. dem Risiko für die von der Verletzung betroffenen personenbezogenen Daten, der Art der von der Verletzung betroffenen Daten, der Zahl der betroffenen Teilnehmer und der unmittelbaren oder potenziellen Auswirkungen der Verletzung auf die Bereitstellung der Dienste." (ebd., 238) Schließlich sah der Änderungsantrag 23 die Befreiung von der Benachrichtigungspflicht der Betroffenen vor, sofern der Verantwortliche nachweisen könne, „dass aufgrund der Anwendung geeigneter technologischer Schutzmaßnahmen nach vernünftigem Ermessen kein Risiko für die von der Verletzung betroffenen personenbezogenen Daten besteht." (ebd.) Nachdem das Parlament im Rahmen der Verhandlungen der ePrivacy-Richtlinie noch keine Einigung bezüglich der Einwilligung im Kontext von Cookies hatte erzielen können und am Ende lediglich ein Kompromiss, der die Entscheidung den Mitgliedstaaten überließ, verabschiedet worden war (vgl. 3.3.2), einigten sich die Fraktionen im Rahmen der Richtliniennovelle darauf, dass die vorherige Einwilligung der Betroffenen verpflichtend sein sollte, doch wurde zugleich vorgesehen, dass bereits eine entsprechende Browser-Einstellung eine solche vorherige Einwilligung darstellen können sollte (vgl. Änderungsantrag 25).

3.3.5.3.2 Geänderter Vorschlag der Kommission

Nachdem das Parlament seine Position verabschiedet hatte, veröffentlichte die Kommission am 6. November 2008 einen geänderten Richtlinienvorschlag (EC 2008), in dessen Rahmen einige der Änderungen des Parlaments akzeptiert, dessen zentralen Forderungen jedoch abgelehnt wurden. So folgte die Kommission weder dem Wunsch des Parlaments und der Datenschutzbehörden, nach der Ausweitung des Anwendungsbereichs der Richtlinie auf private Kommunikationsnetze sowie auf öffentlich zugängliche private Netze noch dem Wunsch nach der Ausweitung der Meldepflicht bei Datenschutzverstößen auf Dienste der Informationsgesellschaft. In ähnlicher Weise wurde auch die vom Parlament geforderte Ausweitung der Klagemöglichkeiten juristischer Personen, wonach das Verbandsklagerecht nicht nur bei Verstößen gegen Art. 13, sondern bei jeglichen Verstößen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gegen die Bestimmungen der ePrivacy-Richtlinie greifen können sollte, abgelehnt (ebd., 29).

Die vom Parlament vorgeschlagene Spezifizierung der Umstände, der Form und Verfahren der Meldung sowie das vorgeschlagene Zwei-Stufen-Modell wurden dagegen in modifizierter Form übernommen. So sollte die unverzügliche Meldung an die Behörde in jedem Fall (siehe Abänderung 187rev und 184) sowie die unverzügliche Meldung an die Betroffenen grundsätzlich immer erfolgen, sofern die zuständige Aufsichtsbehörde keine Ausnahme genehmige. Eine Verletzung des Schutzes personenbezogener Daten sollte gemäß der Kommissionsposition immer dann vorliegen, sobald es zu einer „unbeabsichtigten oder unrechtmäßigen Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von oder zum Zugang zu personenbezogenen Daten" (vgl. neuen Art. 2 lit. i) komme. Die vom Parlament vorgeschlagene (Änderungsvorschlag 125) Spezifizierung der Ernsthaftigkeit einer Verletzung, die eine Benachrichtigung erforderlich mache, wurde dagegen nicht übernommen. Nach der Kommission sollte diese Spezifizierung im Ermessen der Aufsichtsbehörden liegen (ebd., 25 f., 3a. und 3b.).

Ein weiterer Vorschlag der abgelehnt wurde, war Änderungsvorschlag 128, wonach eine Browsereinstellung als Einwilligung gelten können sollte. Die vom Parlament eingebrachten Verweise auf das *Recht auf Vertraulichkeit und Sicherheit der Systeme der Informationstechnologie* wurden ebenfalls ersatzlos gestrichen (ebd., 9 und 29).

Mit kleineren Änderung angenommen wurde der Änderungsantrag 37, wonach die Endnutzer mittels öffentlicher Aufklärungskampagnen zu Selbstdatenschutzmaßnahmen ermutigt werden sollten (ebd., 9 f.).

3.3.5.4 Gemeinsamer Standpunkt des Ministerrats

Der Ministerrat setzte sich erstmals im Rahmen des Ratstreffens „Verkehr, Telekommunikation und Energie" Ende November bzw. Anfang Dezember 2007 mit dem Richtlinienvorschlag der Kommission auseinander, behandelte jedoch zunächst lediglich die nicht den Datenschutz betreffenden Elemente des Telekom-Reformpakets (Council of Ministers 2007, 9 f.). Auf der Arbeitsebene lag die Zuständigkeit für die Erarbeitung des Gemeinsamen Standpunkts des Ministerrats bei der Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft" (Gruppe „Telekommunikation und Informationsgesellschaft" 2008). Mitte 2008 kristallisierte sich schließlich allmählich die finale Position des Rats heraus. So wurden die von der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommission mit der Reform verfolgten politischen Ziele hinsichtlich der Stärkung der Rechte der Verbraucher und des Schutzes personenbezogener Daten zwar begrüßt, im Hinblick auf die von der Kommission vorgebrachten konkreten Änderungsvorschläge verwies der Ministerrat jedoch auf die Notwendigkeit „to maintain an appropriate balance of proportionality and subsidiarity, as well as to avoid unnecessary burdens for both national regulatory authorities and the undertakings concerned while ensuring competition and benefits for end-users." (Council 2008, 8) Der Rat gab an, dass in Bezug auf die ePrivacy-Richtlinie zu diesem Stadium Fragen betreffend die Sicherheit der Verarbeitung und Fragen bezüglich der Umsetzung und Durchsetzung ungeklärt seien (ebd.). Die zuständigen Minister konnten schließlich zunächst Ende November 2008 eine politische Einigung im Rat erzielen (EU-Ministerrat 2008b, 9) und verabschiedeten den Gemeinsamen Standpunkt des Ministerrats schließlich am 16. Februar 2009 (EU-Ministerrat 2009b).

Die von Kommission, Parlament sowie den Datenschutz-Institutionen befürwortete Klarstellung, dass der Anwendungsbereich neue Technologien wie RFID umfasse, wurde auch vom Ministerrat übernommen (ebd., 19, EG 44). Nicht übernommen wurde dagegen die von den Datenschutz-Institutionen und dem Parlament geforderte Ausweitung des Anwendungsbereichs der Richtlinie auf private Kommunikationsnetze und auf öffentlich zugängliche private Netze. Ebenso wurde auch die Ausweitung des Umfangs der Verpflichtung zur Meldung von Datenschutzverletzungen auf Dienste der Informationsgesellschaft vom Ministerrat nicht übernommen. Zudem machte der Ministerrat Änderungsvorschläge, die zu einer deutlichen Schwächung der Verpflichtung geführt hätten. So sollte eine Meldung an die *Teilnehmer*[222] nur im Falle einer ernsthaften Bedrohung der Privatsphäre erfolgen müssen. Zu einer solchen ernsthaften Bedrohung zählte der

222 Dem ursprünglichen Kommissionsvorschlag gemäß, sollten lediglich die *Teilnehmer* eines Dienstes im Falle einer Datenschutzverletzung benachrichtigt werden. Nachdem die Art. 29-Datenschutzgruppe darauf hingewiesen hatte, dass der Begriff des Teilnehmers in einigen Fällen, in denen es sich bei dem Betroffenen formal nicht um einen Teilnehmer handele, zu einer Nicht-Benachrichtigung führen könnte (Artikel 29-Datenschutzgruppe 2008, 3), änderten das Parlament und die Kommission die entsprechenden Textstellen (vgl. Änderungsantrag 123, in: Harbour und Alvaro 2008, 92; vgl. Abänderung 187rev und 184, in: EC 2008, 25). Lediglich der Ministerrat blieb beim Begriff des Teilnehmers, äußerte sich gleichzeitig im Rahmen seiner Begründung aber ansonsten nicht zu dieser Entscheidung (EU-Ministerrat 2009a) und nahm somit die daraus resultierende Schutzlücke in Kauf (EU-Ministerrat 2009b, 55).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ministerrat u. a. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschaden (ebd., 21, EG 47). Zudem sollte entgegen der von allen anderen beteiligten Akteuren vertretenen Position nicht die für einen Dienstleister zuständige Aufsichtsbehörde darüber entscheiden, ob eine Mitteilung an die Teilnehmer erfolgen solle oder nicht, sondern der Dienstleister selbst. Dadurch, dass dem Dienstleister auch die Entscheidung über die Benachrichtigung der zuständigen Aufsichtsbehörde überlassen bleiben sollte, wäre die Meldepflicht schließlich jeglicher Kontrollmöglichkeit beraubt worden, sodass ein Verantwortlicher selbst ernsthafte Sicherheitsverletzungen hätte verschweigen können (ebd.).[223] Auch die von den Datenschutz-Institutionen und dem Parlament befürwortete Ausweitung der von der Kommission in Art. 13 Abs. 6 vorgeschlagenen Verbandsklage auf alle Verstöße gegen die ePrivacy-Richtlinie – sowie die besonders vom EDSB geforderte Einführung eines Sammelklagerechts – wurde vom Ministerrat überhaupt nicht aufgegriffen (ebd., 61). Im Hinblick auf den Umgang mit Cookies folgte der Rat der Kommission und sah neben der verpflichtenden Information der Nutzerinnen und Nutzer seitens des Verantwortlichen u. a. über die Zwecke der Verarbeitung auch die Einholung der Einwilligung des Nutzers für die Platzierung bspw. eines Cookies vor (ebd., 57).

Wesentlich weitreichender als die datenschutzrechtlichen Meinungsunterschiede waren jedoch die Unterschiede in den Positionen der Organe im Hinblick auf die übrigen, den Verordnungsvorschlag zur Einrichtung eines Regulierungsgremiums und den Richtlinienvorschlag zur besseren Rechtsetzung betreffenden, Elemente des Telekom-Reformpakets, auf die an dieser Stelle aber nicht weiter eingegangen werden soll (Bundesnetzagentur 2009, 56 ff. EC 2009b, 3 f.).[224]

223 Der Erwägungsgrund 47 sah zudem vor, dass der Dienstleister nicht verpflichtet sein sollte, den Teilnehmer zu benachrichtigen, sofern er der zuständigen Aufsichtsbehörde glaubhaft machen konnte, „dass er geeignete technische Schutzmaßnahmen für die betroffenen Daten ergriffen hat und diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewandt wurden. Diese technischen Schutzmaßnahmen sollten die Daten für alle unbefugten Personen verschlüsseln." (EU-Ministerrat 2009b, 21)

224 Erwähnt sei lediglich die Diskussion zu urheberrechtspolitischen Fragen im Kontext der sehr kontrovers geführten europäischen Debatte zum Thema der Internetsperren. Die Debatte wurde vor allem von der konservativen französischen Regierung unter Nicolas Sarkozy vorangetrieben, die im Inland über das HADOPI-Gesetz beriet, mittels dessen eine sog. *three-strikes*-Regelung eingeführt werden sollte. So sollte nach zwei Verwarnungen infolge von Urheberrechtsverstößen ohne weitere

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.5.5 Einigung im Trilog und Verabschiedung des Kompromisstextes

Wie in derartigen Fällen üblich, vereinbarten Kommission, Parlament und Rat den Beginn informeller Trilog-Verhandlungen, um noch vor der zweiten Lesung des Parlaments und des Rates einen Kompromiss zu erzielen. Der Trilog wurde unverzüglich nach der am 16. Februar erfolgten Annahme des Gemeinsamen Standpunkts des Ministerrats einberufen und tagte bis Ende April (Council Presidency 2009). Den schwierigsten Teil der Verhandlungen bildete die Frage nach der Meldepflicht bei Datenschutzverstößen. Das Parlament blieb hartnäckig bei seiner Forderung nach dem Einbezug von Diensten der Informationsgesellschaft, der Rat und die Kommission vertraten dagegen die Position, dass der Anwendungsbereich der sektorspezifischen ePrivacy-RL klar auf den Bereich der elektronischen Kommunikation begrenzt bleiben sollte. Kommission und Ministerrat verwiesen das Parlament im Zusammenhang mit der Ausweitung des Anwendungsbereichs auf die mögliche Revision der DS-RL 95/46/EG (Council 2009, 4). Somit wurden letztlich alle vom Parlament und den Datenschutz-Institutionen befürworteten Elemente im Hinblick auf die Ausweitung des Anwendungsbereichs der Richtlinie verworfen: Dies betraf zunächst die Definition des Anwendungsbereichs in Art. 3, darüber hinaus die Meldepflicht bei Datenschutzverstößen in Art. 4 sowie die vorgeschlagene Ausweitung des Verbandsklagerechts aus Art. 13 auf alle Artikel der Richtlinie.

Bei den übrigen umstrittenen Elementen der Meldepflicht konnte allerdings ein Kompromiss erzielt werden: Die vom Rat gewünschte Ermächtigung der Verantwortlichen, selbst über eine Benachrichtigung zu entscheiden, wurde gestrichen. Stattdessen wurde den Positionen der Kommission und des Parlaments entsprechend gemäß Art. 4 Abs. 3 festgelegt, dass im Falle einer Verletzung die zuständige Aufsichtsbehörde unverzüglich zu benachrichtigen sei. Die Kommission und das Parlament konnten sich zudem auch in Bezug auf die Anforderung, wer zu benachrichtigen sei, durchsetzen. So sollten nicht nur – wie vom Rat gefordert – Teilnehmer, sondern *Teilnehmer* und *Personen* unverzüglich benachrichtigt werden, sofern anzunehmen sei, dass durch eine Schutzverletzung deren personenbezogenen Daten oder Privatsphäre beeinträchtigt würden. Dem Vorschlag des Rates entsprechend wurde zudem festgelegt, dass die Pflicht zur Benachrichtigung entfallen sollte, sofern der Verantwortliche „zur Zufriedenheit

richterliche Überprüfung der Internetzugang von Beschuldigten gesperrt werden können (Filippi und Bourcier 2016).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der zuständigen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden." (ebd.)[225]

Im Hinblick auf den in Art. 5 geregelten Umgang mit Cookies wurde lediglich die Opt-in-Pflicht vereinbart und der vom Parlament befürwortete Verweis auf Browser-Einstellungen gestrichen. In der Öffentlichkeit führte diese Verpflichtung zum Opt-in noch kurz vor der Verabschiedung der Richtlinie zu einigen Pressemeldungen, in denen aufgrund der Cookie-Regelung eine unnötige Verkomplizierung der Internetnutzung befürchtet wurde. Auf Spiegel Online war beispielsweise zu lesen, dass die Einwilligungspflicht zu *endlosen Pop-up-Kaskaden* führen werde (Patalong 2009). Insbesondere Akteure aus der Wirtschaft, darunter ein Zusammenschluss verschiedener auf EU-Ebene tätiger Lobbyverbände[226], warnten vor den wirtschaftlichen Folgen aufgrund der zu befürchtenden negativen Auswirkungen auf das Benutzererlebnis (EPC 2009). In der Folge wichen mehrere Mitgliedstaaten von der Verpflichtung zum Opt-in ab und setzen die Vorgabe praktisch als eine Opt-out-Lösung um (A. Schneider 2014).

Schließlich wurden die im politischen Aushandlungsprozess weitgehend unumstrittenen Elemente hinsichtlich der Klarstellung, dass neue Technologien wie RFID in den Anwendungsbereich der Richtlinie fallen sollten, (EG 56) und die Aktualisierung der Vorgaben zur Umsetzung und Durchsetzung (Art. 15) ebenfalls verabschiedet.

In der Folge nahm das Parlament den Kompromisstext am 6. Mai 2009 in zweiter Lesung bei 493 zu 130 Stimmen und 6 Enthaltungen an. Die Fraktionsfronten blieben dieselben, wie sie es bereits bei der ersten Lesung waren: Auf der Seite der Befürworter fanden sich ALDE, EVP-DE, SPE sowie UEN. Auf der Gegenseite fanden sich GUE/NGL, Grüne/EFA und IND/DEM sowie mehrere fraktionslose Abgeordnete und einige Abweichler aus den Reihen der EVP-DE und der SPE (EP 2009c, 9, Nr. 14; epic.org 2009, 65 f.). Nachdem auch der Rat den Kompromisstext am 26. Oktober 2009 angenommen hatte, wurde die *Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und*

225 Wobei diese Regelung freilich etwas paradox ist. Wenn der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsnetzes eine Schutzverletzung sowohl der zuständigen Aufsichtsbehörde als auch den Betroffenen unverzüglich mitzuteilen hat, bleibt dem Betreiber eigentlich keine Zeit, die Aufsichtsbehörde hinsichtlich der Nicht-Benachrichtigung zu konsultieren. So müsste der Betreiber in Kauf nehmen, seine Meldepflicht gegenüber dem Betroffenen ggf. nicht zu erfüllen.

226 Beteiligt waren u. a. ENPA, EPC, FEDMA, WFA, IAB und EuroISPA (EPC 2009).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, die aufgrund der enthaltenen Cookie-Regelung auch den Beinamen *Cookie-Richtlinie* erhalten sollte, am 25. November 2009 von den Präsidenten des Europäischen Parlaments und des Ministerrats unterzeichnet und damit erfolgreich verabschiedet (EU 2009).

3.3.5.6 Zwischenfazit

Die Verhandlungen zur Cookie-Richtlinie stellten die letzte politische Auseinandersetzung vor Beginn der Datenschutzreform dar. Während bei der Aushandlung der DS-RL noch die Frage im Raum gestanden hatte, ob gemeinschaftsweite Datenschutzregelungen überhaupt erforderlich sind, war diese Frage im Rahmen der Aushandlung der ePrivacy-RL zugunsten von inhaltlichen Punkten etwas in den Hintergrund gerückt. Im Kontext der ePrivacy-RL-Novelle erreichte die datenschutzpolitische Debatte nunmehr eine neue Qualität: Die verantwortliche Kommissarin Viviane Reding agierte auf Basis ihrer Policy-Kernüberzeugung, dass Datenschutz zu mehr Vertrauen in digitale Dienste und dadurch zu gesteigertem wirtschaftlichen Erfolg führe, als Policy-Entrepreneurin und forcierte die Anhebung des Datenschutzniveaus im Bereich der elektronischen Kommunikation vor allem durch die Stärkung der Verarbeiterpflichten und die Entlastung der Betroffenen. Kernelemente dieser Politik waren die Einführung der Meldepflicht bei Datenschutzverstößen sowie die Einführung des Verbandsklagerechts. Mit der Einführung der Opt-in-Pflicht wurde zudem angestrebt, die informationelle Selbstbestimmung der Betroffenen im Zusammenhang mit Cookies besser zu gewährleisten.

Weitergehende Forderungen, vor allem des Europäischen Parlaments, hinsichtlich der Ausweitung des Anwendungsbereichs der Cookie-Richtlinie (und damit der Meldepflicht bei Datenschutzverstößen sowie des Verbandsklagerechts) auf alle Dienste der Informationsgesellschaft konnten sich zwar nicht durchsetzen. Die Vertröstung des Parlaments unter Verweis auf die mögliche anstehende Revision der DS-RL verdeutlichte jedoch, dass eine Reform des Datenschutzrahmens in greifbare Nähe gerückt war.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.3.6 Fazit

Der vorangegangene Abschnitt 3.3 zur EU-Datenschutzpolitik seit der Jahrtausendwende hat die relevantesten datenschutzpolitischen Auseinandersetzungen in Gestalt der ePrivacy-RL, des ersten Berichts zur Überprüfung der DS-RL, der Bestimmungen im Sicherheitsbereich (darunter die EU-Richtlinie zur Vorratsdatenspeicherung, der Zugriff auf Fluggastdaten sowie die Erarbeitung des JI-Rahmenbeschlusses) sowie der Cookie-RL untersucht. Die der Untersuchung zugrundeliegende Zielsetzung war die Identifikation der langfristig relevanten Kontextbedingungen der EU-Datenschutzpolitik.

So hat die Untersuchung der Verabschiedung der ersten internationalen Datenschutz-Instrumente in Abschnitt 3.1 und insb. die Entstehung der DS-RL in Abschnitt 3.2 zuvor gezeigt, dass die Entstehung der ersten Datenschutz-Bestimmungen zunächst vor allem im Spannungsfeld zwischen Grundrechtsschutz und der wirtschaftlichen Bedeutung der Datenverarbeitung im Zusammenhang mit der Ermöglichung gemeinschaftsweiter grenzüberschreitender Datentransfers eingebettet war. Die aus dieser Spannung resultierende Kontroverse hatte jedoch schließlich zu einem Stillstand während der Verhandlungen zur DS-RL geführt. Die Überwindung der Pattsituation war letztlich vor allem dadurch möglich, dass die Gegner der Einführung von Datenschutzregelungen mittels des Arguments, dass Datenschutz als vertrauensbildende Maßnahme fungieren und zu mehr wirtschaftlichem Erfolg beitragen würde, überzeugt werden konnten. Diese Überzeugung sollte seit Mitte der 1990er-Jahre als Bindeglied zwischen Datenschutzbefürwortern und Datenschutzgegnern fungieren und zu einer relativen De-Radikalisierung der jeweiligen Standpunkte beitragen.

So gaben die Gegner von Datenschutzregelungen ihre prinzipielle Ablehnung größtenteils auf und arrangierten sich mit der Einführung von Datenschutz-Gesetzen.[227] Die Datenschutzbefürworter hingegen rückten teilweise von ihrer stark grundrechtsorientierten Haltung ab und arrangierten sich damit, dass zur Verabschiedung von Datenschutzgesetzen das Eingehen von Kompromissen zugunsten der wirtschaftspolitischen Bedeutung der Datenverarbeitung notwendig war. Kurz nach der Jahrtausendwende kippte diese fragile Balance jedoch aus zwei Gründen: Zum einen führte das un-

227 Freilich forderten sie, dass die Einführung staatlicher Datenschutzmaßnahmen möglichst wirtschaftsfreundlich ausfällt und auf Elementen der Selbstregulierung aufbaut.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gebremste Bedeutungswachstum, das die Verarbeitung personenbezogener Daten erfuhr, in Kombination mit dem Zeitgeist einer regulierungsskeptischen politischen Haltung zu einer Verschiebung der Balance zugunsten der Befürworter einer möglichst ungezügelten Datenverarbeitung. Datenschutz galt zunehmend als individueller Luxus, dem das potentielle Wirtschaftswachstum infolge der gesteigerten Verarbeitung personenbezogener Daten als Allgemeinwohlinteresse gegenübergestellt wurde. Zum anderen führten die Terroranschläge vom 11. September 2001 und von Madrid und London zu einer deutlichen Verschärfung sicherheitspolitischer Maßnahmen. In der Folge wurden EU-weit zahlreiche Maßnahmen verabschiedet, in denen der Beachtung datenschutzrechtlicher Garantien kaum Wert beigemessen wurde. Die Befürworter von Datenschutzregelungen standen somit einer Legitimationskrise gegenüber und gerieten an allen Fronten in die Defensive.

Eine Veränderung, die schon bald zur Initiierung der Datenschutzreform führen sollte, zeigte sich erst während der Verhandlungen zur Cookie-RL. Die Gründe für diese Veränderung und der Wandel in den relevanten Kontextbedingungen sind Gegenstand des folgenden Abschnitts.

3.4 Wandel weiterer relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform entscheidend waren

Mehrere Faktoren waren für die Initiierung der Datenschutzreform ausschlaggebend. An Subsystem-*internen* Faktoren sind hier die Verabschiedung der EU-GRCh und insbesondere das Inkrafttreten des Lissabon-Vertrags, aber auch das zunehmend selbstbewusste, aber auch überzeugungsgetriebene politische Handeln der Kommission und des Parlaments zu nennen. An Subsystem-*externen* Faktoren sind hingegen insbesondere die Zunahme von Datenschutzskandalen sowie eine relative Steigerung der öffentlichen Sensibilität für den Datenschutz seit Mitte der 2000er-Jahre zu nennen. Dieser Abschnitt widmet sich der Untersuchung der Frage, welche Faktoren in welchem Maße wesentlichen Einfluss auf die Initiierung der Datenschutzreform hatten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.1 Veränderungen in der grundlegenden verfassungsmäßigen Struktur, im Grad der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des politischen Systems

3.4.1.1 Die Erarbeitung der EU-Grundrechtecharta

Über viele Jahrzehnte hinweg wurden in den EU-Organen verschiedene Bestrebungen unternommen, um die Verpflichtung der Europäischen Gemeinschaften bzw. Union im Hinblick auf den Grundrechtsschutz ihrer Bürgerinnen und Bürger auszubauen. Zu diesem Zweck wurde einerseits die Strategie des Beitritts der EG – so etwa von der Kommission im Jahr 1979 vorgeschlagen – zur EMRK verfolgt und andererseits die Strategie der Erarbeitung eines eigenen Katalogs an europäischen Grundrechten (González Fuster 2014, 185). Letztere wurde seit Ende der 1970er-Jahre vor allem vom Europäischen Parlament (1979) vorangetrieben[228] und sollte schließlich in den 1990ern auch Anklang bei der Kommission finden. Wie bereits im Abschnitt zur DS-RL (3.2.2) erwähnt, hatte Ende der 1980er bzw. Anfang der 1990er ein Wandel im Selbstverständnis der EG hin zu einer politischen Union stattgefunden. Nachdem im Jahr 1989 die Gemeinschaftscharta der sozialen Grundrechte der Arbeitnehmer von den EG-Mitgliedstaaten[229] verabschiedet worden, aber die genaue Beziehung zwischen der Charta und EU-Recht noch unklar geblieben war, hatte die Europäische Kommission die Gründung des sog. *Komitees der Weisen* initiiert, um das Verhältnis zwischen der Charta und den geplanten Reformen im Kontext des Amsterdamer Vertrags zu untersuchen (González Fuster 2014, 189). Das Komitee der Weisen, das sein Aufgabenspektrum weiter fasste und das grundsätzliche Verhältnis zwischen EU-Recht und Bürgerrechten diskutierte, empfahl in seinem Abschlussbericht von 1996 die „Aufnahme eines Kernbestands von politischen und sozialen Grundrechten (‚Bill of Rights') in die Verträge" (Komitee der Weisen 1996, 9, Nr. VII.). Zudem vertrat das Komitee die Ansicht, dass der Katalog an Grundrechten nicht unveränderlich, sondern die Entwicklung auch neuer Grundrechte geboten sei, „weil das Konzept des Individuums weiter vertieft wird und die Rechte und

228 So etwa von Altiero Spinelli, der zwischenzeitlich aus der Kommission in das Europäische Parlament gewechselt war und auch von Karel De Gucht (González Fuster 2014, 186–89).

229 Lediglich das Vereinigte Königreich verabschiedete diese erst 1998 unter Tony Blair, da Margaret Thatcher die Verabschiedung stets blockiert hatte (González Fuster 2014, 189).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Pflichten, die ihm die gleichberechtigte Teilhabe an einer lebendigen Gesellschaft ermöglichen, immer umfassender und genauer bestimmt werden; und zum anderen, weil der technische Fortschritt und die Entwicklung allgemein Gefahren für den einzelnen, aber auch neue Aktionsmöglichkeiten mit sich bringen, die hinsichtlich ihrer möglichen Auswirkungen auf den einzelnen reglementiert werden müssen." (ebd., 44) Unter anderem verwies das Komitee darauf, dass die Informationsgesellschaft die *individuelle Privatheit* gefährde (ebd.).

Als der Vertrag von Amsterdam am 2. Oktober 1997 unterzeichnet worden, die vorgeschlagene Aufnahme von EU-Grundrechten allerdings – trotz der im Vertrag von Amsterdam formulierten Bekenntnis der Europäischen Union zu Grundrechten – ausgeblieben war, rief die Europäische Kommission eine weitere Expertengruppe ins Leben. Den Vorsitz der Expertengruppe „Grundrechte" übernahm Spiros Simitis (Expertengruppe „Grundrechte" 1999), der zwischen 1982 und 1986 bereits den Vorsitz des Datenschutzkomitees des Europarates innehatte und seit dem Jahr 1988 als Berater der Europäische Kommission in Datenschutzfragen fungierte (Simitis 2001, 99). Die Aufgabe der Expertengruppe „bestand darin, zu analysieren, welchen Status die sozialen Grundrechte in den Verträgen haben - insbesondere im neuen Vertrag von Amsterdam -, mögliche Lücken aufzuzeigen und die rechtlichen und konstitutionellen Implikationen zu untersuchen. Dabei sollte insbesondere die Möglichkeit geprüft werden, bei der nächsten Revision der Verträge die Grundrechte in Form einer ‚Bill of Rights' zu verbürgen." (Expertengruppe „Grundrechte" 1999, 3)

In seinem Abschlussbericht vom Februar 1999 kritisierte die Expertengruppe den Zustand des Grundrechtsschutzes in der Union schließlich als unzureichend und forderte die Anerkennung der Grundrechte insbesondere auf Grundlage der EMRK auf. Diese habe sich durch die Rechtsprechungsorgane ohnehin bereits zu einer gemeinsamen europäischen „Bill of Rights" entwickelt und müsse daher vollständig in das Gemeinschaftsrecht überführt und durch zusätzliche Bestimmungen spezifiziert und ergänzt werden (ebd., 7). Insbesondere im Bereich der dritten Säule der EU identifizierte die Expertengruppe Mängel und Unstimmigkeiten, die auf die *restriktive Politik* der Mitgliedstaaten zurückzuführen seien, die unter Verweis auf den intergouvernementalen Kooperationscharakter stets danach strebten, die Auswirkungen der Grundrechtsbindung zu begrenzen, wie es insbesondere am Widerstand gegen Datenschutzbestimmungen für die dritte Säule deutlich werde (ebd., 13). Daher vertrat die Expertengruppe die Ansicht, dass der Grundrechtskatalog der EMRK durch weitere Rechte,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

insb. um „das Recht, über die Verwendung personenbezogener Daten zu bestimmen“ (ebd., 26) erweitert werden sollte.

3.4.1.1.1 Entwurfsprozess

Auf dem Treffen des Europäischen Rats in Köln im Juni 1999 wurde schließlich der Beschluss gefasst, dass „die auf der Ebene der Union geltenden Grundrechte in einer Charta zusammengefaßt und dadurch sichtbarer gemacht werden sollten.“ (Europäischer Rat 1999a, 18, Nr. 44) Da sich die Regierungschefs im Hinblick auf die Frage, ob die Charta einen rechtlich verbindlichen Charakter annehmen sollte, indem sie in die Verträge aufgenommen würde, nicht einigen konnten, wurde zunächst ausschließlich deren feierliche Proklamation beschlossen (ebd., Anhang IV). Der Beschluss sah zum Zwecke der Erarbeitung der Charta die Gründung eines Gremiums vor, „das aus Beauftragten der Staats- und Regierungschefs und des Präsidenten der Europäischen Kommission sowie Mitgliedern des Europäischen Parlaments und der nationalen Parlamente besteht. Vertreter des Europäischen Gerichtshofs sollten als Beobachter teilnehmen. Vertreter des Wirtschafts- und Sozialausschusses, des Auschusses [sic] der Regionen und gesellschaftlicher Gruppen sowie Sachverständige sollten angehört werden. Das Sekretariat soll vom Generalsekretariat des Rates wahrgenommen werden.“ (ebd., 43) Das Gremium wählte als Selbstbezeichnung den Titel „Europäischer Konvent“. Die Vorgaben zur genauen Zusammensetzung und Arbeitsweise des Europäischen Konvents wurden auf dem Folgetreffen des Europäischen Rates in Tampere am 15. und 16. Oktober 1999 verabschiedet (Europäischer Rat 1999b). Die Europäische Union umfasste zu diesem Zeitpunkt 15 Mitgliedstaaten. Die wahlberechtigten Mitglieder des Konvents setzten sich aus insgesamt 15 Repräsentanten der Staats- und Regierungschefs der Mitgliedstaaten, 30 Vertretern der nationalen Parlamente (2 pro Parlament), 16 Mitgliedern des Europäischen Parlaments sowie einem Beauftragten des Präsidenten der Europäischen Kommission zusammen (Europäischer Rat 1999b).

Mehrere Mitglieder des Europäischen Konvents hatten einschlägige Erfahrungen im Bereich des Privatheitsschutzes bzw. des Schutzes personenbezogener Daten gesammelt, und sollten entscheidenden Einfluss auf den Einbezug entsprechender Schutzregelungen in den Text der Grundrechtecharta nehmen. Den Vorsitz des Europäischen Konvents übernahm der frühere Bundespräsident Deutschlands, Roman Herzog, der CDU-Mitglied

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

und zudem von 1983 bis zu seiner Wahl zum Bundespräsidenten 1994 Richter und ab 1987 zudem Präsident am Bundesverfassungsgericht war. Herzog war daher in besonderem Maße mit der Rechtsprechung des BVerfG vertraut, das der informationellen Selbstbestimmung im Rahmen des Volkszählungsurteils 1983 den Charakter eines Grundrechts zugesprochen hatte. Daneben nahm Guy Braibant als Vertreter Frankreichs sowie als stellvertretender Vorsitzender am Konvent teil. Erste datenschutzrechtliche Erfahrungen hatte Braibant während der Ausarbeitung des französischen Datenschutzgesetzes (Loi Informatique et Liberté) Ende der 1970er gesammelt und zuletzt einen Bericht für die französische Regierung zur DS-RL 95/46/EG verfasst. Einer der Parlamentsrepräsentanten Spaniens, Jordi Solé Tura, hatte aktiv am Entwurf der spanischen Verfassung von 1978 mitgewirkt und einen entscheidenden Beitrag zum Wortlaut der Bestimmung geleistet, die später als die Einführung eines spanischen Grundrechts auf den Schutz personenbezogener Daten bekannt werden sollte. Zudem war Stefano Rodotà als Vertreter der italienischen Regierung am Konvent beteiligt. Rodotà war zu diesem Zeitpunkt zugleich seit dem Jahr der Gründung der italienischen Datenschutzaufsichtsbehörde 1997 deren Vorsitzender, stellvertretender Vorsitzender der Art. 29-Datenschutzgruppe zwischen 1998 und 2000 (ab 2000 hatte Rodotà den Vorsitz der Art. 29 Datenschutzgruppe inne) sowie eines von zwölf Mitgliedern der *Europäischen Beratungsgruppe für Ethik im Bereich der Wissenschaft und der neuen Technologien*, die die Europäische Kommission seit 1991 beriet (González Fuster 2014, 194). Der Konvent tagte vom 17. Dezember 1999 an und verabschiedete nach etwa 30 Sitzungstagen am 2. Oktober 2000 den Entwurf der Grundrechtecharta (ebd.).

3.4.1.1.2 Konflikte während des Entwurfsprozesses

Einer der Hauptkonflikte während des Entwurfsprozesses entstand infolge des Mandats des Europäischen Konvents. So hatte der Beschluss des Europäischen Rates die *Zusammenfassung und Sichtbarmachung der auf der Ebene der Union geltenden Grundrechte*, allerdings nicht die *Ergänzung* der geltenden Grundrechte um neue vorgesehen.[230] Insbesondere das Vereinigte Königreich zählte zu den Staaten, die die Einführung neuer

230 Bestehende Grundrechte seien in diesem Zusammenhang verstanden als jene Rechte, die damals bereits in der Mehrzahl der EU-Mitgliedstaaten verbrieft waren. Abgesehen davon hatten zu diesem Zeitpunkt bereits einige Mitgliedstaaten moderne

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Grundrechte vehement ablehnten. Die übrigen Staaten, insbesondere die EG-Gründungsmitglieder, waren dagegen der Ansicht, dass der Entwurfsprozess möglichst offen gehalten werden sollte, um auch moderne Gefährdungen des Menschen etwa aus den Bereichen der Bioethik, des Umweltschutzes, des Verbraucherschutzrechts und der Digitalisierung adressieren zu können (González Fuster 2014, 192). Unterstützt wurde die Perspektive der Modernisierungsbefürworter sowohl von der Art. 29-Datenschutzgruppe als auch vom Europäischen Parlament. Beide Institutionen sprachen bereits nach dem ersten Beschluss des Europäischen Ratstreffens von Köln ihre ausdrückliche Unterstützung für die Ausarbeitung einer europäischen Grundrechtecharta aus. Unter Verweis darauf, dass bereits „einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben [… und in] einigen anderen Ländern ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt" (Art. 29 DS-Gruppe 1999, 2) wurde, empfahl die Datenschutzgruppe die Aufnahme des Grundrechts auf Datenschutz in die Grundrechtecharta. Verwiesen wurde auch darauf, dass der Europäische Gerichtshof für Menschenrechte in seiner Spruchpraxis bereits ein Grundrecht aus dem datenschutzrechtlichen Gehalt verschiedener Menschenrechte herausgearbeitet und konkretisiert habe (ebd.). Das europäische Parlament betonte, dass die Charta grundsätzlich eines „offenen und innovativen Ansatzes bedürfe, sowohl hinsichtlich ihrer Merkmale und *der Art der darin aufzuführenden Rechte* als auch hinsichtlich ihrer Funktionen und ihrer Stellung bei der konstitutionellen Weiterentwicklung der Union" (EP 1999, Nr. 3, Hervorhebung durch M.K.).

Zu Beginn der Gespräche im Europäischen Konvent war zwar unklar, ob die zu erarbeitende Grundrechtecharta angesichts des Widerstands seitens einiger Mitgliedstaaten jemals einen unionsweit verbindlichen Charakter annehmen könnte, doch auf Herzogs Vorschlag hin entschieden sich die Mitglieder dazu, so zu arbeiten, *als ob* die Charta später einmal ein rechtlich bindendes Dokument darstellen würde, was laut den Beteiligten positive Auswirkungen auf die Qualität des Textes hatte (J. Meyer und Engels 2001, 89).

Grundrechte wie den Schutz personenbezogener Daten in ihren Verfassungen implementiert, sodass die Einführung derartiger Grundrechte auf EU-Ebene streng genommen kein völliges Novum dargestellt hätte. Abgelehnt wurde also insbesondere die Übertragung moderner Grundrechte über die EU-Ebene auf die Mitgliedstaaten, in denen diese nicht verbrieft waren (González Fuster 2014, 192).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutz wurde erstmals seitens des sozialdemokratischen Bundestagsabgeordneten Prof. Dr. Jürgen Meyer, eines der deutschen Parlamentsvertreter (J. Meyer und Engels 2001, 7), in einem Entwurf der am 6. Januar 2000 an die Konventsmitglieder verteilt wurde, erwähnt. Aufbauend auf der Entschließung des Parlaments aus dem Jahr 1989 schlug Meyer einen Artikel 6 zum Datenschutz sowie einen Artikel 7 zu Privatheit vor (European Convention Presidency 2000a, 4). Der Datenschutz-Artikel baute klar auf Kontrolltheorien, indem die Verantwortung zum Umgang mit personenbezogenen Daten in reduktionistischer Manier dem Individuum übertragen wurde und deren Begrenzung nur im Falle eines überwiegenden öffentlichen Interesses erlaubt sein sollte. Im Falle des Privatheitsartikels wurde diese Dichotomisierung dagegen unterlassen. Hier wurden als mögliche Gründe zur Begrenzung der häuslichen Privatheit beispielhaft spezifische Elemente wie die ernsthafte Gefährdung der öffentlichen Ordnung und besonders schwerwiegende Verbrechen im Kontext häuslicher Privatheit genannt. Eingriffe in die kommunikative Privatheit sollten dagegen nur unter den Bedingungen zulässig sein, die das Strafrecht vorsehe (ebd.). Auch die vom Präsidium[231] ausgearbeitete vorläufige Liste möglicherweise infrage kommender Rechte baute auf der Parlamentsentschließung von 1989 auf und sah – allerdings ohne die weitere Spezifizierung des Gehalts und möglicher Begrenzungsgründe – sowohl ein eigenständiges Recht auf Datenschutz (European Convention Presidency 2000c, 5) als auch ein weiteres Recht auf „Private and family life" (ebd., 4) vor. Bereits zu diesem frühen Stadium der Verhandlungen konnte sich somit die Idee durchsetzen, dass der Schutz personenbezogener Daten zumindest Erwähnung in der Charta finden sollte (González Fuster 2014, 196).

In einem weiteren Entwurf des Präsidiums vom 24. Februar tauchte Datenschutz schließlich erneut als ein eigenständiges Grundrecht auf. Die gewählte Formulierung (European Convention Presidency 2000b, 5) stützte sich auf die Europaratskonvention, sah allerdings abweichend von dieser auch eine spezifischere Alternativfassung (ebd.) vor, wonach die Verarbeitung personenbezogener Daten entweder auf Basis der Einwilligung des Betroffenen oder einer gesetzlich festgelegten legitimen Grundlage entsprechend erfolgen dürfen sollte (European Convention Presidency 2000b, 5). Andere Alternativen, wonach jede Person selbst über die Freigabe sie

231 „Das Präsidium hatte eine ausgesprochen wichtige Rolle, da es nicht nur die Tagesordnung festlegte und die Konventssitzungen leitete, sondern auch die Vorschläge für die Artikelformulierungen vorlegte." (J. Meyer und Engels 2001, 13)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

betreffender personenbezogener Daten entscheiden können sollte, konnten sich nicht durchsetzen. Nach weiteren Debatten über das Ausmaß der zu verbriefenden informationellen Selbstbestimmung, über das Verhältnis zwischen Privatsphäre und Datenschutz sowie Versuchen, den Schutz der Privatheit mit dem Schutz der Ehre, des Rufes, des Hauses sowie der Freiheit und Vertraulichkeit der Kommunikation in Verbindung zu bringen (González Fuster 2014, 196 f.), konnte schließlich Ende Juli eine Einigung erzielt werden (Präsidium des Europäischen Konvents 2000, 4)

Zunächst stimmten die Konventsmitglieder dem Textentwurf für eine Charta der Grundrechte der Europäischen Union bereits Ende September zu und schlossen ihre Arbeit schließlich mit der Annahme der Charta am 2. Oktober 2000 ab (J. Meyer und Engels 2001, 67). Im Anschluss wurde der Entwurf Anfang Oktober an die Staats- und Regierungschefs der EU-Mitgliedstaaten übermittelt. Auf der informellen Sitzung des Europäischen Rates vom 13. und 14. Oktober 2000 in Biarritz wurde der Entwurf schließlich angenommen und das Parlament darum ersucht, gemeinsam mit dem Rat und der Kommission die Charta auf der formellen Sitzung des Europäischen Rates in Nizza feierlich zu proklamieren (J. Meyer und Engels 2001, 69). Nachdem das Europäische Parlament den Entwurf am 14. November gebilligt hatte (EP 2000), unterzeichneten die Präsidentin des Europäischen Parlaments, der Präsident des Rates und der Präsident der Kommission die Charta der Grundrechte auf dem Treffen des Europäischen Rates am 7. Dezember 2000 und verkündeten diese feierlich (Europäischer Rat 2000a).

3.4.1.1.3 Inhalt der Grundrechtecharta

Im Folgenden gehe ich auf die Bedeutung der Grundrechtecharta ein und lege einerseits dar, wie das Verhältnis zwischen Art. 7 und 8 GRCh zu bewerten ist und andererseits, in welchem Verhältnis beide GRCh-Artikel zu Art. 8 EMRK stehen.

Die Grundrechtecharta beinhaltet zwei Artikel, die relevant im Hinblick auf den Datenschutz sind. Art.7 GRCh[232] widmet sich der Achtung des

232 Art. 7 GRCh – *Achtung des Privat- und Familienlebens*: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation." (EU 2010)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Privat- und Familienlebens und Art. 8 GRCh[233] dem Schutz personenbezogener Daten. Der Inhalt von Art. 7 GRCh entspricht weitgehend Art. 8 der EMRK,[234] während Art. 8 GRCh ein eigenständiges Recht auf den Schutz personenbezogener Daten formuliert und damit ein Novum darstellt. Denn bis zu diesem Zeitpunkt hatte beispielsweise der EGMR den Schutz personenbezogener Daten als Ausfluss des in Art. 8 EMRK verbrieften Rechts auf Achtung des Privat- und Familienlebens interpretiert. In ähnlicher Weise wurde der Schutz personenbezogener Daten in der Datenschutz-Konvention des Europarats und auch in der DS-RL stets als bedeutsam im Hinblick auf den Schutz von Rechten und Freiheiten im Allgemeinen bezeichnet. Zwar hatten einige europäische Staaten bereits ein Recht auf Datenschutz anerkannt, allerdings wurde der Schutz personenbezogener Daten mit der Grundrechtecharta erstmals auf internationaler Ebene als eigenständiges Grundrecht verbrieft. Nach González Fuster (2014, 199) könne die Existenz von zwei voneinander getrennten privatheitsrelevanten Artikeln als Kompromiss zwischen jenen Staaten, die Datenschutz als Teil des Privatheitsschutzes betrachteten und jenen, die Datenschutz als eigenständiges Grundrecht verbrieft hatten, bewertet werden. Andererseits könne es auch als das Ergebnis des Konflikts der europäischen Staaten zwischen Konservierung bestehender Grundrechte und grundrechtlicher Innovation bewertet werden. Insofern spiegele die Aufrechterhaltung eines eigenen Artikels zur Achtung des Privat- und Familienlebens und dessen Ergänzung um ein eigenständiges Recht auf Datenschutz den Versuch dar, Konservierung und Innovation in ein Gleichgewicht zu bringen.

233 Art. 8 GRCh – *Schutz personenbezogener Daten*: „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht." (EU 2010)

234 Art. 8 EMRK – *Recht auf Achtung des Privat- und Familienlebens*: „1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. 2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer." (Europarat 2010)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Der erste Unterschied zwischen den Regelungen der Europäischen Grundrechtecharta und der Europäischen Menschenrechtskonvention liegt in der Ersetzung des Begriffs der Korrespondenz durch den Begriff der Kommunikation. Dies ist auf die in der Zeit zwischen der Verabschiedung der beiden internationalen Dokumente erfolgte Rechtsprechung des EGMR zurückzuführen, in der angesichts technologischer Entwicklungen der allgemeinere Begriff der Kommunikation gegenüber dem Begriff der Korrespondenz, der lediglich den Schriftverkehr umfasst, bevorzugt wurde. Hinsichtlich möglicher Einschränkungen der Achtung des Privat- und Familienlebens sind beide Instrumente weitgehend deckungsgleich, doch sieht die Grundrechtecharta – und dies ist der zweite Unterschied – im Gegensatz zur EMRK „von der Union anerkannte[…] dem Gemeinwohl dienende Zielsetzungen" als einen weiteren möglichen Einschränkungsgrund vor. Während dies als eine Abschwächung der EMRK-Regelungen bewertet werden kann, bietet der erste Satz desselben Artikels aber zugleich eine Stärkung, da darin vorgegeben wird, dass jede Einschränkung den Wesensgehalt der entsprechenden Rechte und Freiheiten zu achten hat (González Fuster 2014, 200–202).[235]

Zunächst sei erwähnt, dass die oben ausgeführten Gedanken zur Einschränkung des Art. 7 GRCh auf Basis des horizontalen Artikels 52 Abs. 1 GRCh sich auch auf Art. 8 GRCh übertragen lassen (González Fuster 2014, 203). Gestützt wurde Art. 8 GRCh dagegen auf Art. 286 des EWG-Vertrags,[236] auf die DS-RL 95/46/EG, auf Art. 8 EMRK sowie auf die Datenschutz-Konvention des Europarates. Während die Präambel der Charta die gemeinsamen Verfassungstraditionen und die gemeinsamen internationalen Verpflichtungen der Mitgliedstaaten, die EMRK, sowie die Rechtsprechung des EuGH und des EGMR als Grundlage anführt (EU 2010, 391), fehlen die gemeinsamen Verfassungstraditionen der Mitgliedstaaten sowie

235 Da der Europäische Konvent den Text der Grundrechtecharta im Hinblick auf eine bessere Lesbarkeit möglichst kurzhalten wollte, wurden mögliche Einschränkungsgründe nicht in den entsprechenden Artikeln selbst, sondern an späterer Stelle niedergelegt. Mit Art. 8 Abs. 2 EMRK korrespondiert daher Art. 52 Abs. 1 GRCh: *Tragweite und Auslegung der Rechte und Grundsätze*: (1) Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen." (EU 2010)

236 Nunmehr Art. 16 AEUV und Art. 39 EUV.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Rechtsprechung des EuGH und des EGMR in der Begründung von Art. 8 GRCh (González Fuster 2014, 203).

Darüber hinaus ist eine Besonderheit des Art. 8 GRCh, dass er sich nicht nur auf den abstrakten Schutz personenbezogener Daten, wie er im ersten Absatz geregelt ist, beschränkt, sondern in den folgenden beiden Absätzen insgesamt sechs spezifische Elemente benennt, die bei der Verarbeitung der Daten zu beachten seien: 1. Die Verarbeitung nach Treu und Glauben, 2. das Zweckbindungsprinzip, 3. die Anforderung einer rechtmäßigen Verarbeitungsgrundlage, entweder mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten Grundlage, 4. das Auskunftsrecht, 5. das Recht auf Berichtigung, und 6. die Überwachung der Datenschutz-Vorschriften durch eine unabhängige Aufsichtsstelle. Zudem macht der Artikel keine Unterscheidung zwischen der automatisierten und der manuellen Verarbeitung personenbezogener Daten, ist daher also auf beide Verarbeitungsarten anwendbar. Nicht genannt wurden dagegen einige der zu diesem Zeitpunkt in den geltenden internationalen Datenschutzinstrumenten festgeschriebenen datenschutzrechtlichen Elemente (González Fuster 2014, 204 f.). So waren bereits in den OECD-Richtlinien auch Verarbeiterpflichten in Form von Sicherheitsmaßnahmen, Transparenzvorgaben (wobei fairerweise erwähnt sei, dass das in der GRCh benannte Recht auf Auskunft zumindest als ein wichtiges Element im Rahmen der Transparenzpflichten der Verarbeiter aufgefasst werden kann) sowie die Rechenschaftspflicht der Verarbeiter benannt (vgl. 3.1.1.3). In der Datenschutz-Konvention des Europarats waren zusätzlich die Datenschutzprinzipien der Datenminimierung, der Richtigkeit und der Speicherbegrenzung enthalten. Zudem sah die Europaratskonvention 108 im Gegensatz zu Art. 8 der Grundrechtecharta ein erhöhtes Schutzniveau für besondere Arten personenbezogener Daten sowie das Betroffenenrecht auf Löschung vor. Schließlich hatte die Datenschutz-Konvention zwar keine Vorgaben zur Einrichtung einer Aufsichtsstelle gemacht, sah allerdings im Gegensatz zur GRCh die Schaffung von Sanktionsstrukturen und die Bereitstellung von Rechtsmitteln vor (vgl. 3.1.2.3). Ebenso fehlten die aus der DS-RL bekannten Rechte auf Widerruf bzw. auf Schutz vor automatisierten Einzelentscheidungen (vgl. 3.2.2.7).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.1.1.4 Zwischenfazit

Die Grundrechtecharta war das erste internationale Rechtsinstrument, das den Schutz personenbezogener Daten als eigenständiges Grundrecht verbriefte und stellte insofern eine enorme Innovation dar.

Die in der Charta genannten sechs datenschutzrechtlichen Elemente bezogen sich zwar nur auf einen kleinen Teil des bereits damals verbrieften Schutzes personenbezogener Daten, was jedoch nicht verwundern sollte: Die Verabschiedung der DS-RL lag nur wenige Jahre zurück und nur wenige Mitgliedstaaten hatten diese im vorgegebenen Zeitrahmen in nationales Recht umgesetzt. Zudem war die wirtschaftspolitische Bedeutung personenbezogener Daten zwar bereits während der Aushandlung der DS-RL von Bedeutung, doch Forderungen nach einer Aufweichung der Datenschutzprinzipien zugunsten wirtschaftspolitischer Ziele konnten erst um die Jahrtausendwende stärkere politische Unterstützung auf sich ziehen. Im Ergebnis waren die Befürworter von Datenschutzregelungen in dieser Periode eher darum bemüht, einige als zentral betrachtete, aber politisch umstrittene Datenschutz-Grundsätze zunächst klar zu verankern, anstatt zu versuchen, diese umstrittenen Grundsätze um weitere möglicherweise noch umstrittenere Regelungen zu erweitern.

Auf der inhaltlichen Ebene bedeutete die Vorgabe zur Aufrechterhaltung des Wesensgehalts des Datenschutzes gemäß Art. 52 GRCh (allerdings nur unter der Bedingung, dass die Charta auch tatsächlich Rechtsverbindlichkeit erhalte), dass eine Außerkraftsetzung der Datenschutzprinzipien weder auf Basis von wirtschaftspolitischen Erwägungen noch auf Grundlage sicherheitspolitischer Interessen *so wichtig diese auch sein mögen* erfolgen durfte, wie etwa die Datenschutzgruppe 2002 anmerkte (Artikel 29-Datenschutzgruppe 2002, 5).

Die Verabschiedung der Grundrechtecharta und die Inkorporation insb. eines eigenständigen Datenschutz-Artikels sind als klarer Erfolg der Datenschutzbefürworter zu bewerten. Die Kommission, das Europäische Parlament, institutionelle Datenschützer sowie einzelne bedeutsame Figuren wie Roman Herzog trugen gemeinsam entscheidend zur Aufnahme des Schutzes personenbezogener Daten bei. Zudem stellt die Verabschiedung der GRCh ein Beispiel für *Venue Shopping* dar, bei der Akteure zur Erreichung ihrer politischen Ziele alle sich bietenden politischen Gestaltungsräume auf allen sich bietenden Entscheidungsebenen nutzen (Beyers und Kerremans 2012).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Da die Charta zunächst nur feierlich proklamiert wurde, sie also weder eine unmittelbare Rechtsverbindlichkeit entfaltete noch absehbar war, ob sie dies jemals können würde, hatte sie allerdings zunächst keine direkten Auswirkungen auf die Datenschutzpolitik.[237] Diese sollte sie später mit dem Inkrafttreten des Lissabon-Vertrags in Form des Wandels nicht nur der verfassungsmäßigen Struktur, sondern auch des Grades der erforderlichen Zustimmung für wesentlichen Wandel und der relativen Offenheit des politischen Systems erhalten. Der Entstehung des Lissabon-Vertrags widmet sich das folgende Unterkapitel.

3.4.1.2 Der Vertrag von Lissabon

Wie bereits erwähnt, waren die Mitgliedstaaten der Europäischen Union gespalten im Hinblick auf die Frage des anzustrebenden Rechtscharakters der Grundrechtecharta. Während die Mehrheit der Mitgliedstaaten für eine in die Verträge eingefügte, rechtsverbindliche Charta eintrat, befürworteten Großbritannien, Irland, die Niederlande und die skandinavischen Länder eine lediglich feierlich proklamierte Charta ohne Rechtsverbindlichkeit (P. Becker und Leisse 2005, 48; González Fuster 2014, 229).

Aufgrund dieses Dissenses hatten sich die Staats- und Regierungschefs auf dem Kölner Treffen des Europäischen Rats im Jahr 1999 zunächst lediglich auf die feierliche Proklamation der Charta geeinigt, die Frage nach der endgültigen Rechtsnatur der Charta dagegen bewusst offengelassen und auf die Zeit nach der Proklamation verschoben (Europäischer Rat 1999a, 43). Nachdem auch der Europäische Rat von Nizza, auf dem die feierliche Proklamation der Charta am 7. Dezember 2000 erfolgt war, die Klärung der Frage erneut auf einen späteren Zeitpunkt verlegte (Europäischer Rat 2000a, 1),[238] intensivierte sich die politische Debatte (P. Becker und Leisse 2005, 57–66) und führte auf dem Treffen des Europäischen Rates in Laeken

237 Eine der direkten Folgen der Proklamation der CRCh war die Gründung von FRA, der *Agentur der Europäischen Union für Grundrechte* (Fundamental Rights Agency) im Jahr 2007, die mit der Aufgabe betraut wurde, die bereits in EU-Recht umgesetzten Elemente der Grundrechtecharta zu überwachen und die relevanten Organe, Einrichtungen, Ämter und Agenturen der EU sowie die Mitgliedstaaten bei diesbezüglichen Fragen zu beraten (FRA 2012, 33 f.).

238 Bei der Regierungskonferenz von Nizza war es insbesondere um die Reform der EU gegangen, um ihre Handlungsfähigkeit (im Hinblick auf Größe und Zusammensetzung der Kommission, auf die Reform der Stimmgewichtung im Ministerrat und auf die Ausweitung der qualifizierten Mehrheit) auch angesichts der bevorstehenden Erweiterung der Union um zunächst zehn (bis 15) neue Mitgliedstaaten sicherzu-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Ende 2001 zur Einberufung eines neuen Konvents zur Zukunft Europas (Europäischer Rat 2001, 21 ff.).

3.4.1.2.1 Entwurfsphase

Dieser zweite Konvent, auch als „Verfassungskonvent" bezeichnet, sollte alle wesentlichen die zukünftige Entwicklung der Europäischen Union betreffenden Fragen prüfen. Die Debatte über die Zukunft der Europäischen Union war deshalb notwendig geworden, weil viele der geltenden Gemeinschaftsmechanismen (darunter insb. die hervorgehobene Stellung des Ministerrats und die Schwäche des Europäischen Parlaments, kurzum: das Demokratiedefizit) noch immer auf den Strukturen der 1950er-Jahre basierten und die Mitgliedstaaten sich im Rahmen der Regierungskonferenzen unfähig gezeigt hatten, langfristige Lösungen für diese und weitere strukturelle Probleme zu finden (P. Becker und Leisse 2005, 50–55). In der Hoffnung, dass an den Erfolg des ersten Konvents angeknüpft und nicht die auf den Regierungskonferenzen begangenen Fehler wiederholt würden, übertrug der Europäische Rat von Laeken die Aufgabe zur Schaffung einer demokratischeren, transparenteren und effizienteren Europäischen Union an den besagten zweiten Konvent. Der Konvent sollte sich aus 16 Mitgliedern des Europäischen Parlaments, 30 Mitgliedern der nationalen Parlamente (2 für jeden Mitgliedstaat), 2 Vertretern der Europäischen Kommission und 15 Regierungsvertretern zusammensetzen. Die EU-Beitrittskandidaten wurden ebenfalls mit je zwei parlamentarischen Vertretern und einem Regierungsvertreter in die Verhandlungen eingebunden. Den Vorsitz des zweiten Konvents übernahm der frühere französische Präsident Valéry Giscard d'Estaing (Europäischer Rat 2001, 24 f.). Der Verfassungskonvent tagte zwischen dem 28. Februar 2002 und dem 20. Juli 2003. Der dabei entstandene Entwurf für eine EU-Verfassung wurde daraufhin im Rahmen des Europäischen Rates hitzig debattiert (P. Becker und Leisse 2005, 220–38). Nach weiteren Verhandlungen konnte dann zunächst im

stellen. Die Ergebnisse der Konferenz wurden von der Mehrheit der wissenschaftlichen und politischen Beobachter als Ausdruck des Stillstands des europäischen Integrationsprozesses abgelehnt: „Die enttäuschenden Ergebnisse und die komplizierten Verhandlungen über die Machtfragen über die Machtfragen, insbesondere bei der Frage der Stimmengewichtung im Rat, hatten nochmals deutlich bestätigt, dass nationales Prestigedenken und kurzfristige Interessenpolitik sowie das Denken in Blockadekategorien an Stelle von Handlungs- und Gestaltungsmöglichkeiten die Debatte bestimmten." (P. Becker und Leisse 2005, 53)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Juni 2004 eine politische Einigung erreicht werden, die schließlich auf dem Treffen des Europäischen Rates in Rom am 29. Oktober 2004 mit den Unterschriften der Staats- und Regierungschefs auch förmlich besiegelt wurde. Geplant war, dass der Verfassungsvertrag nach einer zweijährigen Phase der Ratifikation durch alle Mitgliedstaaten zum 1. November 2006 in Kraft treten sollte (P. Becker und Leisse 2005, 239–58). Je nach Mitgliedstaat musste die Ratifikation entweder per Parlamentsbeschluss oder Volksabstimmung erfolgen. In der Mehrzahl der Mitgliedstaaten – beginnend mit Litauen am 11. November 2004 – erfolgte die Ratifikation auf Grundlage eines Parlamentsbeschlusses. Nachdem der Verfassungsvertrag bei den Referenden in Frankreich am 29. Mai 2005 bzw. in den Niederlanden am 1. Juni 2005 abgelehnt worden war, scheiterte die Annahme des Verfassungsvertrags, sodass der Ratifikationsprozess in der Mehrzahl der übrigen Mitgliedstaaten abgebrochen wurde, der Verfassungsvertrag damit also scheiterte (Hellmann 2009, 6).

In der Folge trat die Europäische Union in eine mehr als zwei Jahre andauernde Reflexionsphase ein, in der über den Umgang mit der gescheiterten Annahme des Verfassungsvertrags diskutiert wurde. Zentrale Diskussionspunkte bildeten „institutionelle Fragen wie die Sitzverteilung im Europäischen Parlament […] und die Zusammensetzung der Kommission […]. Zu den nichtinstitutionellen Fragen gehörten die Einbindung der Charta der Grundrechte […], die Gemeinsame Außen- und Sicherheitspolitik […], die Unionsbürgerschaft […] sowie die Symbole der Union […]. Eine bis zuletzt umstrittene Frage bildete die Definition der qualifizierten Mehrheit im Europäischen Rat und im Ministerrat […]." (Hellmann 2009, 11) In der Nacht zum 19. Oktober 2007 konnten sich die Staats- und Regierungschefs der Mitgliedstaaten schließlich auf einen Kompromiss einigen (ebd., 11), dessen endgültige Fassung von diesen am 13. Dezember 2007 als „Vertrag von Lissabon" unterzeichnet wurde. Der ursprüngliche Zeitplan, wonach der Lissabonner Vertrag am 1. Januar 2009 in Kraft treten sollte, konnte aufgrund des gescheiterten irischen Referendums im Juni 2008 allerdings nicht eingehalten werden. Nachdem Irland vertragliche Zugeständnisse[239] gemacht wurden und die irische Bevölkerung den abgeänderten Vertrag in einem Folgereferendum mit ca. 67 % der Stimmen befürwortet

239 So etwa die Hervorhebung der nationalen Souveränität in Steuerfragen und die Beibehaltung des bisherigen Prinzips, dass jedes Land ein eigenes Kommissionsmitglied stellt, das ursprünglich zum Zwecke der effektiveren Regierbarkeit aufgrund der Größe der Union eingeschränkt werden sollte (Hellmann 2009, 44).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

hatte, trat der Vertrag von Lissabon schließlich zum 1. Dezember 2009 in Kraft (Leisse 2010, 389).

Mit dem Vertrag von Lissabon verzichteten die Mitgliedstaaten auf ihr ursprüngliches Ziel der Ersetzung der geltenden Verträge durch einen einzelnen, neuen Verfassungsvertrag. Stattdessen kehrten sie zur alten Formel der Reform der geltenden Verträge zurück, weswegen der Vertrag von Lissabon auch als *Reformvertrag* bezeichnet wird.[240] Abgesehen davon wurden allerdings die wesentlichen Bestimmungen des Verfassungsvertrags übernommen. Diese betrafen einerseits institutionelle Fragen, etwa die Zusammensetzung der EU-Organe, die Spezifika für Mehrheitsentscheidungen im Ministerrat oder die Auflösung der Säulenstruktur der EU, und andererseits nicht-institutionelle Fragen wie die Kompetenzabgrenzung, die Grundrechtecharta, den Beitritt der Union zur Europäischen Menschenrechtskonvention, die gemeinsame Sicherheits- und Verteidigungspolitik oder auch die Regelungen zum Beitritt zur bzw. zum Austritt aus der Union (Hellmann 2009, 12 ff.).

Im Folgenden möchte ich auf die für die vorliegende Arbeit zentralen Aspekte in Gestalt der Grundrechtecharta, die institutionellen Neuerungen in Bezug auf das Europäische Parlament, die Spezifika für Mehrheitsentscheidungen im Ministerrat sowie die Auflösung der Säulenstruktur der EU näher eingehen.

3.4.1.2.2 Inkrafttreten der Grundrechtecharta

Infolge des Vertrags von Lissabon bilden seither der Vertrag über die Europäische Union (EUV) und der Vertrag zur Gründung der Europäischen Gemeinschaft (EGV), der mit dem Lissaboner Vertrag in „Vertrag über die Arbeitsweise der Europäischen Union" (AEUV) umbenannt wurde, die primärrechtlichen Grundlagen der Europäischen Union. Nachdem die im Verfassungsvertrag vorgesehene direkte Einbindung der Grundrechtecharta als Teil II des Vertrages gescheitert war, sah der Vertrag von Lissabon zwar keine direkte Einbettung der Charta in die Verträge vor, setzte diese allerdings dem EU-Primärrecht durch einen Verweis in Art. 6 EUV gleich. Abs. 2 des Artikels 6 EUV sah den Beitritt der Europäischen Union zur

240 Zudem wurde im Rahmen des Vertrags von Lissabon u. a. auf die formelle Einführung staatstypischer Symbole (z. B. eine Europaflagge, Europahymne, Europatag), die Verkleinerung der Kommission und die wörtliche Übernahme der GRCh verzichtet (Hellmann 2009, 12 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Europäischen Menschenrechtskonvention vor und der dritte Absatz nahm wiederum Bezug auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten: „Artikel 6 normiert somit eine dreifache Säule des Grundrechtsschutzes in der Union. Die in der Charta aufgeführten Grundrechte, die Menschenrechte der Europäischen Menschenrechtskonvention und die – künftig weiterhin geltenden – richterrechtlich entwickelten europäischen Grundrechte bilden ein dichtes, wohl lückenloses Netz, das hinreichenden Rechtsschutz gegen die Hoheitsakte der Europäischen Union ermöglicht." (Borowsky 2010, 154) Dies sollte weitreichende Konsequenzen für die Datenschutzpolitik der EU haben, da die Grundrechtecharta dadurch rechtswirksamen, bindenden Charakter erhielt. Zusammen betrachtet mit dem Beitritt der Union zur EMRK wurden die allgemeinen Prinzipien des Unionsrechts fortan mittels der Grundrechtecharta und der EMRK konstituiert. In der politischen Praxis bedeutete diese Verschiebung, dass die Achtung des Privatlebens gemäß Art. 8 EMRK und Art. 7 GRCh sowie der Schutz personenbezogener Daten nach Art. 8 GRCh in legislativen Abwägungsprozessen nunmehr ausdrücklich berücksichtigt werden mussten (Tinnefeld 2009, 504).

3.4.1.2.3 Institutionelle Neuerungen in Folge des Vertrags von Lissabon

Eine weitere Neuerung des Reformvertrags war die Neuregelung der Strukturen der EU sowie der Kompetenzen und Funktionsweisen ihrer Organe. So sah Art. 14 EUV eine deutliche Aufwertung der Stellung des Europäischen Parlaments und dessen weitgehende Gleichstellung gegenüber dem Ministerrat vor. Durch die Überführung des Mitentscheidungsverfahrens zum neuen ordentlichen Gesetzgebungsverfahren wurde zudem vorgesehen, dass die EU-Gesetze fortan von Parlament und Rat gemeinsam und gleichberechtigt entschieden werden sollten. Die Bedeutung dieser Regelung wurde zudem insbesondere durch die Auflösung der Säulenstruktur der EU verstärkt, sodass fortan 95 % der EU-Gesetze von Parlament und Rat gemeinsam entschieden werden sollten.[241] Bedeutsam ist dies vor dem Hintergrund der Schilderungen in Unterabschnitt 3.3.4.2 zur Richtlinie

241 Bis zum Inkrafttreten des Vertrags von Lissabon basierte das politische System der EU auf den drei Säulen: 1. den Europäische Gemeinschaften (Euratom und Europäische Gemeinschaft), 2. der Gemeinsamen Außen- und Sicherheitspolitik (GASP) und 3. der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS). Mit dem Vertrag von Lissabon wurde die Unterscheidung zwischen supranationa-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

zur Vorratsdatenspeicherung, während deren Aushandlung der Ministerrat dem Parlament stets mit dem Entzug seiner Mitwirkungsrechte durch das Umschwenken zum Instrument des Rahmenbeschlusses gedroht hatte. Nach dem Vertrag von Lissabon mussten nunmehr auch jene Gesetze von Parlament und Rat gemeinsam entschieden werden, die die ehemalige dritte Säule betreffen, sodass eine Übergehung des Parlaments nicht mehr möglich war.

3.4.1.3 Das Stockholmer Programm

Das Inkrafttreten des Lissabon-Vertrags ebnete zwar den grundsätzlichen Weg zu einer Reform des Datenschutzrechts auf Grundlage insb. der Vorgaben der EU-Grundrechtecharta. Der typische Weg des EU-Agenda-Settings sah allerdings vor, dass die Kommission nicht einfach einen entsprechenden Legislativvorschlag vorlegt, sondern, dass die entsprechende Legislativmaßnahme zunächst in einen politischen Maßnahmenkontext eingebettet wird, in dem Zielvorgaben gemacht werden. Aufgrund der Bedeutung des Datenschutzes für die PJZS wurden die Materie daher im Rahmen des nächsten Mehrjahresprogramms der Union diskutiert. Der folgende Unterabschnitt widmet sich der Entstehung dieses neuen Mehrjahresprogramms, das den Namen Stockholmer Programm erhalten sollte und das im Rahmen der unionspolitischen Zielvorgaben für die Jahre 2010 bis 2014 auch die Reform des EU-Datenschutzrahmens vorsah. Die Grundlage für das Stockholmer Programm bildeten die Abschlussberichte zweier informeller Arbeitsgruppen, deren Ergebnisse im Folgenden zunächst vorgestellt werden.

3.4.1.3.1 Empfehlungen der Zukunftsgruppe Inneres

Bereits im Jahr 2007 hatte der Ministerrat für Justiz und Inneres zunächst auf einer informellen Sitzung zwischen dem 14. und 16. Januar in Dresden und später am 14. Februar 2007 auf seiner formellen Sitzung den Vorschlag des damaligen deutschen Innenministers und Ratsvorsitzenden Wolfgang Schäuble sowie des Kommissionsvizepräsidenten und Justiz- und Innen-

lem Gemeinschaftsrecht (Binnenmarkt) und intergouvernementalem Unionsrechts (PJZS) aufgehoben (Tinnefeld 2009, 504).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

kommissars Franco Frattini aufgegriffen, eine hochrangige Beratungsgruppe zur Zukunft der europäischen Innenpolitik einzuberufen. Der Gruppe sollten ein Mitglied der Kommission, Franco Frattini, sowie die für Innenpolitik zuständigen nationalen Minister des amtierenden (Deutschland, Portugal, Slowenien) und folgenden Dreiervorsitzes (Frankreich, die Tschechische Republik, Schweden) sowie im Rotationsverfahren ein Mitglied des darauffolgenden Ratsvorsitzes (Spanien, Belgien und Ungarn) angehören. Ein Vertreter des LIBE-Ausschusses, der für Justiz und Inneres zuständige Generalsekretär des Ministerrats sowie ein Vertreter der mit *common law* regierten Mitgliedstaaten sollten als Beobachter partizipieren. Der Vorsitz der Gruppe sollte schließlich zwischen dem Kommissionsvertreter und dem amtierenden Ratsvorsitzenden rotieren (The Future Group 2008, 13, Nr. 8). Die Gruppe erhielt den Beinamen Zukunftsgruppe und wurde vor dem Hintergrund des möglichen Scheiterns auch des Lissabon-Vertrags mit der Erarbeitung eines Konsenses im Bereich der EU-Innenpolitik beauftragt (Monroy 2009b). Von zivilgesellschaftlicher Seite erntete der im Juni 2008 veröffentlichte Abschlussbericht der Zukunftsgruppe massive Kritik. Statewatch äußerte insbesondere große Besorgnis im Hinblick auf die weitere Ausweitung der EU-weiten Überwachungs- und Datensammlungspraktiken sowie die geplante Ausweitung der Zusammenarbeit mit den Vereinigten Staaten auf dem Gebiet der Überwachung. Angesichts der Dominanz von Mitte-Rechts- und Rechtsaußen-Positionen im Ministerrat und im Europäischen Rat wurden die in den Dokumenten der Zukunftsgruppe geäußerten Beteuerungen im Hinblick auf die Herstellung einer Balance zwischen Sicherheit und Freiheit angezweifelt (Bunyan 2008, 59). Konkret lautete der Vorwurf, dass zwar einer Balance das Wort gesprochen werde, jeder praktische Vorschlag der Zukunftsgruppe jedoch vielmehr die Intensivierung der Sammlung und des Austauschs von Bewegungs- und Telekommunikationsdaten und von Fingerabdrücken vorsehe, während ausgleichende Datenschutzmaßnahmen nicht angesprochen oder nur vage skizziert würden.[242] Bemerkenswert ist insbesondere ein Kommentar Franco Frattinis. Auf der ersten Sitzung der Zukunftsgruppe hatte dieser die folgende Aussage getätigt: „Finding a new balance between the right to

242 So wurde im Kapitel zu „Public security, privacy and technology" zwar erwähnt: „In order to achieve a sufficient level of protection, „privacy-enhancing technologies" are absolutely essential to guarantee civil and political rights in the age of cyberspace." (The Future Group 2008, 43, Nr. 132) Zur konkreten Umsetzung äußert sich das Papier hingegen mit keinem Wort.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

security and the protection of fundamental rights is another main challenge for policy-makers. There is a need to overcome the traditional dogma of seeing *collective security* and *individual freedom* as two opposed concepts which exclude each other. Individual rights can only flourish in an atmosphere of collective security." (The Future Group 2007, 3, Hervorhebungen in kursiv: M. K.) Die Aussage, dass die in Sicherheitsdebatten häufig geäußerte Trade-off-Mentalität überwunden werden müsse, wurde allerdings auf die Weise ausgelegt, dass ein mehr an kollektiver Sicherheit erst die Grundlage für die Auslebung individueller Rechte schaffen würde – was freilich weder zu einer Überwindung der Diskrepanz führen würde, noch für eine Balance sprach, sondern die Bedeutung der Sicherheit klar über die Bedeutung von Freiheit stellte.[243] Zudem rahmte Frattini Sicherheit als kollektive Angelegenheit (*collective security*), Freiheit hingegen als Sache des Individuums (*individual freedom*).

3.4.1.3.2 Empfehlungen der Zukunftsgruppe Justiz

Ebenfalls im Jahr 2007 wurde auch die *Hochrangige Beratende Gruppe zur Zukunft der Europäischen Justizpolitik* ins Leben gerufen. Das Ziel der Gruppe war es, Vorschläge für das künftige EU-Programm im Bereich der EU-Justizpolitik zu unterbreiten. Die Mitgliedschaft der Gruppe war vergleichbar jener der Zukunftsgruppe Innenpolitik: Ihr gehörten die nationalen Justizminister des amtierenden (Deutschland, Portugal, Slowenien) und folgenden Dreiervorsitzes (Frankreich, die Tschechische Republik, Schweden) sowie im Rotationsverfahren ein Mitglied des darauffolgenden Ratsvorsitzes (Spanien, Belgien und Ungarn) an. Daneben partizipierten Vertreter des Europäischen Parlaments, insb. Mitglieder des LIBE-Ausschusses und des Rechtsausschusses sowie Irland als Vertreter der mit *common law* regierten Mitgliedstaaten an den Sitzungen der Zukunftsgruppe Justiz. Geleitet wurde die Gruppe vom amtierenden Vorsitz des Ministerrats gemeinsam mit dem Vizepräsidenten der Europäischen Kommission (Hochrangige Beratende Gruppe zur Zukunft der Europäischen Justizpolitik 2008, 5).

243 Es sei daran erinnert, dass Datenschutzbefürworter im Kontext der Balance-Debatten stets darauf hinweisen, dass es einen Kernbereich von Grundrechten gäbe, der solchen Abwägungsprozessen nicht unterworfen werden dürfe und die Gewährleistung von Sicherheit auch ohne die Einschränkung von Grundrechten möglich sei (Bendrath 2009).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Gruppe nahm ihre Arbeit im September 2007 auf und legte ihren Abschlussbericht im Juni 2008 vor (ebd., 6).

Wie von den mit Justiz befassten Ministern bzw. ihren Mitarbeitern zu erwarten war, legte die Zukunftsgruppe Justiz deutlich mehr Wert auf ein hohes Schutzniveau: Der Schutz personenbezogener Daten und das Recht auf Privatleben wurden in dem Dokument als eine Grundsatzfrage demokratischer Gesellschaften bezeichnet und auch das voraussichtliche baldige Inkrafttreten des Lissaboner Vertrags und die damit einhergehende Anwendbarkeit der Grundrechtecharta erwähnt. Der Schutz personenbezogener Daten sei angesichts informationstechnologischer Entwicklungen bedroht, da zunehmend mehr personenbezogene Daten verarbeitet würden, die *die Merkmale, Gewohnheiten oder ein einmaliges Verhalten von Personen offenbarten* und sich zeitlich fast unbegrenzt speichern und mit anderen Datenbanken abgleichen ließen (ebd., 28). Insbesondere wurden die Verarbeitung personenbezogener Daten für andere Zwecke als denjenigen, für den sie erfasst worden waren, sowie der unbegrenzte Abgleich mit anderen Datenbanken bemängelt. In diesem Kontext stellte die Gruppe zudem klar, dass die daraus resultierenden Gefahren nicht nur für den Einzelnen, sondern für die Gesellschaft insgesamt bedrohlich seien. Zudem vertrat die Zukunftsgruppe Justiz die Ansicht, dass eine Unterschreitung des hohen Datenschutzniveaus, insbesondere im Falle terroristischer Bedrohungen und von Großkriminalität, angemessen sei. Demgegenüber forderten Innenpolitiker regelmäßig die Ausweitung umfangreicher Datenverarbeitungen auch auf kleinere Delikte. Zugleich stellten die Justizminister aber klar, dass „das Recht auf Privatsphäre, einschließlich des speziellen Bereichs des Datenschutzes, […] nicht den Notwendigkeiten der Strafverfolgung geopfert werden [sollte]." (ebd., 30) Die sich aus der Europaratskonvention 108, der DS-RL sowie aus dem JI-Rahmenbeschluss ableitenden Grundprinzipien des Datenschutzes dürften auch angesichts der „Notwendigkeit, der globalen Bedrohung durch den Terrorismus und das organisierte Verbrechen zu begegnen, nicht aus der Rechtsordnung ausgeschlossen werden." (ebd.) Denn: „Ein angemessener Ausgleich zwischen den Rechten bedeutet nicht, dass der Rechtsschutz unter bestimmten gesetzlich definierten Umständen völlig fallen gelassen werden kann." (ebd.) Daher formulierte die Zukunftsgruppe Justiz fünf zentrale Anforderungen, die an einen wirksamen Datenschutz im Sicherheitsbereich gestellt werden müssten:

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

- „Datenschutzregeln sind für jeden speziellen Bereich erforderlich.
- Datenschutzregeln müssen angemessen und möglichst genau formuliert sein. Insbesondere müssen diese Vorschriften die spezielle Eingriffsintensität in die Grundrechte bei der Datenerhebung und Datenverwendung für Strafverfolgungszwecke angemessen berücksichtigen.
- Darüber hinaus ist stets sicherzustellen, dass die Betroffenen ein wirksames Recht auf Auskunft, Berichtigung, Löschung, Sperrung und Entschädigung haben.
- Es muss eine unabhängige Datenschutzaufsichtsbehörde mit angemessener Personal- und Sachmittelausstattung sowie wirksamen Befugnissen geben.
- Schließlich müssen die personenbezogenen Daten wirksam geschützt werden, um unbefugten Zugang und Nutzung durch Dritte zu verhindern." (ebd., 29)

3.4.1.3.3 Kommissionsentwurf

Am 10. Juni 2009 veröffentlichte die Europäische Kommission schließlich ihren Entwurf für das nächste Mehrjahresprogramm. Als zentrale Herausforderungen benannte die Kommission das Vorantreiben der Unionsbürgerschaft, Cyberkriminalität, Terrorismus, die Sicherung der EU-Außengrenzen, die Bekämpfung der „illegalen" Einwanderung und die Vereinheitlichung der nationalen Asylsysteme (EC 2009a, 4 f.). Gerade im Bereich der innenpolitisch relevanten Themen basierten die Kommissionsvorschläge weitestgehend auf dem Abschlussbericht der Zukunftsgruppe Inneres und sahen eine Verschärfung sicherheitspolitischer Maßnahmen, insb. die weitere Verbesserung des Informationsaustauschs zwischen nationalen Sicherheitsbehörden, vor (ebd., 16 f.).

Zu Fragen des Datenschutzes äußerte sich die Kommission allerdings in deutlich stärkerer Anlehnung an den Abschlussbericht der Zukunftsgruppe Justiz. Unter Bezugnahme auf die Grundrechtecharta und vor dem Hintergrund der rasanten Entwicklungen auf dem Gebiet datenverarbeitender Technologien problematisierte die Kommission den wachsenden Austausch personenbezogener Daten. Die Kommission hob die Bedeutung der Verarbeitungsgrundsätze der Zweckbindung, Verhältnismäßigkeit und Rechtmäßigkeit der Verarbeitung, der zeitlich begrenzten Speicherung, Vertraulichkeit und Sicherheit der Daten, die Wahrung der Rechte des Einzelnen sowie die Beaufsichtigung durch eine unabhängige Stelle hervor und stellte die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ausarbeitung zusätzlicher Maßnahmen zum Zwecke der Aufrechterhaltung der Grundsätze in Aussicht. Während im Haupttext offengelassen wurde, ob diese Maßnahmen legislativer oder sonstiger Art sein würden (ebd., 9), formulierte der Anhang eine konkretere Vorstellung in Richtung eines gemeinsamen legislativen Instruments, das für alle Politikbereiche der Union (also die dann ehemalige erste und dritte Säule) gelten sollte: „Die Union muss eine umfassende Regelung zum Schutz personenbezogener Daten schaffen, die für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt." (ebd., 33) Mit diesem Vorschlag ging die Kommission zudem deutlich über die Vorschläge der Zukunftsgruppe Justiz hinaus. Darüber hinaus hob die Kommission die Bedeutung *datenschutzfreundlicher Technologien*, *internationaler Datenschutzstandards* und von *Informations- und Aufklärungskampagnen für die Bevölkerung*, insb. die am stärksten gefährdeten Personengruppen, hervor (ebd., 9). Im Hinblick auf die verbesserte Verbreitung datenschutzfreundlicher Technologien wurde vorgeschlagen, Produkte und Dienstleistungen eventuell mit einem europäischen Datenschutzprüfsiegel zu versehen, um deren Marktchancen zu erhöhen (ebd.).

3.4.1.3.4 Stellungnahme des Europäischen Datenschutzbeauftragten zum Kommissionsentwurf

Nachdem der EDSB bereits im Vorfeld der Veröffentlichung des Kommissionsentwurfs informell konsultiert worden war (EDSB 2009, 8, Nr. 2), nahm er am 10. Juli 2009 auch formell Stellung. In seiner Stellungnahme zeigte sich der EDSB erfreut darüber, dass die Kommission den Schutz der Grundrechte und insbesondere den Schutz personenbezogener Daten „als eine der zentralen Fragen für die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts" (ebd., 10, Nr. 21) anerkannt und den Beitritt zur der EU zur EMRK zu einem Handlungsschwerpunkt erklärt habe. Insgesamt bescheinigte der EDSB dem Kommissionsentwurf, dass der „Notwendigkeit eines ausgewogenen Verhältnisses [zwischen Sicherheit und Freiheit], einschließlich der Notwendigkeit des Schutzes personenbezogener Daten, auf gute Weise Rechnung getragen [wird]" (ebd., 10, Nr. 23), weil der Entwurf praktisch auf die Erhöhung des bisherigen Schutzniveaus abziele. Entsprechend formulierte der EDSB dem Ministerrat gegenüber die Hoffnung, dass dieser dem Vorschlag der Kommission folge (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Inhaltlich stellte der EDSB die mit dem Kommissionsentwurf verfolgte Verbesserung des Schutzniveaus als eine notwendige Folge der jahrelang praktizierten Ausweitung von sicherheitsorientierten Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts dar (ebd., 10, Nr. 19). Im selben Zusammenhang wies der EDSB auch auf die gewachsene öffentliche Aufmerksamkeit im Hinblick auf Datenschutzfragen hin (ebd., 11, Nr. 26). Zwar fokussierte sich der EDSB stärker auf die mit dem voraussichtlichen Inkrafttreten des Vertrags von Lissabon geänderte rechtliche Situation als es die Kommission in ihrer Mitteilung tat (ebd., 10, Nr. 18), doch stellte der EDSB dem Kommissionsentwurf folgend klar, dass die von der Kommission vorgeschlagene *Schaffung einer umfassenden Regelung zum Datenschutz, die für sämtliche Zuständigkeitsbereiche der EU gleichermaßen* gelte, auch dann zu begrüßen sei, falls der Vertrag nicht in Kraft träte (ebd., 11, Nr. 27). Unabhängig davon, ob auf Grundlage des Vertrags von Lissabon ein einziger Rechtsrahmen oder mehrere Instrumente in Kraft träten, sei das dabei anzustrebende Ziel die Gewährleistung von Kohärenz, „nötigenfalls durch Harmonisierung und Konsolidierung der verschiedenen Rechtsakte, die für den Raum der Freiheit, der Sicherheit und des Rechts gelten." (ebd., 11, Nr. 28) Allerdings sei ein einzelnes Instrument insbesondere deshalb zu bevorzugen, weil „hierdurch in Zukunft die Schwierigkeiten vermieden [würden], die auftreten, wenn es darum geht, eine Trennungslinie zwischen den Säulen zu ziehen, wenn Daten, die im privaten Sektor zu Geschäftszwecken erhoben wurden, zu einem späteren Zeitpunkt für Strafverfolgungszwecke genutzt werden." (ebd., 12, Nr. 35) Insofern bekräftigte der EDSB die im Kommissionsentwurf genannte Schaffung einer umfassenden Regelung noch einmal und befürwortete insbesondere die Aufnahme der Überarbeitung des JI-Rahmenbeschlusses als einen Handlungsschwerpunkt in das Stockholmer Programm (ebd., 12, Nr. 36). Im Hinblick auf die Frage der Zweckbindung befürwortete der EDSB deren sorgfältige Abwägung und klare politische Regelung im Rahmen des Stockholmer Programms, sodass eine Abweichung in konkreten Einzelfällen und auf Basis eines politischen Konsenses möglich würde, es aber nicht regelmäßig den datenverarbeitenden staatlichen Stellen freigestellt wäre, darüber selbst zu entscheiden.[244] Den Vorschlag der Kommission hinsichtlich der Unterstützung datenschutzfreundlicher Technologien

244 Als Grundsatz formulierte der EDSB dazu: „Wenn immer derartige Maßnahmen vorgeschlagen werden, muss sehr eindeutig nachgewiesen werden können, dass eine derart in die Privatsphäre eingreifende Maßnahme erforderlich ist. Kann dieser

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mittels der Schaffung eines Zertifizierungssystems für Hersteller und Nutzer von Informationssystemen griff der EDSB befürwortend auf, ergänzte diesen allerdings um die Forderung der Einführung „einer rechtlichen Verpflichtung für Hersteller und Nutzer von Informationssystemen, nur solche Systeme zu verwenden, die mit dem Grundsatz des ‚eingebauten Datenschutzes' vereinbar sind." (ebd., 19, Nr. 87) Schließlich unterstützte der EDSB auch die im Kommissionsentwurf genannten Elemente in Bezug auf den Datenaustausch mit Drittstaaten (ebd., 19 f., Nr. 88).

3.4.1.3.5 Ratsentwurf

Nach Bekanntgabe des Kommissionsentwurfs kommentierten die Mitgliedstaaten diesen und die amtierende schwedische Ratspräsidentschaft erarbeitete auf Basis der mitgliedstaatlichen Rückmeldungen einen neuen Entwurfstext, der am 16. Oktober 2009 veröffentlicht wurde (Ratsvorsitz 2009b). Entgegen dem Kommissionsentwurf, der den wachsenden Austausch personenbezogener Daten klar problematisierte, hob der Ratsentwurf auf „ein ausgewogenes Verhältnis zwischen dem Bedarf an einem zunehmenden Austausch personenbezogener Daten und einer größtmöglichen Achtung des Schutzes der Privatsphäre" (ebd., 10) ab. Zudem war die infolge des Inkrafttretens des Lissabonner Vertrags bzw. der Grundrechtecharta erforderlich gewordene Überarbeitung der Datenschutzregelungen der EU (der ersten und dritten Säule) etwas defensiver formuliert. Während die Kommission die Schaffung einer umfassenden Regelung für alle Datenschutzbereiche vorgesehen hatte, schlug der Rat lediglich vor, die Funktionsweise der geltenden Instrumente zunächst zu bewerten, um dann gegebenenfalls weitere legislative und nicht-legislative Initiativen vorzulegen (ebd.). Abgesehen davon wurden die übrigen Punkte des Kommissionsentwurfs übernommen: Auch der Ratsentwurf sprach sich für die Erhaltung und Bekräftigung der Grundprinzipien *wie Zweckgebundenheit, Verhältnismäßigkeit und Rechtmäßigkeit der Verarbeitung, zeitlich begrenzte Speicherung, Sicherheit und Vertraulichkeit*, für die *Aushandlung eines Abkommens mit den Vereinigten Staaten*, die *Ausarbeitung eines Rechtsinstruments mit Datenschutz-Grundsätzen für die Weitergabe von Daten, die sich in privatem Besitz befinden, an Drittstaaten zu Strafverfolgungszwecken*, die *Prü-*

Nachweis geführt werden, so muss sichergestellt werden, dass die Rechte des Einzelnen uneingeschränkt gewahrt werden." (ebd., 16, Nr. 64)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

fung der Einführung eines europäischen Prüfsiegels für „datenschutzfreundliche" Technologien, Produkte und Dienstleistung und für *Informationskampagnen insbesondere zur Sensibilisierung der Öffentlichkeit* aus (ebd., 10 f.). Zudem übernahm der Ratsentwurf auch weitestgehend den Kommissionsvorschlag, wonach die Europäische Union bei der Entwicklung und Förderung internationaler Standards im Bereich des Datenschutzes und beim Abschluss geeigneter bilateraler oder multilateraler Instrumente als treibende Kraft fungieren solle (ebd., 11).

3.4.1.3.6 Parlamentsposition

Auf Seiten des Parlaments waren der Rechtsausschuss (Berichterstatter: Luigi Berlinguer (Italien, sozialdemokratisch/linksliberal/christlich-soziale Partito Democratico/S&D)), der LIBE-Ausschuss (Berichterstatter: Juan Fernando López Aguilar[245] (Spanien, sozialdemokratische PSOE/S&D)) sowie der Ausschuss für konstitutionelle Fragen (Berichterstatter: Carlo Casini (Italien, christdemokratische UDC/EVP)) mit den Entwürfen der Kommission und des Ministerrats befasst (Berlinguer, López Aguilar, und Casini 2009). Der Entschließungsantrag des Parlaments wurde am 25. November 2009 mit der Stimmenmehrheit von ALDE, EVP, SDE sowie mit Hilfe einiger grüner Stimmen mit 487 Für-Stimmen – bei 122 Gegenstimmen von EKR, EFD, GUE/NGL, NI und einigen wenigen Abgeordneten der Grünen und 49 Enthaltungen durch vor allem grüne Europaabgeordnete – angenommen (EP 2009e, 104 f., 2009d, 15). Die Grünen gaben als Grund für ihre Wahlentscheidung weniger inhaltliche als prozedurale Bedenken an: Das Ausschussverfahren, das zur Erarbeitung der Entschließung geführt habe, sei *in hohem Maße intransparent und teils chaotisch* gewesen. Zudem seien die kleinen Fraktionen gezielt von der Erarbeitung der Entschließung weitestgehend ausgeschlossen worden (Jan Philipp Albrecht, in: EP 2009f). Die GUE/NGL begründete ihre Wahlentscheidung mit der generellen Ablehnung des „volksfeindlichen" Stockholmer Programms: „Der Raum der Freiheit, der Sicherheit und des Rechts der EU und die Programme zu dessen Umsetzung dienen nicht den Interessen der Menschen; sie bilden im Gegenteil einen Maßnahmenkatalog, der individuelle und

245 López Aguilar, der zwischen 2004 und 2007 in der Regierung Zapatero das Amt des Justizministers innehatte, war im Juli 2009 zum Vorsitzenden des LIBE-Ausschusses gewählt worden. Das Amt hatte er bis Ende Juni 2014 und damit noch während der DSGVO-Verhandlungen inne (EP 2020c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

soziale Rechte und demokratische Freiheiten erstickt und Autoritarismus und Repression zu Lasten von Arbeitern, Einwanderern und Flüchtlingen intensiviert, das politische System und die Herrschaft von Monopolen aufrecht erhält und darauf abzielt, Arbeiter- und Volksbewegungen zu zerschlagen, was die Voraussetzungen für den brutalen Angriff des Kapitals auf Arbeitnehmerrechte und soziale Rechte der Arbeiterklassen und des Volkes schafft." (Charalampos Angourakis, in: EP 2009g) Von der EKR wurden Elemente des Stockholmer Programms, wie „die Zusammenarbeit und Solidarität in den Bereichen Polizei, Bekämpfung von grenzüberschreitender Kriminalität und Korruption, Schutz der Grundrechte und das Erzielen von Lösungen in Einwanderungsfragen durch die Unterstützung der Länder in Südeuropa, die sich großen Einwanderungsproblemen gegenübersehen," (Timothy Kirkhope, in: EP 2009g) zwar begrüßt, das Stockholmer Programm als Ganzes jedoch trotzdem abgelehnt, da mit ihm zu viel Entscheidungsmacht in strafrechtlichen und asylpolitischen Belangen an die EU-Ebene übertragen werde (ebd.). In ähnlicher Weise kritisierten auch die beiden rechtsgerichteten fraktionslosen Abgeordneten Philip Claeys (Vlaams Belang, Belgien) und Bruno Gollnisch (Front National, Frankreich) die Machtverlagerung auf die Unionsebene (ebd.).

Im Entschließungsantrag bekräftigte das Parlament vor allem die von der Kommission angeführten Erwägungsgründe und datenschutzpolitischen Vorschläge, ging in einzelnen Bereichen allerdings noch weiter als die Kommission. So teilte das Parlament die Besorgnis der Kommission hinsichtlich der Zunahme der Verarbeitung personenbezogener Daten, konkretisierte die schriftlichen Äußerungen der Kommission allerdings um mehrere spezifische Probleme: Zum einen wurde als konkreter Grund für die Zunahme von Datenschutzproblemen auf die wachsende Bedeutung des Internets und grenzüberschreitender Datenverarbeitungen verwiesen. Darauf aufbauend wurde argumentiert, dass diese Entwicklungen die Verabschiedung weltumspannender Datenschutzstandards erforderlich machten (EP 2009f, Nr. 82). Zudem machte das Parlament klar, dass die Datenschutzvorschriften in einem etwaigen Drittstaat, in den personenbezogene Daten von EU-Bürgerinnen und -Bürgern übertragen werden sollten, den europäischen Vorschriften entsprechen müssten (ebd., Nr. 89). Daneben wurde auf die bei der weiteren Umsetzung des Grundsatzes der Verfügbarkeit anhaltende Gefahr verwiesen, auch solche personenbezogenen Daten intensiviert auszutauschen, die nicht rechtmäßig erhoben worden seien (ebd., Nr. 86). Auch die zunehmende Verbreitung der Praxis der Erstellung von Persönlichkeitsprofilen im Kontext von *data-mining*-Technologien und der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Vorratsdatenspeicherung für präventive und polizeiliche Zwecke wurden problematisiert (ebd., Nr. 88).

In Bezug auf die von Kommission und Rat hervorgehobene Bedeutung datenschutzfreundlicher Technologien drückte das Parlament lediglich aus, dass dieser Schritt begrüßt werde, schlug allerdings keine praktischen Umsetzungsschritte (etwa in Bezug auf Datenschutz-Gütesiegel bzw. Zertifizierungen) vor (ebd., Nr. 91). Deutlich umfangreicher widmete sich das Parlament hingegen dem von Kommission und Rat nicht erwähnten Prinzip des eingebauten Datenschutzes („privacy by design"), das „wesentlicher Bestandteil jeder Entwicklung sein muss, bei der die Sicherheit personenbezogener Daten sowie das Vertrauen in diejenigen und die Glaubwürdigkeit derjenigen, die über solche Daten verfügen, gefährdet werden könnten" (ebd., Nr. 85).

Schließlich forderte auch das Parlament „eine gründliche Evaluierung aller einschlägigen Rechtsvorschriften (betreffend u. a. Terrorismusbekämpfung, polizeiliche und justizielle Zusammenarbeit, Einwanderung, transatlantische Abkommen) im Bereich des Schutzes der Privatsphäre und des Datenschutzes" (ebd., Nr. 90) und forderte mehrfach die Einführung einer allumfassenden einheitlichen Regelung zum Schutz personenbezogener Daten in der Europäischen Union (ebd., Nr. 83, 146). Im Hinblick auf das bevorstehende Inkrafttreten des Vertrags von Lissabon kritisierte das Parlament die Kommission und den Rat dahingehend, dass dieser in Kraft treten werde, „ohne dass Rat und Kommission die notwendigen Maßnahmen für einen ‚Neubeginn' im Raum der Freiheit, der Sicherheit und des Rechts angemessen vorbereitet haben" (ebd., Nr. 148). Daher forderte das Parlament die Kommission dazu auf, einen Legislativvorschlag „zur Umsetzung von Artikel 16 AEUV und Artikel 39 EUV, insbesondere im Hinblick auf den Datenschutz bei Fragen der Sicherheit und gleichzeitig zur Ausweitung des Anwendungsbereichs der Verordnung (EG) Nr. 45/2001 im Hinblick auf den Datenschutz durch die Organe der Europäischen Union" (ebd.) zu unterbreiten.

3.4.1.3.7 Das finale Stockholmer Programm

Während der Monate Oktober und November setzte sich der Ministerrat auf weiteren Sitzungen mit dem Stockholmer Programm auseinander, nahm weitere Änderungen vor (Ratsvorsitz 2009a, 1) und entschied schließlich auf der JI-Ratssitzung vom 30. November über den finalen Ent-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wurf. Dieser wurde an den Europäischen Rat weitergeleitet, der das Stockholmer Programm schließlich auf seiner Sitzung vom 10. und 11. Dezember 2009 verabschiedete (Europäischer Rat 2009, 1).

Vor dem Eindruck des gescheiterten Verfassungsvertrags und des wachsenden Misstrauens (Piquer 2014) in die Europäische Union und ihre Institutionen war das Stockholmer Programm in besonderem Maße darum bemüht, die Bedeutung des Dokuments für die Bürgerinnen und Bürger der EU herauszustellen. Die Herausforderungen, denen sich die Union aus der Perspektive des Europäischen Rats gegenübersah, fanden sich nunmehr im Abschnitt „politische Prioritäten". Als solche wurden benannt: *Förderung der Unionsbürgerschaft und der Grundrechte*; *Europa als Raum des Rechts und der Justiz*; *ein Europa, das schützt*; *Zugang zu Europa in einer globalisierten Welt*; e*in Europa der Verantwortung, der Solidarität und der Partnerschaft in Migrations- und Asylfragen*; sowie *die Rolle Europas in der globalisierten Welt*. Somit knüpfte das Stockholmer Programm zwar an den bereits in den Vorläufer-Programmen vorhandenen Fokus auf die Einrichtung einer einheitlichen europäischen Sicherheitsarchitektur an und intensivierte diese Pläne weiter, doch zugleich räumte es erstmals grundrechtlichen Fragen einen zentralen Platz ein. Bereits unter dem Punkt „Förderung der Unionsbürgerschaft und der Grundrechte" wurde die herausgehobene Stellung deutlich, die dem Datenschutz im Rahmen des Stockholmer Programms zuerkannt wurde: „Die Achtung der menschlichen Person und ihrer Würde sowie der übrigen in der Grundrechtecharta der Europäischen Union und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten verankerten Rechte zählen zu den zentralen Werten. Dazu gehören die Wahrung der persönlichen Rechte und Freiheiten, insbesondere der Privatsphäre, über Staatsgrenzen hinweg, vor allem durch den Schutz personenbezogener Daten." (Europäischer Rat 2010, 4, Nr. 1.1)

Detailliert wurde auf das Thema Datenschutz schließlich im Kapitel 2.5 „Schutz der Rechte der Bürger in der Informationsgesellschaft" eingegangen. Unter Bezugnahme auf die Grundrechtecharta wurde dargelegt, dass die Union „dem zunehmenden Austausch personenbezogener Daten und dem Erfordernis der Sicherstellung des Schutzes der Privatsphäre Rechnung tragen [müsse]." (ebd., 10, Nr. 2.5) Auf das kurz zuvor am 1. Dezember 2009 erfolgte Inkrafttreten des Vertrags von Lissabon wurde bereits in der Einleitung positiv Bezug genommen (ebd., 4, Nr. 1). Die Forderung des Parlaments und des EDSB nach einer umfassenden Strategie zum Datenschutz innerhalb der EU wurde übernommen, ebenso wie die Forderung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nach dem Beitritt der Union zur Datenschutzkonvention des Europarats. Übernommen wurde auch die zur Reduktion (sicherheits-)behördlicher Willkür gestellte Forderung, dass die Union klare Bedingungen festlegen solle, „unter welchen Umständen ein Eingriff öffentlicher Stellen in die Ausübung" der Datenschutzrechte gerechtfertigt sei (ebd.). Entgegen den üblichen Formulierungen aus ähnlichen Dokumenten aus der nahen Vergangenheit wurde zudem die Aussage, dass die *Union der Notwendigkeit zu einem verstärkten Austausch personenbezogener Daten Rechnung tragen müsse*, um die Aussage ergänzt, dass *dabei gleichzeitig eine größtmögliche Achtung des Schutzes der Privatsphäre* sicherzustellen sei. Übernommen wurde auch die Forderung der Einhaltungen der Datenschutz-Grundprinzipien der *Zweckbindung*, *Verhältnismäßigkeit* und *Rechtmäßigkeit der Verarbeitung*, der *Speicherbegrenzung*, der *Sicherheit und Vertraulichkeit*, der *Achtung der Betroffenenrechte*, der *Kontrolle durch unabhängige nationale Aufsichtsbehörden* sowie des *Zugangs zu einem wirksamen Rechtsschutz* (ebd.). Als konkrete Maßnahmen, um deren Umsetzung der Europäische Rat die Kommission ersuchte, wurden genannt (ebd., 11):

- die Bewertung der Funktionsweise der verschiedenen Datenschutz-Rechtsinstrumente und ggf. die Vorlage legislativer und nicht-legislativer Initiativen;
- die Verbesserung der Einhaltung der Datenschutzgrundsätze durch die Entwicklung geeigneter datenschutzfreundlicher Technologien, indem die Zusammenarbeit zwischen privatem und öffentlichem Sektor, speziell im Bereich der Forschung, verbessert werde.
- die Prüfung der Einführung eines europäischen Prüfsiegels für datenschutzfreundliche Technologien, Produkte und Dienstleistungen;
- die Durchführung von Informationskampagnen, insbesondere zur Sensibilisierung der Öffentlichkeit;
- die Vorlage einer Empfehlung zur Aushandlung von Abkommen mit den Vereinigten Staaten über Datenschutz und Datenaustausch zu Zwecken der Strafverfolgung;
- die Prüfung der notwendigen Hauptelemente für Datenschutzabkommen mit Drittstaaten für Strafverfolgungszwecke, bei denen möglicherweise im Bereich des privaten Datenschutzrechts gesammelte personenbezogene Daten an Sicherheitsbehörden weitergereicht werden könnten.

In abgeschwächter Weise gegenüber der EDSB- und Parlamentsposition wurde die Forderung nach einer Entwicklung und Förderung internationaler Datenschutzstandards übernommen. Dieser Aussage wurde die ab-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schwächende Formulierung, wonach die Union „in einem allgemeineren Rahmen" als treibende Kraft fungieren müsse, hinzugefügt.

Nicht übernommen wurde hingegen die zentrale Forderung von Kommission, EDSB und Parlament nach der Einführung einer allumfassenden, einheitlichen Regelung zum Schutz personenbezogener Daten in der EU, welche die ehemalige erste und dritte Säule einschließen würde. In diesem Zusammenhang verwies der Europäische Rat lediglich auf die Überprüfung der bestehenden Rechtsinstrumente, legte sich aber weder im Hinblick auf deren Überarbeitung eindeutig fest noch äußerte es sich dahingehend, ob ein allgemeiner Rahmen für alle ehemaligen Säulen wünschenswert sei (Europäischer Rat 2010, 11, Nr. 2.5). Die Streichung dieses Passus' ist daher als Kompromiss gegenüber jenen Staaten zu interpretieren, die kein Interesse an einer umfassenden Regelung hatten.

3.4.1.3.8 Reaktionen auf das Stockholm-Programm

Sowohl vor als auch nach seiner Verabschiedung erntete das Stockholmer Programm massive Kritik seitens bürgerrechtspolitischer Akteure. So wurde bereits vor seiner Verabschiedung der Erarbeitungsprozess des Programms vonseiten des European Civil Liberties Network (ECLN)[246] im Hinblick auf die mangelnde Umsetzung demokratischer Diskursstandards kritisiert.[247] Weder habe man die europäische Öffentlichkeit in ausreichendem Maße[248] miteinbezogen, noch sei es vertretbar, dass die Letztentscheidung beim Rat allein liege, die nationalen Parlamente und das Europäische Parlament dagegen nur unverbindlich konsultiert würden (ECLN 2009, 1). Der Datenschutzrat – die österreichische Datenschutzaufsichtsbehörde – bemängelte Mitte Juli 2009 die Beibehaltung des Verfügbarkeitsgrundsatzes

246 Das ECLN war im Jahr 2005 unter anderem von Statewatch, der Bürgerrechte & Polizei/CILIP sowie vom Komitee für Grundrechte und Demokratie gegründet worden. Im Jahre 2009 hatte das ECLN mehr als 40 Unterstützerorganisationen (Monroy 2009a).

247 Für einen Überblick über die Kritiken an der Erarbeitungsweise der Programme von Tampere und Haag, siehe: (Bunyan 2008, 3–4). Für eine ausführlichere Analyse des Entscheidungsprozesses, der zum Programm von Tampere führte, siehe: (Bunyan 2003).

248 Tatsächlich hatte die Kommission im Herbst 2008 eine öffentliche Online-Konsultation initiiert. Allerdings konnten die vorgegebenen Fragen nur mittels Multiple Choice beantwortet werden, es konnten also keine eigenen Antworten – in anderen Worten: Keine eigene Meinung – eingebracht werden (Monroy 2009a).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

bzw. die Förderung der Interoperabilität unterschiedlicher Datenbanken und brachte sein generelles Misstrauen gegenüber den angekündigten datenschutzpolitischen Maßnahmen zum Ausdruck (Monroy 2009a). Nicht glaubwürdig erschienen die bürgerrechtlichen Beteuerungen des Ministerrats allerdings auch den Europaabgeordneten, die den Prozess beobachteten. So wies die linksliberale niederländische Europaabgeordnete Sophie in 't Veld (ALDE/D66) darauf hin, dass die Ankündigung des Ministerrats „einen Bruch mit der [bisherigen] Tradition bedeuten würde und dass man – ausgehend von den Erfahrungen mit den Urteilen zu SWIFT, ACTA und CIA und der Einschätzung von aktuellen Anti-Terrorismusmethoden – davon ausgehen müsse, dass sich nicht viel verändert habe." (McNamee 2009)

Nach der Verabschiedung des Stockholm-Programms fokussierte sich die Kritik besonders auf die im Rahmen der Interoperabilität geplante Zusammenführung von polizeilichen Großdatenbanken, die weitere Intensivierung des Verfügbarkeitsgrundsatzes, die Nutzung der Daten zu für präventive Zwecke sowie die Einführung eines europäischen Systems zur Fluggastdatensammlung (Krempl 2009b, 2009a)

3.4.1.3.9 Umsetzung des Stockholm-Programms: Die formelle Geburt der Datenschutzreform

Nachdem das Stockholm-Programm verabschiedet worden war, war es an der Kommission, die auf höchster EU-Ebene beschlossenen politischen Leitlinien im Rahmen eines Aktionsplans zu konkretisieren. Am 20. April 2010 veröffentlichte die Europäische Kommission daher ihren „Aktionsplan zur Umsetzung des Stockholmer Programms" (EC 2010). Bereits in der Einleitung des Aktionsplans machte die Kommission auf die infolge des Inkrafttretens des Vertrags von Lissabon veränderten europapolitischen Bedingungen aufmerksam: „Mit der Aufwertung der Rolle des Europäischen Parlaments, das ab jetzt in den meisten Bereichen Mitgesetzgeber ist, und der engeren Einbeziehung der nationalen Parlamente unterliegt die EU in Bezug auf ihr Handeln im Interesse der Bürger künftig einer größeren Rechenschaftspflicht, wodurch auch die demokratische Legitimität der Union gestärkt wird. Die Abstimmung mit qualifizierter Mehrheit, die künftig für die meisten Politikbereiche gilt, wird die Beschlussfassung im Rat erleichtern. Nicht zuletzt wird auch die gerichtliche Kontrolle verbessert, da dem Europäischen Gerichtshof jetzt die gerichtliche Nachprüfung aller Aspekte

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des Bereichs Freiheit, Sicherheit und Recht obliegt und die Grundrechtecharta der EU rechtsverbindlich wird." (ebd., 3)

Gleich im ersten inhaltlichen Kapitel widmete sich die Kommission dem Schutz der Grundrechte und bekannte sich wortgewaltig und unzweifelhaft zum Schutz dieser: „Der Schutz der in der Grundrechte-Charta verankerten Rechte muss uneingeschränkt gelten, und die Rechte müssen effektiv und konkret wirken. Die Grundrechte-Charta muss zur Richtschnur unseres Handelns werden. Verstöße gegen die Charta wird die Kommission unter keinen Umständen dulden." (ebd.) Wie angesichts der bisherigen, im Rahmen der Erarbeitung des Stockholm-Programms gezeigten, Haltung der Kommission zu erwarten war, legte sie großen Wert auf das Thema Datenschutz: „In einer globalen Gesellschaft, die durch raschen technologischen Wandel mit grenzenlosem Informationsaustausch geprägt ist, kommt der Sicherung der Privatsphäre größte Bedeutung zu. Die Union muss deshalb für eine konsequente Anwendung des Grundrechts auf Datenschutz sorgen. Wir müssen die Position der EU bezüglich des Schutzes personenbezogener Daten bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Kriminalprävention, sowie in unseren internationalen Beziehungen stärken." (ebd.)

Im Maßnahmenkapitel machte die Kommission dann auch ihre datenschutzpolitisch bedeutsamste Ankündigung. Für das Jahr 2010 wurde die Vorlage eines „neuen umfassenden Rechtsrahmens für den Datenschutz" angekündigt. Daneben wurde für dasselbe Jahr eine „Mitteilung über einen neuen Rechtsrahmen für den Schutz personenbezogener Daten nach Inkrafttreten des Vertrags von Lissabon", eine weitere „Mitteilung über Datenschutz und Vertrauen im ‚Digitalen Europa': Stärkung des Vertrauens der Bürger in neue Dienste" sowie eine „Empfehlung zur Aufnahme von Verhandlungen mit den Vereinigten Staaten von Amerika über ein Datenschutzabkommen für Strafverfolgungszwecke" in Aussicht gestellt. Eine „Mitteilung über Hauptelemente für Datenschutzabkommen zwischen der Europäischen Union und Drittstaaten für Strafverfolgungszwecke" wurde für das Jahr 2012 angekündigt. Zudem teilte die Kommission mit, dass *Maßnahmen zur Aufklärung über die Datenschutzrechte* in Arbeit seien (ebd., 72). Im Hinblick auf sicherheitsbehördliche Datenverarbeitungssysteme wurde deren gründliche Prüfung im Hinblick auf ihre *Zweckmäßigkeit, Effizienz, Wirkung, Verhältnismäßigkeit* sowie die *Achtung des Rechts auf Privatsphäre* angekündigt. Schließlich sei prioritär eine Bilanz der in den letzten Jahren eingeführten Anti-Terror-Maßnahmen zu ziehen und diese auf Verbesserungsmöglichkeiten hin zu prüfen (ebd., 6).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.1.3.10 Zwischenfazit

Die Erarbeitung des Stockholmer Programms stellt eindrucksvoll einerseits die Versuche der EU zur Schau, sich hin zu einer stärker am Bürger ausgerichteten Politik zu orientieren und veranschaulicht andererseits die inneren Widersprüche im Institutionengefüge der EU. Ursächlich für die weitere Fokussierung der EU-Politik auf die Bürgerinnen und Bürger der Union war das sinkende Vertrauen der Bevölkerung in die Unionspolitiken insbesondere im Zuge der Finanzkrise 2007 und des letztlich gescheiterten Verfassungsvertrags. Beunruhigend für EU-Politikerinnen und -Politiker war aber auch das verzögerte Inkrafttreten des Vertrags von Lissabon. Obwohl die Mehrheit der EU-Bevölkerung weiterhin hinter den verabschiedeten Anti-Terror-Politiken stand, wuchs in der Bevölkerung angesichts der zunehmenden Verarbeitung ihrer personenbezogenen Daten seitens privater und staatlicher Stellen das Misstrauen an. Nachdem die Ausweitung von Anti-Terror-Maßnahmen über Jahre hinweg konstant vorangetrieben worden war und die während dieser Zeit vom Europäischen Parlament und anderen eher bürgerrechtlich orientierten Akteuren vertretenen Positionen ignoriert worden waren, hatte sich mit dem Stockholmer Programm und dem Inkrafttreten des Vertrags von Lissabon die Gelegenheit ergeben, die Prioritäten der Union in Richtung des Schutzes der Grundrechte zu verschieben. Während der Erarbeitungsphase des Stockholm-Programms traten noch einmal die unterschiedlichen Positionen der Unionsorgane im Hinblick auf den Umgang mit Fragen des Grundrechtsschutzes offen zu Tage: Der Ministerrat auf dem einen Ende des Spektrums mit Vorschlägen, die eher der Fortsetzung vorheriger sicherheitsorientierter Politiken entsprachen, aber erstmals auch mehr Raum für Datenschutzpolitiken ließen als noch zur Hochphase der Anti-Terror-Politik. Das Parlament auf dem anderen Ende der Skala als Vertreter bürgerrechtlicher Positionen, der unnachgiebig auf eine Politikwende drängt. Und schließlich die Kommission als Vermittlerin zwischen den Polen mit Neigungen zum Datenschutz.

Viel bemerkenswerter als die grundsätzlichen institutionellen Positionierungen sind am Erarbeitungsprozess des Stockholmer Programms allerdings die veränderten Nuancen: So hatte die für Justizfragen zuständige Zukunftsgruppe des Ministerrats vergleichsweise bürgerrechtsnahe Positionen vertreten und damit eine kleine Wende in der Ministerratspolitik bewirkt. Zeitgleich hatten sich die innerhalb der Kommission mit Grundrechts- bzw. Datenschutzfragen befassten Stellen dahingehend durchsetzen können, dass im Kommissionsentwurf eher die aus der Justizgruppe statt die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

aus der Innenpolitik-Zukunftsgruppe stammenden datenschutzpolitischen Vorschläge aufgegriffen wurden. Nachdem die Bürgerrechtsorientierung der Kommission (insb. die Befürwortung der Vorlage eines neuen legislativen Rahmens für den Datenschutz) im finalen Stockholmer Programm noch einmal relativiert worden war, zeigte sich die Kommission im Gegensatz zu ihren früheren Rückziehern im Bereich der Datenschutzpolitik überraschenderweise unnachgiebig und nahm den Punkt in ihrem Aktionsplan wieder auf.

Diese Vorgehensweise der Kommission deckte sich auch mit der bereits begonnenen Konsultation zum EU-Datenschutzrahmen, die im Mai 2009 ihren Anfang genommen hatte. Auf die konkreten Reformschritte soll an späterer Stelle (vgl. 4) detailliert eingegangen werden.

3.4.1.4 Fazit und Auswirkungen auf die Datenschutzpolitik der EU

Mit dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 hatte ein *Wandel der grundlegenden verfassungsmäßigen Struktur* der EU stattgefunden. Der in der EU-Grundrechtecharta formulierte Schutz personenbezogener Daten war nicht mehr nur Teil des EU-Sekundärrechts, sondern nunmehr Teil des EU-Primärrechts, der zwingendermaßen gemäß den primärrechtlichen Vorgaben im Bereich des Sekundärrechts gewährleistet werden musste. Indem außerdem die Säulenstruktur der Union abgeschafft und das Parlament dem Ministerrat weitgehend gleichgestellt wurde, fand eine bedeutsame Änderung im *Grad der erforderlichen Zustimmung für wesentlichen politischen Wandel* und hinsichtlich der *relativen Offenheit des politischen Systems* der EU statt. Parlament und Ministerrat mussten künftig gem. Art. 16 Abs. 2 AEUV über die ehemalige erste und dritte Säule betreffende Datenschutzangelegenheiten auf Augenhöhe gemeinsam entscheiden. Problematischen Entscheidungen wie dem JI-Rahmenbeschluss, der nur deshalb eine Einigung auf dem kleinsten gemeinsamen Nenner darstellte, weil der Ministerrat einstimmig und ohne die formelle Beteiligung des Parlaments entscheiden musste, wurde mit den jüngsten Vertragsänderungen die Grundlage entzogen. Die zuvor seitens des Ministerrats praktizierte Strategie der Einforderung von Zugeständnissen vom Europäischen Parlament im Bereich von Politiken der ersten Säule konnte somit nicht mehr fortgeführt werden.

Die *Policy-Entscheidung aus einem anderen Subsystem* in Form des Stockholmer Programms beeinflusste die Reform des Datenschutzes ebenfalls, da sich die EU-Organe im Rahmen des Stockholmer Programms erst-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mals auf eine Datenschutzpolitik einigten, deren Eckpunkte auf einem bis dahin nicht da gewesenen Maß an interinstitutionellem Konsens aufbauten.

3.4.2 Weitere Faktoren: Veränderung sozioökonomischer Bedingungen und der öffentlichen Meinung

In etwa zur selben Zeit, in der der *Wandel der grundlegenden verfassungsmäßigen Struktur*, des *Grades der erforderlichen Zustimmung für wesentlichen politischen Wandel* als auch der *relativen Offenheit des politischen Systems* stattgefunden hatte, fand auch ein *Wandel in den sozioökonomischen Bedingungen* und *in der öffentlichen Meinung* statt, dessen Auswirkungen wichtig im Hinblick sowohl auf die Initiierung der Datenschutzreform als auch auf den politischen Aushandlungsprozess der DSGVO waren. Während die wirtschaftspolitisch motivierten Datenschutz-Gegner einerseits und die sicherheitspolitisch motivierten Datenschutz-Gegner andererseits an der Aushöhlung der datenschutzrechtlichen Grundlagen wirkten, formierte sich allmählich der Widerstand gegen die zunehmende Verarbeitung personenbezogener Daten zu Wirtschafts- und Sicherheitszwecken sowohl auf Ebene der politischen Entscheider als auch im Bereich der Zivilgesellschaft. Die folgenden Unterabschnitte widmen sich der Analyse der wichtigsten Eckpunkte dieser Entwicklung in Form der Zunahme von Datenschutzskandalen, des Wandels der öffentlichen Meinung, der Erstarkung des außerparlamentarischen Widerstands sowie in Gestalt des wachsenden Policy-Entrepreneurships für eine Stärkung des Datenschutzes insb. im Europäischen Parlament, aber auch in der Europäischen Kommission.

3.4.2.1 Zunahme von Datenschutzskandalen

Eine der wichtigsten Ursachen für die gesteigerte gesellschaftliche Sensibilität im Hinblick auf die Verarbeitung personenbezogener Daten stellte die Zunahme von Datenschutzskandalen dar. Die ersten großen Datenschutz-Skandale ereigneten sich bereits im Laufe der 1990er-Jahre (Culnan 1997; Siering 1999). In der breiten deutschen und europäischen Öffentlichkeit bekannt wurde das Thema Datenmissbrauch allerdings erst durch eine Reihe von öffentlichkeitswirksamen Skandalen seit der Mitte der 2000er-Jahre. Im Folgenden möchte ich auf einige der größten dieser Skandale eingehen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nachdem die Schwartz-Unternehmensgruppe bereits 2004 mit missbräuchlichem Verhalten gegenüber Mitarbeitern in Filialen des Tochter-Unternehmens Lidl aufgefallen war, kam 2008 heraus, dass Lidl-Mitarbeiterinnen und Mitarbeiter systematisch und sehr weitgehend per Videoüberwachung bespitzelt wurden (Ziegler 2008). Es folgten Skandale um illegalen Datenhandel, u. a. mit sensiblen personenbezogenen Daten aus den Datenbeständen der Deutschen Telekom und Bankkontendaten aus Datenbeständen der Südwestdeutschen Kassenlotterie (Krempl 2008b). Zudem wurde Mitte 2008 zunächst über die Deutsche Telekom (Balzli u. a. 2008) und Anfang 2009 über die Deutsche Bahn (Christ und Hildebrand 2009) bekannt, dass sie ihre Mitarbeiter ausspähten. Insbesondere die Telekom-Affäre zog große öffentliche Aufmerksamkeit auf sich, weil neben Mitarbeitern auch Aufsichtsräte, Gewerkschaftsfunktionäre, Betriebsratsangehörige und ein Vorstandsmitglied von der Überwachung betroffen waren (Schäfer 2010). Schließlich wurden im selben Zeitraum mehrere große Datenpannen bekannt: Darunter neben einer Datenpanne des deutschen Zolls (Regnery 2011) insbesondere der 2006 begangene Datendiebstahl an 17 Millionen Kundendaten von T-Mobile, der von der Deutschen Telekom fast zwei Jahre verheimlicht worden war (Murphy und dpa-AFX 2008).[249]

International aufsehenerregend war eine von Facebook Inc. im Jahr 2006 ins Leben gerufene Funktion, mit der die Freunde eines Facebook-Nutzenden sehr detailliert über dessen Aktivitäten auf Facebook informiert wurden (Westlake 2008). Trotz der Kritiken an dieser Praxis entschied sich der Konzern Ende 2009 dazu, die Standard-Einstellungen des Dienstes dahingehend zu ändern, dass Text-, Foto- und Videobeiträge der Nutzerinnen und Nutzer sowie Name, Profilfoto, die Liste der Freunde und Facebook-Seiten, denen man folgte, Geschlecht und regionale Zugehörigkeit nicht nur dem Freundeskreis, sondern standardmäßig sowohl allen anderen Facebook-Nutzerinnen und -Nutzern als auch Nicht-Nutzenden angezeigt wurden und sogar von Suchmaschinen indexiert werden konnten (Bahrke 2011, 45–47). Zudem ging Facebook im Jahr 2009 dazu über, die Daten der Nutzerinnen und Nutzer auch dann noch weiterzuverwenden, wenn diese von den Betroffenen selbst gelöscht oder das Konto deaktiviert worden war (Walters 2009). Eine weitere Änderung aus dem Jahr 2009

249 Die an dieser Stelle genannten Beispiele stellen freilich eine kleine, der deutschen Leserschaft bekannte, Auswahl an Datenpannen dar. International ereigneten sich seit der Jahrtausendwende dutzende vergleichbare Fälle. Für einen Überblick, siehe z. B.: (Wikipedia 2019b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zeigte die Aktivitäten eines Facebook-Nutzers auf anderen Webseiten dessen Facebook-Freunden, sofern sich der Nutzer auf Facebook-Partnerseiten bewegte (McCarthy 2009).

Schließlich zogen mehrere im Vereinigten Königreich stattgefundene Datenverluste erhebliche Kritik auf sich und führten die mangelnde Sicherheit personenbezogener Daten im öffentlichen Bereich vor Augen: Im November 2007 kam zunächst heraus, dass die Daten von 25 Millionen Steuerzahlern abhandengekommen waren. Im Januar 2008 verschwand ein PC der britischen Streitkräfte, auf dem personenbezogene Daten von Rekruten gespeichert waren. Später verschwanden Daten über 80.000 Häftlinge und 33.000 Wiederholungstäter (Focus Online 2008). Schließlich kam im Oktober 2008 heraus, dass eine Festplatte des britischen Verteidigungsministeriums mit personenbezogenen Daten über 1,7 Millionen Rekruten verschwunden war. Unter den betroffenen Daten seien personenbezogene Daten über Angehörige, Pass- und Sozialversicherungsnummern, Führerschein- und Bankdaten sowie die Mitgliedsnummer beim National Health Service gewesen. Zudem gab das britische Verteidigungsministerium im Juli 2008 bekannt, dass im Laufe der vergangenen vier Jahre insgesamt 658 Laptops und 26 USB-Sticks verschwunden waren (BBC News 2008).

Anti-Terror-Maßnahmen

Neben den Datenschutzskandalen im Bereich wirtschaftlicher Datenverarbeitung wirkten sich auch einige der Skandale im Bereich der (internationalen) Sicherheitspolitik auf das Bürgerrechtsbewusstsein der europäischen Bevölkerung aus. So verabschiedeten die vom internationalen Terrorismus direkt und indirekt betroffenen Staaten zunächst eine Reihe von Anti-Terror-Maßnahmen, die von den jeweiligen Bevölkerungen mehrheitlich grundsätzlich begrüßt wurden (European Commission 2008, 47 ff. Priscilla M. Regan 2015, 59). Die Verabschiedung von staatlichen Anti-Terror-Maßnahmen stellt insofern eine *normale* Reaktion des Staates dar, als die Regierung eines Staates aufgrund der verübten oder befürchteten Anschläge zur Reaktion gezwungen wird: „Unternähme sie nichts, müsste sie befürchten, dass dies von der eigenen Bevölkerung, von anderen Staaten und nicht zuletzt von den Terroristen als Schwäche oder Nachgiebigkeit ausgelegt wurde. Deshalb muss sie zunächst versuchen, weitere Anschläge zu verhindern." (B. Meyer 2002, 3) Zugleich liegt dieser Handlungslogik eine inhärente Problematik zugrunde, denn „die Furcht, bei der Prävention Lücken zu lassen, verleitet wegen der Unbestimmbarkeit künftiger Risiken

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

dazu, die Freiheitsrechte der Bürger stärker einzuschränken als es mit Blick auf die wahrscheinlichen Gefahren erforderlich wäre." (ebd.)

3.4.2.2 Wandel in der öffentlichen Meinung gemäß Umfragewerten in den 2000er-Jahren

Im Laufe der 2000er-Jahre nahm insbesondere die Anfangs hohe Bereitschaft zur Unterstützung von Anti-Terror-Maßnahmen EU-weit signifikant ab, während die Datenschutz-Sorgen der Bevölkerung sowie die Unterstützung einer EU-weiten Datenschutzregelung eine leichte Zunahme verzeichneten.

So sprach sich zwar die Mehrheit der EU-Bürgerinnen und -Bürger für die Ausweitung von Sicherheitsgesetzen zum Zwecke der Terrorbekämpfung aus. Doch die Verarbeitung personenbezogener Daten für sonstige sicherheitsbehördliche und wirtschaftliche Zwecke wurde von der Mehrheit der EU-Bevölkerung mit Sorge betrachtet. Die EU-weit repräsentativen Eurobarometer-Studien aus den Jahren 2003 und 2008 demonstrierten etwa, dass eine Mehrheit der Bürgerinnen und Bürger der EU Einschränkungen ihrer Datenschutzrechte zum Zwecke der Bekämpfung des internationalen Terrorismus in Kauf zu nehmen bereit war. Im Jahre 2003 befürworteten 64 % der Befragten die Überwachung der Internetnutzung zum Zwecke der Terrorbekämpfung. Im Jahre 2008 stieg dieser Wert sogar auf 77 % an. Die Zahl der mit dieser Maßnahme nicht einverstandenen Menschen fiel im selben Zeitraum von 25 % auf 18 % (European Commission 2008, 51). Der Zuspruch für die Überwachung von Telefongesprächen zum Zwecke der Terror-Bekämpfung erhöhte sich im selben Zeitraum ebenfalls, von 61 % im Jahr 2003 auf 73 % im Jahr 2008 während die Ablehnung von 33 % auf 25 % sank (ebd., 52).

Im Hinblick auf das Thema der Datenschutz-Sorgen hatten in der ersten Eurobarometer-Studie aus dem Jahr 1991 66 % der Befragten ihre Besorgnis über den Schutz ihrer personenbezogenen Daten geäußert. Dieser Wert sank im Jahr 1996 auf 58 %, stieg 2003 leicht auf 60 % und schließlich im Jahr 2008 auf den Höchstwert von 68% an (European Commission 2008, 7). Den höchsten Anstieg verzeichnete der Wert zwischen 2003 und 2008 in Österreich, Deutschland und Dänemark: Die Zahl der über den Umgang mit ihren personenbezogenen Daten besorgten Menschen stieg in Österreich von 51 % im Jahr 2003 auf 86 % im Jahr 2008 an, in Dänemark von 42 % auf 73 % und in Deutschland von 58 % auf 86 % (European Commission 2008, 7 f.). Zudem korrelierte diese Entwicklung mit dem sinkenden

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bedrohungsgefühl der Bevölkerung vor Terroranschlägen: Während noch in der kurz nach dem 11. September 2001 durchgeführten Eurobarometer-Studie Anfang 2002 78 % der EU-Bevölkerung den Terrorismus als Hauptsorge einstuften (Europäische Kommission 2002, 5), sank dieser Wert im Laufe der Folgejahre kontinuierlich bis auf nur 7 % im Jahr 2007 (Europäische Kommission 2008b, 12). Daneben vertrat eine große Mehrheit von 82 % der im Jahr 2008 befragten EU-Bürgerinnen und -Bürger die Ansicht, dass die Übertragung personenbezogener Daten über das Internet unsicher sei (European Commission 2008, 41). Eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter der deutschen Bevölkerung fand 2007 heraus, dass die sechsmonatige Vorratsdatenspeicherung von 54 % und die Online-Durchsuchung von 59 % der Befragten abgelehnt wurde. Schließlich gaben 54 % der Befragten an, dass sie die bestehenden Sicherheitsgesetze in der Bundesrepublik für ausreichend hielten, während 44 % für eine Ausweitung der Sicherheitsgesetzgebung eintraten (Datenspeicherung.de 2007).

Zeitgleich wurde auch der Ruf nach einer unionsweiten, statt nationalen, Lösung von Datenschutzproblemen lauter. Während im Jahr 2003 noch 41 % der befragten EU-Bürgerinnen und Bürger der Ansicht waren, dass die nationale Gesetzgebung für einen angemessenen Schutz personenbezogener Daten nicht ausreichend sei und 26 % der Befragten diese für ausreichend befanden, äußerten sich im Jahr 2008 56 % der Befragten dahingehend, dass nationale Gesetzgebung alleine nicht ausreichend sei (29 % hielten nationale Gesetzgebungsmaßnahmen für ausreichend) (European Commission 2008, 24).

3.4.2.3 Außerparlamentarischer Widerstand

Der Wandel in der öffentlichen Meinung zeigte sich auch und insbesondere am zunehmenden außerparlamentarischen Widerstand gegen die Ausweitung sicherheitspolitischer Maßnahmen. Nachdem zunächst ein allgemeiner Überblick über das Erstarken europaweiter zivilgesellschaftlicher Datenschützer geliefert wird, gehe ich näher auf das Beispiel des zivilgesellschaftlichen Widerstands gegen die Einführung der Vorratsdatenspeicherung in Deutschland ein.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.2.3.1 Entstehung europaweiter digitaler Bürgerrechtsgruppen

Mit der zunehmenden gesellschaftlichen Bedeutung der Datenverarbeitung und der Zunahme sicherheitspolitischer Maßnahmen ging auch die Entstehung und Erstarkung netzpolitischer Aktivisten im Allgemeinen und zivilgesellschaftlicher Datenschutzbefürworter im Besonderen einher. In verschiedenen europäischen Staaten wurden entsprechende Organisationen ins Leben gerufen: *Bits of Freedom* (2000, Niederlande), *Associação Nacional para o Software Livre* (2001, Portugal), *IT-Political Association of Denmark* (2002, Dänemark), *Open Rights Group* (2005, Vereinigtes Königreich), *La Quadrature du Net* (2008, Frankreich), *Icelandic Digital Freedom Society* (2008, Island), *Panoptykon Foundation* (2009, Polen), *Digitale Gesellschaft* (2010, Deutschland).

Der für die Datenschutzpolitik bedeutendste Schritt der Zivilgesellschaft erfolgte allerdings im Jahr 2002 mit der Gründung von *European Digital Rights* (EDRi). Angetrieben von Bestrebungen zur Internet-Zensur auf EU-Ebene, planten Statewatch, CCC und GILC gemeinsam mit weiteren Organisationen Anfang 2002 die Gründung einer europäischen Dachvereinigung der nationalen netzpolitischen Bürgerrechtsorganisationen (Krempl 2002). Mitte 2002 wurde EDRi schließlich von insgesamt zehn Gruppierungen ins Leben gerufen, um gemeinsam gegen die auf EU-Ebene stattfindenden Entwicklungen in den Bereichen Vorratsdatenspeicherung, Telekommunikationsüberwachung, Cybercrime-Abkommen sowie Internet-Zensur vorzugehen (Ziegler 2002). Nachdem EDRi Anfangs zunächst eher auf Ebene des zivilgesellschaftlichen Aktivismus tätig war, trat sie auch zunehmend als Beobachter relevanter Entwicklungen auf und beteiligte sich in zunehmendem Maße an politischen Entscheidungsprozessen und an Multi-Stakeholder-Expertengruppen als Vertreter der europäischen Zivilgesellschaft (EDRi 2004, 2005a, 2007). Ihre enorme Mobilisierungsfähigkeit sollte EDRi schließlich während der erfolgreichen Proteste gegen das Anti-Counterfeiting Trade Agreement (ACTA), das aufgrund der massiven öffentlichen Kritik schließlich vom Europäischen Parlament abgelehnt wurde, zur Schau stellen (EDRi 2013b; James Losey 2014). Wie jüngere Forschungsergebnisse zeigen, ist der Einfluss internationaler zivilgesellschaftlicher Organisationen auf politische Prozesse auf EU-Ebene im Laufe der vergangenen Jahrzehnte insbesondere aufgrund ihrer Adaption an die Multi-Level-Governance-Struktur der EU und der damit einhergehenden Anpassung ihrer Mobilisierungs- und Lobbying-Strategien gewachsen (Caiani und Graziano 2018).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.4.2.3.2 Zivilgesellschaftlicher Widerstand in Deutschland gegen die Einführung der Vorratsdatenspeicherung

Deutlich wird das Erstarken des netzpolitisch motivierten zivilgesellschaftlichen Widerstands besonders bei einem Blick auf die Entwicklungen in der Bundesrepublik. So kann der netzpolitische Aktivismus in Deutschland – neben dem in den Vereinigten Staaten (C. J. Bennett 2008) – auf eine vergleichsweise lange Tradition zurückblicken (Stöcker 2011). Als älteste Organisation auf dem Gebiet des bürgerrechtlichen Datenschutzes war insbesondere die Deutsche Vereinigung für Datenschutz (DVD) bereits seit dem Jahr 1977 an zahlreichen datenschutzpolitischen und öffentlichkeitswirksamen Aktivitäten beteiligt, darunter die Anti-Volkszählungskampagnen 1983 und 1987, die Begleitung der Novellierungsbemühungen des BDSG in den 1980ern sowie im Rahmen der Umsetzung der Vorgaben der DS-RL oder auch im Kontext der Kritik an der Videoüberwachung öffentlicher Räume. Die Aktivitäten der DVD stützten sich überwiegend auf die Arbeit des Vorstands, der sich in der Anfangszeit aus der Gesellschaft für Mathematik und Datenverarbeitung (GMD) bzw. dessen Umfeld rekrutierte (Weichert 2007).[250] Der Chaos Computer Club (CCC) etablierte sich 1981 und war entgegen der eher politisch, bürgerlich und zentralistisch agierenden DVD ein vergleichsweise offener und dezentral agierender Hort für Aktivisten aus Hacker-Kreisen und technologisch versierte bzw. interessierte Individuen. Dem Grundsatz *öffentliche Daten nützen, private Daten schützen* folgend, machte sich der CCC für die Stärkung des Datenschutzes (und insb. des Selbstdatenschutzes) stark und zog auch durch öffentlichkeitswirksame Aktivitäten wie etwa den BTX-Hack im Jahr 1984 schon früh Aufmerksamkeit auf sich (Golem 2018). Ein weiterer Verein, der durch öffentlichkeitswirksame Aktivitäten immer wieder gegen die zunehmende Verarbeitung personenbezogener Daten vorgegangen ist, ist Digitalcourage e. V. Insbesondere mit dem seit dem Jahr 2000 verliehenen Negativpreis, den BigBrotherAwards, konnte Digitalcourage regelmäßig öffentliche Aufmerksamkeit generieren (Tangens und padeluun 2011).

Einen vorläufigen Höhepunkt erreichten die zivilgesellschaftlichen Datenschutzbefürworter schließlich im Rahmen der Proteste gegen die Volkszählung von 1983: Zehntausende Menschen in vielen deutschen Städten

250 Andere Organisationen wie die *Gesellschaft für Datenschutz und Datensicherheit e. V. (*GDD) oder der *Berufsverband der betrieblichen Datenschutzbeauftragten* (BvD) sind nicht primär bürgerrechtlich orientiert und vertreten eher die Interessen betrieblicher bzw. behördlicher Datenschutzbeauftragter (Weichert 2007, 57).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gingen auf die Straße. Die Proteste wurden von 52 % der deutschen Bevölkerung befürwortet und mehr als tausend Verfassungsbeschwerden wurden eingereicht (Der Spiegel 1983b, 1983a). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahr 1983, dem Ausbleiben der Orwell'schen Dystopie im Jahr 1984, und der zunehmenden Verbreitung und Normalisierung der Computernutzung im weiteren Verlauf der 1980er-Jahre, wich die gesellschaftliche Angst vor den negativen Folgen der Computerisierung allerdings einer positiven, auf Chancen und Potentiale ausgerichteten Wahrnehmung (Berlinghoff 2013b, 106 ff.).

Eine vergleichbare öffentliche Mobilisierung gelang den zivilgesellschaftlichen Datenschützern erst mehr als 20 Jahre später: Der Auslöser war die Verabschiedung des Gesetzes zur Vorratsdatenspeicherung[251] in der Bundesrepublik im Jahr 2007, mit der die EG-Richtlinie zur Vorratsdatenspeicherung 2006/24/EG in nationales Recht umgesetzt wurde. Vor dem Hintergrund des generellen Trends hin zur Versicherheitlichung der Europäischen Politik hatten sich zahlreiche Bürgerrechtsorganisationen und zivilgesellschaftliche Datenschutzorganisationen wie der CCC, DVD und Digitalcourage seit Ende 2005 zunächst gegen die Verabschiedung der EG-Richtlinie und später gegen das deutsche Umsetzungsgesetz im Rahmen des *Arbeitskreis Vorratsdatenspeicherung* (AK Vorrat) zusammengeschlossen. Im Jahr 2006 organisierte der Zusammenschluss Demonstrationen in Berlin, Bielefeld und Frankfurt am Main, an denen zunächst nur wenige hunderte Personen teilnahmen (AK Vorrat 2006; Lüke 2006). Auf den Folgeveranstaltungen unter dem Titel „Freiheit statt Angst" konnte das Bündnis hingegen viele zehntausende Demonstranten anziehen. Den Höhepunkt markierte der *Freiheit statt Angst*-Aktionstag am 11. Oktober 2008, an dem in weltweit 15 Ländern Aktionen gegen zunehmende Überwachung stattfanden (AK Vorrat 2008b). Allein in Berlin beteiligten sich an der Demonstration nach Veranstalterangaben 100.000 und nach Polizeiangaben 15.000 bis 50.000 Menschen (DPA 2008). Das Besondere am Format des AK Vorrat war neben der breiten Unterstützung seitens der Bevölkerung auch die enorme Unterstützung seitens Organisationen, die sich in der Vergangenheit eher unkritisch oder passiv im Hinblick auf die Ausweitung von Sicherheits- und Überwachungsgesetzen gezeigt hatten. So wurde das Bündnis von insgesamt 117 Organisationen unterstützt, darunter nicht nur

251 „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Bundesgesetzblatt 70/2007".

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

datenschutzpolitisch oder allgemein auf dem Gebiet der Bürgerrechte aktive Gruppen, sondern beispielsweise auch die Oppositionsparteien aus dem Bundestag sowie deren Jugendorganisationen, die Gewerkschaften ver.di, DGB und GEW, Friedensinitiativen und mehrere Berufsverbände (AK Vorrat 2008a). Zudem organisierte der AK Vorrat in den Jahren 2007 und 2008 die größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik, an der sich 34.939 Personen beteiligten (AK Vorrat 2008c) und die bereits im März 2008 zur Einschränkung der Vorratsdatenspeicherung per einstweiliger Anordnung des BVerfG führte (BVerfG 2008). In der Folge konnten sich die Vertreter zivilgesellschaftlicher Organisationen als Netzpolitik-Experten einen festen Platz in zahlreichen Polit-Talkshows, in den großen Massenmedien, aber auch in parlamentarischen und parteipolitischen Diskussions- und Beratungsrunden sichern (Schütz und Karaboga 2015, 39; Wendelin und Löblich 2013). Ihr Erfolg zeigte sich nicht zuletzt auch am zeitweisen politischen Erfolg der Piratenpartei seit 2009 (Bieber 2012, 39 ff.).

Trotz des im Vergleich zu den zivilgesellschaftlichen Akteuren in den Vereinigten Staaten niedrigen Budgets europäischer zivilgesellschaftlicher Akteure (Schütz und Karaboga 2015, 38, Fn. 80), gelang es diesen somit während des Betrachtungszeitraums der Kontextanalyse, in zunehmendem Maße Einfluss auf die Politik-Gestaltung zu nehmen. Der im vorausgegangenen Unterabschnitt dargestellte Ausbau der Lobbying-Kapazitäten der Zivilgesellschaft auf EU-Ebene wurde somit durch den Ausbau der Mobilisierungsfähigkeit zivilgesellschaftlicher Akteure auf nationaler Ebene flankiert (Caiani und Graziano 2018).

3.4.2.4 Policy Entrepreneurship im Europäischen Parlament

Schließlich erzeugte die fortschreitende Versicherheitlichungspolitik in Verbindung mit den zunehmenden Datenschutz-Skandalen auch bei den politischen Entscheidern des Europäischen Parlaments deutlichen Widerstand. Dies war ein Novum, da gerade die Europaabgeordneten in den ersten Jahren nach den Terroranschlägen vom 11. September vonseiten des Ministerrats stets dazu aufgefordert worden waren, Verantwortung für die Gesellschaft und Europa auf die Weise zu übernehmen, dass sie die von einigen Mitgliedstaaten mit allen politischen Mitteln durchgesetzten Anti-Terror-Maßnahmen unterstützten (siehe insb. die Unterabschnitte zur ePrivacy-Richtlinie 3.3.2 und zur Vorratsdatenspeicherung 3.3.4.2). Das Europäische Parlament, das jahrzehntelang im Gegensatz zum Ministerrat

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

als ein offener Diskussionsort für bürgerrechts-, umweltschutz-, verbraucherschutz- oder auch geschlechterpolitische Anliegen gegolten hatte (Dür, Bernhagen, und Marshall 2013; Kluger Dionigi 2017), wandelte sich seit den 1990er-Jahren infolge seines allmählichen Aufstiegs zum Mitgesetzgeber deutlich zu Lasten der früheren Positionen (Greis 2015; Ripoll Servent 2013). Nachdem dutzende die Bürgerrechte einschränkende nationale und europäische Anti-Terror-Maßnahmen verabschiedet worden waren, diese nicht immer die erhofften Ergebnisse gezeitigt und teils zu massiven Datenpannen geführt hatten und die Mitgliedstaaten sich nicht einmal auf ein angemessenes Mindestmaß an Datenschutzbestimmungen für den Bereich der dritten Säule hatten einigen können (vgl. 3.3.4.4), wurde der europaparlamentarische Widerstand erstmals lauter. So äußerte der ALDE-Politiker Alexander Alvaro im Rahmen der Europaparlamentsdebatte zum JI-Rahmenbeschluss: „Mit einer unglaublichen Aktivität bemühen sich Kommission und Rat, im Bereich des wirtschaftlichen Schutzes personenbezogener Daten zu handeln. Wenn wir sehen, was in Großbritannien, in Deutschland und in anderen Mitgliedstaaten mit persönlichen Daten geschieht, die von öffentlichen Behörden verwaltet werden und zum Teil verloren gehen oder gestohlen werden, haben wir dort einen genauso dringenden Handlungsbedarf. Hier geht es schließlich mehr denn je um die Rechte des Bürgers, denn gegen das Verhalten seines Staates kann er sich nicht wehren. Bei einem Unternehmen kann er im Zweifelsfall noch ein anderes wählen." (EP 2008c) Unter direkter Bezugnahme auf die im Vereinigten Königreich stattgefundenen Datenpannen äußerte selbst der zu diesem Zeitpunkt der euroskeptischen UEN angehörende Europaabgeordnete Brian Crowley: „Wir müssen beim Thema Datenschutz und Erfassung personenbezogener Daten sehr vorsichtig sein, da viele von uns wissen, dass es in unseren eigenen Mitgliedstaaten zahllose Behörden auf nationaler und auf lokaler Ebene gibt, die zu jeder einzelnen Person Daten erfassen. Der größte Schrecken, der derzeit Großbritannien erschüttert, betrifft diese Angelegenheit des Identitätsdiebstahls und es gibt große Bedenken, weil Computer verloren gegangen sind, die Informationen von staatlichen Behörden enthalten – ob es nun Sozialämter oder Verteidigungs- oder Polizeibehörden sind – persönliche Daten, Informationen, die Sie selbst niemals weitergeben würden. Dennoch scheint es keinen Schutz für diese Daten zu geben." (EP 2008c) Die liberale Europaabgeordnete Sarah Ludford machte auf die Zweckentfremdung der im Rahmen der Vorratsdatenspeicherung gespeicherten sensiblen personenbezogenen Daten aufmerksam: „Ich kann dem Haus berichten, dass in Großbritannien die Richtlinie über die Vor-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ratsspeicherung von Daten – der Meilenstein des britischen Ratsvorsitzes vor drei Jahren – dazu genutzt wird, hunderten von Behörden, die nicht mit der Strafverfolgung befasst sind, Zugang zu persönlichen Daten zu gewähren. Gemeinden verwenden sie, um zu überprüfen, ob Eltern lügen, wenn sie angeben, im Einzugsbereich einer beliebten Schule zu leben – was nicht richtig wäre, aber kein schweres Verbrechen ist." (EP 2008c)

Schließlich wurde auch die Wirksamkeit der Anti-Terror-Maßnahmen infrage gestellt. Der italienische Sozialdemokrat Claudio Fava drückte sein Unbehagen im Namen der PSE-Fraktion folgendermaßen aus: „Nach sieben Jahren der Terrorismusbekämpfung glaube ich, dass wir jetzt in der Lage sind, die Risiken des Terrorismus, seine Auswirkungen und verheerenden Konsequenzen einzuordnen. Ich glaube auch, dass eine der dramatischsten Konsequenzen der Verlust der Ausgewogenheit ist – ein Verlust des Gespürs für Ausgewogenheit bei der Reaktion auf die Bedrohung durch den Terrorismus." (EP 2008c) Deutliche Kritik an dieser EU-Strategie wurde auch von der linken GUE/NGL geäußert. Der aus Italien stammende Giusto Catania befand etwa, „dass die Strategie zur Bekämpfung des Terrorismus der letzten Jahre nicht erfolgreich war, und dass sie sich mit der Formulierung der Terrorliste und den Einschränkungen des Rechtsstaatsprinzips zu stark den US-Interessen im Krieg im Irak und in Afghanistan untergeordnet hat. Es gab zu viele Fälle eines regelwidrigem [sic] Umgangs mit personenbezogenen Daten, und ich glaube, dass wir alle zusammenarbeiten müssen […], um zu gewährleisten, dass wir die persönlichen Freiheiten nicht einschränken, um demokratische Bereiche zu erweitern und um sicherzustellen, dass wir nicht im Namen der Sicherheit und der Bekämpfung des Terrorismus dazu beitragen, dass die Terrororganisationen ihre eigentlichen Ziele erreichen." (EP 2008c) Die aus den Niederlanden stammende grüne Europaabgeordnete Kathalijne Maria Buitenweg verwies auch auf den Zusammenhang zwischen der Zunahme von Grundrechtseinschränkungen und dem wachsenden Misstrauen der Bevölkerung gegenüber ihren Regierungen: „Wenn wir die Beziehung zwischen Regierung und Bürger aus der historischen Perspektive betrachten, sehen wir, dass die Regierung das Gewaltmonopol innehat und die Bürger über Grundrechte verfügen, die von der Regierung nur verletzt werden dürfen, wenn dies notwendig, effektiv und angemessen ist. Wenn die Bürger aber allzu oft feststellen müssen, dass Maßnahmen der Regierung weder notwendig noch gerechtfertigt sind, wird ihr Vertrauen in diese Regierung und damit ihre Bereitschaft zur Zusammenarbeit mit ihr schwinden. Dann werden wir

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

langfristig massive Sicherheitsprobleme erleben. Vertrauen ist schwer zu gewinnen, aber leicht zu verlieren." (EP 2008c)

Die im linken und liberalen Spektrum des Parlaments angesiedelten Parteien und Fraktionen wandten sich somit, entgegen vorherigen Meinungsverschiedenheiten insb. auf Seiten der Sozialdemokraten und Liberalen, erstmals geschlossen und entschieden gegen die Fortsetzung der bis dahin praktizierten Anti-Terror-Strategie. Wie zu erwarten war, wurde die Ausweitung der Sicherheitsgesetzgebung hingegen von den konservativen und europaskeptischen bzw. feindlichen Parteien, insb. der EVP-ED sowie Polen-stämmigen Abgeordneten der UEN, befürwortet (EP 2008c).[252]

3.4.2.5 Policy Entrepreneurship auf Ebene der Kommission

Franco Frattini, EU-Kommissar für Justiz, Freiheit und Sicherheit, hatte noch Ende 2007 – den Ankündigungen im 2007er Bericht entsprechend – darauf gesetzt, einerseits die Implementierung der DS-RL weiter voranzubringen und andererseits die Erforderlichkeit von sektorspezifischen Regulierungsmaßnahmen zu überprüfen, um die Anwendbarkeit der Datenschutz-Grundsätze auch auf neue Technologien aber auch angesichts der Gefährdungen der Öffentlichkeit durch neue Formen der Kriminalität und terroristischer Gefahren zu gewährleisten. Trotz der Hervorhebung von nicht-unterlaufbaren Datenschutz-Prinzipien und der Betonung der Gleichwertigkeit von Datenschutz und Sicherheit hinterfragte Frattini allerdings keine der zu Sicherheitszwecken erlassenen EU-Maßnahmen, sondern identifizierte als Ziel lediglich die Erreichung einer angemessenen Balance zwischen beiden Polen (Frattini 2007).

Erst als Jacques Barrot 2008 zum neuen Kommissar für Justiz, Freiheit und Sicherheit wurde, änderte sich die Haltung der Kommission zur Reform des Datenschutzrechts. Bereits in seiner Vorstellungsrede vor dem Europäischen Parlament legte Kommissar Barrot, in einem deutlich gewandelten Zungenschlag im Vergleich zu seinem Amtsvorgänger, die Schwerpunkte seiner künftigen Arbeit auf die Stärkung der Unionsbürgerschaft und die Gewährleistung des Grundrechtsschutzes. Zudem kündigte er bereits zu jenem Zeitpunkt die Durchführung einer *umfassenden Konsultation, die auf eine Stärkung des Datenschutzes abziele*, an. Angesichts der

252 Ausnahmen bilden die weiter oben zitierten Äußerungen Brian Crowleys, aber auch des neofaschistischen italienischen Politikers Luca Romagnoli (NI) (EP 2008c),

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

jahrelangen Ignoranz des Ministerrats gegenüber den Vorschlägen des Parlaments und des EDSB kündigte Barrot zudem an, besondere Rücksicht auf deren Positionen zu nehmen (Barrot 2008, 4).[253] Die in dieser Phase von Kommissar Barrot eingenommene Rolle ist daher als die eines *Policy Entrepreneurs* zu bewerten, da er das Thema Datenschutz entgegen der bis dahin vom Kommissariat vertreten Position zunächst auf die Kommissionsagenda setzte und anschließend auf die Agenda des Stockholmer Programms. Zudem zeichnete er letzten Endes dafür verantwortlich, dass der Reformprozess des datenschutzrechtlichen Rahmens der EU eingeleitet wurde.

3.5 Zwischenfazit

Das Ziel des Abschnitts 3 bestand darin, die relevanten (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik zu identifizieren, die entscheidend im Hinblick auf das Zustandekommen der DSGVO waren, um so die zweite Forschungsfrage zu beantworten:

FF 2: Welche politischen und historischen Faktoren wirkten als kausale, treibende Faktoren auf dem Weg zur DSGVO?

Unter Rückgriff auf das ACF wurden relativ stabile Parameter, externe Systemereignisse im Vorfeld der DSGVO sowie langfristig wichtige politische Gelegenheitsstrukturen als die Eckpunkte dieses Analyseschrittes bestimmt, von denen mit dem ACF angenommen werden kann, dass sie entscheidend im Hinblick auf das Zustandekommen der DSGVO waren. Der folgende Unterabschnitt fasst die Ergebnisse des Abschnitts im Hinblick auf die Beantwortung der zweiten Forschungsfrage zusammen.

Im darauffolgenden Unterabschnitt wird schließlich auf Grundlage der Erkenntnisse aus der Kontextanalyse ein erster Überblick über die Advocacy-Koalitionen im Bereich der EU-Datenschutzpolitik geliefert, die als Grundlage für die Akerurs- und Prozessanalyse dienen werden.

253 Das Generaldirektorat Justiz, Freiheit und Sicherheit veröffentlichte zudem, noch während es von Barrot kommissarisch geleitet wurde, eine Ausschreibung für eine vergleichende Studie, die verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen untersuchen sollte (European Commission: Directorate-General for Justice, Freedom and Security - Directorate C: Civil Justice, Fundamental Rights and Citizenship - The Director 2008). Douwe Korff und Ian Brown erhielten den Auftrag und veröffentlichten die Studienergebnisse im Jahr 2010 (Korff und Brown 2010).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

3.5.1 Zusammenfassung

Die zweite Forschungsfrage lässt sich folgendermaßen beantworten: Die Initiierung der Datenschutz-Reform, die später in der Verabschiedung der DSGVO und der JI-Richtlinie mündete, war aufgrund einer Mischung aus verschiedenen Einflussfaktoren möglich. Veränderungen in der verfassungsmäßigen Struktur der EU in Gestalt des Inkrafttretens des Lissabon-Vertrags und des Verbindlichwerdens der EU-Grundrechtecharta machten den Erlass von umfassenden sekundärrechtlichen Datenschutzregelungen erforderlich. Die an stärkeren Datenschutzregelungen für den Sicherheitsbereich interessierten Akteure, insb. die EU-Parlamentsfraktionen links der Mitte sowie die liberale Fraktion, aber auch Teile der EU-Kommission (insb. das Kommissariat für Justiz, Freiheit und Sicherheit), deren Positionen trotz gegenüber dem Ministerrat erbrachter Zugeständisse und klarer Absprachen letztlich nicht erhört wurden, übten schließlich gemeinsam mit den Regierungen einiger Mitgliedstaaten Druck aus, damit die Datenschutzreform initiiert werden konnte. Eine abnehmende Anzahl an Terroranschlägen, eine wachsende Sorge vor dem Missbrauch personenbezogener Daten seitens privatwirtschaftlicher als auch staatlicher Akteure und zunehmende Proteste gegen Überwachungsmaßnahmen gaben den Forderungen der Datenschutzbefürworter zusätzlichen Auftrieb. Diese Punkte werden im Folgenden ausführlich diskutiert.

Grundlegende Merkmale des betrachteten Problems: Da es sich beim Thema Datenschutz um kein natürliches, sondern ein soziales Phänomen handelt, bildet das grundlegende Merkmal der Datenschutzpolitik die Bedeutung die der Verarbeitung personenbezogener Daten seitens verschiedener Akteure zugesprochen wird. Einig sind sich alle wesentlichen Akteure dahingehend, dass die Verarbeitung personenbezogener Daten grundsätzlich möglich sein sollte. Uneinigkeit herrscht jedoch im Hinblick darauf, inwieweit und auf Grundlage welcher Regeln diese Verarbeitung möglich sein sollte.

Verteilung natürlicher Ressourcen: Als die Kerncharakteristik aller datenschutzpolitischen Auseinandersetzungen in Europa im Betrachtungszeitraum (von den 1970er-Jahren bis ca. 2008/2009) lässt sich der Konflikt zwischen Akteuren, die an einer möglichst ungehinderten Verarbeitung personenbezogener Daten interessiert sind einerseits und Akteuren, die an der Eindämmung der Risiken jener Verarbeitung in Gestalt von Datenschutzgesetzen interessiert sind andererseits definieren. Wie die Ausführungen gezeigt haben, lassen sich die Befürworter einer ungehinderten

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Verarbeitung wiederum in zwei Gruppen unterteilen: Solche, die aus einer wirtschaftspolitischen Perspektive und solche, die aus einer sicherheitspolitischen Perspektive heraus, jedoch in beiden Fällen stets unter Verweis auf den gesellschaftlichen Nutzen der Verarbeitung personenbezogener Daten, argumentieren. Den Befürwortern von Datenschutzregelungen gelang es im Laufe der Jahrzehnte trotz des Widerstands beider Gruppen Datenschutzregelungen zunächst auf nationaler und später auch auf internationaler Ebene zu erlassen.

Grundlegende soziokulturelle Wertvorstellungen und Sozialstruktur: Der wesentliche Disput im Hinblick auf soziokulturelle Wertvorstellungen besteht zwischen Akteuren, die grundsätzlich einer kontinentaleuropäischen Herangehensweise an Regulierung folgen und solchen, die einer anglo-amerikanischen Herangehensweise näherstehen. Erstere räumen der staatlichen Pflicht zur Verhinderung von individuellem und gesellschaftlichem Schaden durch Praktiken der Wirtschaftsteilnehmer größeren Raum ein, während letztere nicht den Staat, sondern die Wirtschaftsakteure selbst in der Pflicht sehen, mögliche Gefährdungen zu adressieren.

Auf nationaler Ebene war der Erlass von Datenschutzgesetzen in der Frühphase des Datenschutzes insbesondere auf die Beschränkung staatlicher Kontrollmacht fokussiert und von grundrechtlichen Erwägungen getrieben. Der entscheidende Anlass für die Verabschiedung internationaler Regelungen war hingegen nicht der grundrechtliche Schutzaspekt, wie seitens der Datenschutzbefürworter stets gefordert worden war, sondern die Assoziation wirtschaftlichen Wachstums mit der Gewährleistung eines möglichst ungehinderten Flusses personenbezogener Daten über nationale Grenzen hinweg, indem die nationalen Gesetze mittels internationaler Instrumente harmonisiert wurden. Alle allgemeinen Datenschutzgesetze, die bis zum Beginn der Datenschutzreform verhandelt wurden, waren von diesen Konfliktlinien in wesentlichem Maße geprägt.

Mit den Terroranschlägen auf das World Trade Center im Jahr 2001 und in Madrid und London 2004 bzw. 2005 wandelte sich der Datenschutzdiskurs fort vom Konflikt zwischen der grundrechtlichen und wirtschaftlichen Bedeutung schlagartig hin zur sicherheitspolitischen Bedeutung der Verarbeitung personenbezogener Daten. In der Folge konnten sich die staatlichen Befürworter einer möglichst ungehinderten Datenverarbeitung in praktisch allen datenschutzpolitisch relevanten Auseinandersetzungen gegenüber Datenschutzbefürwortern klar durchsetzen und die Ausweitung staatlicher Verarbeitungsspielräume vorantreiben.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Entgegen bisherigen Einschätzungen (Koops 2014; Sloot 2014) zeigt meine Analyse, dass der Schutz personenbezogener Daten insb. im Kontext sicherheitspolitisch motivierter Politiken seitens der Datenschutzbefürworter unter Rückgriff sowohl auf dessen individuelle als auch gesellschaftliche Bedeutung gefordert wurde. Weniger deutlich zeigte sich dies hingegen bei den allgemeinen Datenschutzpolitiken. Allerdings lag der Fokus der Kontextanalyse nicht auf der Untersuchung dieses Aspekts, sodass diese Einschätzung lediglich ergänzend erfolgt. Für eine sorgfältigere Bewertung dieses Aspekts wäre insb. eine tiefergehende Untersuchung der einzelnen Argumente und ggf. eine andere Methodik (Frage nach den Erwägungsgründen in persönlichen Interviews mit den Beteiligten) notwendig gewesen.

Grundlegende verfassungsmäßige Struktur: Die in der vorliegenden Arbeit untersuchten Datenschutzpolitiken[254] wurden im Rahmen der Zuständigkeit der Europäischen Union bzw. von deren Vorgänger in Form der Europäischen Gemeinschaften erlassen. Die verfassungsmäßige Struktur der EU baut auf den völkerrechtlichen Verträgen auf, die zwischen den EU-Mitgliedstaaten abgeschlossen wurden. Anders als im ACF (vor allem Hinblick auf Nationalstaaten) angenommen wird, unterlag die verfassungsmäßige Struktur der Union allerdings einem steten Wandel, der einen großen Einfluss auf das Subsystem der Datenschutzpolitik hatte. So war der Erlass von gemeinschaftlichen Datenschutzregelungen während der 1970er- und 1980er-Jahre deshalb nicht möglich, weil die Ziele der Gemeinschaft laut EWG-Vertrag bzw. den Römischen Verträgen in der Gewährleistung des freien Warenverkehrs, der Freizügigkeit von Arbeitnehmern, von Dienstleistungen sowie von Kapital lagen und der Datenschutz schlicht nicht Teil der Verträge war. Auch die 1977 verabschiedete gemeinsame Erklärung von Parlament, Rat und Kommission, in der diese sich der Wahrung der Grundrechte auf Grundlage der Verfassungen der Mitgliedstaaten und der EMRK verpflichteten, stellte lediglich eine freiwillige Maßnahme und keine bindende verfassungsrechtliche Verpflichtung dar. Erst die für 1992 vorgesehene Vollendung des Binnenmarktes ermöglichte schließlich vor allem aus wirtschaftspolitischen Erwägungsgründen heraus den Erlass der Datenschutzrichtlinie. Die formell verbindliche Achtung der Grundrechte auf Unionsebene fand schließlich erst viele Jahre später mit dem Inkrafttreten des Lissabon-Vertrags 2009 Eingang in das EU-Primärrecht, insb. indem die EU-Grundrechtecharta zum verbindlichen Teil

254 Mit Ausnahme der OECD-Richtlinien und der Europaratskonvention.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des EU-Primärrechts wurde. Der in der EU-Grundrechtecharta formulierte Schutz personenbezogener Daten ist seither Teil des EU-Primärrechts, das zwingendermaßen gemäß den primärrechtlichen Vorgaben im Bereich des Sekundärrechts gewährleistet werden muss.

Grad der erforderlichen Zustimmung für wesentlichen Wandel: Die EU-Datenschutzpolitik ist eingebettet in das komplexe politische Mehrebenensystem der Europäischen Union. Die in den Betrachtungszeitraum der Kontextanalyse fallenden datenschutzpolitischen Auseinandersetzungen spiegeln dieses Verhältnis stets wider, indem einzelne nationale Akteure den Transfer bestimmter Politiken auf die EU-Ebene vorangetrieben haben. Beispiele hierfür sind die nationalen Datenschutzaufsichtsbehörden, die mit ihrer Blockadeandrohung grenzüberschreitender Datentransfers in Mitgliedstaaten, die über keine Datenschutzgesetze verfügten, die Kommission zur Initiierung der Datenschutzrichtlinie antrieben oder die Mitgliedstaaten, die die Vorratsdatenspeicherung erfolgreich auf die EU-Agenda setzen konnten. Die konkreten Auseinandersetzungen zwischen den Unionsorganen spiegeln wiederum das über viele Jahre etablierte Kräfteverhältnis untereinander wider. Während das Europäische Parlament bei den allgemeinen Datenschutzgesetzen über ein formelles Mitspracherecht verfügte, die letztlichen Entscheidungen jedoch vor allem im Ministerrat getroffen wurden, hatte das EP im Bereich der sicherheitspolitischen Datenschutzmaßnahmen praktisch überhaupt keine Entscheidungsmacht. Allerdings ereignete sich am Ende des Betrachtungszeitraums ein signifikanter Wandel im Grad der erforderlichen Zustimmung für wesentlichen Wandel. Am 1. Dezember 2009 trat der Lissabonner Vertrag in Kraft, in dessen Folge das EP zum gleichberechtigten Mitgesetzgeber in nahezu allen Bereichen der Unionspolitik und durch die gleichzeitig erfolgte weitgehende Abschaffung der Säulenstruktur auch im Bereich der PJZS aufgestiegen ist.

Relative Offenheit des politischen Systems: Zentrale Charakteristika des politischen Systems der EU sind dessen Offenheit und die Involvierung einer großen Zahl an Akteuren. Sowohl Private als auch öffentliche Akteure aus allen Ebenen (lokal, national, europäisch) bilden auf EU-Ebene komplexe Akteursnetzwerke, die in Abhängigkeit von den behandelten Themen potentiell auf allen Ebenen im Hinblick auf die Beeinflussung von Politiken aktiv sind. Zudem gilt als ausreichend belegt, dass administrative Akteure, privatwirtschaftliche und zivilgesellschaftliche Interessengruppen sowie Wissenschaftler aus verschiedenen EU-Mitgliedstaaten z. B. ökologisch oder privatwirtschaftlich motivierte Koalitionen auf EU-Ebene bilden (Rozbicka 2013, 843 f.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Traditionelle Konfliktlinien: Das Phänomen der traditionellen Konfliktlinien spielte in der Datenschutz-Politik keine größere Rolle. Der einzige Aspekt, der bei der Datenschutz-Politik an traditionelle Konfliktlinien erinnert, ist der, dass die Gegner staatlicher (Wirtschafts-)Regulierung häufig auf Seiten der Datenschutz-Gegner zu finden waren. Insbesondere die konservativen Parteien, aber auch die Liberalen stellten sich gegen die Einführung von aus ihrer Perspektive restriktiven Datenschutz-Gesetzen. Parteien, die eher grundsätzlich für eine Regulierung der Wirtschaft eintreten, forderten zugleich auch die Verabschiedung von Datenschutz-Gesetzen, so insb. Parteien links der Mitte.

Wandel sozioökonomischer Bedingungen: Einen signifikanten Wandel in den sozioökonomischen Bedingungen hat es im Betrachtungszeitraum im Hinblick auf das Bedeutungswachstum der Verarbeitung personenbezogener Daten gegeben. In dem Maße, in dem die Preisgabe personenbezogener Daten zu einer alltäglichen Praxis wurde, stieg auch die wirtschaftspolitische Bedeutung, die der Verarbeitung personenbezogener Daten zugesprochen wurde. In der Datenschutz-Politik äußerte sich diese Verschiebung in der Veränderung der Rahmung des Themas. Je stärker die wirtschaftspolitische Bedeutung in den Vordergrund rückte, umso weniger wurde über die grundrechtliche Bedeutung des Datenschutzes gesprochen. Stattdessen setzte sich allmählich die Vorstellung durch, dass Gesetze zum Schutz personenbezogener Daten letztlich Vertrauen schaffen und dadurch zu Wirtschaftswachstum auf Grundlage der Verarbeitung personenbezogener Daten führen sollten.

Wandel in der öffentlichen Meinung: Im Laufe der 2000er fand in mehrfacher Hinsicht ein Wandel in der öffentlichen Meinung statt. Obwohl die Unterstützung der europäischen Bevölkerung für Anti-Terror-Maßnahmen konstant hoch blieb und diese von einer Bevölkerungsmehrheit befürwortet wurden, nahmen zugleich auch die Datenschutz-Sorgen der Bevölkerung zu, sodass zwei Drittel aller europäischen Bürgerinnen und Bürger der Meinung waren, dass ihre personenbezogenen Daten nicht ausreichend geschützt seien. Gleichzeitig sank das Bedrohungsgefühl vor Terror-Anschlägen in signifikantem Maße und insbesondere in einigen Mitgliedstaaten wie Deutschland stieg die Ablehnung gegenüber Gesetzen, von denen ein zu weitreichender Eingriff in die Grund- und Persönlichkeitsrechte befürchtet wurde. Schließlich hielt erstmals eine Mehrheit aller Europäerinnen und Europäer im Jahr 2008 den Erlass nationaler Datenschutzgesetze für nicht ausreichend und trat stattdessen für die Verabschiedung von Datenschutzgesetzen auf EU-Ebene ein.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Wandel maßgeblicher (Regierungs-)Koalitionen: Im Bereich der EU-Datenschutzpolitik hat es keinen relevanten Wandel maßgeblicher Regierungskoalitionen gegeben. Eine Veränderung hat es dagegen durchaus auf Ebene der Koalitionen im EP gegeben. Während die Sozialdemokraten und teils auch die Liberalen immer wieder gegen die Stärkung des Datenschutzes stimmten, gelangten beide Fraktionen gegen Ende des Betrachtungszeitraums an einen Punkt, an dem sie sich mit der datenschutzrechtlichen Situation in der Union höchst unzufrieden zeigten und im Ergebnis an die Seite der Fraktionen der Linken und Grünen stellten.

Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen: Die im Feld der Datenschutz-Politik relevanteste Policy-Wirkung aus anderen Subsystemen erfolgte aus dem Bereich der Sicherheitspolitik infolge eines externen Schocks in Gestalt der Terroranschläge in New York, Madrid und London, die zur Versicherheitlichung der Politiken westlicher Staaten führten. Außerdem kann das für 1992 vorgesehen Inkrafttreten des Europäischen Binnenmarktes als ein externer Schock bezeichnet werden, den die Datenschutzaufsichtsbehörden als Policy Entrepeneure zu ihren Gunsten zu nutzen wussten.

3.5.2 Identifikation von Advocacy-Koalitionen

Entlang der während der Kontextanalyse diskutierten politischen Auseinandersetzungen lassen sich drei Koalitionen auf dem Feld der Europäischen Datenschutzpolitik unterscheiden.

Datenschutzbefürworter: Eine Koalition, die sich aus Datenschutzbefürwortern[255] zusammensetzt.

Sicherheitsbefürworter: Eine zweite, aus Befürwortern der Ausweitung von Sicherheitsgesetzen bestehende Koalition.

255 Die m. E. sprachlich präziseste Bezeichnung dieser Koalition ist „Datenschutz-Regulierungsbefürworter", da diese Formulierung deutlich macht, dass es bei deren Mitgliedern nicht nur um die Befürwortung von Datenschutz im Allgemeinen, sondern um die Befürwortung des Erlasses datenschutzspezifischer verbindlicher staatlicher Regelungen geht. Aus Gründen der Lesbarkeit bezeichne ich diese Koalition im Folgenden als „Datenschutzbefürworter". Diese sprachliche Vereinfachung hat jedoch den Nachteil, dass sie suggerieren könnte, dass die anderen Koalitionen homogene Datenschutz-Gegner seien. Tatsächlich sind unter deren Mitgliedern auch viele Akteure vorzufinden, die Sicherheitsaspekte bzw. Maßnahmen der Selbstregulierung priorisieren, ohne die Bedeutung des Schutzes personenbezogener Daten vollständig zu negieren.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Flexibilitätsbefürworter: Sowie eine dritte Koalition, die sich im Allgemeinen gegen staatliche Regulierung bzw. für die möglichst flexible Ausgestaltung erlassener staatlicher Regeln ausspricht.

Im Weiteren werde ich nun die Koalitionen der Datenschutzbefürworter und der Flexibilitätsbefürworter näher darstellen. Die Koalition der Sicherheitsbefürworter werde ich dagegen nicht näher betrachten, da ich den Betrachtungsrahmen der Arbeit auf das allgemeine Datenschutzrecht beschränke und sicherheitspolitisch relevante Aspekte lediglich dann diskutiere, wenn dies relevant im Hinblick auf die Beantwortung der Forschungsfragen ist. Während der Diskussion der Koalitionen der Datenschutzbefürworter bzw. der Flexibilitätsbefürworter nehme ich allerdings durchaus Bezug auf sicherheitspolitische Argumente und Akteure.

Zudem sei darauf hingewiesen, dass die an dieser Stelle erfolgende Identifikation der Advocacy-Koalitionen nicht auf einer ähnlich ausführlichen Methodik basiert, wie sie zur Identifikation der Advocacy-Koalitionen bei der Aushandlung der DSGVO verwendet wurde. Daher kann es etwa vorkommen, dass Akteure, die eigentlich auf Grundlage des ACFs einbezogen werden müssten, aus dem Blick geraten.

3.5.2.1 Datenschutzbefürworter-Koalition:

Die Koalition der Datenschutzbefürworter vereinigt alle Akteure, die für den Ausbau von gesetzlichen, verpflichtenden Regelungen zum Schutz personenbezogener Daten eintreten.

3.5.2.1.1 Zusammensetzung der Datenschutzbefürworter-Koalition

Die Koalition der Datenschutzbefürworter ist die am längsten bestehende Advocacy-Koalition im Bereich der Datenschutzpolitik. Den Kern dieser Koalition bilden die *Datenschutzaufsichtsbehörden*. Die Entstehung dieser Koalition lässt sich mindestens bis zur DS-RL 95/46/EG zurückverfolgen. Im Vorfeld und während der Verhandlungen der Richtlinie traten die nationalen Datenschutzaufsichtsbehörden in Gestalt eines *transgovernmental network of policy entrepeneurs* (A. L. Newman 2008a) gemeinsam und grenzübergreifend für die Stärkung der Datenschutzregelungen ein (vgl. 3.2.2). Nach der Verabschiedung der DS-RL bzw. der DS-VO kamen zur Gruppe der Datenschutzaufsichtsbehörden auch die *Art. 29-Datenschutz-*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

gruppe im Jahr 1996 sowie die Institution des *Europäischen Datenschutzbeauftragten* im Jahr 2004 hinzu (vgl. 3.2.2.7 und 3.2.5). Das Parlament, das bereits in den 1970er-Jahren die Kommission mehrfach zum Erlass gemeinschaftlicher Datenschutzregelungen aufgefordert hatte, nahm zwar zwischenzeitlich – während der Aushandlung der DS-RL – eine ambivalente Rolle ein, setzte sich bei den folgenden Gesetzgebungsprozessen allerdings wieder für die Durchsetzung eines hohen Datenschutzniveaus ein (vgl. 3.2.4 ff.).[256] Noch etwas schwieriger ist diese Bewertung im Hinblick auf die Europäische Kommission. Während die Kommission zwar einerseits immer wieder als Verfechterin eines hohen Datenschutzniveaus aufgetreten ist,[257] war sie zugleich andererseits auch immer wieder jene Akteurin, die sich dem Druck des Ministerrates noch am ehesten beugte.[258] Da der Großteil der bedeutenden EU-Datenschutz-Instrumente dennoch auf die Kommission bzw. die in ihr mit dem Thema Datenschutz befassten Generaldirektionen bzw. Referate zurückgeht, werte ich die Kommission als Teil der Datenschutzbefürworter-Koalition.

Die Datenschutzbefürworter-Koalition setzte sich somit zunächst vor allem aus Akteuren aus dem politischen bzw. politik-nahen Umfeld zusammen. Weitere Akteure traten der Koalition erst im Laufe der Jahre bei.

Ende der 1990er-Jahre weitete der Europäische Verbraucherverband BEUC seine Aktivitäten auf das Feld der Datenschutzpolitik aus und vertrat eine verbraucher- und datenschutzfreundliche Linie. (vgl. die Fn. 153, 177 und 214).

Datenschutz-Organisationen aus dem Bereich der Zivilgesellschaft waren zwar auf nationaler Ebene seit längerer Zeit aktiv (vgl. 3.4.2.3.1), doch ein Engagement auf EU-Ebene erfolgte erst einige Jahre später. Die ersten zivilgesellschaftlichen Akteure aus diesem Bereich waren Privacy International und EPIC. Obwohl sich beide Akteure zwar in unregelmäßigen

256 Ich zähle das Europäische Parlament grundsätzlich zur Koalition der Datenschutzbefürworter hinzu. Bei näherer Betrachtung des Parlaments ergeben sich aber auch Widersprüche. Auf diese gehe ich im folgenden Unterabschnitt über die Überzeugungssysteme etwas näher ein.

257 Vgl. insbesondere die Kommissionsentwürfe zur DS-RL, zur ePrivacy-Richtlinie und zum JI-Rahmenbeschluss (vgl. 3.2.2, 3.3.2 und 3.3.4.4) bzw. die ursprüngliche Haltung der Kommission hinsichtlich der Vorratsdatenspeicherung oder auch des Zugriffs auf Fluggastdaten (vgl. 3.3.4.2 und 3.3.4.3).

258 Vgl. insbesondere die Änderung der Kommissionsposition im Zusammenhang mit der Vorratsdatenspeicherung und dem Zugriff auf Fluggastdaten (vgl. 3.3.4.2 und 3.3.4.3).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Abständen am Policy-Subsystem der EU-Datenschutzpolitik beteiligten, richtete sich ihr Fokus auf die Politik ihres jeweiligen Herkunftslandes. Erst mit EDRi formierte sich eine zivilgesellschaftliche Organisation, die ihren Fokus auf die EU-Politik setzte und die seit Mitte der 2000er-Jahre zunehmend sichtbarer wurde (vgl. 3.4.2.3.1).[259]

Akteur	Akteursgruppe
Nationale Datenschutzaufsichtsbehörden	Datenschutzbehörden
Art. 29-Datenschutzgruppe	Datenschutzbehörden
EDSB	Datenschutzbehörden
Europäische Datenschutz-Konferenz	Datenschutzbehörden
Europäisches Parlament (insb. GUE/NGL, Grüne/EFA, aber immer wieder auch S&D sowie ALDE)	EU-Politik
Europäische Kommission (genauer: die mit Datenschutz befassten Kommissionsstellen)	EU-Politik
BEUC	Verbraucherschutzverband
EPIC	Zivilgesellschaft
EDRi	Zivilgesellschaft
Privacy International	Zivilgesellschaft

3.5.2.1.2 Überzeugungssystem der Datenschutzbefürworter-Koalition

Da die Mitglieder der Koalition tendenziell eher dem linken und linksliberalen gesellschafts- bzw. parteipolitischen Spektrum entstammen, ist auf Ebene der Grundüberzeugungen eine Betonung individueller und gesellschaftlicher Freiheit vorherrschend, während im überwiegenden Teil der Koalition zugleich eine starke Abneigung insbesondere gegen sicherheitspolitisch motivierte Eingriffe in diese Freiheit vorhanden ist.

Die Policy-Kernüberzeugung, die die Mitglieder der Datenschutzbefürworter-Koalition in erster Linie eint, ist die Betrachtung des Schutzes personenbezogener Daten als Grundrecht. Zudem wird dieses Datenschutz-Grundrecht in der Tradition des Volkszählungsurteils als funktional wich-

259 Wissenschaftler(innen) und Fachjournalist(inn)en traten während der politischen Aushandlungsprozesse in eher geringem Maße in Erscheinung. Nennenswert sind hier insb. die deutsche Nachrichten-Webseite „Heise Online“ sowie das Blog Netzpolitik.org

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

tiges Element im Hinblick auf die Wahrung der Demokratie gesehen.[260] Neue Sicherheits- und Überwachungsmaßnahmen werden seitens der Datenschutzbefürworter-Koalition daher immer an ihren Auswirkungen auf die Demokratie gemessen. So wird im Zusammenhang mit JI-Politiken der Erhalt demokratischer Kontrollmechanismen gefordert. Aufgrund der Skepsis gegenüber zu großer staatlicher Macht werden insbesondere jene Sicherheits- und Anti-Terror-Maßnahmen abgelehnt, denen eine Untergrabung demokratischer Grundwerte zugerechnet wird.[261] Angesichts der in Folge des 11. Septembers zunehmend ausgeweiteten Sicherheits- und Anti-Terrorgesetze bestand das Kernanliegen dieser Koalition während der 2000er-Jahre darin, ein der DS-RL äquivalentes Schutzniveau für die im Rahmen der dritten EU-Säule stattfindenden Verarbeitungen zu etablieren. Allerdings vermochte es die Koalition weder dieses Anliegen in die Tat umzusetzen, noch konnte es andere, den Datenschutz direkt betreffende Überwachungsmaßnahmen wie den Zugriff auf Fluggastdaten verhindern. Insofern muss resümiert werden, dass sich die Koalition der Datenschutzbefürworter während der 2000er-Jahre in einer andauernden Defensiv-Rolle befunden hat.

Koalitionsinternes Konfliktpotential auf Überzeugungsebene besteht insbesondere zwischen den liberalen, sozialdemokratischen und linken Teilen der beteiligten Akteure, wie bei mehreren einschlägigen Auseinandersetzungen im Europäischen Parlament deutlich wurde. Am anschaulichsten zeigten sich die Fronten während der Verhandlungen der ePrivacy-Richtlinie. Als sich der politische Streit anfangs noch um die Frage des Opt-ins/Opt-outs drehte, forderte der liberale Parlamentsberichterstatter Cappato, dass die Lösung der Frage den Unternehmen überlassen bleiben und

260 Vgl. hierzu etwa das Selbstverständnis von EDRi: „To ensure a functioning democracy, basic rights and freedoms need to be guaranteed. In Europe, these rights are established by the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and by national constitutions. In the digital environment, among the most relevant are the right to privacy and data protection, the right to a fair trial, freedom of thought, expression and information and the right to an effective remedy when our rights have been breached." (EDRi 2019)

261 In diesem Zusammenhang wird immer wieder auch auf das Missbrauchsanfälligkeitsargument verwiesen: „Was passiert denn etwa mit den Daten, die der Staat über Sie und Ihr Surfverhalten sammelt? Die Daten werden zusammen gespeichert. Sie werden an die nächste Regierung weiter gegeben. Ob dann Le Pen, Haider oder Rasmussen darauf Zugriff haben oder nur die normalen obrigkeitsstaatlichen Sozialdemokraten, weiß niemand." (vgl. Ilka Schröder, in: Europäisches Parlament 2002b)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nicht gesetzlich geregelt werden sollte. Am Ende der Auseinandersetzung brachten die sozialdemokratische, grüne und linke Fraktion den Berichtsvorschlag Cappatos schließlich zum Scheitern, da er nicht die von ihnen bevorzugte verbindliche Opt-in-Regel beinhaltete. Als Cappato später einen modifizierten Vorschlag vorlegte, der am Opt-out-Prinzip im Wesentlichen festhielt, kam der größte Widerstand seitens der linken und grünen Fraktionen, während die halbe sozialdemokratische Fraktion sich hinter Cappatos Vorschlag stellte. Schließlich verschoben sich die Fronten ein weiteres Mal, nachdem sich die Sozialdemokraten und die Christdemokraten wenig später dem Druck des Ministerrats im Zusammenhang mit der sicherheitspolitisch motivierten Speicherung von Verkehrsdaten elektronischer Kommunikation beugten. Während die Sozialdemokraten gemeinsam mit den konservativen Fraktionen den sog. Kompromissvorschlag annahmen, stimmten die Grünen, Linken und Liberalen gegen ihn (vgl. 3.3.2).

3.5.2.1.3 Ressourcen der Datenschutzbefürworter-Koalition

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die Koalition der Datenschutzbefürworter ist in hohem Maße in politische Entscheidungsprozesse eingebunden. Historisch kam diese Rolle insbesondere der EU-Kommission zu, da ihr gemäß Europäischer Verträge eine wesentliche Rolle bei der Vorbereitung, Verabschiedung, Durchführung und Kontrolle von EU-Politiken zukommt (Wessels 2008, 225). Allerdings hat die Macht der Kommission auch ihre Grenzen: Während sie zwar in der Regel (Lelieveldt und Princen 2015, 86) als einziges EU-Organ das Initiativrecht zur Einbringung von Legislativvorschlägen innehat, ist sie trotzdem an die durch die EU-Verträge bestimmten Grenzen gebunden. Diese Verträge wiederum werden seitens der Mitgliedstaaten geschlossen und können, müssen aber nicht zwangsläufig dem Kommissionsinteresse entsprechen (Princen und Rhinard 2006b).

Eine im Laufe der Jahrzehnte zunehmend wichtige Rolle hat das EP eingenommen. Noch zu Beginn der Aushandlung der DS-RL hatte das Parlament (im Rahmen des Kooperationsverfahrens) ein eingeschränktes Mitspracherecht. Mit der Einführung des Mitentscheidungsverfahrens im Rahmen des Maastrichter Vertrags entwickelte sich das Parlament allerdings in zunehmendem Maße zum Mitgesetzgeber. Alle das allgemeine Datenschutzrecht betreffenden Gesetzesvorschläge (Datenschutz-, ISDN-,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ePrivacy- und Cookie-Richtlinie) wurden im dem Mitentscheidungsverfahren verhandelt. Ausgeschlossen war das Parlament dagegen von allen die dritte EU-Säule betreffenden Angelegenheiten. Die Grenzen des Einflusses des Parlaments zeigten sich besonders offenkundig während der Verhandlung des JI-Rahmenbeschlusses. Trotz der Zusagen mehrerer Ratspräsidentschaften, dass die Parlamentsposition ernsthaft berücksichtigt werden würde, einigte sich der Ministerrat aufgrund des Widerstands einiger Mitgliedstaaten letztlich nur auf einen Minimalkonsens. Erst durch die Aufhebung der EU-Säulenstruktur und durch die Aufwertung des Mitentscheidungsverfahrens zum neuen ordentlichen Gesetzgebungsverfahren der EU stieg das Parlament endgültig zu einem formal gleichberechtigten Mitgesetzgeber auf.

Neben diesen beiden Akteuren sind die Art. 29-Datenschutzgruppe (gemäß Art. 30 DS-RL) sowie der Europäische Datenschutzbeauftragte (gemäß Art. 46 lit. d DS-VO) formell in politische Entscheidungsprozesse eingebunden. Allerdings beschränkt sich die Gestaltungsmacht beider Akteure formell auf eine rein beratende Funktion. Besonders seitdem die Kommission in ihrem Überprüfungsbericht aus dem Jahr 2003 feststellte, dass die DS-RL in den Mitgliedstaaten uneinheitlich angewendet wurde, kam der Datenschutzgruppe eine zentrale Rolle bei der Ausarbeitung von Harmonisierungsempfehlungen zu, die zu einer deutlichen Aufwertung ihrer Beratungsfunktion führte. Beide Institutionen stehen insbesondere in regem Austausch mit dem Datenschutz-Referat der Kommission, das für die Datenschutz-Aktivitäten der Kommission zuständig ist sowie dem LIBE-Ausschuss des Parlaments, der für die Ausarbeitung der Parlamentspositionen im Hinblick auf Datenschutzpolitiken zuständig ist. Insofern verfügen beide Akteure über eine besonders große informelle Handlungsmacht im Hinblick auf politische Entscheidungsprozesse. Schwieriger gestaltete sich dagegen das Verhältnis beider Institutionen gegenüber dem Ministerrat, da dieser ein eher geringes Interesse an den Positionen der Datenschützer zeigte.

Die Akteure aus dem Bereich des Verbraucherschutzes und der Zivilgesellschaft sind in legislative Entscheidungsprozesse allenfalls so stark eingebunden, wie die zentralen politischen Entscheider auf ihre Stellungnahmen Rücksicht nehmen.

Unterstützung durch die Öffentliche Meinung

Der Schutz personenbezogener Daten wird von einem Großteil der EU-Bevölkerung als wichtig angesehen. Eine konstante Mehrheit der im Rahmen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

von EU-weit repräsentativen Eurobarometer-Studien befragten Personen gibt in allen seit 1991 durchgeführten Studien regelmäßig an, dass sie sich angesichts der praktizierten Datenverarbeitungen unwohl fühlt, während der gesetzliche Schutz personenbezogener Daten befürwortet wird. Allerdings kann nicht von einer uneingeschränkten Befürwortung des Datenschutzes die Rede sein. So befürwortete eine Mehrheit der europäischen Bürgerinnen und Bürger die Einschränkung von Datenschutzrechten zum Zwecke der Bekämpfung von Straftaten, insb. des internationalen Terrorismus. Diese Feststellung trifft jedoch nicht auf die Verarbeitung durch privatwirtschaftliche Akteure zu. Die Mehrheit der EU-Bürgerinnen und Bürger zeigte sich in den 1990ern und 2000ern über die Nutzung ihrer personenbezogenen Daten besorgt (vgl. 3.4.2.2).

Informationen/Informationshoheit

Als die für die Durchführung und Kontrolle aller Unionsmaßnahmen zum Datenschutz hauptverantwortliche Akteurin verfügt die Kommission über zentrales Wissen zu vielen datenschutzpolitischen Fragen. In ähnlicher Weise verfügen die nationalen Datenschutzbehörden bzw. die Art. 29-Datenschutzgruppe sowie der Europäische Datenschutzbeauftragte über erhebliches Praxiswissen hinsichtlich der Anwendung der Datenschutzbestimmungen und ihrer Wirksamkeit. Die zivilgesellschaftlichen Akteure, Verbraucherschutzverbände und Wissenschaftler erstellen Studien und erarbeiten auf diese Weise wertvolles Wissen zu verschiedensten Aspekten des Datenschutzes.

Fähigkeit zur politischen Mobilisierung,

Die Fähigkeit zur politischen Mobilisierung der Koalition ist zwar ausgeprägter als bei der Koalition der Flexibilitätsbefürworter, doch leiden die Datenschutzbefürworter unter dem grundsätzlichen Problem, die in der Bevölkerung vorherrschende generelle Zustimmung für Datenschutzmaßnahmen nicht in eine effektive politische Mobilisierung umsetzen zu können. Eine Ausnahme in diesem Zusammenhang bildeten die enormen Proteste gegen die Vorratsdatenspeicherung insb. in Deutschland, aber auch in einigen weiteren EU-Mitgliedstaaten (vgl. 3.4.2.3.2).

Finanzielle Ressourcen

Über nennenswerte finanzielle Ressourcen verfügen insbesondere die mit Datenschutz befassten Referate der Kommission sowie der LIBE-Ausschuss des Europäischen Parlaments. Beide Institutionen nutzen ihre finanziellen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Mittel für die Durchführung zahlreicher Aktivitäten im Bereich der Datenschutzpolitik. Die mit Datenschutz befassten Kommissionsstellen sind beispielsweise treibender Akteur im Hinblick auf die Diskussion verschiedener Themen wie PETs oder Datenschutzbedenken im Hinblick auf RFID gewesen. Diese und weitere formelle wie auch informelle Diskussionen wurden insbesondere durch die Durchführung von Konsultationen, Anhörungen, Konferenzen und Workshops vorangetrieben. Daneben geben die mit Datenschutz befassten Stellen der Kommission und des Parlaments bereits seit der Frühphase des Datenschutzes regelmäßig Studien zur Untersuchung datenschutzpolitischer Fragen in Auftrag (vgl. 3.2.2.1), (European Commission 2017; Karaboga 2018, 154).

Die zivilgesellschaftlichen Akteure der Koalition verfügen über weitaus geringere finanzielle Mittel. Die einzige im Betrachtungszeitraum auf EU-Ebene aktive zivilgesellschaftliche Organisation EDRi befand sich immer noch weitgehend in der Entstehungsphase. Die anderen Akteure (EPIC, Privacy International, usw.) sind als etablierter einzustufen, doch auch ihnen mangelte es während der 2000er-Jahre an finanziellen Mitteln (Dobusch 2014). Im Falle der niederländischen Bits of Freedom resultierte der Geldmangel – ausgerechnet zur Hochphase der Anti-Vorratsdatenspeicherungsproteste – in der Einstellung ihrer Aktivitäten (Sokolov 2006).

Das *Vorhandensein einer fähigen Führung*

Die Koalition der Datenschutzbefürworter verfügt über keine zentrale Führungsinstanz, die alle Mitglieder der Koalition umspannt. Auf Ebene der einzelnen Akteure kann hingegen durchaus von der Einnahme von Führungspositionen die Rede sein: Im Falle des Parlaments kam diese Rolle den jeweiligen Berichterstattern (z. B. Cappato) bzw. den Schattenberichterstattern (z. B. In't Veld) zu. Bei der Kommission kam eine vergleichbare Rolle zunächst Martin Bangemann zu, später dann auch Barrot und Reding. Auch einzelne Datenschutzbeauftragte bzw. Leiter von Datenschutzaufsichtsbehörden nehmen regelmäßig eine Führungsrolle ein, darunter insb. Peter Hustinx, der von 1996 bis 2000 zunächst Vorsitzender der Art. 29-WP war und von 2004 bis 2014 das Amt des EDSB inne hatte.

3.5.2.2 Flexibilitätsbefürworter-Koalition

Die Koalition der Flexibilitätsbefürworter vereinigt Akteure, die sich gegen eine staatliche Regulierung auf dem Felde der Datenschutzpolitik ausspre-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

chen und die stattdessen für eine möglichst flexible Ausgestaltung erlassener staatlicher Regeln eintreten.

3.5.2.2.1 Zusammensetzung der Flexibilitätsbefürworter-Koalition und ihr Verhältnis zur Flexibilitätsbefürworter-Community

Die Flexibilitätsbefürworter-Koalition setzt sich aus Akteuren aus der Privatwirtschaft sowie aus den Regierungen einiger Mitgliedstaaten bzw. aus deren im Ministerrat versammelten Repräsentanten zusammen, unterstützt von den wirtschaftsnahen Kommissionsstellen sowie insb. dem konservativen Teil des EP. Die in dieser Koalition versammelten Akteure eint das gemeinsame Interesse an einem Datenschutzrahmen, der den Unternehmen das höchstmögliche Maß an Freiheit beim Umgang mit personenbezogenen Daten überlässt und keine Kosten durch verpflichtend zu ergreifende Datenschutzmaßnahmen verursacht. Den Nukleus dieser Koalition bilden folglich jene Unternehmen, deren Kerntätigkeit in der massenhaften Verarbeitung personenbezogener Daten liegt. Diese Unternehmen erhalten Unterstützung seitens der Regierungen verschiedener Mitgliedstaaten, die sich aus dieser Unterstützung wiederum vor allem eine Stärkung ihrer heimischen Volkswirtschaften versprechen (vgl. insb. 3.2.2).

Die Kooperation der Flexibilitätsbefürworter ist allerdings weniger stark ausgeprägt als bei den Datenschutzbefürwortern. In der Frühphase des Datenschutzes, während der 1970er- und 1980er-Jahre, verhinderten die Mitgliedstaaten gemeinschaftliche Datenschutzmaßnahmen zunächst noch eher *aus Gewohnheit*: Datenschutz war zu jenem Zeitpunkt noch kein gemeinschaftliches Aktionsfeld und die Bedeutung grenzüberschreitender Datentransfers im Kontext der Binnenmarktpolitik befand sich gerade erst im Entstehen. Folglich hatten die mitgliedstaatlichen Regierungen keine triftigen Gründe für die Abtretung ihrer nationalen – und sich selbst noch gerade erst im Entstehen befindenden – Kompetenzen auf dem Gebiet des Datenschutzes an die Gemeinschaftsebene. In ähnlicher Weise berührte das Thema Datenschutz Ende der 1980er bzw. Anfang der 1990er-Jahre zunächst nur wenige Wirtschaftsbereiche bzw. Unternehmen wie die Direktmarketing- und Kreditbranche, Banken und Versicherungen (Ellger 1990, 108–29; Priscilla M. Regan 1999, 200 f.). Erst mit dem Widerstand gegen den ursprünglichen Richtlinienvorschlag der Kommission, der die weitgehende Abtretung mitgliedstaatlicher Kompetenzen an die Kommission vorsah, wurde der gegenseitige Nutzen zwischen Privatwirtschaft und den

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Regierungen der Mitgliedstaaten offenkundig: Die Mitgliedstaaten des sog. nördlichen Blocks traten für nationale statt Gemeinschaftsregelungen ein. Die Privatwirtschaft dagegen unterstützte diese Position, da sie in der Fragmentierung der mitgliedstaatlichen Gesetze kein Problem erkannte. Zum einen konnten durch die Verschiebung von Datenschutz-Kompetenzen in Richtung der Mitgliedstaaten hohe gemeinschaftliche Schutzstandards verhindert werden. Zum anderen eröffnete die Kompetenzverschiebung die Möglichkeit, niedrigere Schutzstandards im *eigenen* Mitgliedstaat als in anderen Mitgliedstaaten zu verabschieden (vgl. 3.2.2). Aus dieser losen *Koalition aus Gewohnheit* entwickelte sich in den Folgejahren schließlich eine zunehmend festere Struktur auf Basis geteilter Überzeugungen.

Dem in anderen Politikbereichen stattfindenden Lobbying im Mehrebenensystem der EU entsprechend (Dialer und Richter 2019), wird auch das Lobbying im Datenschutz-Subsystem in der Regel weniger von einzelnen Unternehmen als vielmehr von Unternehmensverbänden praktiziert. Die am längsten im Bereich der EU-Datenschutzpolitik aktiven Verbände sind FEDMA, der *Verband des europäischen Direkt- und interaktiven Marketings*, der die Interessen datengestützter Marketingspezialisten gegenüber den EU-Organen vertritt; die ICC (*International Chamber of Commerce* – Internationale Handelskammer) mit Sitz in Paris, die die Interessen von inzwischen mehr als 6 Millionen weltweiten Unternehmen und Verbänden aus nahezu allen Wirtschaftsbereichen vertritt; sowie Businesseurope (ehemals UNICE), der europäische Zusammenschluss 40 nationaler Arbeitgeberverbände. In dem Maße, in dem die Verarbeitung personenbezogener Daten zentraler für viele Geschäftsprozesse und für die Steigerung von Unternehmensgewinnen im Laufe der 1990er und 2000er-Jahre wurde, nahm auch die Zahl und die Verschiedenartigkeit der Branchen der Subsystem-Akteure zu. Die Interessen der Werbe- und Marketingbranche wurden in den Folgejahren auch vom *Interactive Advertising Bureau* (IAB) mit Sitz in den Vereinigten Staaten vertreten. Die Interessen der Versicherungsbranche wurden von der europäischen Dachorganisation *Insurance Europe* vertreten. Die *American Chamber of Commerce to the European Union (*AmCham EU) repräsentiert die Interessen der US-Wirtschaft in Europa.[262] Zu den langjährigen Akteuren auf dem Feld der EU-Datenschutzpolitik zählen zudem auch mehrere Verbände aus dem Bereich der Printmedien und des Fernsehens. Die *Association of Commercial Television in Europe*

262 https://lobbypedia.de/wiki/AmCham_EU

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(ACT) vertritt die Interessen privater Fernsehsender. Die *European Newspaper Publishers' Association* (ENPA) vertritt die Interessen von über 5.000 Zeitungen aus 25 europäischen Staaten.[263] Das *European Publishers Council* (EPC) ist ebenfalls ein Zusammenschluss europäischer Zeitungs- und Magazinverleger.[264]

Akteur	Akteursgruppe
FEDMA	Privatwirtschaft
ICC	Privatwirtschaft
UNICE (Businesseurope)	Privatwirtschaft
IAB	Privatwirtschaft
AmCham EU	Privatwirtschaft
ACT	Privatwirtschaft
ENPA	Privatwirtschaft
EPC	Privatwirtschaft
EU-Ministerrat	EU-Politik

Tabelle 3-5: Zentrale Akteure der Flexibilitätsbefürworter-Koalition (eigene Zusammenstellung)

3.5.2.2.2 Überzeugungssystem der Flexibilitätsbefürworter-Koalition

Das Hauptinteresse der Flexibilitätsbefürworter besteht in der Reduzierung regulierungsbedingter Kosten bei der ökonomischen Nutzbarmachung personenbezogener Daten. Die in der Koalition versammelten Akteure vertreten tendenziell eher wirtschaftsliberale und konservative Grundüberzeugungen. so wird zwar ebenso wie vonseiten der Datenschutzbefürworter individuelle Freiheit betont, doch eher in einem stark marktwirtschaftlichen Sinne. Fokussiert wird also eher auf das Moment der Abwesenheit von Unterdrückung (negative Freiheit) statt auf die Erweiterung individueller Handlungsspielräume, um die Potentiale der negativen Freiheit auch real nutzen zu können. Das zentrale Argument der Datenschutzbefürworter-Koalition, wonach es sich beim Datenschutz um ein Grundrecht handele, das gegenüber konkurrierenden Interessen grundsätzlich bevorzugt werden sollte, wird abgelehnt. Stattdessen wurde mit verschiedenen Begründungen

263 https://www.enpa.eu/association/mission#board
264 http://epceurope.eu/about/

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die Wichtigkeit des unternehmerischen Zugriffs auf personenbezogene Daten betont. Der größte gemeinsame Nenner der verschiedenen seitens der Flexibilitätsbefürworter vorgebrachten Argumente ist die Hervorhebung des gesellschaftlichen Nutzens der privatwirtschaftlichen Datenverarbeitung.[265]

Obwohl viele datenverarbeitende Unternehmen und mitgliedstaatliche Regierungen bzw. Ministerratsdelegierte schon in der Frühphase der EU-Datenschutzpolitik im Vorfeld der Erarbeitung der DS-RL ein gemeinsames Interesse an möglichst niedrigen Datenschutzregulierungsstandards hatten, könnte das damalige Akteursnetzwerk im Sinne des ACF allenfalls als *Advocacy-Community* (Stritch 2015, 442) oder als eine *coalition of convenience* (Koalition aus Bequemlichkeit) (Zafonte und Sabatier 2004, 100) bezeichnet werden. Zwar waren gemeinsame, grundsätzlich gegen eine gemeinschaftsweite Datenschutzregulierung gerichtete Überzeugungen vorhanden, doch hatte es bis zum DS-RL-Vorschlag der Kommission keine Notwendigkeit für eine Kooperation untereinander gegeben, da der Status Quo den Verarbeitungsbedürfnissen ausreichend Rechnung trug. Erst vor dem Hintergrund der als zu restriktiv wahrgenommenen Datenschutzregelungen der DS-RL-Entwürfe der Kommission entwickelten und verfestigten sich erste Kooperationsstrukturen (Priscilla M. Regan 1999). Zu jener Zeit und bis hinein in die Phase der Verhandlung der ePrivacy-Richtlinie lehnten Akteure aus dem Bereich der Wirtschaft jegliche verbindliche Regulierung des Schutzes personenbezogener Daten auf Gemeinschaftsebene ab und verwiesen stattdessen zur Lösung möglicherweise vorhandener Probleme auf Maßnahmen der Selbstregulierung (vgl. 3.2.2 und 3.3.2). Erst mit der Konsultation im Vorfeld des ersten Berichts der Kommission über die Durchführung der DS-RL setzte die datenverarbeitende Wirtschaft einen ernsthaften inhaltlichen Dialog in Gang und stellte Datenschutzregulierung nicht mehr grundsätzlich infrage (vgl. 3.3.3).[266] Stattdessen setzte die Koalition einerseits darauf, dass Datenschutzregeln möglichst flexibel ausgestal-

265 Ein relativ universalistisches Argument ist dabei, dass die gesamte Volkswirtschaft von der möglichst wenig regulierten Verarbeitung personenbezogener Daten profitiere (vgl. z. B. die Diskussion in: Culnan und Bies 2003). Aus der US-amerikanischen Tradition stammt das Argument, dass Datenschutz die für eine Demokratie notwendige, freie Zirkulation von Informationen verhindere (Walker 2001). Andere Argumente verweisen eher auf gesellschaftliche Teilbereiche, wie den Nutzen der Datenverarbeitung für Gesundheitszwecke (Lahmann 2015).

266 Dies ist auch der Grund, weshalb ich für die Koalition die Bezeichnung Flexibilitätsbefürworter statt Regulierungsgegner wählte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tet werden und andererseits darauf, dass anstelle von *harten* Regulierungsinstrumenten (wie Verordnungen, Richtlinien, usw.) *weiche* Regulierungsalternativen (bspw. Kommissionsempfehlungen) verabschiedet werden.

Insofern besteht die zentrale Policy-Kernüberzeugung der Flexibilitätsbefürworter-Koalition in der Ablehnung staatlicher Regulierungsmaßnahmen. Im Falle einer staatlichen Regulierung setzt die Koalition schließlich vor allem auf Selbstregulierung.

3.5.2.2.3 Ressourcen der Flexibilitätsbefürworter-Koalition

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Eine ausgesprochen wirkmächtige Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse besteht beim Ministerrat. Seit der Frühphase der Datenschutzpolitik hat der Ministerrat immer wieder erfolgreich auf die Reduzierung des von der Kommission und dem Parlament vorgeschlagenen bzw. geforderten Datenschutzniveaus gedrängt, indem entweder eine entsprechende Regelung unmittelbar abgeschwächt wurde oder die Details ihrer Umsetzung den Mitgliedstaaten überlassen wurde. Letzteres kam zwar nicht formal, aber doch praktisch der Durchsetzung eines niedrigeren Schutzniveaus gleich, da das von den Datenschutzbefürwortern angestrebte EU-weit einheitliche Schutzniveau somit untergraben werden konnte. Gerade in der Frühphase des Datenschutzes, aber auch noch bis in die 2000er-Jahre hinein, hatte der Ministerrat aufgrund der gemeinschaftsrechtlichen Situation eine dominante Position im Institutionengefüge der EU inne. Spätestens mit dem Inkrafttreten des Lissabon-Vertrags erfolgte allerdings eine deutliche Annäherung der Machtpotentiale des Parlaments und des Ministerrats (Pittella, Vidal-Quadras, und Papastamkos 2014, 5).

Die in der Koalition vertretenen privatwirtschaftlichen Akteure sind in die interinstitutionellen Entscheidungsprozesse der EU zwar nicht direkt eingebunden, doch kommt der Konsultation ihrer Positionen seitens des Ministerrats, der Kommission und des Parlaments, darunter insbesondere der in erster Linie mit wirtschaftlichen Themen betrauten Ausschüsse IMCO und ITRE, große Bedeutung zu. Daneben hatten und haben die nationalen Mitgliedsverbände eine wichtige Rolle bei der nationalen Implementierung von Richtlinien inne.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Unterstützung durch die Öffentliche Meinung

Obwohl viele Menschen datenverarbeitende Produkte und Dienstleistungen rege nutzen, wird der Verarbeitung personenbezogener Daten seitens privatwirtschaftlicher Akteure nur von einer gesellschaftlichen Minderheit ausdrücklich vertraut während sich die Mehrzahl besorgt über die Verwendung ihrer personenbezogenen Daten zeigt (vgl. 3.4.2.2). Insofern kann davon ausgegangen werden, dass die Flexibilitätsbefürworter nicht auf die Unterstützung durch die öffentliche Meinung bauen können. Den Umstand, dass viele Menschen ihre Produkte und Dienstleistungen nutzen, versuchten die Datenverarbeiter dennoch politisch nutzbar zu machen, indem darauf verwiesen wurde, dass bestimmte Regulierungen die Bedienung der entsprechenden Dienste und Produkte beeinträchtigen würden. Dies war etwa der Fall im Hinblick auf die von der Datenschutzbefürworter-Koalition geforderte Opt-in-Regelung beim Setzen von Cookies (vgl. 3.3.5).

Informationen/Informationshoheit

Die im Ministerrat versammelten Regierungsvertreter bringen große fachliche Expertise zu Datenschutzfragen mit und die Verbände akkumulieren das Wissen ihrer Mitglieder.

Fähigkeit zur politischen Mobilisierung

Die Koalition der Flexibilitätsbefürworter verfügt über keine nennenswerte Fähigkeit zur politischen Mobilisierung.

Finanzielle Ressourcen

Die Koalition verfügt über enorme finanzielle Ressourcen. Diese werden insbesondere seitens der privatwirtschaftlichen Koalitionsmitglieder erfolgreich dafür genutzt, sich systematisch in alle relevanten politischen Entscheidungsprozesse im Mehrebenensystem der EU einzubringen.

Das *Vorhandensein einer fähigen Führung*

Da die Koalition keinem hierarchischen Aufbau folgt, ist keine zentrale Führungsposition vorhanden. Differenziert werden kann dagegen durchaus zwischen den Koalitionsmitgliedern, die sich besonders aktiv in das datenschutzpolitische Geschehen einbringen und jenen, die sich dem seitens der zentralen Akteure vorgegebenen Kurs eher anschließen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

4 Akteurs- und Prozessanalyse

Im vergangenen Abschnitt habe ich zur Beantwortung der zweiten Forschungsfrage die zentralen (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik gemäß des Advocacy Coalition Frameworks untersucht, die den Rahmen für den politischen Aushandlungsprozess der Datenschutz-Grundverordnung definieren: *Relativ stabile Parameter*, *langfristig wichtige Gelegenheitsstrukturen* sowie die Bedeutung *externer Systemereignisse*.

Dieser Abschnitt untersucht nun die Hauptfrage der vorliegenden Arbeit:

FF 1: Wie lässt sich die Entstehung der EU-Datenschutz-Grundverordnung (DSGVO) erklären?

Die Beantwortung der Forschungsfrage erfolgt mittels einer Akteurs- und Prozessanalyse, wie sie in Unterabschnitt 2.3 vorgestellt wurde. Der Abschnitt ist in vier Unterabschnitte gegliedert. Die ersten drei Unterabschnitte (4.1, 4.2 und 4.3) widmen sich den drei Phasen (1. Orientierungsphase, 2. Entwurfsphase, 3. Konfliktphase), in die ich den Aushandlungsprozess der DSGVO in Unterabschnitt 2.3 unterteilt habe. Jede Phase beginnt mit einer Akteursanalyse, in der zunächst auf Grundlage einer Clusteranalyse die Koalitionszugehörigkeit auf Grundlage der empirisch erhobenen Akteurspositionen ermittelt wird. Die Cluster-Analyse dient zu insgesamt drei Zwecken: (1) Zunächst erlaubt sie die Unterteilung der am Aushandlungsprozess beteiligten Akteure in Advocacy-Koalitionen; (2) Daneben erlaubt sie es, die Akteurspositionierungen zu den zentralen Konflikten bei der Aushandlung der DSGVO detailliert nachzuvollziehen; (3) Schließlich trägt die Cluster-Analyse zur Beantwortung der Frage bei, welche Akteurspositionen dem finalen Inhalt der DSGVO (bzw. den als Anknüpfungspunkt gewählten Dokumenten)[267] am ehesten entsprechen.[268] Im Anschluss werden für jede Koalition deren konkrete Zusammensetzung und Kooperationsstrukturen, Überzeugungssysteme sowie die ihnen zur Verfügung stehenden Ressourcen herausgearbeitet. Im prozessanalytischen

267 1. Phase: Datenschutz-Gesamtkonzept der EU-Kommission, 2. Phase: DSGVO-Entwurf der EU-Kommission, 3. Phase: Finaler DSGVO-Kompromiss.

268 Der dritte Schritt entspricht zugleich der Durchführung des Hoop-Tests im Sinne des Process-Tracing.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Teil wird schließlich aufgezeigt, wie die entsprechenden Koalitionen Einfluss auf den Aushandlungsprozess der DSGVO nehmen konnten. Dabei wird für jede Phase einzeln untersucht, welche Akteurspositionen sich mit dem Politik-Ergebnis der jeweiligen Phase am meisten überschneiden und ob und inwiefern eine inhaltliche Übereinstimmung auf das Akteurshandeln zurückgeführt werden kann. Dadurch verfolge ich das Ziel, die inhaltliche Entwicklung der Datenschutzreform im Detail nachzuvollziehen und in jeder der drei Phasen bestimmen zu können, welche Akteure in welcher Hinsicht am stärksten Einfluss auf das jeweilige Politik-Ergebnis nehmen konnten.[269]

Eine zusammenfassende Beantwortung beider Forschungsfragen erfolgt schließlich im Unterabschnitt 4.4.

4.1 Orientierungsphase (2009–2010)

Im Vorfeld der Veröffentlichung des Kommissionsentwurfs zur Datenschutz-Grundverordnung führte die Kommission erstmals einen zweistufigen öffentlichen Konsultationsprozess im Bereich der Datenschutzpolitik durch. Den Beginn der ersten Konsultationsphase markierte – noch zehn Monate vor der Veröffentlichung des Aktionsplans der Kommission zur Umsetzung des Stockholmer Programms – die Veranstaltung einer von der Kommission durchgeführten Konferenz am 19. und 20. Mai 2009 (European Commission 2009c).[270] Auf diese Konferenz folgte eine öffentliche Konsultation, in dessen Rahmen Bürgerinnen und Bürgern, Organisationen aus Wirtschaft und Zivilgesellschaft sowie öffentlichen Einrichtungen die Gelegenheit geboten wurde, sich zwischen dem 9. Juli 2009 und dem 31. Dezember 2009 zu den *neuen Herausforderungen, denen sich der Schutz*

269 Sofern in der Prozessanalyse auf Akteurspositionen Bezug genommen wird, die bereits in der Akteursanalyse dargestellt wurden, wird sowohl aus Gründen der besseren Lesbarkeit als auch aus Platzgründen in der Regel auf die weitere Angabe der Quellen verzichtet. Die Angabe der Quelle erfolgt hingegen immer bei Positionen, die nicht in der Akteursanalyse besprochen wurden. Teilweise, insbesondere bei eher strittigen Debatten, erfolgt ein Verweis auf die entsprechende Stelle in der Akteursanalyse oder auf weiterführende Quellen.

270 An der Konferenz mit dem Titel „Personal data – more use, more protection?" nahmen vor allem Vertreter der nationalen Datenschutzaufsichtsbehörden, Wissenschaftler, Wirtschaftsvertreter und Vertreter der Zivilgesellschaft teil. Zu den weiteren beteiligten Akteuren zählten Vertreter der Mitgliedstaaten, der EU-Organe und anderer EU-Institutionen (European Commission 2009c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

personenbezogener Daten gegenübersieht, zu äußern (European Commission 2009a). Auf diesen offenen Konsultationsschritt folgten weitere geschlossene, *gezielte* Konsultationen mit Schlüsselakteuren.[271]

Die erste Konsultationsrunde im Vorfeld der Initiierung der Datenschutzreform diente der Kommission dazu, Orientierungswissen darüber zu erlangen, *welchen Herausforderungen sich der Schutz personenbezogener Daten in der EU gegenübersieht*, *ob der geltende EU-Datenschutz-Rechtsrahmen diesen Herausforderungen genügt* und falls nein, *welche zusätzlichen Schritte seitens der Kommission notwendig zur Erreichung dieses Ziels wären* (European Commission 2009b, 2009a, 2010d).

Die Ergebnisse der ersten Konsultationsrunde wurden schließlich am 04. November 2010 veröffentlicht. Am selben Tag veröffentlichte die Kommission auch eine Mitteilung, mit der die zweite Konsultationsrunde (und damit auch die Entwurfsphase) initiiert wurde (vgl. 4.2). In der Mitteilung legte die Kommission zudem ihr *Gesamtkonzept für den Datenschutz in der Europäischen Union* vor, mit der sie die „Reform der EU-Vorschriften für den Schutz personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU unter besonderer Berücksichtigung der Herausforderungen der Globalisierung und der neuen Technologien dar, damit auch weiterhin ein hohes Schutzniveau für den Einzelnen bei der Verarbeitung personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU gewährleistet ist“ (EK 2010) ankündigte.

Während der Konsultation hielt sich die Kommission mit eigenen inhaltlichen Äußerungen noch sehr zurück. Im Rahmen der Ankündigung der Datenschutz-Konferenz hatte die Kommission die *Globalisierung*, den *technologischen Wandel*, den *Umgang privater als auch öffentlicher Stellen*

271 So etwa mit der Art. 29-Datenschutzgruppe im Juni 2009 (Article 29 WP 2009) oder mit Akteuren aus der Wirtschaft im Juni und Juli 2010 (European Commission 2010d). An letzterer partizipierten insgesamt 95 Schlüsselakteure (sog. *key stakeholder*), die überwiegend die datenverarbeitende Wirtschaft repräsentierten. Als Vertreter der Zivilgesellschaft waren lediglich EDRi und BEUC geladen (European Commission 2010a). Den Teilnehmenden dieses exklusiven Treffens wurde zudem die Möglichkeit geboten, weitere Stellungnahmen einzureichen (European Commission 2010b). Weder die Liste der Teilnehmer dieses Treffens, noch die eingereichten Stellungnahmen oder die Ergebnisse des Treffens wurden von der Kommission veröffentlicht. Die Kommissionswebseite informierte lediglich über das Ziel und den exklusiven Charakter des Treffens sowie über die Fragen, die auf dem Treffen erörtert wurden (European Commission 2011a). Ich erhielt Zugang zur Teilnehmerliste und der Zusammenfassung der Ergebnisse des Treffens auf Grundlage einer Informationsfreiheitsanfrage. Zu den eingereichten Stellungnahmen der *key stakeholder* erhielt ich allerdings keinen Zugang.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mit personenbezogenen Daten sowie *grenzüberschreitende Übertragungen personenbezogener Daten angesichts von Cloud-Computing* als die zentralen Herausforderungen benannt (European Commission 2009b). In der sehr knappen Aufforderung zur Partizipation am ersten offenen Konsultationsprozess stellte die Kommission den Teilnehmenden drei Fragen: Was deren Ansichten zu den neuen Herausforderungen des Datenschutzes – insb. neuer Technologien und der Globalisierung – sind; ob der Datenschutzrahmen diesen Herausforderungen genügt; und welche zukünftigen Aktivitäten erforderlich wären, um die identifizierten Herausforderungen bewältigen zu können (European Commission 2009a).

4.1.1 Akteursanalyse

In der Orientierungsphase standen sich noch keine Advocacy-Koalitionen, sondern zwei Advocacy-Communities gegenüber: Die Community der Datenschutzbefürworter und die Community der Flexibilitätsbefürworter. Im Folgenden stelle ich zunächst die zur Identifikation der entsprechenden Communities genutzte Cluster-Analyse vor und gehe anschließend dazu über, beginnend mit der Datenschutzbefürworter-Koalition, die Zusammensetzung, die Überzeugungssysteme und die Ressourcen beider Akteursgruppen vorzustellen.

4.1.1.1 Cluster-Analyse

Im Folgenden diskutiere ich das zum Clustering der Akteure gewählte Vorgehen. Anders als die Cluster-Analyse-Abschnitte der Entwurfs- und Konfliktphase beinhaltet dieser Abschnitt allerdings eine ausführlichere Darlegung methodischer Erwägungen, die bei den Cluster-Analysen für alle drei Phasen handlungsanleitend waren.

4.1.1.1.1 Grundlegende methodische Erwägungen zur Cluster-Analyse

Zu Beginn einer Cluster-Analyse gilt es zunächst, jene Charakteristiken bzw. Items (z. B. Variablen) auszuwählen, die im Laufe der Cluster-Analyse dazu verwendet werden, die Untersuchungsgegenstände in voneinander getrennte Cluster einzuordnen. Wie bereits in Unterabschnitt 2.3 diskutiert, folgte ich hierbei einer deduktiv-induktiven Vorgehensweise. Ein Teil der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Items leitete sich deduktiv unmittelbar aus der Literatur ab. Diese bestehende Item-Liste wurde zudem im Anschluss induktiv um weitere Items aus dem empirischen Material erweitert. Dadurch umfasste die Item-Liste am Ende insgesamt 101 Items. Im nächsten Schritt galt es, diese Item-Liste auf eine sinnvolle und handhabbare Menge zu kondensieren. Eine Cluster-Analyse auf Grundlage aller Items kam nicht infrage, da sie dazu neigt, die Ergebnisse zu verzerren, weil irrelevante oder weniger relevante Items nicht aus der Analyse ausgeschlossen werden (Bortz und Schuster 2010, 454). Deshalb folgte ich der Empfehlung, eine theoretische Vorauswahl der Items zu treffen, von denen eine besonders große Aussagekraft im Hinblick auf die Forschungsfrage angenommen wird. Zudem legte ich bei allen Cluster-Analysen darauf Wert, dass nach Möglichkeit dem Clustering jene Items mit dem geringsten Anteil an fehlenden Werten zugrunde gelegt wurden. Schließlich berücksichtigte ich auch, dass die ausgewählten Items nicht zu stark miteinander korrelieren, da dies die Clusterbildung erschweren, bzw. die Ergebnisse verfälschen kann (Garritzmann 2016, 79 f.).

Aus diesem Grund verwende ich für das Clustering der Akteure der Orientierungsphase insgesamt 20 Items (vgl. Tabelle 4-1 für eine Auflistung der verwendeten Items).[272] Obwohl ich bereits jene Items mit dem geringsten Anteil an fehlenden Werten verwendete, beinhaltete selbst in der finalen Version des Datensatzes immer noch ein Großteil der Items einen hohen Anteil fehlender Werte (>50%). Dies stellte ein Problem dar, da Cluster-Algorithmen in der Regel einen vollständigen Datensatz für das Clustering benötigen. Im Folgenden diskutiere ich mehrere Vorschläge zur Lösung des Problems fehlender Werte und begründe, weshalb ich mich für die Vorgehensweise in Form einer K-Means-Analyse in Kombination mit einer Teil-Imputation entschieden habe.[273]

Die erste übliche Methode sieht den Verzicht auf alle Items vor, die fehlende Werte beinhalten. Da beinahe alle Items, die der vorliegenden Untersuchung zugrunde liegen, unvollständig sind, konnte diese Vorgehensweise nicht infrage kommen. Die zweite und beliebteste Methode zum Umgang mit fehlenden Werten besteht in der sog. Imputation, dem Vervollständigen der fehlenden Werte auf Basis unterschiedlicher Verfahren. Eine beliebte

272 Vgl. auch die Missing Value Analysis für alle 27 infrage kommenden Items in Tabelle Anhang 2 im Anhang.

273 Ich danke den vielen Kolleginnen und Kollegen (insb. Elias Kyewski, Lavinia Zinser, Peter Neuhäusler, Stephanie Daimer), die mir bei der Lösung dieses Problems in zahlreichen Gesprächen behilflich waren.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Imputationsmethode ist die Schlussfolgerung eines fehlenden Werts auf Grundlage der vorhandenen Werte.[274] Da diese Vorgehensweise also letztlich Aussagen an die Stelle von nicht getätigten Aussagen setzt, die aus den getätigten Äußerungen geschlussfolgert wurden, kommt auch sie nicht infrage. Schließlich ist mein Ziel an dieser Stelle nicht die Vervollständigung des Datensatzes, sondern die akkurate Repräsentation der im politischen Feld getätigten Akteursaussagen. Zudem offenbart die Äußerung bzw. Nicht-Äußerung eines Akteurs dessen politische Prioritäten (vgl. die Analyse der Überzeugungssysteme).[275] Eine Imputation würde derartige Priorisierungen also unsichtbar machen. Zum anderen würde diese Form der Imputation auch der Mehrdimensionalität von Akteurspositionen nicht gerecht werden: Natürlich ist davon auszugehen, dass ein Akteur, der kritisch gegenüber dem Recht auf Vergessen und anderen Betroffenenrechten eingestellt ist, mit hoher Wahrscheinlichkeit auch kritisch gegenüber dem Recht auf Datenportabilität oder dem Verbandsklagerecht eingestellt sein wird. Nichtsdestotrotz wäre es schlicht falsch, dies in jedem Fall zu unterstellen und die Akteure entsprechend eindimensional zu etikettieren.

Eine weitere Imputationsmethode wurde von Stephanie Daimer verwendet, kam jedoch für meine Zwecke letztlich auch nicht infrage. Im Zusammenhang mit Arbeitsdokumenten des Ministerrats, die den Stand von Ratsdebatten abbilden, interpretierte Daimer das Schweigen von Akteuren als Zustimmung zum Kommissionsentwurf, da die entsprechenden Ratsdokumente in den Fußnoten lediglich die Konflikte abbilden, sofern keine Einwände benannt sind, also sinnvollerweise angenommen werden kann, dass Zustimmung herrscht (Daimer 2008, 48). Gegen diese Vorgehensweise sprachen zwei Gründe. Erstens kann diese Methode in Abhängigkeit davon, wie konfliktbeladen oder friedlich ein zu untersuchender Konflikt ist, dazu führen, dass die Mehrzahl der diskutierten Punkte (also Items) mit gleichen Werten codiert wird. Damit würde die Zahl der miteinander korrelierenden Items steigen, sodass die Ergebnisse der Cluster-Analyse verzerrt würden. Zweitens kann sich dieses Vorgehen nur für Kontexte eignen, in denen Schweigen auch tatsächlich als Zustimmung anerkannt ist. Beim Aushandlungsprozess zur DSGVO kann m. W. n. nicht von einer derartigen sozialen

274 Übertragen auf die hier vorliegenden Daten und vereinfacht beschrieben, würde dies bedeuten: Wenn die einem Akteur zugeordneten Variablen meines Datensatzes immer mit einer 5 codiert wurden, würden die fehlenden Werte also mit dem Wert 5 vervollständigt werden.

275 Insofern handelt es sich bei den fehlenden Werten dieser Arbeit um *missing completely at random* (MCAR) (Little und Rubin 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Regel die Rede sein. Mitgliedstaaten können auch deshalb zu einem Thema schweigen, weil sie (noch) keine Meinung dazu haben.

Letztlich entschied ich mich dazu, auf den *K-Means-Algorithmus* mit einer Kombination aus vollständigen und fehlenden Werten zurückzugreifen. Damit eine K-Means-Analyse durchgeführt werden kann, ist es notwendig, dass der Datensatz zu mindestens einem Item vollständige Werte enthält. Damit diese Bedingung erfüllt wird, führte ich eine Teil-Imputation von zwei Items durch. Bei der Auswahl der zwei Items galt es zudem zwei Faktoren zu berücksichtigen.

Erstens muss das zu vervollständigende Item tatsächlich in authentischem Maße die Varianz aller Werte (bzw. die Varianz der inhaltlichen Standpunkte) abbilden und darf, in anderen Worten, zu keinen korrelationsbasierten Verzerrungen führen. Denn der K-Means-Algorithmus ist eine nicht-hierarchische Cluster-Methode, die, vereinfacht gesagt, die „sukzessive Zusammenfassung der einander ähnlichsten Beobachtungseinheiten" (Wiedenbeck und Züll 2010, 532 ff.) in Cluster durchführt. Das Problem des K-Means-Algorithmus im Hinblick auf fehlende Werte besteht allerdings darin, dass die Cluster-Mittelpunkte ausschließlich auf Basis der vollständig vorhandenen Items berechnet werden. Insofern kann K-Means also nur dann gültige Ergebnisse produzieren, falls die vollständigen Items bereits in hinreichendem Maße die Varianz der unvollständigen Items abbilden (Bock 2017). Die anderen Cluster-Analyse-Varianten kamen nicht infrage, da sie im Falle fehlender Werte keine Ergebnisse produzieren (Wiedenbeck und Züll 2010).

Zweitens muss sich das zu vervollständigende Item auch dazu eignen, in glaubwürdigem Maße vervollständigt werden zu können. In anderen Worten muss das Item dafür geeignet sein, dass die Positionen aller Akteure in authentischer Weise von dem vervollständigten Item abgedeckt werden. Beispielsweise würde es sich nicht eignen, für eine Teil-Imputation auf ein Randthema wie die Haltung zur Definition des Verantwortlichen zurückzugreifen, da bei einem solchen Thema nicht mit Sicherheit davon ausgegangen werden kann, dass jeder Akteur eine Haltung dazu hat.

Die zwei Items, die für die Teil-Imputation genutzt wurden, sind die zwei wichtigsten Policy-Kernüberzeugungen „Grad an erwünschter staatlicher oder privater Aktivität" und „grundlegende Policy-Orientierung im Falle staatlicher Intervention". Wie in Abschnitt 3 gezeigt wurde, stand im Zentrum aller datenschutzpolitischen Konflikte der vergangenen Jahrzehnte die Frage, ob und inwiefern eine staatliche Regulierung zum Schutz personenbezogener Daten erfolgen sollte. Die gewählten Items bzw. Policy-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kernüberzeugungen bilden beide Dimensionen dieser Debatte ab, wodurch sowohl die erste Bedingung (Varianz) erfüllt wird, da sich die Positionen aller Akteure in den Items abbilden lassen, als auch die zweite Bedingung. Denn viele Statements der untersuchten Akteure – ob zum Thema Betroffenenrechte, DSFA oder Aufsichtsbehörden – enthalten zugleich Aussagen darüber, ob eine Regulierung prinzipiell gewünscht wird oder nicht. Die Teil-Imputation erfolgte manuell auf Basis der erneuten Durchsicht der Statements aller Akteure, bei denen bei beiden Items noch kein Wert enthalten war.

Die letzte Bedingung, die für eine valide Cluster-Analyse erfüllt sein muss, sieht schließlich vor, dass die Skalen der verwendeten Items vergleichbar sein müssen. Da alle in den folgenden Cluster-Analysen verwendeten Items intervallskaliert sind und immer die jeweiligen Endpunkte der entsprechenden Debatten abbilden, ist eine Vergleichbarkeit der Items gegeben (Bortz und Schuster 2010, 12 ff.).[276]

Item	N	Mean	Std. Deviation	Missing	
				Count	Percent
B1 Einschätzung des techn. Wandels	44	2,98	1,303	15	25,4
B2 Grad an erwünschter staatlicher oder privater Aktivität	59	2,85	1,387	0	0
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	59	2,66	1,372	0	0
B8 Einschätzung der Globalisierung	29	2,86	1,356	30	50,8
B12 Überarbeitung des bestehenden Datenschutzrahmens	45	2,96	1,429	14	23,7
C1C Definition personenbezogener Daten	27	2,89	1,281	32	54,2
C3D Bedingungen für die Einwilligung	25	3,24	1,234	34	57,6
C5A Transparenz	27	3,59	1,248	32	54,2
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	21	3,52	1,03	38	64,4
C5L Benachrichtigung bei Datenschutzverletzung	23	3,57	1,08	36	61
C6B Privacy by Design	22	3,86	1,207	37	62,7

276 In jeder Debatte (also bei jedem Item und pro Phase) wurde die Position, die die größtmögliche Einschränkung einer Datenschutzmaßnahme forderte, mit einer 1 codiert, während die Forderung nach einer größtmöglichen Stärkung mit einer 5 codiert wurde. Dadurch, dass die konkrete Codierung stets in Relation zu allen anderen Werten erfolgte, ist somit über alle Werte hinweg eine Vergleichbarkeit gegeben,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	N	Mean	Std. Deviation	Missing Count	Missing Percent
C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten	28	2,71	1,049	31	52,5
C6N Rechenschaftspflicht	45	2,64	1,246	14	23,7
C7 Übermittlung in Drittstaaten	36	2,36	1,125	23	39
C10D Bedeutung von Technologieneutralität	35	2,06	1,282	24	40,7
C13A Verhaltensregeln	20	2,8	1,152	39	66,1
C13B Zertifizierungen/Gütesiegel	18	3,17	1,465	41	69,5
C13C Bestellung eines organisationsinternen Datenschutzbeauftragten	19	3,26	1,147	40	67,8
C17D Verbands-/Sammelklagerecht	17	3,65	1,412	42	71,2
C17E Sanktionen und Geldbußen	18	3,89	1,231	41	69,5
Durchschnitt der fehlenden Werte					47,7

Tabelle 4-1: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS)

4.1.1.1.2 Ergebnisse der Cluster-Analyse

Wie bereits dargestellt, bauen alle folgenden Analysen auf dem K-Means-Algorithmus auf, und die oben benannten zwei Policy-Kernüberzeugungen bilden die zwei Items, auf deren Grundlage die Cluster-Mittelpunkte berechnet werden. Nichtsdestotrotz macht es einen Unterschied, welche weiteren Items in die Analyse einbezogen werden. Daher führte ich eine große Anzahl von Clusteranalysen mit verschiedenen Item-Kombinationen durch. Zunächst verwendete ich die vollständigen Items. Anschließend fügte ich schrittweise mehr Items hinzu bis ich alle Items durchgetestet hatte und mich auf die o. g. 20 Items festlegte.

Ein Problem, mit dem alle Clusteranalysen konfrontiert sind, ist die Bestimmung der Cluster-Anzahl. Dieses Problem besteht bei Clusteranalysen auf Basis des K-Means-Algorithmus noch in verstärkter Weise, da der Wissenschaftler die Menge der zu identifizierenden Cluster bei diesem Algorithmus selbst vorgeben muss, während hierarchische Clusteranalysen, auf Basis beispielsweise des Ward-Algorithmus, die mögliche Cluster-Anzahl eigenständig bestimmen (Wiedenbeck und Züll 2010, 530).

Die Anzahl der Cluster, auf die in einer K-Means-Analyse letztendlich zurückgegriffen wird, bestimmt sich einerseits aus der Anzahl der Beobach-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tungsgruppen, die dem Forschenden selbst bekannt sind und andererseits aus der Ungewissheit, dass neben den bekannten Gruppen, auch weitere, unbekannte Gruppen existieren könnten. Aufgrund dieser Unsicherheit bietet es sich daher an, die Analyse mit verschiedenen Cluster-Größen durchzuführen und die unterschiedlichen Ergebnisse auf ihre Sinnhaftigkeit hin zu überprüfen (Rupp 2013).

Im Falle der Clusteranalyse für die erste Phase kamen zwei bis drei Cluster infrage. Den theoretischen Ausgangspunkt für die Analyse bilden die in der Kontextanalyse identifizierten Communities der Datenschutzbefürworter bzw. Flexibilitätsbefürworter. Da ich ausschließlich Items in Bezug auf das allgemeine Datenschutzrecht codiert habe und die Datenbasis somit keine sicherheitspolitischen Items enthält, war nicht davon auszugehen, dass die Koalition der Sicherheitsbefürworter in den von mir im Hinblick auf die DSGVO untersuchten Debatten eine Rolle spielen würde. Dennoch hielt ich es für angebracht, die Daten sowohl im Hinblick auf die Existenz von zwei als auch drei Koalitionen hin zu untersuchen. Im Folgenden möchte ich zunächst für die erste Phase die Möglichkeiten des Rückgriffs auf eine Cluster-Größe von zwei bzw. drei Clustern diskutieren.

2-Cluster-Modell

Das 2-Cluster-Modell auf Grundlage aller in Tabelle 4-1 genannten Items ergibt eine Community der Datenschutzbefürworter und eine Community der Flexibilitätsbefürworter. Die Zuteilung der Akteure zu beiden Clustern bzw. Communities kann Tabelle 4-2 entnommen werden und zeigt 37 Akteure auf Seiten der Flexibilitätsbefürworter und 15 Akteure auf Seiten der Datenschutzbefürworter. Die Zuordnung der Akteure deckt sich zudem mit den Advocacy-Communities, die am Ende des vergangenen Abschnitts auf Basis der Sekundärliteraturanalyse identifiziert worden waren.

Flexibilitätsbefürworter	Datenschutzbefürworter
ACCIS	Art. 29-Datenschutzgruppe
ACT	BEUC
AmCham EU	Breyer, Patrick
BDIU	CDT
BITKOM	Christopher Kuner
BSA	DouweKorff
BT	DSAB-DE-Land
DDV	DSAB GBR - ICO

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Flexibilitätsbefürworter	Datenschutzbefürworter
DEU-Regierung	EDRi
DIGITALEUROPE	Europ. DSBeauftragte
eBay	GDD
EBF	NLD-Regierung
ECTA	Paul de Hert
EMOTA	PI
EPA	VZBV
EPC	
ETNO	
Eurofinas	
EuroISPA	
FAEP	
FBF	
FEDMA	
GBR-Regierung	
GDV	
Google	
GSMA	
IAB Europe	
ICC	
Intel	
Liberty Global	
Microsoft	
TechAmerica (formerly AeA)	
UEAPME	
VDZ	
WFA	
Yahoo	
ZAW	

Tabelle 4-2: K-Means-Clusteranalyse mit 2 Koalitionen (berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Betrachtung der inhaltlichen Positionen der Akteure, auf deren Basis die Cluster erstellt wurden, ist mittels der Analyse der finalen Cluster-Zentren möglich. Tabelle 4-3 zeigt für jede der verwendeten 20 Items das finale Cluster-Zentrum. Auch die Zuordnung der Cluster-Zentren entspricht den vorherigen Ergebnissen der Cluster-Zuordnung.

Item	Cluster	
	1	2
B1 Einschätzung des techn. Wandels	2	5
B2 Grad an erwünschter staatlicher oder privater Aktivität	2	5
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	2	4
B8 Einschätzung der Globalisierung	2	5
B12 Überarbeitung des bestehenden Datenschutzrahmens	2	5
C1C Definition personenbezogener Daten	2	4
C3D Bedingungen für die Einwilligung	2	5
C5A Transparenz	2	4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4
C5L Benachrichtigung bei Datenschutzverletzung	2	4
C6B Privacy by Design	2	5
C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten	2	4
C6N Rechenschaftspflicht	2	4
C7 Übermittlung in Drittstaaten	2	4
C10D Bedeutung von Technologieneutralität	1	4
C13A Verhaltensregeln	2	4
C13B Zertifizierungen/Gütesiegel	2	4
C13C Bestellung eines organisationsinternen Datenschutzbeauftragten	2	4
C17D Verbands-/Sammelklagerecht	2	4
C17E Sanktionen und Geldbußen	2	5

Tabelle 4-3: Finale Cluster-Zentren der K-Means-Clusteranalyse mit 2 Koalitionen (berechnet mit SPSS)

3-Cluster-Modell

Das 3-Cluster-Modell beinhaltet ebenfalls alle in Tabelle 4-1 genannten Items und teilt einige der Akteure einem neuen, dritten Cluster zu (vgl. Tabelle 4-4). Die Koalition der Flexibilitätsbefürworter umfasst am Ende noch 36 Akteure, während die Koalition der Datenschutzbefürworter von 15 Akteuren auf 11 schrumpft. Die neue, dritte Koalition fasst 5 Akteure.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1 **Flexibilitätsbefürworter**	**Cluster 2** **Datenschutzbefürworter**	**Cluster 3**
ACCIS	Christopher Kuner	CDT
ACT	Paul de Hert	DEU-Regierung
AmCham EU	Art. 29-Datenschutzgruppe	DSAB GBR - ICO
BDIU	BEUC	GDD
BITKOM	DSAB-DE-Land	NLD-Regierung
BSA	EDRi	
BT	Breyer, Patrick	
DDV	PI	
DIGITALEUROPE	VZBV	
eBay	DouweKorff	
EBF	Europ. DSBeauftragte	
ECTA		
EMOTA		
EPA		
EPC		
ETNO		
Eurofinas		
EuroISPA		
FAEP		
FBF		
FEDMA		
GBR-Regierung		
GDV		
Google		
GSMA		
IAB Europe		
ICC		
Intel		
Liberty Global		
Microsoft		
TechAmerica (formerly AeA)		

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1 Flexibilitätsbefürworter	Cluster 2 Datenschutzbefürworter	Cluster 3
UEAPME		
VDZ		
WFA		
Yahoo		
ZAW		

Tabelle 4-4: K-Means-Clusteranalyse mit 3 Koalitionen (berechnet mit SPSS)

Die Betrachtung der Distanzen der Cluster-Zentren in Tabelle 4-5 veranschaulicht, dass die größte Distanz zwischen den Clustern 1 und 2 vorzufinden ist. Das neue, dritte Cluster weist eine geringere Distanz zu den ersten beiden Clustern auf und steht mit 3,977 dem Cluster 2 besonders nahe. Tabelle 4-6, der die Cluster-Zentren aller Items im Detail zu entnehmen sind, veranschaulicht, welche Items der jeweiligen Cluster wie nah zueinander sind. Eine Überlappung der Zentren von Cluster 2 und Cluster 3 ist bei den folgenden Items anzutreffen: *C5L Benachrichtigung bei Datenschutzverletzung*, *C5L Benachrichtigung bei Datenschutzverletzung*, *C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten*, *C6N Rechenschaftspflicht*, *C13B Zertifizierungen/Gütesiegel*, *C17E Sanktionen und Geldbußen* (vgl. auch die grau unterlegten Items in Tabelle 4-6). Doch auch bei den übrigen Items ist eine große Nähe zwischen den Clustern 2 und 3 anzutreffen. Nur im Falle des Items *B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen* beträgt die Differenz mehr als einen Wert. Die übrigen Werte unterscheiden sich nur dahingehend, ob eine extreme (codiert mit 5) oder normale (codiert mit 4) Befürwortung vorliegt.

Cluster	1	2	3
1		10,875	7,583
2	10,875		3,977
3	7,583	3,977	

Tabelle 4-5: Distanzen der finalen Cluster-Zentren (berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster		
	1	2	3
B1 Einschätzung des techn. Wandels	2	5	4
B2 Grad an erwünschter staatlicher oder privater Aktivität	2	5	4
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	2	5	3
B8 Einschätzung der Globalisierung	2	5	4
B12 Überarbeitung des bestehenden Datenschutzrahmens	2	5	4
C1C Definition personenbezogener Daten	2	5	4
C3D Bedingungen für die Einwilligung	2	5	4
C5A Transparenz	2	5	4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4	4
C5L Benachrichtigung bei Datenschutzverletzung	2	4	4
C6B Privacy by Design	2	5	4
C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten	2	4	4
C6N Rechenschaftspflicht	2	4	4
C7 Übermittlung in Drittstaaten	2	4	3
C10D Bedeutung von Technologieneutralität	1	4	3
C13A Verhaltensregeln	2	4	3
C13B Zertifizierungen/Gütesiegel	2	4	4
C13C Bestellung eines organisationsinternen Datenschutzbeauftragten	2	4	3
C17D Verbands-/Sammelklagerecht	2	5	4
C17E Sanktionen und Geldbußen	2	5	5

Tabelle 4-6: Finale Cluster-Zentren der K-Means-Clusteranalyse mit 3 Koalitionen (berechnet mit SPSS)

Somit ergibt das 3-Cluster-Modell ein mögliches, drittes Cluster, das bei näherer Betrachtung allerdings sehr viele Überschneidungen mit dem zweiten Cluster aufweist. Der Rückgriff auf das 3-Cluster-Modell hätte, trotz aller Schwachpunkte, den Vorteil, dass die zwar geringen, aber doch sichtbaren Differenzen zwischen den Clustern 2 und 3 Berücksichtigung finden würden. Dagegen spricht, dass die inhaltlichen Übereinstimmungen mit dem dritten Cluster dermaßen groß sind, dass die Einstufung als eigenes Cluster aus inhaltlichen Gründen nur wenig sinnvoll erscheint. Dies wäre hingegen beispielsweise besonders dann gerechtfertigt, wenn die Zentren des zweiten Clusters mehrheitlich bei einer 3 liegen würden, sodass – unter Hinzuziehung weiterer Informationen aus dem Policy-Prozess – davon ausgegangen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

werden könnte, dass sich diese Koalition aus neutralen, vermittlungsorientierten Akteuren zusammensetzt.

Trotz der Gefahr, dass potentiell relevante Differenzen zwischen den Akteuren des Clusters 2 und des Clusters 3 verwischt werden, entschied ich mich letztlich dazu, auf das 2-Cluster-Modell zurückzugreifen. Die Akteure aus dem 3-Cluster-Modell behandelte ich dabei unter Rückgriff auf Weible, Sabatier und McQueen (2009, 130) als *randständige Mitglieder* der Advocacy-Community der Datenschutzbefürworter. Sowohl die Flexibilitätsbefürworter als auch die Datenschutzbefürworter bezeichnete ich in diesem Schritt noch nicht als Koalition, da zu diesem frühen Stadium der Datenschutzreform noch keine nicht-trivialen Kooperationsstrukturen zwischen den Akteuren bestanden, die eine Aggregation zu einer Advocacy-Koalition rechtfertigen würden.[277]

Die Zuverlässigkeit der verschiedenen Clusteranalysen habe ich durchgängig mittels einer Varianzanalyse, der sogenannten ANOVA, getestet und optimiert. Alle Items, die keine signifikante Varianz (>0,60) aufwiesen, wurden nach und nach aus dem Sample entfernt, bis nur noch signifikante Items (<0,02) übrigblieben (vgl. Tabelle 4-7). Der F-Wert in der ANOVA-Tabelle zeigt an, welche der verwendeten Items am stärksten zur Identifizierung der Cluster beigetragen haben. Demnach trugen, wie zu erwarten war, die beiden vollständig vorliegenden Items B2 (208,953) und B3 (165,790) am stärksten zur Identifikation der jeweiligen Cluster bei. Daneben waren aber auch die Items C6N (183,791), C1C (141,667) sowie C3D (123,665) entscheidend für die Cluster-Erstellung.

Item	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
B1 Einschätzung des techn. Wandels	47,092	1	0,616	42	76,408	0,000
B2 Grad an erwünschter staatlicher oder privater Aktivität	87,703	1	0,420	57	208,953	0,000
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	81,277	1	0,490	57	165,790	0,000
B8 Einschätzung der Globalisierung	40,948	1	0,389	27	105,296	0,000
B12 Überarbeitung des bestehenden Datenschutzrahmens	64,112	1	0,600	43	106,854	0,000

277 Natürlich bestanden zwischen einzelnen Akteuren (wie z. B. zwischen PI und EDRi) nicht-triviale Kooperationsstrukturen, doch war der Anteil dieser Akteure dermaßen gering, dass mir die Aggregation aller Akteure unter einer Advocacy-Community als der beste Weg schien.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
C1C Definition personenbezogener Daten	36,267	1	0,256	25	141,667	0,000
C3D Bedingungen für die Einwilligung	30,827	1	0,249	23	123,665	0,000
C5A Transparenz	28,036	1	0,499	25	56,148	0,000
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	14,766	1	0,341	19	43,347	0,000
C5L Benachrichtigung bei Datenschutzverletzung	17,377	1	0,394	21	44,099	0,000
C6B Privacy by Design	23,758	1	0,342	20	69,534	0,000
C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten	15,001	1	0,566	26	26,508	0,000
C6N Rechenschaftspflicht	55,359	1	0,301	43	183,791	0,000
C7 Übermittlung in Drittstaaten	25,760	1	0,545	34	47,227	0,000
C10D Bedeutung von Technologieneutralität	42,526	1	0,405	33	105,041	0,000
C13A Verhaltensregeln	15,408	1	0,544	18	28,325	0,000
C13B Zertifizierungen/Gütesiegel	28,900	1	0,475	16	60,842	0,000
C13C Bestellung eines organisationsinternen Datenschutzbeauftragten	14,784	1	0,524	17	28,240	0,000
C17D Verbands-/Sammelklagerecht	24,113	1	0,518	15	46,555	0,000
C17E Sanktionen und Geldbußen	19,747	1	0,377	16	52,390	0,000

Tabelle 4-7: ANOVA-Ergebnisse für das 2-Cluster-Modell (berechnet mit SPSS)

4.1.1.1.3 Zwischenfazit zur Cluster-Analyse

Somit können auf Basis der Ergebnisse der Clusteranalyse für die erste Phase zwei Advocacy-Communities unterschieden werden: Eine Advocacy-Community, die sich überwiegend aus Akteuren aus der Privatwirtschaft sowie einigen Regierungen von EU-Mitgliedstaaten zusammensetzt und die sich eher für flexible Datenschutzmaßnahmen einsetzt sowie eine zweite Advocacy-Community, die sich aus Datenschutzbehörden, zivilgesellschaftlichen Datenschützern, Wissenschaftlern und wenigen mitgliedstaatlichen Regierungen zusammensetzt und die sich für die deutliche Stärkung von Datenschutzmaßnahmen einsetzt. Die Ergebnisse der empirischen Clusteranalyse der Orientierungsphase des Aushandlungsprozesses der DSGVO bestätigen somit die Feststellungen vorheriger Studien (Fritz 2013; A. L. Newman 2008b; Scheffel 2016) und der Kontextanalyse, in denen diese

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

grundsätzlichen Koalitionen im Bereich der Datenschutzpolitik auf Basis qualitativer Methoden für die Ebene der EU, Deutschlands und Großbritanniens identifiziert worden waren. Aus Gründen der Präzision bezeichne ich die in die jeweiligen Cluster eingruppierten Akteure allerdings noch nicht als Koalition, da ich in der ersten Phase aufgrund der geringen Politisierung der Thematik zunächst nur die inhaltliche Überschneidung der Akteurspositionen zugrunde lege und nicht auch Kooperationsstrukturen herausstelle.

4.1.1.2 Datenschutzbefürworter-Community:

Die Datenschutzbefürworter-Community vereinigt alle Akteure, die für den Ausbau von gesetzlichen, verpflichtenden Regelungen zum Schutz personenbezogener Daten eintreten.

4.1.1.2.1 Zusammensetzung der Datenschutzbefürworter-Community während der Orientierungsphase

Die Zusammensetzung der Community der Datenschutzbefürworter veränderte sich zu Beginn des Datenschutzreformprozesses gegenüber der im Rahmen der Kontextanalyse erfolgten Analyse nur unwesentlich. Neben den Datenschutzaufsichtsbehörden, die sich sowohl einzeln, als auch in Gestalt der Art. 29-Datenschutzgruppe sowie der Konferenz der europäischen Datenschutzbeauftragten am Konsultationsprozess beteiligten, sprachen sich das Europäische Parlament, BEUC, EDRi und PI für ein hohes Datenschutzniveau aus. Daneben trat erstmals auch die deutsche Verbraucherschutzorganisation *Verbraucherzentrale Bundesverband* VZBV auf Ebene der EU-Politik für die Stärkung des Datenschutzes ein.

Da gerade in der ersten Konsultationsphase der Einholung externer und wissenschaftlicher Expertise eine große Bedeutung zukam, können auch die Wissenschaftler Douwe Korff, Paul De Hert und Christopher Kuner als Teil der Community der Datenschutzbefürworter betrachtet werden. Douwe Korff, inzwischen emeritierter Professor für Internationales Recht an der London Metropolitan University, ist der am längsten im EU-Datenschutz-Subsystem aktive Wissenschaftler. Seit Ende der 1990er-Jahre verfasste er Studien für die Europäische Kommission zu zentralen Fragen wie der Implementation der DS-RL (Korff 2002) oder zum Um-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gang mit den neuen Herausforderungen, denen sich der Datenschutz gegenübersah (Korff und Brown 2010). Er fungierte überdies regelmäßig als Sachverständiger bei Kommissionsanhörungen. Paul de Hert ist Experte u. a. für internationales Menschen-, Datenschutz- und Strafrecht und als Professor an der Freien Universität Brüssel tätig. Er wirkte als Studienautor und Berater sowohl für die Europäische Kommission als auch für das Europäische Parlament. Daneben ist De Hert Leiter der jährlich in Brüssel stattfindenden internationalen Datenschutz-Konferenz CPDP, auf der Vertreter aus Wissenschaft, Politik und Wirtschaft in einen Dialog zu überwiegend die EU-Ebene betreffenden Datenschutzfragen treten.[278] Christopher Kuner ist ebenfalls Rechtsprofessor an der Freien Universität Brüssel. In seiner Karriere als Wirtschaftsberater, u. a. für die ICC, trat er für die Institutionalisierung von Datenschutz-Maßnahmen ein und war in diesem Zusammenhang insbesondere für die Aushandlung zweier von der Europäischen Kommission angenommener Standardvertragsklauseln verantwortlich. Zudem wirkte Kuner an der 2007 von der Art. 29-Datenschutzgruppe verabschiedeten Standardmerkliste für Verantwortliche zur Konformitätsüberprüfung unternehmensinterner Vorschriften mit.[279] Im Rahmen des Aushandlungsprozesses der DSGVO steuerte Kuner Stellungnahmen im Rahmen der Konsultationsrunden bei und wurde zudem von der Kommission angehört.

Patrick Breyer, der im Vorfeld der Datenschutz-Grundverordnung durch bürgerrechtspolitische Aktivitäten – insbesondere im Rahmen des AK Vorrat – gegen Überwachungsmaßnahmen bekannt geworden war, ist ebenfalls Teil dieser Advocacy-Community.

Die im Zuge des 3 Cluster-Modells identifizierten und im Rahmen des 2 Cluster-Modells der Datenschutzbefürworter-Community hinzugefügten Akteure Center for Democracy and Technology CDT, die britische Datenschutzbehörde Information Commissioner's Office (ICO), die Gesellschaft für Datenschutz und Datensicherheit (GDD) sowie die deutsche und niederländische Regierung betrachte ich als randständige Mitglieder der Advocacy-Community, da sich die Überzeugungen dieser Akteure nur in

278 http://www.privacysalon.org/board https://www.vub.be/FRC/events/frc-researchers-paul-de-hert-barbara-huylebroek-contribute-to-european-parliament-study-on-effective-access-to-justice.shtml https://lsts.research.vub.be/en/paul-de-hert/ https://www.researchgate.net/profile/Paul_Hert

279 https://www.wsgr.com/WSGR/DBIndex.aspx?SectionName=attorneys/BIOS/l2684.htm https://be.linkedin.com/in/christopher-kuner-888500

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mancher Hinsicht überschneiden, in anderer Hinsicht jedoch relevante Abweichungen festzustellen sind.

Community der Datenschutzbefürworter	
Akteur	**Akteursgruppe**
Christopher Kuner	Wissenschaft
Paul de Hert	Wissenschaft
Art. 29-Datenschutzgruppe	Datenschutzbehörden
BEUC	Verbraucherschutz
DSAB-DE-Land	Datenschutzbehörden
EDRi	Zivilgesellschaft
Patrick Breyer	Zivilgesellschaft
PI	Zivilgesellschaft
VZBV	Verbraucherschutz
DouweKorff	Wissenschaft
Europ. DSBeauftragte	Datenschutzbehörden
Randständige Mitglieder	
CDT	Zivilgesellschaft
DEU-Regierung	Mitgliedstaaten
DSAB GBR - ICO	Datenschutzbehörden
GDD	Zivilgesellschaft
NLD-Regierung	Mitgliedstaaten

Tabelle 4-8: Die Advocacy-Community der Datenschutzbefürworter

4.1.1.2.2 Überzeugungssystem der Datenschutzbefürworter-Community während der Orientierungsphase

Die Darstellung des Überzeugungssystems folgt zwei Schritten. Im ersten Schritt folgt ein Überblick der Überzeugungen der Advocacy-Community der Datenschutzbefürworter. Dieser Überblick basiert auf den im vorangegangenen Abschnitt durchgeführten Berechnungen der Cluster-Zentren für jede Variable. Der Blick auf Tabelle 4-9 zeigt, dass die Community insgesamt für eine Stärkung des Datenschutzrahmens bei allen angesprochenen Themen eingetreten ist. Tabelle 4-10 wiederum zeigt im zweiten Schritt die Positionierung eines jeden Akteurs der Community im Hinblick auf alle während der Orientierungsphase relevanten Themen bzw.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutzmaßnahmen. Tabelle 4-10 enthält daher mehr – an der Zahl 30 – Themen bzw. Items, als der Cluster-Analyse aufgrund des Missing Value-Problems und der Varianzanalyse zugrunde gelegt worden war. Die Darstellung der Sekundärüberzeugungen folgt dann auch der in Tabelle 4-10 dargestellten Übersicht. Als zentrales Kriterium zur Diskussion der Sekundärüberzeugungen ziehe ich den Politisierungsgrad heran, den ich anhand der Häufigkeit der Nennung eines Themas bestimme. So ist davon auszugehen, dass Akteure in ihren Stellungnahmen, aufgrund dessen, dass sie stets unter dem Problem begrenzter Ressourcen leiden, vor allem jene Themen diskutieren bzw. Vorschläge unterbreiten, denen sie eine hohe Priorität einräumen (Weishaar, Collin, und Amos 2016, 126). Insofern kann ein Thema grundsätzlich dann als besonders wichtig betrachtet werden, wenn alle oder der Großteil der beteiligten Akteure dieses Thema diskutiert, während ein Thema als eher unwichtig betrachtet werden kann, wenn nur ein Akteur oder wenige Akteure dieses ansprechen. Allerdings gibt es auch Ausnahmen, wie die folgenden Unterabschnitte (bspw. im Hinblick auf das Recht auf Datenübertragbarkeit) zeigen werden.[280]

Policy-Kernüberzeugungen

Zwei wichtige Policy-Kernüberzeugungen der Datenschutzbefürworter bestehen darin, dass die Globalisierung und der technologische Wandel als Herausforderungen für den Datenschutz betrachtet werden. Aus diesem Bedrohungsszenario leitet sich dann auch die zentrale Policy-Kernüberzeugung der Community ab: Weil der Schutz personenbezogener Daten als Grundrecht angesehen und weil der bestehende Schutz angesichts von Globalisierung und technologischem Wandel als bedroht bzw. unzureichend bewertet wird, fordern die Community-Mitglieder staatliche Regulierungsmaßnahmen, um der attestierten Bedrohung angemessen begegnen zu können. Die Lösung der Datenschutzprobleme seitens des Marktes kommt für die Akteure hingegen überhaupt nicht infrage. Schließlich setzt die Datenschutzbefürworter-Community im Falle einer staatlichen Regulierung eher

280 Zudem sagt der Politisierungsgrad nur wenig über die reale Bedeutung der Themen aus. Ein viel diskutiertes Thema kann für die Praxis wenig relevant sein, während ein von den Stakeholdern unbeachtetes Thema eine größere Tragweite haben kann. So wurde das Thema der Definition des Verantwortlichen zwar im Aushandlungsprozess stellenweise thematisiert, doch erst einige Jahre später stellte sich beispielsweise heraus, dass die in der DSGVO verwendete Definition große Schwierigkeiten für die Umsetzung von Blockchain-Anwendungen mit sich bringt (Finck u. a. 2019, 37 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auf *harte* Regulierungsinstrumente (wie Verordnungen, Richtlinien, usw.) statt auf *weiche* Regulierungsalternativen (bspw. Kommissionsempfehlungen und sonstige, auf Selbstregulierung basierende Maßnahmen). Letztere werden jedoch nicht vollständig abgelehnt, sondern als weniger prioritär eingestuft.

5 Techn. Wandel birgt vor allem Herausforderungen, die eingehegt werden müssen
5 Für ausschließliche staatliche Aktivität
4 Umfassende Regulierung (hard regulation), die aber auch Raum für Selbstregulierung lässt
5 Globalisierung birgt vor allem Herausforderungen, die eingehegt werden müssen
4 Für die Reform des Datenschutzrahmens
5 Für eine starke Ausweitung der Definition
5 Für eine deutliche Stärkung der Einwilligung
4 Für eine Stärkung der gesetzlichen Transparenz-Vorschriften
4 Für eine Verbesserung des Auskunftsrechts d. Betroffenen bzw. der Informationspflicht d. Verantwortlichen
4 Für die Benachrichtigung im Falle einer Datenschutzverletzung
5 Für die Einführung einer verbindlichen Privacy by Design-Vorschrift für alle Betreiber und Hersteller
4 Für die Beibehaltung der Meldepflicht, bzw. umfangreicher Dokumentationspflichten des Verarbeiters
4 Für die Einführung einer verbindlichen Rechenschaftspflicht
4 Für die konsequentere Durchsetzung des Datenschutzes bei Drittstaatentransfers
4 Für die Anpassung des Rechts an technologische Entwicklung unter Wahrung der Technologieneutralität
4 Für die Ausarbeitung von Verhaltensregeln auf Basis eines relativ verbindlichen Verfahrens
4 Für Zertifizierungen auf Basis eines relativ verbindlichen Verfahrens
4 Für die Einführung der Pflicht zur Bestellung eines Datenschutzbeauftragten
4 Für die Einführung eines Verbands- bzw. Sammelklagerechts
5 Für die deutliche Ausweitung der Regelungen zu Sanktionen und Geldbußen

Tabelle 4-9: Überblick der Überzeugungen der Datenschutzbefürworter-Community (eigene Erhebung bzw. Berechnung mit SPSS)

Sekundärüberzeugungen

Gemäß der Häufigkeit ihrer jeweiligen Erwähnung, können die folgenden Sekundärüberzeugungen als zentral bestimmt werden. Insbesondere die Stärkung der gesetzlichen Vorschriften zur Gewährleistung von Transparenz wurde von fast allen (13 von 16) beteiligten Akteuren gefordert. Die Forderung nach Transparenz wurde damit begründet, dass neue Technologien die Verarbeitung personenbezogener Daten unsichtbar machten bzw. die Auswirkungen der jeweiligen Verarbeitungen den Betroffenen nicht

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

offengelegt würden. Im Kontext der Forderungen nach Transparenz wurde zudem auch Wert auf eine einfache Sprache bei der Information der Betroffenen gelegt, weil Datenschutzerklärungen in der Regel so kompliziert formuliert seien, dass nur Fachleute diese verstehen würden (vgl. BEUC 2009, 4 f. VZBV 2009, 6). Ebenfalls im Zusammenhang mit Transparenz wurde von 12 Akteuren die Ausweitung des Anwendungsbereichs der bereits im Rahmen der Verabschiedung der Cookie-Richtlinie für Telekommunikationsdienste beschlossenen Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten auf alle Bereiche des allgemeinen Datenschutzrechts gefordert. Unter Verweis auf regelmäßige Pressemeldungen über neue Datenpannen wurde diese Forderung damit begründet, dass die Betroffenen auf Grundlage der Meldung in die Lage versetzt würden, Gegenmaßnahmen (beispielsweise die Änderung ihrer Passwörter) zu ergreifen, bevor eine Datenpanne zu größeren Problemen wie einem Identitätsdiebstahl führt (vgl. BEUC 2009, 16 f. EDRi und BoF 2009, 4).[281] 11 Akteure forderten die Einführung verpflichtender Privacy by Design-Regelungen, damit potentielle Datenschutz-Probleme künftig bereits in der Technologieentwicklungsphase seitens der Technologiehersteller als auch –Anwender berücksichtigt werden (Article 29 WP und WPPJ 2009, 13, Nr. 46). Daneben forderten 8 Akteure die Einführung einer verpflichtenden Privacy by Default-Regelung. Grundsätzlich argumentierten die Datenschutzbefürworter, dass technische Schutzmöglichkeiten in Form von Privacy by Design und Default-Vorgaben zu einer Verbesserung der Nutzerkontrolle führen würden, indem sie die Betroffenen in die Lage versetzten, selbstständig das gewünschte Öffentlichkeitslevel eines Dienstes einstellen zu können (Article 29 WP und WPPJ 2009, 13; BEUC 2009, 9). In diesen Zusammenhang wurde (10 Nennungen) auch die generelle Ausweitung der Verarbeiterpflichten im Hinblick auf die Gewährleistung der Datensicherheit gefordert (ebd.). Für riskante Verarbeitungen personenbezogener Daten wurde (9 Nennungen) gleichzeitig die Einführung einer gesetzlichen Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gefordert (Article 29 WP und WPPJ 2009, 20; BEUC 2009, 13).[282]

281 Einige der Akteure forderten zudem die Ausweitung der Haftungs- und Schadensersatzregelungen auch auf Fälle einer moralischen Schädigung. Dieser Debattenstrang konnte allerdings keine nennenswerte Resonanz im politischen Aushandlungsprozess generieren und soll daher nicht weiter beachtet werden.

282 Seitens EDRi, PI sowie der Konferenz der Europ. Datenschutzbeauftragten wurde zudem gefordert, dass eine DSFA auch immer dann durchgeführt werden sollte, wenn staatliche Überwachungsmaßnahmen vorgeschlagen werden (EDRi und BoF

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Damit die für die Verarbeitung Verantwortlichen diesen neu auferlegten Pflichten auch tatsächlich nachkommen müssen, wurde (9 Nennungen) zudem die Einführung einer sog. Rechenschaftspflicht gefordert (Article 29 WP und WPPJ 2009, 20). Als ein wichtiges Element zur gewissenhaften Einhaltung der Datenschutzbestimmungen forderten 6 Akteure, darunter insb. die Art. 29-Datenschutzgruppe zudem die Einführung einer EU-weiten Pflicht zur Bestellung eines Datenschutzbeauftragten bei datenverarbeitenden Unternehmen (Article 29 WP und WPPJ 2009, 19; BEUC 2009, 13). Damit Verarbeiter künftig bei Nichtbefolgung datenschutzrechtlicher Bestimmungen nicht mehr mit kleineren Geldbußen davonkommen können wurde zudem die deutliche Ausweitung der Regelungen zu Sanktionen und Geldbußen auf ein abschreckendes Niveau gefordert (10 Nennungen) (Article 29 WP und WPPJ 2009, 22; BEUC 2009, 14; EDRi und BoF 2009, 5). Im Zusammenhang mit der Gewährleistung der Einhaltung der Datenschutzbestimmungen wurde insbesondere die EU-weite, vollständige Harmonisierung des Datenschutzrechts gefordert (9 Nennungen), damit sich Verarbeiter nicht mehr in Staaten mit einem niedrigen Datenschutzniveau niederlassen können und zugleich die Gefahr implementierungsbedingter Divergenzen möglichst reduziert wird. Im Hinblick auf die Themen Verhaltensregeln und Zertifizierungen begrüßten einige Akteure (3 bzw. 6) zwar die Ausweitung der Richtlinienbestimmungen, allerdings nur im Rahmen eines verbindlichen Verfahrens (Korff und Brown 2010, 63 ff.).

Deutlich seltener äußerten sich die Akteure zu Themen, die die Betroffenen unmittelbar betreffen: Während die Einführung eines Verbands- bzw. Sammelklagerechts noch von 9 Akteuren gefordert wurde, traten nur 5 Akteure für die Stärkung der Bestimmungen zur Einwilligung ein. Die Forderung nach der Einführung eines Verbands- bzw. Sammelklagerechts folgte beispielsweise bei BEUC der Auffassung, dass die Verantwortung zur Gewährleistung eines effektiven Datenschutzes nicht allen auf die Schultern der Individuen gelegt werden sollte: Da die Betroffenen selbst aus verschiedenen Gründen meist nicht vor Gericht zögen, sei es erforderlich die Möglichkeit einer Verbands- bzw. Sammelklage EU-weit zu gewährleisten (BEUC 2009, 14 f. Korff und Brown 2010, 55). Der Forderung nach der Stärkung der Einwilligung lag hingegen die Kritik an den Richtlinienbestimmungen zugrunde. So waren die Bestimmungen der DS-RL von der anfänglich seitens der Kommission vorgeschlagenen konkreten und aus-

2009, 5; PI 2009, 7). Diese Forderung wurde im weiteren Verlauf der DSGVO-Verhandlungen jedoch nicht mehr weiter debattiert.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

drücklichen Einwilligung in eine sog. *Einwilligung ohne jeden Zweifel* (*unabiguous consent*) abgeschwächt worden. Auf deren Grundlage verzichteten einige Verarbeiter auf die Einholung der Einwilligung, wenn sie der Ansicht waren, dass davon ausgegangen werden kann, dass der Betroffene mit einer bestimmten Handlung (z. B. dem Aufrufen einer Webseite oder der Nutzung eines Dienstes) seine Einwilligung signalisiert. Daneben wurde von 6 Akteuren auch die Stärkung des Auskunftsrechts bzw. der Informationspflicht der Verarbeiter gefordert, damit die Betroffenen auf zuverlässige Weise Auskunft darüber erhalten können, welche ihrer Daten zu welchen Zwecken, von welchem Anbieter verarbeitet werden (EDRi und BoF 2009, 3 f.). Schließlich wurde von 5 Akteuren auch die Einführung eines Rechts auf Vergessenwerden gefordert, damit personenbezogene Informationen, die nachteilig für Betroffene sein könnten, nicht mehr ohne Ablaufdatum online verfügbar sein sollten (BEUC 2009, 19 f.). Nur 3 Akteure forderten die Einschränkungen von Profiling-Maßnahmen. Kritik wurde dabei insbesondere an unsichtbarem Profiling und Scoring geübt, das ohne die Information der Betroffenen bzw. ohne deren Einwilligung durchgeführt werde (VZBV 2009, 4 f.). Das Recht auf Datenübertragbarkeit wurde lediglich von BEUC genannt. Als Grund gab BEUC den „lock-in"-Effekt einiger Webseiten und sozialer Netzwerke an, die den Anbieterwechsel erschweren bzw. verunmöglichen würden. Daher müsse es den Betroffenen rechtlich ermöglicht werden, ihre Kommunikation, Fotos, E-Mails und Videos frei und unter Gewährleistung der Interoperabilität zwischen Diensten hin- und her bewegen zu können (BEUC 2009, 20).

Schließlich nannten 4 Akteure im Kontext mit der Harmonisierung des Datenschutzrahmens auch die Verbesserung der Bestimmungen zum anwendbaren Recht. An den bestehenden Bestimmungen wurde bemängelt, dass diese einerseits zu Unklarheiten bei mehreren Niederlassungen eines Verarbeiters führten und dass andererseits jene Verarbeiter nicht in den Anwendungsbereich der Richtlinie fielen, die zwar personenbezogene Daten von EU-Bürgern verarbeiten, aber nicht in der EU ansässig sind und zur Verarbeitung auch nicht auf Mittel zurückgreifen, die in der EU belegen sind (Article 29 WP und WPPJ 2009, 9 f.). Zudem nahmen einige Akteure (5) Bezug auf die, einige Jahre vor der Datenschutzreform geführten Debatten rund um die Definition des Begriffs der personenbezogenen Daten. Unter direkter und auch indirekter Bezugnahme auf die einschlägige Stellungnahme der Art. 29-Datenschutzgruppe traten sie für eine weite Definition ein, die sowohl IP-Adressen miteinschließt als auch Spielraum dafür lässt, neue Datentypen als personenbezogenes Datum zu identifizieren, sofern

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

dies aufgrund technologischer Entwicklungen erforderlich wird (vgl. z. B. EDRi und BoF 2009, 4).

Name	KOM	Kuner	EDSB	EDRi	De Hert	Art. 29-Datenschutzgruppe	BEUC	DSAB-DE-Land	EDRi	Breyer	PI	VZBV	Korff	Konf. europ. DSB	CDT	DEU-Regierung	ICO	GDD	NLD-Regierung	Häufigkeit d. Nennung
B1 Techn. Wandel	5		4			5	5	5	5		5	5	4	5		3	4			11
B2 Staatl./Private Aktivität	5	5	4	5	5	5	5	5	5	5	4	5	4	5	3	3	4	3	4	18
B3 Policy-Orientierung	4	4	4	5	5	5	5	5	5	5	4	5	4	5	3	3	2	3	3	18
B6 Harmonisierung	5	5				5	4	5	4		5		5	4			4			9
B8 Globalisierung	4		5			5	5	5			5	5	4				4			8
B12 Reformwunsch	5					5	4	4	5		4	5	5	5	3	3	4		4	12
C 1 B Räuml. Anwendungsbereich	4					4	5	4					4							4
C 1 C Definition personenb. Daten	4						5		5	4	4						4			5
C 3 D Einwilligung	4					5	5	5		4					4					5
C 5 A Transparenz	4		5	4	5	5	5	5	5	4		5		4	5		5		4	13
C 5 C Auskunftsrecht/Inf.-Pflicht	4				5				5	4				4			5		4	6
C 5 E Recht auf Vergessenwerden	4						5		5	5	5								4	5
C 5 G Recht auf Datenübertragb.	4						5													1
C 5 I Automat. Verarb./Profiling					5							5		4						3
C 5 L Meldung v. Verletzungen	4		4	4		4	5	4	5	4	5	4	4					4	4	12
C 6 A Privacy by Default	4				5	5	5	4	5	5			5				4			8
C 6 B Privacy by Design	4				5	5	5	5	5	5			5	5			4	4	4	11
C 6 C Meldepflicht/VA-Verzeichnis	4		4			4		4									5		3	5
C 6 H Datensicherheit					5	5	5	5	5	5			4	4	5		5			10
C 6 N Rechenschaftspflicht	4		4			5	5	5			4			4	5		5		4	9
C 7 Drittstaatentransfers	3					4		4					4				4	2	2	6
C 10 D Technologieneutralität	4					5	4	5				2						3		5
C 13 A Verhaltensregeln	3					5		5					5							3
C 13 B Zertifizierungen/Gütesiegel	4			4	5	5		5			4		5							6
C 13 C Bestellung eines DSB	4	4		4		5		5										4	3	6
C 13 D DSFA	4					5	5	5	5		5		5	4			5		4	9

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	KOM	Kuner	EDSB	EDRi	De Hert	Art. 29-Datenschutzgruppe	BEUC	DSAB-DE-Land	EDRi	Breyer	PI	VZBV	Korff	Konf. europ. DSB	CDT	DEU-Regierung	ICO	GDD	NLD-Regierung	Häufigkeit d. Nennung
C 15 B Datenschutzbehörden	4		5	4	5	5	5	5	5		5	5							4	10
C 16 C Art. 29-Datenschutzgruppe	3					5	5						4							3
C 17 D Verbands-/Sammelklagen	4			4	4		5		5	5		5	4				4		4	9
C 17 E Sanktionen & Geldbußen	4		4	4		4	5	4	5	5		5	4						4	10

Tabelle 4-10: Positionierung der Datenschutzbefürworter zu allen relevanten Themen in der Orientierungsphase (eigene Erhebung)

4.1.1.2.3 Ressourcen der Datenschutzbefürworter-Advocacy-Community während der Orientierungsphase

Die Ressourcen der Advocacy-Community der Datenschutzbefürworter blieben in der Orientierungsphase gegenüber der Vor-Reformphase im Wesentlichen unverändert (vgl. 3.5.2.1.3).

4.1.1.3 Flexibilitätsbefürworter-Community

Die Community der Flexibilitätsbefürworter vereinigt alle Akteure, die für ein möglichst geringes Maß an expliziter Datenschutzregulierung eintreten und die im Falle einer staatlichen Regulierung Selbstregulierungsmaßnahmen bevorzugen.

4.1.1.3.1 Zusammensetzung der Flexibilitätsbefürworter-Community

Die Cluster-Analyse bestätigt, dass alle privatwirtschaftlichen Akteure, die an der Orientierungsphase beteiligt waren, der Community der Flexibilitätsbefürworter zugeordnet werden können. Da vor allem eine Überlappung auf der Ebene der Überzeugungen festzustellen ist, aber bei den

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

allermeisten Akteuren[283] keine nicht-trivialen Kooperationsstrukturen vorhanden sind, bezeichne ich auch die Flexibilitätsbefürworter weiterhin als Advocacy-Community.

In dem Maße, in dem die Verarbeitung personenbezogener Daten zu einem wichtigen Teil der Geschäftsmodelle von einer zunehmenden Zahl von Unternehmen wurde, erweiterte sich auch das Spektrum der Flexibilitätsbefürworter. Waren es in den 1990er-Jahren vor allem noch Akteure aus der Werbe- und Kreditbranche, kamen mit der Verbreitung des Internets auch Akteure aus anderen Branchen hinzu. So erweiterte sich das Akteursnetz der Flexibilitätsbefürworter insbesondere um Akteure aus der IKT-Branche: Die *European Telecommunications Networks Operators Association* (ETNO) vertritt die Interessen der europäischen Netzbetreiber, zu denen beispielsweise *Telefónica*, die *British Telecom* oder die *Deutsche Telekom AG* zählen. EuroISPA ist der europäische Zusammenschluss der nationalen Verbände der Internetwirtschaft. Die Interessen der Informations- und Telekommunikationsbranche werden vom europäischen Dachverband DIGITALEUROPE bzw. dem deutschen *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien* (BITKOM) vertreten. Daneben können auch TechAmerica Europe, der die Interessen von US-Unternehmen aus der Technologiebranche vertritt sowie die Business Software Alliance (BSA), der die Interessen von US-Unternehmen aus der Softwarebranche vertritt, zum Policy-Subsystem der Europäischen Datenschutzpolitik hinzugezählt werden.[284] Neben den nationalen und europäischen (Dach-)Verbänden können aber auch einzelne Unternehmen wie Google, Intel, Microsoft, Yahoo, Nokia, British Telecom und Telefónica zu den Mitgliedern der Advocacy-Community gezählt werden. Auch die britische Regierung war Teil dieser Advocacy-Community.

283 Doch sei erwähnt, dass sich in dieser Phase auch eine offizielle Advocacy-Koalition der Werbe- und Medienindustrie formierte, die eine gemeinsame Stellungnahme einreichte und aus u. a. ACT, EPC, FEDMA, IAB Europe und WFA bestand (ACT u. a. 2009).

284 Neben den genannten Verbänden etablierten sich auch einzelne Unternehmen als fester Teil des Subsystems der EU-Datenschutzpolitik, darunter: British Telecom, Google, Intel, Microsoft, Nokia, Telefónica, Yahoo.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Community der Flexibilitätsbefürworter	
Akteur	**Akteursgruppe**
ACCIS	Privatwirtschaft
ACT	Privatwirtschaft
AmCham EU	Privatwirtschaft
BDIU	Privatwirtschaft
BITKOM	Privatwirtschaft
BSA	Privatwirtschaft
BT	Privatwirtschaft
DDV	Privatwirtschaft
DIGITALEUROPE	Privatwirtschaft
eBay	Privatwirtschaft
EBF	Privatwirtschaft
ECTA	Privatwirtschaft
EMOTA	Privatwirtschaft
EPA	Zivilgesellschaft (Astro-Turfing)
EPC	Privatwirtschaft
ETNO	Privatwirtschaft
Eurofinas	Privatwirtschaft
EuroISPA	Privatwirtschaft
FAEP	Privatwirtschaft
FBF	Privatwirtschaft
FEDMA	Privatwirtschaft
GBR-Regierung	Mitgliedstaaten
GDV	Privatwirtschaft
Google	Privatwirtschaft
GSMA	Privatwirtschaft
IAB Europe	Privatwirtschaft
ICC	Privatwirtschaft
Intel	Privatwirtschaft
Liberty Global	Privatwirtschaft
Microsoft	Privatwirtschaft
TechAmerica (formerly AeA)	Privatwirtschaft
UEAPME	Privatwirtschaft

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Community der Flexibilitätsbefürworter	
Akteur	**Akteursgruppe**
VDZ	Privatwirtschaft
WFA	Privatwirtschaft
Yahoo	Privatwirtschaft
ZAW	Privatwirtschaft

Tabelle 4-11: Zentrale Akteure der Flexibilitätsbefürworter-Community (eigene Zusammenstellung)

4.1.1.3.2 Überzeugungssystem der Advocacy-Community der Flexibilitätsbefürworter während der Orientierungsphase

Auch an dieser Stelle folgt die Diskussion des Überzeugungssystems zwei Schritten. Im ersten Schritt folgt ein Überblick der Überzeugungen der Flexibilitätsbefürworter-Advocacy-Community auf Grundlage der für jede – im Rahmen der Cluster-Analyse verwendeten – Variable berechneten Cluster-Zentren (vgl. Tabelle 4-12).

Nachdem ein Überblick der Policy-Kernüberzeugungen hergestellt wurde, widmet sich die Diskussion im zweiten Schritt der Diskussion der Sekundärüberzeugungen. Diese wird nicht anhand der berechneten Cluster-Zentren geführt, sondern anhand der in Tabelle 4-13 zusammengestellten Daten. Tabelle 4-13 kann die Positionierung eines jeden Akteurs der Flexibilitätsbefürworter-Community im Hinblick auf alle während der Orientierungsphase diskutierten, relevanten Themen bzw. Datenschutzmaßnahmen entnommen werden. Da die Benennung eines Themas als zentrales Kriterium herangezogen wird, orientiert sich die Diskussion der Sekundärüberzeugungen an der Häufigkeit, mit der bestimmte Themen seitens der Community-Akteure in ihren jeweiligen Stellungnahmen erwähnt wurden.

Policy-Kernüberzeugungen

Entgegen den Policy-Kernüberzeugungen der Datenschutzbefürworter sehen die Akteure der Flexibilitätsbefürworter-Community im technologischen Wandel und in der Globalisierung eher Chancen statt Herausforderungen. Als eine zentrale Herausforderung wird eher der EU-weit uneinheitliche Datenschutzrahmen angesehen. Insofern fordern die Flexibilitätsbefürworter insbesondere die Harmonisierung der europäischen Datenschutzgesetze. Bei diesem Wunsch nach Harmonisierung fungiert

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

allerdings der grundsätzliche Wunsch nach marktbasierten Lösungen als zentrale Policy-Kernüberzeugung. Daher lässt sich die Haltung der Flexibilitätsbefürworter folgendermaßen zusammenfassen: Staatliches Handeln soll sich auf die Herstellung eines EU-weit einheitlichen Datenschutzrahmens beschränken, indem regulatorische Hemmnisse abgebaut werden. Die Bereiche, die zum Zwecke der Herstellung eines einheitlichen Rahmens reguliert werden, sollen zudem möglichst auf weichen (Selbst-)Regulierungsinstrumenten basieren, die den Datenverarbeitern einen möglichst großen Spielraum bei der Befolgung der Vorschriften überlassen. Folglich wurden die bestehenden Regeln als ineffektiv, schwerfällig und unflexibel kritisiert (vgl. Microsoft 2009, 2).

Variable	**Code**
Technischer Wandel bringt eher Vorteile	2
Eher für private Aktivität	2
Eher für marktbasierte Lösung des Problems	2
Für mehr Raum für Selbstregulierungsmaßnahmen	2
Eher gegen die Überarbeitung des Datenschutzrahmens	2
Eher für eine enge Definition personenbezogener Daten	2
Für eher flexible Einwilligungsregeln	2
Starke Befürwortung von Transparenz bei gleichzeitiger Ablehnung von verbindlichen Vorschriften	3
Für die Beibehaltung der bestehenden, unverbindlichen Regelungen im Hinblick auf das Auskunftsrecht bzw. Informationspflichten des Verantwortlichen	3
Für flexible Benachrichtigungserfordernisse bei Datenschutzverletzungen	3
Gegen verpflichtende Privacy by Design-Vorgaben	2
Für die Abschaffung der Meldepflicht bzw. deutliche Vereinfachungen bei der Meldepflicht	2
Für eine flexibel ausgestaltete Rechenschaftspflicht	2
Für vereinfachte Drittstaatentransfers	2
Gegen jegliche technologiespezifische Regulierung bzw. für möglichst abstrakte Vorgaben	1
Für die flexible Ausarbeitung von Verhaltensregeln	2
Für die flexible Verfahren zur Erteilung von Zertifizierungen bzw. Gütesiegeln	2

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Variable	Code
Gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten	2
Gegen ein Verbands-/Sammelklagerecht, für flexible alternative Streitschlichtungsverfahren	2
Für die Beibehaltung der bestehenden, unverbindlichen Regelungen zu Sanktionen und Geldbußen	2

Tabelle 4-12: Überblick der Überzeugungen der Flexibilitätsbefürworter-Advocacy-Community (eigene Erhebung bzw. Berechnung mit SPSS)

Sekundärüberzeugungen

Die zentrale Sekundärüberzeugung, die von 33 der 40 als Flexibilitätsbefürworter identifizierten Akteure vertreten wurde, besteht in der Befürwortung einer flexiblen bzw. risikobasierten Rechenschaftspflicht. Die Debatte um die Rechenschaftspflicht war entfacht worden, nachdem der von RAND Europe im Auftrag des ICO erstellte Bericht zur Überprüfung der DS-RL Mitte 2009 veröffentlicht wurde. Viele Datenverarbeiter nahmen direkten bzw. indirekten Bezug auf dieses Dokument,[285] weshalb dessen Kernergebnisse im Folgenden kurz vorgestellt werden. Der RAND-Bericht kritisierte die DS-RL in erster Linie dafür, dass sie anstelle von erwünschten Ergebnissen auf Prozessformalitäten setze, die weder zu einem verbesserten Schutz der Betroffenen noch zu einer wirtschaftsfreundlichen Atmosphäre beitrügen. Als Beispiele für derartige Formalitäten wurden die Einholung der Einwilligung der Betroffenen, die Formulierung von Datenschutzerklärungen und die Meldepflicht genannt. Aufgrund der Komplexität von Datenschutzerklärungen verkomme die informierte Einwilligung zum Ticken einer Box. Und auch die Meldepflicht habe in einer Welt allgegenwärtiger Datenverarbeitungen ihre ursprüngliche Bedeutung (Herstellung von Transparenz) verloren. Daneben wurden auch die Bestimmungen zu Drittstaatentransfers als zu träge und kompliziert kritisiert sowie der im Datenschutzrecht vorherrschende Schutz aller als personenbezogen klassifizierter Daten unter Absehung von den aus einer Datenverarbeitung

285 Einige Akteure (GSMA Europe 2009; Microsoft 2009; UK Ministry of Justice 2010) nahmen direkten Bezug auf den RAND-Bericht. Andere Akteure (z. B. AmCham, TechAmerica, Yahoo) nutzten die von RAND entwickelte Argumentationsfolie bzw. die von RAND eingeführten Begrifflichkeiten, ohne aber auf den RAND-Bericht direkt Bezug zu nehmen, während eine Reihe weiterer Akteure (z. B. IAB) ein anderes Vokabular verwendete, aber letztlich für die im RAND-Vorschlag vorgesehene Flexibilisierung des Datenschutzrechts eintrat.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

resultierenden, tatsächlichen Privatheitsgefährdungen bemängelt (N. Robinson u. a. 2009, 26 ff.). Stattdessen schlug der RAND-Bericht unter dem Schlagwort des Rechenschaftsprinzips einen Datenschutzrahmen vor, der auf allgemeinen Prinzipien bzw. auf mittels des Datenschutzes zu erreichenden Zielen aufbaut, aber die Umsetzung der Prinzipien bzw. die Erreichung der Ziele nicht entlang der Erfüllung von Prozessformalitäten gewährleistet, sondern die Details der Umsetzung den Unternehmen überlässt. Als Eckpfeiler der Umsetzung schlug der Bericht daher eine Reihe von Instrumenten (Privacy Policies, Datenschutzerklärungen, betriebliche Datenschutzbeauftragte, Meldung einer riskanten Verarbeitung, Verhaltensregeln, unternehmensweit verbindliche Kodexe, Standards, Gütesiegel, Datenschutzfolgenabschätzungen, PETs, Meldung von Datenschutzverstößen, alternative Streitschlichtungen) vor, forderte allerdings zugleich, dass die Entscheidung über deren Verwendung allein dem Verarbeiter überlassen bleiben sollte. Diesem System solle wiederum ein sog. *risikobasierter Ansatz*[286] zugrunde liegen, der die Zielerreichung anhand dessen bestimmt, wie riskant eine Verarbeitung ist und ob ein tatsächlicher Schaden eingetreten ist (ebd., 46 ff.). Die Ressourcen der Aufsichtsbehörden sollten daher in die Richtung der Aufdeckung tatsächlicher Schadensfälle kanalisiert und zugleich die Durchsetzungsmöglichkeiten der Behörden gestärkt werden. Das von der Advocacy-Community der Flexibilitätsbefürworter vorgesehene Rechenschaftsprinzip folgte diesem von RAND Europe vorgestellten Muster. Einige der Akteure argumentierten eher in Richtung des Wechsels von einem ex ante- zu einem ex post-System, während andere den risikobasierten Ansatz oder die Rechenschaftspflicht betonten.[287] Das Gemeinsame an den Vorschlägen ist die Befürwortung eines Datenschutzrahmens, der nicht auf die Benennung klarer Pflichten abzielt, sondern lediglich zu erreichende Ziele formuliert, deren Erreichung den für die Verarbeitung Verantwortlichen überlassen wird.

Obwohl der Großteil der beteiligten Akteure die Harmonisierung des Datenschutzrechts forderte, kam für die Mehrheit eine grundlegende Re-

286 Aufgrund des Fokus' auf den tatsächlichen Schaden wird in verschiedenen Stellungnahmen statt des risikobasierten Ansatzes auch häufig die Bezeichnung harms based approach (schadensbasierter Ansatz) verwendet (vgl. bspw. AmCham EU 2010, 11 f.).

287 Yahoo beschrieb das anvisierte System folgendermaßen: „The legislative framework should aim to maximise consumer welfare by promoting an ex-post, market surveillance, and harm-focused approach to compliance and enforcement, i.e. a focus on outcomes rather than process." (Yahoo! Europe 2009, 4)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

form des Datenschutzrechts nicht infrage. Stattdessen wurde auf die Verbesserung der Implementierung verwiesen. Änderungen wurden seitens einiger Akteure nur in mancherlei Hinsicht gefordert, etwa (seitens 17 Akteuren) im Hinblick auf die Vereinheitlichung bzw. starke Reduktion der EU-weit uneinheitlich umgesetzten Meldepflicht. Ein Grund für die Ablehnung einer Reform war, dass staatliche Regelungsmaßnahmen als zu träge und unflexibel im Hinblick auf die Beachtung der realen Bedingungen angesehen wurden, denen die Datenverarbeitung unterliegt. Anstelle von trägen, staatlichen Regulierungsmaßnahmen wurde daher der Fokus auf Instrumente der Selbstregulierung gelegt. Dies betraf insbesondere die Bestimmungen zu Drittstaatentransfers, die von einem Großteil der Akteure (26) als zu umständlich kritisiert wurden. So wurde vorgeschlagen, diese nicht in erster Linie von Angemessenheitsentscheidungen abhängig zu machen, sondern stattdessen vermehrt auf unternehmensinterne Vorschriften (Binding Corporate Rules) und vergleichbare Selbstregulierungsinstrumente bzw. Ausnahmeregelungen zu setzen, mittels derer die Befolgung der Datenschutzregeln seitens eines bestimmten Verarbeiters und nicht die in einem Staat geltenden Datenschutzgesetze als Maßstab zur Bewertung der Zulässigkeit einer Verarbeitung herangezogen werden sollten. Hinsichtlich der Ausgestaltung derartiger Maßnahmen zur Erleichterung von Drittstaatentransfers forderten die Akteure zudem einen möglichst großen Spielraum für die Verarbeiter (AmCham EU 2010). Als ein Kernelement der Selbstregulierung wurde seitens einiger Akteure (13) die Vereinfachung der Erarbeitung von Verhaltensregeln seitens der Wirtschaft befürwortet. Zum Thema Zertifizierungen äußerte sich nur eine Minderheit (6 Akteure). Insgesamt wurden Zertifizierungen im Sinne begleitender Maßnahmen begrüßt, sofern ihre Ausgestaltung den Verarbeitern überlassen bliebe (BSA 2009, 8 f.).

Angesichts der von der Kommission angekündigten Überarbeitung des Datenschutzrahmens sowie der Anpassung des Rahmens an die Herausforderungen neuer Technologien vertraten die Akteure der Flexibilitätsbefürworter-Community (26) die Position, dass die Überarbeitung zu keinerlei technologiespezifischen Maßnahmen führen dürfe. Manche Akteure argumentierten, dass eine grundsätzliche Überarbeitung der Richtlinie deshalb nicht erforderlich sei, weil die Richtlinie aufgrund ihrer Technologieneutralität auch auf neue Technologien und die in diesem Zusammenhang entstehenden Herausforderungen anwendbar sei (ACT u. a. 2009, 4). Im Hinblick auf die Definition personenbezogener Daten (18) und die Bestimmungen zur Einwilligung (16) verteidigten die Akteure die flexiblen Bestim-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mungen der geltenden DS-RL, die den Verarbeitern in den meisten Fällen einen ausreichenden Raum für einen kontextspezifischen Umgang böte. Einige Akteure (9) hoben die Wichtigkeit der Transparenz von Datenverarbeitungen hervor, lehnten jedoch staatliche Transparenzvorschriften ab. Im Hinblick auf das Auskunftsrecht äußerten die Unternehmen dagegen lediglich, dass sich dieses zwar bewährt habe (BSA 2009, 2; TechAmerica Europe 2009, 3), eine Stärkung allerdings auch zu missbräuchlicher Verwendung führen könne (Intel 2009, 7).

Einige Akteure, wie die BSA, schlugen die Einführung einer Meldepflicht bei Datenschutzverstößen vor. Damit es nicht zu häufigen und irrelevanten Benachrichtigungen kommt und damit keine Benachrichtigungsermüdung – wie im Falle von Datenschutzerklärungen – eintritt, forderten diese zudem eine Beschränkung der Meldung auf relevante Fälle (IAB Europe 2010, 5). Zu anderen Themen wie Privacy by Design (4), Privacy by Default (0), Datensicherheit (2), Datenschutzfolgenabschätzung (2), Profiling (2), dem Recht auf Vergessenwerden (1), oder dem Recht auf Datenübertragbarkeit (0), Verbandsklagerecht (2) oder Sanktionen (3) äußerte sich nur ein sehr geringer Anteil der Akteure. Diese lehnten die Einführung neuer Instrumente (Privacy by Design, Verbandsklagerecht[288]) ab bzw. traten gegen eine Stärkung der bestehenden Regelungen (bei Profiling und Sanktionen) ein. Einige Akteure (9) wünschten sich zudem Verbesserungen im Bereich des anwendbaren Rechts. Insbesondere die europäischen Wirtschaftsvertreter (ACCIS IVZW 2009, 6; BITKOM 2009, 1) forderten in diesem Zusammenhang die EU-weite Angleichung der Wettbewerbsbedingungen (*level playing field*). Vertreter der Telekommunikationsbranche (ETNO 2009, 2 f. Liberty Global 2009, 4) befürworteten in diesem Zusammenhang vor allem die Ausweitung der Bestimmungen der ePrivacy-Richtlinie auf alle Verarbeitungssektoren bzw. auf alle Verarbeiter.

Ein kleiner Teil der Akteure (5) trat für die Stärkung der Befugnisse und Ressourcen der Datenschutzaufsichtsbehörden ein. Zwei Akteure (Yahoo und UEAPME) wichen allerdings deutlich von dieser Position ab und stellten die Arbeit der Behörden grundsätzlich infrage.[289] Die Mehrzahl

288 Während der GDV (2009, 10 f.) die Rechtsbehelfe der DS-RL für ausreichend hielt und jede Änderung ablehnte, schlug Eurofinas die Einführung alternativer Streitschlichtungsverfahren vor (eurofinas 2009, 9).

289 Ausgehend von einer Kritik am grundrechteorientierten Datenschutzverständnis vertrat insbesondere UEAPME die Ansicht, dass „supervisory authorities have become fundamental rights defenders which put their judgements into question. For these reasons there is a need for better separation of powers, as supervisory

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Akteure, die sich zum Thema der Datenschutzgruppe äußerten, befürworteten zwar, dass die Art. 29-Datenschutzruppe mehr Befugnisse im Hinblick auf den Erlass EU-weit gültiger Vorgaben zum Zwecke der Verbesserung der Harmonisierung erhält. Sie bemängelten den Prozess, auf dessen Grundlage die Stellungnahmen der Art. 29-Datenschutzgruppe in der Vergangenheit erarbeitet wurden aber zugleich als intransparent. Die Lösungsvorschläge der Akteure (vgl. z. B. AmCham EU 2010; IAB Europe 2010, 4; UEAPME 2009, 4) reichten dabei von dem Ruf nach mehr Beteiligung bis hin zu einer Umgestaltung der Gruppe nach Vorbild US-amerikanischer Multi-Stakeholder-Modelle, wie sie beispielsweise bei der FTC oder dem US Department of Commerce praktiziert werden (Gellman und Dixon 2016; Tene und Hughes 2014). IAB Europe forderte auch, dass die Art. 29-Datenschutzgruppe Folgenabschätzungen ihrer Stellungnahmen durchführen sollte (IAB Europe 2010, 4).

authorities should not act as EU policy makers and they should limit themselves to law enforcement concerning the national implementation of the Directive 95/46/EC." (UEAPME 2009, 4)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	KOM	DS-RL	Google	ACCIS	ACT	EPC	FEDMA	IAB Europe	WFA	AmCham EU	BDIU	BITKOM	BSA	BT	DDV	DIGITALEUROPE	eBay	EBF	ECTA	EMOTA	FAEP	EPA	EPC	ETNO	Eurofinas	EuroISPA	FBF	FEDMA	GBR Regierung	GSMA	GDV	IAB Europe	ICC	Intel	Liberty Global	Microsoft	TechAmerica	UEAPME	VDZ	Yahoo	ZAW	Häufigkeit d. Nennung
B1 Techn. Wandel	4		3	4	2	2	2	2	2	2	2	3	2	1	1	2			2	2		2	2	3	2	4	2	2	3	1	2		3	4	4		2	2	1	3	4	34
B2 Staatl./Private Aktivität	5	4	2	2	2	2	2	2	2	1	1	2	2	2	1	2	2	1	2	2	2	2	2	2	2	4	2	2	2	1	2	1	2	2	3	1	2	2	2	2	1	39
B3 Policy-Orientierung	4	2	2	2	2	2	2	2	2	1	1	2	2	1	1	2	2	1	2	2	2	2	2	2	2	4	2	2	2	2	2	1	2	2	2	1	2	2	2	2	1	39
B6 Harmonisierung	5			4	4	4	4	4	4		4	5	5	5		4			4	5			5	5	4	4	5	5	4		4	5	5	5	4	5	4	4		4	29
B8 Globalisierung	4			4	2	2	2	2	2	2		3	2	1		2							2				2	2		1			2									20
B12 Reformwunsch	5		4	2	2	2	2	2	2	2			3		1	2	2	1	2	1	2		1	2	1		2	2		3	2	3	2	2	1	2				1	4	30
C 1 B Räuml. Anwendungsbereich	4	3	2							2		4							2				3	4						4	2	2										9
C 1 C Definition personenb. Daten	4	3		2	2	2	2	2	2	1	1											2	2					2		2	2				2						18
C 3 D Einwilligung	4	3							2	2					2						3		2				2			2			3		2						16
C 5 A Transparenz	3	3	2								1		3			2					2	4	2				3						2		3						9
C 5 C Auskunftsrecht/Inf.-Pflicht	4	3		2									2												2							3		3		2			3		7
C 5 E Recht auf Vergessenwerden	4	2																									2														1
C 5 G Recht auf Datenübertragb.	5	1																																							0
C 5 I Automat. Verarb./Profiling		3																					1		1																2
C 5 L Meldung v. Verletzungen	4	1											2									3													3	3					6
C 6 A Privacy by Default	4	2																																							0
C 6 B Privacy by Design	4	2								2																						3		2							4
C 6 C Meldepflicht/VA-Verzeichnis	4	5								1		2	2	2		2			2	3		2	2		3							2	2			2	2				17
C 6 H Datensicherheit		3																				4													3						2

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	KOM	DS-RL	Google	ACCIS	ACT	EPC	FEDMA	IAB Europe	WFA	AmCham EU	BDIU	BITKOM	BSA	BT	DDV	DIGITALEUROPE	eBay	EBF	ECTA	EMOTA	FAEP	EPA	EPC	ETNO	Eurofinas	EuroISPA	FBF	FEDMA	GBR Regierung	GDV	GSMA	IAB Europe	ICC	Intel	Liberty Global	Microsoft	TechAmerica	UEAPME	VDZ	Yahoo	ZAW	Häufigkeit d. Nennung
C 6 N Rechenschaftspflicht	4	2	2	2	2	2	2	2	2	1	1		2		2	1		2	2	2	2		2	2		2	2	2	2	2	2	2	2	2		2	2	2	2	1	2	33
C 7 Drittstaatentransfers	4	3			2	2	2	2	2	2		2	2	2		1	3		2	1		2	2	2		1	2	2		2		2	1	1		1	1			1		26
C 10 D Technologieneutralität	4	2			1	1	1	1	1	1			1		1	1	1		1	1	1		1			2	3	1			2	1		2	2	1	1		1	1	2	26
C 13 A Verhaltensregeln	3	3			2	2	2	2	2									2		2			2	2				2		2		2					2					13
C 13 B Zertifizierungen/Gütesiegel	3	1																					1	2							2	2					2	2				6
C 13 C Bestellung eines DSB	4	2								2		4				2						2								3			2	2								7
C 13 D DSFA	4	1																				4							4													2
C 15 B Datenschutzbehörden	4	3											4									4						4			4		4					1		2		7
C 16 C Art. 29-Datenschutzgruppe		2								2					1	1				2	1					1	2	2				2	2		4			1		1	1	14
C 17 D Verbands-/Sammelklagen	4	1																							1					1												2
C 17 E Sanktionen & Geldbußen	4	1																		2	2	3																				3

Tabelle 4-13: Positionierung der Flexibilitätsbefürworter zu allen relevanten Themen in der Orientierungsphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

4.1.1.3.3 Ressourcen der Flexibilitätsbefürworter-Community während der Orientierungsphase

Auch die Ressourcen der Advocacy-Community der Flexibilitätsbefürworter blieb gegenüber der Vor-Reformphase stabil (vgl. 3.5.2.2.3).

4.1.2 Prozessanalyse: Der Pfad zum Datenschutz-Gesamtkonzept der Kommission

Die Orientierungsphase, die ihren Anfang mit der Konferenz am 19. und 20. Mai 2009 genommen hatte, gelangte mit der Veröffentlichung der Konsultationsergebnisse am 4. November 2010 an ihr Ende.[290] Im Zentrum der Ergebnisse stand das *Gesamtkonzept für den Datenschutz in der Europäischen Union*, mit dem die Kommission ihre Vision für den neuen Datenschutzrahmen der EU präsentierte und in dem sie die Veröffentlichung eines Legislativvorschlags im Jahr 2011 ankündigte (EK 2010, 21).[291]

Das Gesamtkonzept unterteilt sich in zwei Abschnitte. Ausgehend von einer kurzen Analyse der neuen Herausforderungen für den Datenschutz im ersten Abschnitt, unterbreitete die Kommission im zweiten Abschnitt eine Reihe von Vorschlägen. Entgegen den Äußerungen und Empfehlungen der Advocacy-Community der Flexibilitätsbefürworter identifizierte die Kommission als die zwei zentralen Herausforderungen des Datenschutzes die fortschreitende technologische Entwicklung und die Globalisierung. Unter Verweis auf gesteigerte Möglichkeiten zur Preisgabe personenbezogener Daten, beispielsweise mittels sozialer Online-Netzwerke, auf neue *raffinierte* Verfahren zur Erfassung und Verarbeitung personenbezogener Daten

290 Die im Rahmen der öffentlichen Konsultationsrunde eingegangenen Stellungnahmen machte die Kommission auf ihrer Webseite öffentlich zugänglich und fasste die Positionen der verschiedenen Stakeholder im Rahmen eines Dokuments zusammen. Die Kommission hatte insgesamt 168 Rückmeldungen auf ihre Aufforderung zur Teilnahme erhalten. 29 Antworten kamen von Bürgerinnen und Bürgern, 127 von Organisationen (vor allem europäische bzw. internationale Wirtschaftsvertreter sowie einige wenige Vertreter der Zivilgesellschaft) und 12 weitere Antworten seitens öffentlicher Einrichtungen (EU Commission 2010).

291 Zuvor hatte die Kommission (2010, 12) angekündigt, den neuen umfassenden Datenschutz-Rechtsrahmen im Jahre 2010 vorzustellen. Ihren Verordnungsvorschlag veröffentlichte die Kommission jedoch schließlich erst im Januar 2012. Laut Jančiūtė (2018, 225 f.) war das Ende des Kommissionsmandats 2009 und der Übergang in eine neue Kommission entscheidend für die Verzögerungen auf Seiten der Kommission.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

und die Entgrenzung der Verarbeitung im Rahmen des Cloud-Computing, stellte die Kommission die Notwendigkeit der *Beherrschung der Auswirkungen neuer Technologien* fest (EK 2010, 2–5). Entgegen den Wünschen der Flexibilitätsbefürworter identifizierte die Kommission im Gesamtkonzept nicht die seitens der Wirtschaftsvertreter beklagten Schwierigkeiten bei der Verarbeitung personenbezogener Daten als die zentrale Herausforderung, sondern die Gewährleistung eines hohen Schutzniveaus: „In der vorliegenden Mitteilung legt die Kommission ihr Konzept für eine Reform der EU-Vorschriften für den Schutz personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU unter besonderer Berücksichtigung der Herausforderungen der Globalisierung und der neuen Technologien dar, damit auch weiterhin ein *hohes Schutzniveau* für den Einzelnen bei der Verarbeitung personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU gewährleistet ist." (ebd., 5, Hervorhebung im Original)

Auf der Ebene der Policy-Kernüberzeugungen ist somit eine weitgehende Übereinstimmung zwischen den Vorstellungen der Datenschutzbefürworter-Community und den Vorschlägen der Kommission festzustellen (siehe auch die Gegenüberstellung der Positionen in Tabelle 4-14).

Auch die Gegenüberstellung der übrigen, im Gesamtkonzept vorgeschlagenen Maßnahmen und der Positionen beider Advocacy-Communities zeigt, dass im Hinblick auf die große Mehrzahl der Themen eine Überlappung der Kommissionsvorschläge mit den Positionen der Datenschutzbefürworter zu finden ist (vgl. Tabelle 4-14). Die Maßnahmenvorschläge bzw. Hauptziele des Gesamtkonzepts unterteilte die Kommission dabei in fünf Teile: (1) *Die Stärkung der Rechte des Einzelnen*; (2) d*ie Stärkung der Binnenmarktdimension*; (3) *die Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit von Polizei- und Justizbehörden*; (4) *die Gewährleistung eines hohen Schutzniveaus bei außerhalb der EU übermittelten Daten*; sowie (5) *die wirksamere Durchsetzung der Vorschriften*. Im Bereich der Betroffenenrechte kündigte die Kommission neue Verpflichtungen für die Verarbeiter an, etwa Details im Hinblick auf die Art der zur Verfügung zu stellenden Information und die Modalitäten der Bereitstellung dieser Informationen im Kontext der Verbesserung der Transparenz (ebd., 6 f.). Ebenfalls im Kontext der Transparenz kündigte die Kommission die Einführung einer allgemeinen Meldepflicht bei Datenschutzverstößen an. Dabei nahm die Kommission Bezug auf ihre eigene Absichtserklärung, die sie im Rahmen der Plenardebatte zur Cookie-Richtlinie gegenüber dem Parlament abgegeben hatte (ebd., 7, vgl. auch 3.3.5.5). Die Wünsche der Datenschutzbefürworter spiegeln sich zudem auch in den Ankündigungen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

der Kommission zur Verbesserung des Auskunftsrechts, zur Einführung eines Rechts auf Vergessen und des Rechts auf Datenübertragbarkeit sowie zur Präzisierung und Stärkung der Einwilligung wider. Unter Rückgriff auf die Forderungen der Datenschutzbefürworter kündigte die Kommission schließlich auch die Prüfung der Einführung eines Verbandsklagerechts und der Verschärfung der Sanktionsregelungen an.

In einem weiteren Kapitel widmete sich die Kommission der Stärkung der Binnenmarktdimension. Trotz des Versuchs, durch sprachliche Beteuerungen ein Entgegenkommen gegenüber den Wünschen der Verarbeiter zu signalisieren,[292] spiegelten nur drei der konkreten Kommissionsvorschläge die Maßnahmenwünsche der Flexibilitätsbefürworter wider: So kündigte die Kommission insbesondere die Vereinfachung und Harmonisierung der geltenden Melderegelungen an, und adressierte somit einen der zentralen Kritikpunkte der Flexibilitätsbefürworter. Daneben griff die Kommission auch die Kritik an der divergierenden Umsetzung der Richtlinienbestimmungen sowie an den unpräzisen Bestimmungen zum anwendbaren Recht auf und kündigte in diesem Zusammenhang Verbesserung an. Änderungen in diesen Bereichen wurden allerdings auch seitens der Datenschutzbefürworter gefordert, sodass die Vorschläge der Kommission eher als Entgegenkommen gegenüber allen Beteiligten gedeutet werden müssen. Deutlich aussagekräftiger im Hinblick auf den Umgang der Kommission mit den Forderungen der datenverarbeitenden Wirtschaft war dagegen die Haltung der Kommission gegenüber der Rechenschaftspflicht, die von einigen Datenverarbeitern befürwortet worden war. Während die privatwirtschaftliche Perspektive auf die Rechenschaftspflicht diese an die Stelle verbindlicher rechtlicher Regelugen zu setzen anstrebte, machte die Kommission unmissverständlich deutlich, dass die seitens der Kommission angestrebten verwaltungstechnischen Vereinfachungen „nicht dazu führen, dass *die für die Verarbeitung Verantwortlichen weniger Verantwortung für den Datenschutz tragen*. Nach Meinung der Kommission sollten die Pflichten vielmehr stärker rechtlich verankert werden, darunter auch durch Vorschriften über interne Kontrollverfahren und die Zusammenarbeit mit den Datenschutzbehörden." (ebd., 13, Hervorhebung im Original) Mit letzterer Aussage kündigte die Kommission zugleich an, die Einführung einer neuen Verpflichtung in Form der Benennung eines betrieblichen Datenschutzbe-

292 Durch Formulierungen wie: „Gleichzeitig wird sie [die Kommission, M. K.] der Binnenmarktdimension mehr Gewicht geben und den freien Verkehr personenbezogener Daten fördern." (EK 2010, 5)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auftragten für größere Unternehmen zu überprüfen. Daneben sollte auch die Möglichkeit der Einführung einer Pflicht zur Durchführung einer Datenschutzfolgenabschätzung bei besonders riskanten Datenverarbeitungen überprüft werden sowie die Förderung von Privacy Enhancing Technologies und des Privacy by Design-Konzepts (ebd., 14). Abschließend kündigte die Kommission auch die Überprüfung von Möglichkeiten zur verstärkten Förderung von unternehmensinternen Verhaltensregeln sowie von EU-Zertifizierungsregeln an. Während die Kommission im Hinblick auf Verhaltensregeln die Kritik der datenverarbeitenden Wirtschaft zum Anlass der Überprüfung nahm, aber den Grad der staatlichen Kontrolle offenließ, kündigte sie im Hinblick auf die Gewährleistung der Zuverlässigkeit der Zertifizierungsregeln – entgegen den Wünschen der Flexibilitätsbefürworter – ein strenges staatliches Verfahren an und folgte somit auch bei diesem Thema den Vorschlägen der Datenschutzbefürworter.

Ein weiterer Bereich, in dem die Kommission den Forderungen der Flexibilitätsbefürworter immerhin entgegenkam, sind die Bestimmungen zum grenzüberschreitenden Transfer personenbezogener Daten. Dabei übernahm die Kommission insbesondere die Kritik in Bezug auf die divergierende Umsetzung der Richtlinienvorgaben im mitgliedstaatlichen Recht, in deren Ergebnis für grenzüberschreitende Datentransfers EU-weit unterschiedliche Bedingungen galten. So kündigte die Kommission an, die bestehenden Verfahren zu überprüfen und eine Verbesserung auf dem Gebiet sowohl der rechtsverbindlichen Instrumente (darunter auch die Prüfung der Angemessenheit eines Drittstaates) als auch auf dem Gebiet verbindlicher unternehmensinterner Vorschriften zu erzielen, indem die Vereinheitlichung der entsprechenden Bestimmungen angestrebt wird (ebd., 17-19). Die von der Kommission vertretene Haltung bewerte ich trotz des Entgegenkommens gegenüber den Forderungen der Datenverarbeiter als eine kompromissorientierte Position, weil die Kommission im selben Atemzug den aus der divergierenden Umsetzung resultierenden uneinheitlichen Schutz der Betroffenen als ein Hauptproblem artikulierte. Die angekündigten Verbesserungen adressieren daher die Forderungen beider Advocacy-Communities.

Im abschließenden Teil der Mitteilung kündigte die Kommission schließlich die Stärkung der Durchsetzung des Datenschutzrahmens an. Diese sollte erreicht werden, indem *erstens* die Rechtsstellung und die Befugnisse der Datenschutzaufsichtsbehörden gestärkt, präzisiert und harmonisiert werden, indem *zweitens* die Zusammenarbeit und Abstimmung zwischen den Behörden verbessert wird, und *drittens*, indem die Koordinationsrol-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

le der Datenschutzgruppe – allerdings unter der übergeordneten Zuständigkeit der Kommission – gestärkt und ihre Arbeit transparenter wird (ebd., 19 f.). Bei näherer Betrachtung der einzelnen Akteurspositionen entspricht die vorgesehene Stärkung der Datenschutzaufsichtsbehörden den Forderungen eines Großteils der Akteure beider Advocacy-Communities. Schwieriger war hingegen die Bewertung der Kommissionsposition im Hinblick auf den Umgang mit der Rolle der Datenschutzgruppe. So kündigte die Kommission zwar die Stärkung der Rolle der Gruppe im Hinblick auf die Gewährleistung der EU-weit kohärenten Befolgung der Datenschutzgesetze an. Andererseits sah diese Stärkung zugleich eine noch bedeutsamere Stärkung der Aufsichtsrolle der Kommission über die Tätigkeiten der Gruppe vor, was praktisch zu einer Einschränkung der Unabhängigkeit der Datenschutzgruppe und damit also zu deren Schwächung geführt hätte. Zudem kam die Kommission der Kritik der Wirtschaftsvertreter insofern entgegen, dass mehr Transparenz bei der Arbeit der Datenschutzgruppe angekündigt wurde. Somit berücksichtigte die Kommission die Forderungen beider Advocacy-Communities in nur geringem Maße.

4.1.2.1 Entscheidende Gründe für das Zustandekommen des Gesamtkonzepts der Kommission

Abschließend wird an dieser Stelle die Frage beantwortet, auf den Einfluss welcher Akteure das in der jeweiligen Phase zur Debatte stehende Politikergebnis zurückgeführt werden kann. Die vorangegangene Diskussion hat gezeigt, dass das Gesamtkonzept die Forderungen der Datenschutzbefürworter weitestgehend widerspiegelt. Diese inhaltliche Überschneidung erfüllt somit die Bedingungen des Hoop-Tests: Wenn eine Beeinflussung tatsächlich stattgefunden hat, muss sich diese in Form weitgehender inhaltlicher Überschneidung äußern, andernfalls kann ein Einfluss mit Sicherheit ausgeschlossen werden. Das Bestehen des Hoop-Tests ist somit notwendig, aber nicht hinreichend im Hinblick auf die Beantwortung der Frage der Beeinflussung. Schließlich kann die Stärkung des Datenschutzniveaus auch andere Gründe gehabt haben. Daher führe ich im Folgenden aus, welche Gründe auf Seiten der Kommission entscheidend für die Erarbeitung des Gesamtkonzepts waren.

Zur Beantwortung dieser Frage kann zunächst auf die Erkenntnisse der Kontextanalyse zurückgegriffen werden. Die Ausführungen in Abschnitt 3 haben verdeutlicht, dass die Europäische Kommission, bzw. deren für die datenschutzpolitischen Vorhaben federführenden Stellen zumindest seit

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

den 1990er-Jahren stets eine eher datenschutzbefürwortende Position vertreten hatten. Aufgrund der gewachsenen sicherheits- und wirtschaftspolitischen Bedeutung der Datenverarbeitung befanden sich die Datenschutzbefürworter und damit auch die Kommission während der 2000er-Jahre zunehmend in einer Defensivposition. Nachdem der Lissabon-Vertrag Ende 2009 in Kraft getreten und die EU-Grundrechtecharta verbindlich geworden und auch in der EU-Bevölkerung Sorgen vor einem Missbrauch personenbezogener Daten gewachsen waren, hatte sich ein politisches Gelegenheitsfenster geöffnet, das es erstmals erlaubte, den seit Jahren gehegten Wunsch der Datenschutzbefürworter nach einer umfassenden Datenschutzreform (insb. im Hinblick auf die Datenschutzregeln der ehemaligen dritten Säule) anzugehen.

Zudem hatten sich, noch bevor die Ergebnisse der ersten Konsultationsrunde veröffentlicht worden waren, personelle und institutionelle Änderungen innerhalb der Kommission ergeben, die von weitreichender Bedeutung für den weiteren Reformprozess sein sollten. So war zwar die konservative EVP siegreich aus der Europawahl Anfang Juni 2009 hervorgegangen, doch benötigte sie die Unterstützung weiterer Parteien, um die Wiederwahl des Kommissionspräsidenten Barroso zu gewährleisten (Mahony 2009a). Ausgehend von der Debatte um den als zu breit kritisierten Zuschnitt des Kommissariats für Justiz, Freiheit und Sicherheit und vor dem Hintergrund des bevorstehenden Inkrafttretens des Lissabon-Vertrags, hatte insbesondere die liberale ALDE-Fraktion von Barroso die Schaffung eines Kommissarspostens für Grundrechte und bürgerliche Freiheiten gefordert, der dieser Forderung letztlich zugunsten seiner Wiederwahl nachgab (Mahony 2009b). Am 27. November 2009 stellte Barroso die Mitglieder und die Verteilung der Politikressorts der neuen Kommission vor.[293] Darin war die Aufteilung des Kommissarspostens für Justiz, Freiheit und Sicherheit in ein Ressort für Inneres unter der Leitung von Cecilia Malmström und ein Ressort für Justiz, Grundrechte und Bürgerschaft unter der Leitung von Viviane Reding vorgesehen (EU-Kommission 2009). Reding übte in der Folgezeit Druck auf Barroso aus, damit die für Justiz, Freiheit und Sicherheit zuständige Generaldirektion der Europäischen Kommission dem Zuschnitt der neuen Kommissarsposten – und der Aufgabenverteilung vieler mitgliedstaatlicher Regierungssysteme in ein Justiz- und ein Innen-

293 Nachdem die neuen Kommissionsmitglieder Anfang Februar 2010 seitens des Parlaments bestätigt wurden, trat die Kommission Barroso II am 10. Februar ihre Ämter an.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ministerium – entsprechend zweigeteilt wird (Taylor 2010). Anfang Juni wurde die entsprechende Generaldirektion schließlich Redings Wünschen entsprechend in zwei geteilt.[294] Das Datenschutz-Referat der Kommission, das die Federführung für die Datenschutzreform inne hatte, ging dabei in den Zuständigkeitsbereich der GD Justiz und damit auch von Justiz-Kommissarin Reding über (KOM 2010a).[295]

Diese Entwicklung war aus zwei Gründen folgenreich für den weiteren Reformprozess des EU-Datenschutzrahmens. Erstens war fortan das Justizkommissariat bzw. die für Justiz zuständige Generaldirektion alleine und federführend für alle datenschutzpolitischen Anliegen zuständig. Der zuvor seitens der im Referat für Datenschutz zuständigen Mitarbeiter als zu groß kritisierte Einfluss von innenpolitisch motivierten Kommissionsmitgliedern (Zerdick 2008) wurde auf diese Weise wirksam zurückgedrängt. Zweitens übernahm mit Viviane Reding eine ausgesprochene und mächtige Befürworterin[296] eines hohen Datenschutzniveaus die Aufgabe der federführenden Kommissarin. Als langjährige Europapolitikerin, sowohl auf Seiten des Parlaments als auch auf Seiten der Kommission, genoss Reding eine herausgehobene Stellung im Kommissionsgefüge. Dies spiegelte sich nicht zuletzt an ihrer Ernennung zur zweiten Kommissionsvizepräsidentin wider. Reding, die bereits als Kommissarin für die Informationsgesellschaft und Medien mit öffentlichkeitswirksamen Politiken wie der Abschaffung der Roaming-Gebühren innerhalb der EU aufgefallen war, machte die Förderung bürgerorientierter Politiken zu einem ihrer Kernanliegen. Zu diesem

294 Die Verlagerung der Verantwortung über allgemeine Datenschutzpolitiken vom GD MARKT zur GD Justiz stieß auf Widerstand bei einigen Akteuren. Insbesondere Yahoo (2009, 6 f.) kritisierte, dass diese Verlagerung den Fokus auf den Binnenmarkt neutralisiert hätte, sodass nur noch einseitig auf den Grundrechtsaspekt fokussierte Datenschutzpolitiken zu erwarten seien – womit Yahoo faktisch recht behalten sollte. Kurz nach Veröffentlichung des Verordnungsvorschlags wurde zudem auch in der für die Konsultationen im Ministerrat zuständigen Ratsarbeitsgruppe seitens einer Ratsdelegation der Versuch unternommen, die DSGVO, unter Verweis auf die Binnenmarktrelevanz des Vorschlags, aus der Zuständigkeit von DAPIX in die Zuständigkeit einer Binnenmarktratsarbeitsgruppe zu übertragen (DAPIX 2012, 1).

295 Die genannten Umstrukturierungen waren dann auch entscheidend dafür (Jančiūtė 2018, 225 f.), dass die Konsultationsergebnisse erst Ende 2010 und nicht, wie erwartet worden war (Euractiv 2009), bereits Anfang des Jahres veröffentlicht wurden.

296 Relativierend sei erwähnt, dass Reding in ihrer Rolle als Justizkommissarin wenig später zwar ankündigte, die EU-Richtlinie zur Vorratsdatenspeicherung aufgrund der datenschutzrechtlichen Bedenken auf den Prüfstand stellen zu wollen, doch maßregelte sie zugleich die Bundesrepublik dafür, die Richtlinie nicht schnell genug umgesetzt zu haben (Bergius 2011).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zweck initiierte sie mehrere Maßnahmen, darunter insbesondere die im Oktober 2010 vorgestellte Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union (KOM 2010b). Bereits in ihrer Antrittsrede vor dem LIBE-Ausschuss im Januar 2010 hatte Reding zudem die Stärkung des Datenschutzrahmens der EU zu ihrer ersten Priorität erklärt (Reding 2010). Zudem war sie bereits im Kontext der Erarbeitung der Cookie-Richtlinie mit der Befürwortung eines hohen Schutzniveaus aufgefallen. Noch in ihrer Rolle als Kommissarin für die Informationsgesellschaft und Medien hatte sie im Kontext der Debatten um die Meldepflicht bei Datenschutzverstößen ihre Haltung zu dem Thema deutlich gemacht: "Those who profit from the information revolution must respond to the public policy responsibilities that come with it." (Reding 2009, 2 f.) Nachdem sich bereits der frühere Kommissar für Justiz, Freiheit und Inneres Jacques Barrot intensiv für die Initiierung der Datenschutzreform eingesetzt hatte, gelangte mit Reding somit ein Policy Entrepreneur auf den Posten des neu-geschaffenen Justizkommissars, die den Datenschutz zu ihrer politischen Priorität erklärte. Entsprechend intensiv verfolgte Reding fortan den Reformprozess bzw. die Kommissionskonsultation und positionierte sich klar für die Stärkung des Datenschutzrechts.[297]

Die Ausführungen verweisen darauf, dass sowohl vor der Datenschutzreform als auch zu Beginn und während der ersten Konsultationsrunde auf Seiten der Kommission ein inhärentes Interesse nach einer Anhebung des Datenschutzniveaus vorhanden war. Gleichzeitig war die Kommission Teil der Advocacy-Community der Datenschutzbefürworter, teilte somit also weitgehend deren Überzeugungssystem wie die übrigen, datenschutzbefürwortenden Akteure. Insofern möchte ich an dieser Stelle den Begriff der Beeinflussung nicht verwenden. Dieser suggeriert m. E., dass ein eher neutraler Akteur von eher nicht-neutralen Akteuren dahingehend beeinflusst

297 So veröffentlichte Reding im Jahr 2011 zwei Namensartikel in Datenschutz-Journals, in denen sie das Gesamtkonzept der Kommission für den Datenschutz vorstellte (Reding 2011c, 2011b). Später veröffentlichte sie auch einen Beitrag, in dem sie den Kommissionsentwurf zur DSGVO vorstellte (Reding 2012). Das Thema der Datenschutzreform war zudem Gegenstand bei vielen von Redings öffentlichen Reden. https://ec.europa.eu/archives/commission_2010-2014/reding/multimedia/speeches/index_en.htm Auf die bedeutende Rolle, die Viviane Reding zukam, wurde später etwa auch seitens des damaligen EDSB Peter Hustinx hingewiesen (Hustinx 2014, 25). Ein weiteres Zeugnis ihres persönlichen Einsatzes für die Stärkung des Datenschutzes bildet der Dokumentarfilm „Democracy – Im Rausch der Daten", der neben Jan Philipp Albrecht auch Viviane Reding während der Verhandlungen zur DSGVO begleitet (Bernet 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

worden wäre, etwas zu unternehmen, was dieser ansonsten nicht getan hätte. Stattdessen machte sich die Kommission, der exekutive Arm der Datenschutzbefürworter-Advocacy-Community, das politische Gelegenheitsfenster zu nutze, um die von der Community (also sowohl von der Kommission als auch von den übrigen Datenschutzbefürwortern) lange gehegten Vorstellungen über ein besseres Datenschutzniveau in die politische Praxis zu überführen.

4.1.2.2 Zwischenfazit

Zusammenfassend kann festgellt werden, dass die Kommission im Gesamtkonzept Positionen vertrat, die eine deutliche Steigerung des Datenschutzniveaus vorsahen und einseitig den Forderungen der der Datenschutzbefürworter entsprachen (vgl. auch die Gegenüberstellung der einzelnen Positionen in Tabelle 4-14).

Die Vorschläge der Kommission sahen sowohl die Verlagerung von mehr Verantwortung an die Betroffenen als auch an die Verarbeiter vor. So hielt die Kommission am Konzept der informierten Einwilligung fest und sah die Verbesserung bzw. Standardisierung der Informationen vor, die den Betroffenen vor einer Einwilligung angezeigt werden sollten. Ebenso sah sie die Verbesserung der Modalitäten zur Wahrnehmung der Betroffenenrechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung die Beteiligung der Betroffenen vor. Schließlich stellt auch das Recht auf Datenübertragbarkeit eine Übertragung der Verantwortung an das Individuum dar, sofern keine direkte und zuverlässige Übertragbarkeit der Daten auf andere Dienste gewährleistet wird. Relativierend sei jedoch hinzugefügt, dass die vorgenannten Maßnahmen trotz der Übertragung von Verantwortung an den Betroffenen die Verbesserung der vorherrschenden Situation anstrebten. So plante die Kommission die Vorgabe EU-weit gültiger Standard-Datenschutzhinweise, mittels derer die Verbesserung der Lesbarkeit derartiger Hinweise angestrebt wurde, was praktisch so lange zu weniger Verantwortung für den Betroffenen geführt hätte, wie die Anzahl der Datenschutzhinweise keinen enormen Anstieg erfährt. Ebenso betraf das Recht auf Datenübertragbarkeit Situationen, in denen Betroffene von einem Dienst zu einem anderen umzuziehen gedachten, daran aber aufgrund des nicht gewährleisteten Zugangs zu den eigenen Daten oder aufgrund von Interoperabilitätsproblemen gehindert wurden. Die Datenübertragbarkeit sollte also zu einer Vereinfachung führen. Mit der Einführung des Verbandsklagerechts strebte die Kommission schließlich die Gewährleistung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Wahrnehmung von Rechtsbehelfen in Situationen an, in denen Individuen aufgrund der geringen individuellen Not den Gerichtsweg scheuen würden.

Die Mehrzahl der von der Kommission vorgeschlagenen Maßnahmen sah dagegen die Ausweitung der Pflichten vor, denen die Verarbeiter künftig unterliegen sollten. Dies betrifft die folgenden Aspekte: Strengere Einwilligungserfordernisse; strengere Transparenzvorgaben; Stärkung des Auskunftsrechts bzw. Ausweitung der Informationspflichten der Verarbeiter; Umsetzung des Rechts auf Vergessenwerden sowie des Rechts auf Datenübertragbarkeit; Einführung einer allgemeinen Meldepflicht bei Datenschutzverstößen; Einführung von Privacy by Default bzw. by Design-Vorgaben; die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten und die Verpflichtung zur Durchführung einer DSFA bei riskanten Datenverarbeitungen. Mit der Verschärfung der Sanktionsregelungen kündigte die Kommission zudem an, Regelverstöße künftig deutlich strenger zu ahnden.

Item	Flexibilitätsbefürworter-Community	KOM	Datenschutzbefürworter-Community
B1 Techn. Wandel	2	5	5
B2 Staatl./Private Aktivität	2	5	5
B3 Policy-Orientierung	2	4	4
B6 Harmonisierung	4	5	5
B8 Globalisierung	2	4	5
B12 Reformwunsch	2	5	4
C 1 B Räuml. Anwendungsbereich	3	4	4
C 1 C Definition personenb. Daten	2	4	5
C 3 D Einwilligung	2	4	5
C 5 A Transparenz	2	4	4
C 5 C Auskunftsrecht/Inf.-Pflicht	3	4	4
C 5 E Recht auf Vergessenwerden	2	4	5
C 5 G Recht auf Datenübertragb.		5	5
C 5 L Meldung v. Verletzungen	3	4	4
C 6 B Privacy by Design	2	4	5
C 6 C Meldepflicht/VA-Verzeichnis	2	2	4
C 6 N Rechenschaftspflicht	2	4	4
C 7 Drittstaatentransfers	2	3	4

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Flexibilitätsbefürworter-Community	KOM	Datenschutzbefürworter-Community
C 10 D Technologieneutralität	1	4	4
C 13 A Verhaltensregeln	2	3	4
C 13 B Zertifizierungen/Gütesiegel	2	3	4
C 13 C Bestellung eines DSB	2	4	4
C 15 B Datenschutzbehörden	3	4	5
C 16 C Art. 29-Datenschutzgruppe	2	3	5
C 17 D Verbands-/Sammelklagen	2	4	4
C 17 E Sanktionen & Geldbußen	2	4	5

Tabelle 4-14: Die Positionen der Advocacy-Communities im Vergleich zur Kommissionsposition während der Orientierungsphase (eigene Erhebung, Berechnung mittels SPSS, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum Kommissionsentwurf)

4.2 Entwurfsphase (2010–2012)

Nachdem die Kommission im Rahmen der Orientierungsphase ein erstes Feedback eingeholt und Ende 2010 ihr Gesamtkonzept für den Datenschutz in der EU vorgestellt hatte, eröffnete sie eine zweite öffentliche Konsultationsphase, in der sie alle interessierten Akteure um die Kommentierung des Gesamtkonzepts bat. Diese fand zwischen dem 4. November 2010 und dem 15. Januar 2011 statt (European Commission 2010c). Es folgten weitere Konsultationen, darunter insb. eine gemeinsam mit dem Europarat organisierte High-Level Conference am 28. Januar 2011, ebenfalls im Januar 2011 ein ENISA-Workshop zum Thema der Meldung von Datenschutzverletzungen, ein Treffen mit Vertretern der Mitgliedstaaten zu den sicherheitsrelevanten Aspekten der Datenschutzreform Anfang Februar 2011, eine Stakeholder-Konsultation der Europäischen Grundrechteagentur FRA Ende Februar 2011 sowie weitere Treffen mit Vertretern von Datenschutzaufsichtsbehörden Mitte 2011. Daneben gab die Kommission eine datenschutz-spezifische Eurobarometer-Studie in Auftrag, die zwischen November und Dezember 2010 durchgeführt und im Juni 2011 veröffentlicht wurde (EU Commission 2012, 9 f.). Auf Grundlage des Stakeholder-Inputs und unter Einbeziehung weiterer Kommissionsstellen erarbeitete die Kommission im Laufe des Jah-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

res 2012 ihren Legislativvorschlag, mit deren Veröffentlichung am 25. Januar 2012 schließlich auch die Entwurfsphase an ihr Ende gelangte.

4.2.1 Akteursanalyse

4.2.1.1 Cluster-Analyse

Erneut führte ich eine große Anzahl von Clusteranalysen mit verschiedenen Item-Kombinationen durch. Beginnend mit den Items mit einem möglichst geringen Anteil fehlender Werte, verwendete ich schrittweise mehr Items, bis die Ergebnisse der Clusteranalyse verfeinert wurden. Nach zahlreichen Durchgängen wurden als Grundlage für die Cluster-Analyse schließlich die in Tabelle 4-15 dargestellten 24 Items verwendet. Der Anteil der fehlenden Werte war mit 37,7% niedriger als bei dem Datensatz zur ersten Phase (47,7%). Vollständige Werte lagen wieder für die beiden Items B2 *Grad an erwünschter staatlicher oder privater Aktivität* und B 3 *Grundlegende Policy Orientierung im Falle staatliche Intervention* vor, mit denen die Policy-Kernüberzeugungen der Akteure abgebildet werden. Auf diese folgen die Items C 5A Transparenz (21,3% fehlende Werte), C6 B Privacy by Design (25,3%) und C 3 D *Bedingungen für die Einwilligung* (28%). Demgegenüber sind die höchsten Anteile fehlender Werte bei den Items C 2 C *Grundsatz der Datenminimierung* (57,3%), C 17E *Sanktionen und Geldbußen* (56%) und C 2 C *Grundsatz der Datenminimierung* (57,3%) zu finden.

Variable	N	Mean	Std. Deviation	Missing	
				Count	Percent
B1 Einschätzung des techn. Wandels	44	3,80	1,047	31	41,3
B2 Grad an erwünschter staatlicher oder privater Aktivität	75	3,20	1,325	0	0,0
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	75	2,76	1,324	0	0,0
C1C Definition personenbezogener Daten	36	2,83	1,424	39	52,0
C 2 C Grundsatz der Datenminimierung	32	3,25	1,047	43	57,3
C3D Bedingungen für die Einwilligung	54	2,89	1,383	21	28,0
C 4 A Besondere Kategorien personenbezogener Daten	37	3,22	1,228	38	50,7
C 4 D Datenschutz bei Kindern	34	3,59	1,258	41	54,7
C5A Transparenz	59	2,92	1,290	16	21,3

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Variable	N	Mean	Std. Deviation	Missing	
				Count	Percent
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	40	3,48	0,877	35	46,7
C 5 E Recht auf Vergessenwerden	53	2,92	1,174	22	29,3
C 5 G Recht auf Datenportabilität	42	2,86	1,317	33	44,0
C 5 L Benachrichtigung bei Datenschutzverletzungen	50	3,12	1,288	25	33,3
C 6 B Privacy by Design	56	3,11	1,423	19	25,3
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	52	2,46	1,038	23	30,7
C 6 N Rechenschaftspflicht	35	2,91	1,401	40	53,3
C 7 Übermittlung in Drittstaaten	51	2,61	1,168	24	32,0
C 13 A Verhaltensregeln	42	2,19	1,042	33	44,0
C 13 B Zertifizierungen/Gütesiegel	41	2,68	1,404	34	45,3
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	51	2,84	1,239	24	32,0
C 13 D Datenschutz-Folgenabschätzung	43	3,09	1,288	32	42,7
C 17 D Verbands- /Sammelklagerecht	40	2,80	1,344	35	46,7
C 17 E Sanktionen und Geldbußen	33	3,18	1,310	42	56,0
Durchschnitt					37,7

Tabelle 4-15: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS)

Als mögliche Cluster-Anzahl kamen erneut zwei oder drei Cluster infrage, sodass die entsprechenden Analysen für beide Möglichkeiten durchgeführt wurden. Ich stelle im Folgenden zunächst die Ergebnisse des 2-Cluster-Modells und danach die des 3-Cluster-Modells vor. Daran schließt sich die Diskussion der Ergebnisse sowie die Begründung der Entscheidung, das 3-Cluster-Modell zu verwenden.

2-Cluster-Modell

Das 2-Cluster-Modell ergab 43 Akteure auf Seiten der Flexibilitätsbefürworter und 23 Akteure auf Seiten der Datenschutzbefürworter (vgl. Tabelle 4-16). Die Zuordnung der Akteure deckt sich weitgehend mit den Ergebnissen der vorherigen Analysen aus der Orientierungsphase (vgl. 4.1.1.1.2) als auch der Kontextanalyse (vgl. 3).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1	Cluster 2
ACCIS	Art. 29-Datenschutzgruppe (Kohnstamm Rede)
ACT	AUT-Regierung
AmCham EU	BEUC
BDIU	Breyer, Patrick
BITKOM	CDT
BRAK	DG JUST-Le Bail
BSA	DSAB-AUT
BT	DSAB-BEL
DDV	DSAB-CAN
DEU-Regierung	DSAB-GER alle
DIGITALEUROPE	DSAB-LIE
eBay	DSAB-NOR
EBF	DSAB-PRT
ECTA	DSAB-SWE
EMOTA	EDPS
ENPA & FAEP	EDRi
EPC	EPA
ETNO	Europ. DSBeauftragte
Eurofinas	GDD
EuroISPA	LVA-Regierung
Facebook	PI
FBF	VZBV
FEDMA	
FTC	
GDV	
GSMA	
IAB Europe	
ICC	
ICO	
Industry Coalition for DP	
Intel	
Liberty Global	
Microsoft	
Ministerrat	
Mitgliedstaaten - GBR- Justizministerium	
Nokia	

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1	Cluster 2
TechAmerica (formerly AeA)	
Telefonica	
UEAPME	
VDZ	
WFA	
Yahoo	
ZAW	

Tabelle 4-16: K-Means Cluster-Analyse mit 2 Clustern (berechnet mit SPSS)

Die berechneten Cluster-Zentren, bzw. die den Clustern zugeordneten Idealpositionen im Hinblick auf die einzelnen Items, können Tabelle 4-17 entnommen werden.

Item	Cluster	
	1	2
B1 Einschätzung des techn. Wandels	3	4
B2 Grad an erwünschter staatlicher oder privater Aktivität	2	5
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	2	4
C1C Definition personenbezogener Daten	2	4
C 2 C Grundsatz der Datenminimierung	3	4
C3D Bedingungen für die Einwilligung	2	4
C 4 A Besondere Kategorien personenbezogener Daten	2	4
C 4 D Datenschutz bei Kindern	3	5
C5A Transparenz	2	4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4
C 5 E Recht auf Vergessenwerden	2	4
C 5 G Recht auf Datenportabilität	2	4
C 5 L Benachrichtigung bei Datenschutzverletzungen	2	4
C 6 B Privacy by Design	2	5
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	2	3
C 6 N Rechenschaftspflicht	2	4
C 7 Übermittlung in Drittstaaten	2	4
C 13 A Verhaltensregeln	2	3
C 13 B Zertifizierungen/Gütesiegel	2	4
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	2	4

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster	
	1	2
C 13 D Datenschutz-Folgenabschätzung	2	4
C 17 D Verbands- /Sammelklagerecht	2	4
C 17 E Sanktionen und Geldbußen	2	5

Tabelle 4-17: Finale Zentren der K-Means-Clusteranalyse mit 2 Clustern (berechnet mit SPSS)

3-Cluster-Modell

Im 3-Cluster-Modell wurden dem ersten Cluster 38 Akteure, dem zweiten Cluster 15 und dem dritten Cluster 13 Akteure zugeordnet. Der Blick auf die Akteure, die neu zugeordnet wurden zeigt, dass diese sich aus 5 Akteuren des ersten Clusters des 2-Cluster-Modells und aus 8 Akteuren des zweiten Clusters zusammensetzen. So wurden aus dem ersten Cluster die Bundesrechtsanwaltskammer BRAK, die deutsche Bundesregierung, die FTC, das britische Justizministerium und die Ministerratsentschließung neu zugeordnet. Aus dem zweiten Cluster wurden dagegen die österreichische Regierung, CDT, die Datenschutzbehörden Norwegens, Portugals und Schwedens, die European Privacy Association EPA, die GDD sowie die die lettische Regierung neu zugeordnet (vgl. Tabelle 4-18).

Cluster 1	Cluster 2	Cluster 3
ACCIS	Art. 29-Datenschutzgruppe	AUT-Regierung
ACT	BEUC	BRAK
AmCham EU	Breyer, Patrick	CDT
BDIU	DG JUST	DEU-Regierung
BITKOM	DSAB-AUT	DSAB-NOR
BSA	DSAB-BEL	DSAB-PRT
BT	DSAB-CAN	DSAB-SWE
DDV	DSAB-GER alle	EPA
DIGITALEUROPE	DSAB-LIE	FTC
eBay	EDPS	GDD
EBF	EDRi	LVA-Regierung
ECTA	EU-PARL	Mitgliedstaaten - GBR- Justizministerium
EMOTA	Europ. DSBeauftragte	Ministerrat
ENPA & FAEP	PI	
EPC	VZBV	

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1	Cluster 2	Cluster 3
ETNO		
Eurofinas		
EuroISPA		
Facebook		
FBF		
FEDMA		
GDV		
GSMA		
IAB Europe		
ICC		
ICO		
Industry Coalition for DP		
Intel		
Liberty Global		
Microsoft		
Nokia		
TechAmerica (formerly AeA)		
Telefonica		
UEAPME		
VDZ		
WFA		
Yahoo		
ZAW		

Tabelle 4-18: K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS)

Die Betrachtung der Zentren des 3-Cluster-Modells in Tabelle 4-19 zeigt gegenüber den Ergebnissen der ersten Phase ein verändertes Bild. Während im 3-Cluster-Modell der Orientierungsphase eine weitgehende Überlappung der Zentren der Cluster 2 und 3 festzustellen war, ordnet sich das zusätzliche Cluster im Rahmen des 3-Cluster-Modells der Entwurfsphase zwischen den Positionen der ersten beiden Cluster ein. Auch der Blick auf die inhaltlichen Positionen der entsprechenden Akteure verdeutlicht, dass die von ihnen vertreten Positionen als eine Art Zwischenposition

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zwischen der Koalition der Flexibilitätsbefürworter und der Koalition der Datenschutzbefürworter anzusehen ist.[298]

Item	Cluster		
	1	2	3
B1 Einschätzung des techn. Wandels	3	5	4
B2 Grad an erwünschter staatlicher oder privater Aktivität	2	5	3
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	2	5	3
C1C Definition personenbezogener Daten	2	5	3
C 2 C Grundsatz der Datenminimierung	3	4	4
C3D Bedingungen für die Einwilligung	2	4	3
C 4 A Besondere Kategorien personenbezogener Daten	2	5	3
C 4 D Datenschutz bei Kindern	3	5	4
C5A Transparenz	2	4	4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4	3
C 5 E Recht auf Vergessenwerden	2	4	3
C 5 G Recht auf Datenportabilität	2	5	4
C 5 L Benachrichtigung bei Datenschutzverletzungen	2	4	4
C 6 B Privacy by Design	2	5	4
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	2	4	3
C 6 N Rechenschaftspflicht	2	5	4
C 7 Übermittlung in Drittstaaten	2	4	3
C 13 A Verhaltensregeln	2	4	3
C 13 B Zertifizierungen/Gütesiegel	2	4	3
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	2	5	3
C 13 D Datenschutz-Folgenabschätzung	2	5	3
C 17 D Verbands- /Sammelklagerecht	2	5	3
C 17 E Sanktionen und Geldbußen	2	5	3
Mittelwert	2	4	3

Tabelle 4-19: Finale Zentren der K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS)

298 Zur Vergewisserung, dass die Akteure auch tatsächlich einem eigenen Cluster entsprechen, führte ich eine weitere Cluster-Analyse mit einem 4-Cluster-Modell durch. Da bei diesem Modell keiner der Akteure des neuen Clusters mit den Akteuren des ersten Clusters gemeinsam neu zugeordnet wurden, kann das neue Cluster als eigenständiges Cluster betrachtet werden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Wie bereits bei der Cluster-Analyse der ersten Phase, testete ich die Zuverlässigkeit der Ergebnisse durchgängig mittels einer Varianzanalyse (ANOVA).

Tabelle 4-20 zeigt die ANOVA-Ergebnisse für das 3-Cluster-Modell der zweiten Phase: Alle verwendeten Items weisen eine hohe Signifikanz (<0,02) auf. Am stärksten trugen die Items B3 (F-Wert von ca. 195), C6B (155), B1 (119), C5G (105) zur Identifizierung der Cluster bei.

	Cluster		**Error**			
Item	Mean Square	df	Mean Square	df	**F**	**Sig.**
B1 Einschätzung des techn. Wandels	8,246	2	0,748	41	11,025	0,000
B2 Grad an erwünschter staatlicher oder privater Aktivität	49,893	2	0,420	72	118,900	0,000
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	54,735	2	0,281	72	195,004	0,000
C1C Definition personenbezogener Daten	21,738	2	0,834	33	26,061	0,000
C 2 C Grundsatz der Datenminimierung	11,575	2	0,374	29	30,938	0,000
C3D Bedingungen für die Einwilligung	33,827	2	0,660	51	51,224	0,000
C 4 A Besondere Kategorien personenbezogener Daten	16,256	2	0,640	34	25,404	0,000
C 4 D Datenschutz bei Kindern	19,871	2	0,403	31	49,312	0,000
C5A Transparenz	36,630	2	0,416	56	87,974	0,000
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	8,489	2	0,351	37	24,165	0,000
C 5 E Recht auf Vergessenwerden	23,688	2	0,486	50	48,695	0,000
C 5 G Recht auf Datenportabilität	29,981	2	0,287	39	104,566	0,000
C 5 L Benachrichtigung bei Datenschutzverletzungen	27,603	2	0,555	47	49,758	0,000
C 6 B Privacy by Design	47,563	2	0,306	53	155,315	0,000
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	13,668	2	0,563	49	24,278	0,000
C 6 N Rechenschaftspflicht	19,465	2	0,869	32	22,395	0,000
C 7 Übermittlung in Drittstaaten	24,108	2	0,415	48	58,028	0,000
C 13 A Verhaltensregeln	14,607	2	0,391	39	37,327	0,000
C 13 B Zertifizierungen/Gütesiegel	28,254	2	0,589	38	47,997	0,000

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	29,178	2	0,383	48	76,163	0,000
C 13 D Datenschutz-Folgenabschätzung	25,298	2	0,476	40	53,168	0,000
C 17 D Verbands- /Sammelklagerecht	27,447	2	0,419	37	65,496	0,000
C 17 E Sanktionen und Geldbußen	20,386	2	0,471	30	43,260	0,000

Tabelle 4-20: ANOVA-Ergebnisse für das 3-Cluster-Modell der zweiten Phase (berechnet mit SPSS)

Auf Basis der Ergebnisse der Cluster-Analyse für die zweite Phase können drei Cluster unterschieden werden. Zwei der Cluster bilden dabei die Flexibilitätsbefürworter und Datenschutzbefürworter ab, während ein drittes Cluster jene Akteure abbildet, die eher abwägende Positionen vertraten.

4.2.1.2 Datenschutzbefürworter

4.2.1.2.1 Zusammensetzung der Datenschutzbefürworter während der Entwurfsphase: Von der Community zur Koalition

Die Zusammensetzung der Koalition der Datenschutzbefürworter während der Entwurfsphase blieb weitgehend identisch gegenüber der Orientierungsphase. Neu hinzu kam insbesondere das Europäische Parlament, das in Form einer Entschließung auf das Gesamtkonzept der Kommission reagierte. Da allerdings auch vermehrt einzelne Datenschutzaufsichtsbehörden am Konsultationsprozess partizipierten, zeigten sich Meinungsverschiedenheiten unter den Datenschutzaufsichtsbehörden. Während die Positionen der österreichischen, belgischen, kanadischen, deutschen und liechtensteinischen Datenschutzaufsichtsbehörden in der Cluster-Analyse eindeutig dem Lager der Datenschutzbefürworter zugeordnet wurden, wurden die Datenschutzbehörden Norwegens, Portugals und Schwedens einem weiteren, dritten Cluster zugeordnet.

Zugleich intensivierte sich der Austausch zwischen Kommission, Zivilgesellschaft und Datenschutzbehörden, sodass in der Entwurfsphase von einem allmählichen Übergang von einer Advocacy-Community zu einer Advocacy-Koalition die Rede sein kann. Insbesondere EDRi verfügte über gute Kontakte zu den für Datenschutz verantwortlichen Kommissionsstellen in DG JUST (Schildberger 2016, lxiii). Die entsprechenden Kommissionsstellen traten darüber hinaus im Laufe des Jahres 2011 mehrfach mit

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Vertretern der Datenschutzbehörden in den Dialog (EU Commission 2012, 9 f.) Daneben baute auch der EDPS die Kooperation mit anderen gleichgesinnten Datenschutz-Organisationen aus (EDPS 2011, 5).

Datenschutzbefürworter	
Akteur	**Akteursgruppe**
Art. 29-Datenschutzgruppe	Datenschutzbehörden
BEUC	Verbraucherschutz
Breyer, Patrick	Zivilgesellschaft
DG JUST / Reding	EU-Politik
DSAB-AUT	Datenschutzbehörden
DSAB-BEL	Datenschutzbehörden
DSAB-CAN	Datenschutzbehörden
DSAB-GER alle	Datenschutzbehörden
DSAB-LIE	Datenschutzbehörden
EDPS	Datenschutzbehörden
EDRi	Zivilgesellschaft
EU-PARL / LIBE-Ausschuss	EU-Politik
Europ. DSBeauftragte	Datenschutzbehörden
PI	Zivilgesellschaft
VZBV	Verbraucherschutz

Tabelle 4-21: Die Advocacy-Koalition der Datenschutzbefürworter

4.2.1.2.2 Überzeugungssytem der Datenschutzbefürworter-Koalition während der Entwurfsphase

Während viele Aspekte des Überzeugungssystems der Datenschutzbefürworter in der Orientierungsphase noch relativ unklar waren, formierte sich in der Entwurfsphase eine deutlich klarere Haltung zu den meisten diskutierten Themen.

Policy-Kernüberzeugungen

Die Policy-Kernüberzeugungen der Datenschutzbefürworter blieben in der Entwurfsphase gegenüber der vorausgegangenen Orientierungsphase weitgehend stabil. So wurde im Hinblick auf den technologischen Wandel und die Globalisierung weiterhin vor allem auf die Herausforderungen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

verwiesen. Um diesen Herausforderungen begegnen zu können wurde auch weiterhin auf staatliche Regulierungsmaßnahmen verwiesen. Das seit Ende der 1990er-Jahre zunehmend wichtig gewordene wirtschaftspolitisch motivierte Framing, dass ein hohes Datenschutzniveau zur Herstellung von Vertrauen in Dienste der Informationsgesellschaft nötig sei, war auch in der Entwurfsphase von keiner nennenswerten Relevanz, weil alle Datenschutzbefürworter klar für die Stärkung des Datenschutzes aus einer Grundrechtsperspektive heraus eintraten.[299]

Während die Akteure in der Orientierungsphase noch eine zwar geringe, aber doch gewisse Unterstützung für Maßnahmen auf Basis von Selbstregulierung geäußert hatten, beschränkte sich diese in der Entwurfsphase lediglich auf die Erarbeitung von Verhaltensregeln. Dagegen forderten die Datenschutzbefürworter für praktisch alle anderen Maßnahmenvorschläge der Kommission den Erlass verbindlicher staatlicher Vorschriften anstelle von Selbstregulierungsmaßnahmen. Zudem traten die Datenschutzbefürworter geschlossen für die Reform der DS-RL und den Übergang zu einer verpflichtenden Verordnung ein (EDPS, 2011, ab Rn. 64).

Unterm Strich vertrat die Datenschutzbefürworter-Koalition die Position, dass eine sinnvolle Anhebung des Datenschutzniveaus nur durch die Kombination aus einer Intensivierung der Verarbeiterpflichten und der Stärkung der Betroffenenrechte sowie der Durchsetzungsmöglichkeiten der Aufsichtsbehörden zu erreichen wäre. Sehr pointiert wurde das Überzeugungssystem der Datenschutzbefürworter in einer Rede Anfang 2010 vom Leiter der niederländischen Datenschutzaufsichtsbehörde Jacob Kohnstamm auf den Punkt gebracht:

> *„I believe that to restore the balance […] in the European Data Protection field, data subjects should be more informed but carry a lesser burden, data controllers should take up their responsibility and be more accountable*

299 Erwähnenswert ist beispielsweise der inhaltliche Umschwung im Vertrauensargument, das vom EDSB vollzogen wurde, indem Vertrauen nicht nur als wirtschaftspolitisch, sondern in einem breiteren Sinne als gesellschaftlich relevant geframed wurde: „However, a strong framework for data protection also serves wider public and private interests in an information society with ubiquitous data processing. Data protection fosters trust, and trust is an essential component of the well functioning of our society. It is essential that arrangements for data protection are construed in a way that they - as much as possible - actively support rather than hamper other legitimate rights and interests. […] Important examples of other legitimate interests are a strong European economy, the security of individuals, as well as the accountability of governments." (EDPS 2011, 6)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

and Data Protection Authorities should have more powers to make sure the law will be abided by." (Kohnstamm 2010, 6)

Und auch der EDPS hob die Bedeutung der Pflichten der Verantwortlichen hervor:

„An information society where abundant amounts of information about everyone are being processed needs to be built on the concept of control by the individual, in order to allow him or her to act as an individual and to use his freedoms in a democratic society such as the freedoms of expression and speech. […] Furthermore, it is difficult to imagine control of the individual without obligations on controllers to limit processing in accordance with principles of necessity, proportionality and purpose limitation." (EDPS 2011, 8)

Sekundärüberzeugungen

Während viele Forderungen in der Orientierungsphase noch ohne Begründung gestellt wurden, begründeten die Akteure ihre Forderungen in der Entwurfsphase deutlich ausführlicher. Von den 15 Akteuren, die der Koalition der Datenschutzbefürworter zugehörig waren, forderten jeweils 12 Akteure die Stärkung der Einwilligung, die Verbesserung der Vorgaben zur Transparenz und die Einführung von Privacy by Design-Vorgaben. Im Hinblick auf die Einwilligung kritisierten die Datenschutzbefürworter insbesondere die divergierende Umsetzung der Richtlinienvorgaben und die daraus resultierende Untergrabung der Einwilligung. So erforderte das Datenschutzrecht einiger Mitgliedstaaten (Portugal, Spanien und Schweden) die Einwilligung *ohne jeden Zweifel*, in Luxemburg war zusätzlich auch die *ausdrückliche* Einwilligung erforderlich während die britische Datenschutzaufsichtsbehörde in ihren Orientierungshilfen die *abgeleitete* bzw. *implizite* Einwilligung nahe legte (Korff und Brown 2010, 37 f.). Viele Datenverarbeiter hatten sich daher insbesondere auf die letztere Variante gestützt und beispielsweise sowohl das Aufrufen einer Webseite als auch das Nicht-Handeln von Betroffenen als Einwilligung interpretiert, sofern dies aus der Perspektive des Datenverarbeiters als dem Kontext angemessen erschien (beispielsweise, wenn eine von Verarbeiter-Seite aus bereits vorbelegte Box nicht vom Betroffenen geändert wurde). Im Ergebnis hatten viele Datenverarbeiter auf die abgeleitete Einwilligung gesetzt, da sie auf diese Weise am einfachsten an personenbezogene Daten gelangen konnten. Die Datenschutzbefürworter sahen in dieser Form der abgeleiteten Einwilligung jedoch eine Untergrabung der Richtlinienvorgaben, da sie

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

eine zentrale Transparenzanforderung, nämlich die Willensbekundung *in Kenntnis der Sachlage (Art. 2 h DS-RL)*, als in vielen Fällen nicht erfüllt ansahen. Entsprechend wurden sowohl ganz allgemein die Stärkung der Einwilligung (vgl. BEUC 2011, 9 f.) als auch die Ausweitung der ausdrücklichen Einwilligung, die im Rahmen der DS-RL ausschließlich für besondere Kategorien personenbezogener Daten vorgesehen war, auf die Verarbeitung aller personenbezogenen Daten gefordert (vgl. EDPS 2011, 17 f.). Damit zusammenhängend wurde die Bereitstellung der zur Gewährleistung einer transparenten Datenverarbeitung erforderlichen Informationen kritisiert. Statt einer präzisen und kurzen Zusammenfassung beispielsweise darüber, ob preisgegebene personenbezogene Daten weiterverkauft, zu welchen Zwecken sie verarbeitet und wie lange sie gespeichert werden, würden Verarbeiter auf Datenschutzerklärungen setzen, die komplex und juristisch formuliert, also für viele Menschen schwer verständlich seien. Im Ergebnis würden die meisten Betroffenen diese Erklärungen nicht lesen, sodass die Ausübung ihrer Datenschutzrechte beeinträchtigt werde. Als Lösungsvorschlag wurden unter anderem die von der Kommission vorgeschlagenen Standard-Datenschutz-Erklärungen (standard privacy notices), bzw. die Spezifizierung der zur Verfügung zu stellenden Informationen aufgegriffen und unterstützt (BEUC 2011; vgl. Breyer 2011; PI 2011). Daneben wurde aber auch auf den zu dieser Zeit populärer werdenden Behavioural Economics (of Privacy)-Forschungszweig verwiesen, der die Grenzen der individuellen Aufnahmebereitschaft untersuchte und demonstrierte, dass Betroffene in der Regel eher dazu neigten, weder Datenschutzerklärungen zu lesen, noch die Standard-Konfiguration eines datenverarbeitenden Dienstes abzuändern, auch wenn diese den eigentlichen Datenschutzansprüchen der jeweiligen Betroffenen nicht entsprachen (BEUC 2011, 6; PI 2011, 5). Eine daraus resultierende Schlussfolgerung war die Forderung nach mehrschichtigen Datenschutz-Erklärungen, mit denen der Komplexität ausufernder Datenschutzerklärungen begegnet werden sollte (BEUC 2011, 6). Eine andere, von vielen Akteuren vertretene und weitaus zentralere Forderung war dagegen die nach Privacy by Design bzw. Privacy by Default. So wurde argumentiert, dass insbesondere mittels einer gesetzlichen Verpflichtung sowohl der Betreiber als auch der Hersteller datenverarbeitender Dienste bzw. Produkte zur Einhaltung von Privacy by Design bzw. Privacy by Default-Vorgaben für alle Betroffenen ein allgemeingültiges, hohes Datenschutzniveau sichergestellt werden könne. So sollten Produkte und Dienste bereits während ihrer Entwicklung dahingehend konfiguriert werden, dass sie die Grundsätze der Datenminimierung und Zweckbegrenzung einhalten, die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datensicherheit gewährleisten, und stets mit der im Hinblick auf die Verarbeitung personenbezogener Daten minimal invasiven Standard-Einstellung angeboten werden (BEUC 2011, 13; EDPS 2011, 23 f. PI 2011, 4, 9). Damit die Verarbeiter wiederum in die Lage versetzt werden, die datenschutzrechtlichen Probleme zu identifizieren, zu deren Lösung Privacy by Design- bzw. Privacy by Default-Maßnahmen umgesetzt werden, wurde (von 9 Akteuren) die Einführung verpflichtender Datenschutzfolgenabschätzungen vorgeschlagen (EDRi 2011b, 8). Einige Akteure (7) befürworteten daneben auch die Einführung EU-weit einheitlicher Zertifizierungssysteme und Datenschutz-Prüfsiegel. Der EDSB sah in dem Instrument einerseits eine Möglichkeit für Verarbeiter, die Einhaltung der Datenschutzgesetze nachzuweisen und auf diese Weise einen Wettbewerbsvorteil gegenüber anderen Anbietern zu erhalten und andererseits eine Erleichterung der Prüftätigkeit der Datenschutzaufsichtsbehörden (EDPS 2011, 24). BEUC sah in dem Instrument darüber hinaus auch die Möglichkeit der Kenntlichmachung von Produkten und Diensten, die nicht nur die ohnehin geltenden Gesetze einhalten, sondern ein Datenschutzniveau bieten, das über das gesetzlich vorgeschriebene Mindestmaß hinausgeht und die Betroffenen bei der Auswahl entsprechender Produkte unterstützt (BEUC 2011, 16). Einig waren sich die Datenschutzbefürworter auch dahingehend, dass die Zertifizierungen und Prüfsiegel seitens unabhängiger Zertifizierungsstellen festgelegten Gütekriterien und nicht auf Basis selbstregulatorischer Initiativen der Wirtschaft vergeben werden sollten (BEUC 2011, 16; EDPS 2011, 24). Skeptisch gegenüber dem Erfolg des Instruments, sofern es auf einem System kommerzieller Prüfsiegel basiert, zeigten sich EDRi und insbesondere Privacy International (EDRi 2011b, 8; PI 2011, 10).

Nur 4 Akteure aus der Koalition der Datenschutzbefürworter äußerten sich im Hinblick auf die von der Wirtschaft stark befürwortete Ausweitung der Selbstregulierung in Form der Spezifizierung der datenschutzrechtlichen Vorgaben mittels Codes of Conducts bzw. Verhaltensregeln. Kritisch wurde auf vergangene Initiativen der Selbstregulierung verwiesen, die datenschutzrechtlichen Ansprüchen nicht genügt hätten.[300] Entsprechend wurden derartige Maßnahmen abgelehnt bzw. nur unter der Bedingung

300 Verwiesen wurde in diesem Zusammenhang insbesondere (vgl. BEUC 2011, 15 f. PI 2011, 9 f.) auf die Selbstregulierungsinitiative der European Advertising Standards Alliance (EASA), zu der u. a. die IAB, WFA, FEDMA und weitere Akteure zählten, die in einer späteren Stellungnahme der Art. 29-Datenschutzgruppe für nicht-konform mit den Vorgaben der ePrivacy-Richtlinie befunden wurde (Artikel 29-Datenschutzgruppe 2011).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

begrüßt, dass sie einen datenschutzrechtlichen Mehrwert böten, durch alle in einem Wirtschaftssektor tätigen Unternehmen angewendet und durch die zuständigen Datenschutzaufsichtsbehörden genehmigt würden (BEUC 2011, 15 f. EDRi 2011b, 9; PI 2011, 9 f.).

Schließlich wurde (von 9 Akteuren) mittels der Forderung nach der Einführung einer Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten intendiert, dass eine zentrale und kompetente[301] Stelle innerhalb datenverarbeitender Organisationen für die Umsetzung der Maßnahmen eingerichtet wird, die von dem jeweiligen Verarbeiter zur Einhaltung der Datenschutzgesetze praktiziert werden (BEUC 2011, 15; EDRi 2011b, 8). Die grundlegende Idee, dass die Betroffenen beim Schutz ihrer Privatheit möglichst entlastet werden, spiegelt sich auch in weiteren Forderungen der Datenschutzbefürworter wieder. So wurde seitens einiger Akteure die Stärkung des Grundsatzes der Datensparsamkeit (bzw. Datenminimierung bzw. Datenvermeidung) gefordert, um auf regulatorischem Wege eine Begrenzung der von einem Anbieter erhobenen Daten zu erreichen, die unabhängig von der dabei einzuholenden Einwilligung wirkt (BEUC 2011, 7; EDRi 2011b, 7 f. VZBV 2011, 6). Im selben Zusammenhang bemängelte BEUC zudem die unbegrenzte Speicherung einmal erhobener personenbezogener Daten, da diese den Ansprüchen der Datenminimierung und Zweckbestimmung nicht genüge (BEUC 2011, 7). Schließlich wurde im Zusammenhang mit der Verantwortung der Datenverarbeiter auch das von diesen betriebene Profiling problematisiert, allerdings legten vor allem die VZBV sowie die deutschen Datenschutzaufsichtsbehörden konkrete Vorschläge vor, wonach die Erstellung von Profiling unter dem Einwilligungsvorbehalt verboten werden (VZBV 2011, 2 f.) bzw. alternativ nur auf Basis einer konkreten gesetzlichen Grundlage zulässig sein sollte (BfDI 2011, 3 f., Rn. 3-5). Eine weitere Reihe an Vorschlägen (von 9 Akteuren) befasste sich mit dem Schutz der personenbezogenen Daten von Kindern bzw. Minderjährigen. In diesem Zusammenhang wurden verschiedene, querschnittsartig mehrere datenschutzrechtliche Aspekte betreffende Sonderregelungen im Hinblick auf den Datenschutz bei Kindern gefordert, darunter ein ausnahmsloses Profiling-Verbot, die Anpassung bei der Erhebung personenbezogener Daten darzustellender Informationen an die Auf-

301 Auf den Aspekt der Kompetenz hob insbesondere BEUC ab, indem auf die Eurobarometer-Studie aus dem Jahr 2008 verwiesen wurde, in deren Rahmen nur 13% der innerhalb einer Organisation für den Datenschutz zuständigen Personen ihr eigenes Wissensniveau über das Datenschutzrecht als *vertraut* bezeichnet hatten (BEUC 2011, 15).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nahmefähigkeit von Kindern, die Pflicht zur Einholung der Einwilligung bei Kindern unter einer festzulegenden Altersgrenze von deren Erziehungsberechtigten, aber auch das Verbot der Erhebung bestimmter Daten-Kategorien, selbst im Falle des Vorliegens einer Einwilligung (BEUC 2011, 6 f. EDPS 2011, 19 f. Rn. 92-94; VZBV 2011, 4)

Mit einer Reihe weiterer, begleitender Maßnahmen, sollte schließlich die Durchsetzung der Datenschutzregeln sichergestellt werden. Dazu sahen die Vorschläge der Datenschutzbefürworter die Stärkung der Datenschutzaufsichtsbehörden (9 Akteure) sowie der Art. 29-Datenschutzgruppe (7 Akteure) vor. Die Ausweitung von deren Aufgaben und Befugnissen sollte schließlich (gefordert von 7 Akteuren) durch die EU-weite Vereinheitlichung und deutliche Erhöhung der Sanktionen, die im Falle von Regelübertritten seitens der Datenschutzaufsichtsbehörden verhängt werden können, flankiert werden (EDPS 2011, 13; EDRi 2011b, 16; VZBV 2011, 8).

Neben diesen, die Verantwortlichen unmittelbar betreffenden Maßnahmen sollte schließlich mittels Präzisierungen im Bereich des räumlichen Anwendungsbereichs (gefordert von 9 Akteuren) und bei der Übermittlung personenbezogener Daten in Nicht-EU-Staaten (gefordert von 9 Akteuren) sichergestellt werden, dass das EU-Datenschutzrecht nicht umgangen wird, indem die Verarbeitung bzw. die personenbezogenen Daten unter Ausnutzung von Regelungslücken in Datenoasen ausgelagert werden. Als Regelungslücken oder zumindest als nicht ausreichend präzise wurden auch die Richtlinienbestimmungen zum Begriff personenbezogener Daten und zu besonderen Kategorien personenbezogener Daten angesehen. Im Hinblick auf den Begriff personenbezogener Daten traten die Datenschutzbefürworter für die Ausweitung der Definition ein, die insbesondere IP-Adressen miteinschließt (EDRi 2011b, 5; PI 2011, 4). Seitens der VZBV wurde auch darauf verwiesen, dass Daten, die alleine keinen Personenbezug haben, durch die Kombination mit weiteren Daten, insbesondere im Rahmen einer Profilbildung, zu personenbezogenen Daten werden können und dass dies bei der Aktualisierung der Definition berücksichtigt werden sollte (VZBV 2011, 2 f.). Im Hinblick auf besondere Kategorien personenbezogener Daten verwiesen die Datenschutzbefürworter darauf, dass die technologische Entwicklung voraussichtlich neue besonders schützenswerte Datenarten herausbilden werde, und dass deshalb der Katalog zwar zunächst insbesondere um genetische Daten erweitert werden, jedoch grundsätzlich offenbleiben sollte, um auch neu entstehende besondere Datenkategorien als solche behandeln zu können (BfDI 2011, 5 f. PI 2011, 7 f.). Einen Schritt weiter ging der Vorschlag von Privacy International: Ausgehend von der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Erkenntnis, dass abhängig vom Kontext oder in Kombination mit weiteren Daten auch nicht-sensible Daten durchaus zu sensiblen Daten werden bzw. für diskriminierende Zwecke genutzt werden könnten, wurde gefordert, dass die Regulierung ganz grundsätzlich Abstand vom Konzept besonderer Kategorien personenbezogener Daten nimmt, und alle personenbezogen Daten mit demselben hohen Schutzniveau ausstattet (PI 2011, 7).

Neben der Schaffung eines Standard-Datenschutzniveaus durch die Ausweitung der Verarbeiterpflichten wurde gleichzeitig aber auch angestrebt, die Stellung des Betroffenen durch Maßnahmen zu verbessern, die den individuellen Handlungsspielraum des Betroffenen erweitern sollten. Dazu wurde insbesondere (von 10 Akteuren) die Vereinheitlichung und Stärkung des Auskunftsrechts bzw. der Modalitäten zur Wahrnehmung der Betroffenenrechte gefordert: Darunter die unentgeltliche Ausübbarkeit des Auskunftsrechts (solange dieses Recht nicht missbraucht wird) und die Einführung verbindlicher Fristen, innerhalb derer ein Verantwortlicher dem Auskunftsersuchen entsprechen muss (BEUC 2011, 8). Seitens der VZBV wurde überdies auch gefordert, dass seitens des Verantwortlichen kein *Medienbruch* erzwungen werden darf, indem die Einwilligung zwar elektronisch eingeholt wird, ein Auskunftsanliegen usw. dagegen auf schriftlichem Wege erfolgen muss (VZBV 2011, 5 f.). Eine weitere prominente Forderung der Datenschutzbefürworter (die von 10 Akteuren vertreten wurde) war die Einführung einer horizontalen, also bei jeder Verarbeitung personenbezogener Daten geltenden, Verpflichtung der Hersteller zur Mittelung von Datenschutzverletzungen an die Datenschutzaufsichtsbehörden und die von der Verletzung Betroffenen (BEUC 2011, 7; EDPS 2011, 17; EDRi 2011b, 8 f. PI 2011, 6). Erwähnenswert in diesem Zusammenhang ist die von BEUC vertretene Position, dass die Mitteilung jeder Datenschutzverletzung zu einer Überbelastung der Betroffenen und damit zum Übersehen von ernsten Verletzungen führen könnte und dass deshalb die Datenschutzaufsichtsbehörden auf Basis gemeinsamer, EU-weit gültiger Handlungsorientierungen darüber entscheiden sollten, welche Verletzungen den Betroffenen mitgeteilt werden sollten (BEUC 2011, 7). Ebenfalls relevant ist auch ein Unterschied in der Intention, mit der die Mitteilung von Datenschutzverletzungen gefordert wurde. Während EDRi die Bedeutung der Mitteilung für die Individuen hervorhob, damit die Betroffenen Gegenmaßnahmen (Änderung von Passwörtern usw.) einleiten können (EDRi 2011b, 8 f.), verwies der Europäische Datenschutzbeauftragte auf drei gleichwertige Ziele. So diene die Mitteilung über das von EDRi hervorgehobene und

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

im Gesamtkonzept seitens der Kommission benannte *offensichtlichste* Ziel hinaus sowohl der Implementierung besserer Sicherheitsmaßnahmen seitens der Verantwortlichen, um künftige Verletzungen aus reputationsbezogenem Eigeninteresse zu vermeiden als auch als den Datenschutzaufsichtsbehörden im Hinblick auf die Identifikation möglicher Gesetzesübertreter (EDPS 2011, 17). Verbreitet war auch die (von 9 Akteuren vertretene) Forderung nach einem Recht auf Vergessenwerden für Datenverarbeitungen im Internet bzw. im Kontext sozialer Medien und des Cloud Computing. Allerdings waren die entsprechenden Forderungen teils eher vage gehalten (Datenschutzkommission 2010, 3; EDRi 2011b, 8; PI 2011, 6). Spezifischere Vorschläge kamen von Seiten des Europäischen Datenschutzbeauftragten und der VZBV. Demnach sollten in der Onlinewelt erhobene personenbezogene Daten grundsätzlich mit einem Verfallsdatum versehen werden, nach dessen Ablauf die Daten ohne weiteres Zutun des Betroffenen automatisch gelöscht werden (EDPS 2011, 18 f. VZBV 2011, 6) oder der Betroffene aktiv und freiwillig dem Aufschub der Löschung zustimmen kann (VZBV 2011, 6). Im Zusammenhang mit dem Recht auf Vergessenwerden bzw. im Kontext der datenschutzrechtlichen Herausforderungen einiger Dienste der Informationsgesellschaft (allen voran Soziale Netzwerke, aber auch sonstige Online-Plattformen zum Hochladen von Bildern, Videos oder E-Mails) forderten einige (6) Akteure zudem die Einführung eines Rechts auf Datenportabilität. So bemängelten die Datenschutzbefürworter, dass die Möglichkeiten der Betroffenen, die von ihnen auf einer Plattform selbst hochgeladenen personenbezogenen Daten auf eine andere Plattform zu übertragen seitens der Verantwortlichen eingeschränkt würden. Mit dem Recht auf Datenportabilität wurde intendiert, den Transfer selbst zur Verfügung gestellter personenbezogener Daten zu erleichtern, indem die Verantwortlichen dazu verpflichtet werden, den Betroffenen Zugang zu den entsprechenden Daten zu gewähren, diese in einem interoperablen Format bereitzustellen, das für einen Anbieterwechsel geeignet ist und die entsprechenden Daten, nachdem sie auf die neue Plattform transferiert wurden, auf der alten Plattform zu löschen (BEUC 2011, 8 f. EDPS 2011, 18 f. VZBV 2011, 6). Schließlich wurde vonseiten der Datenschutzbefürworter (6 Akteure) die Einführung von Mechanismen für kollektive Rechtsbehelfe gefordert. Gefordert wurde insbesondere die Einführung eines Verbandsklagerechts (Breyer 2011; PI 2011, 8). Einige Akteure nannten aber auch

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

explizit bzw. implizit[302] das Recht auf Sammelklagen (BEUC 2011, 11 f. VZBV 2011, 8). Als Gründe gaben die Akteure die Schwierigkeiten an, denen sich individuell agierende Klägerinnen und Kläger gegenübersahen. Im Einzelnen wurden die Länge der Prozessdauer, die Kosten, rechtliche Unsicherheiten (BEUC 2011, 11 f.) und die Umsetzung eines Urteils im Falle eines Klageerfolgs lediglich für den jeweiligen Klagenden und nicht für alle Betroffenen genannt (Breyer 2011).

Item	Code
B1 Techn. Wandel birgt vor allem Herausforderungen, die eingehegt werden müssen	5
B2 Für ausschließliche staatliche Aktivität	5
B3 Umfassende Regulierung (hard regulation), die wenig Raum für Selbstregulierung lässt	5
C1C Für eine starke Ausweitung der Definition personenbezogener Daten	5
C 2 C Für die Stärkung des Grundsatzes der Datenminimierung	4
C3D Für die Stärkung der Einwilligung	4
C 4 A Besondere Kategorien personenbezogener Daten	5
C 4 D Für starke Regelungen zum Datenschutz bei Kindern	5
C5A 4 Für eine Stärkung der gesetzlichen Transparenz-Vorschriften	4
C5C Für eine Verbesserung des Auskunftsrechts d. Betroffenen bzw. der Informationspflicht d. Verantwortlichen	4
C 5 E Für die Einführung eines Rechts auf Vergessenwerden	4
C 5 G Für die Einführung eines Recht auf Datenportabilität, welches den Verarbeitern weitreichende Vorgaben macht	5
C 5 L Für die Benachrichtigung im Falle einer Datenschutzverletzung	4
C 6 B Für die Einführung einer verbindlichen Privacy by Design-Vorschrift für alle Betreiber und Hersteller	5
C 6 C Für die Beibehaltung der Meldepflicht, bzw. umfangreicher Dokumentationspflichten des Verarbeiters	4
C 6 N Für die Einführung einer stark verbindlichen Rechenschaftspflicht	5
C 7 Für die konsequentere Durchsetzung des Datenschutzes bei Drittstaatentransfers	4
C 13 A Für die Ausarbeitung von Verhaltensregeln auf Basis eines relativ verbindlichen Verfahrens	4
C 13 B Für Zertifizierungen auf Basis eines relativ verbindlichen Verfahrens	4
C 13 C Für die Einführung der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten	5

302 BEUC etwa sprach in ihrer Stellungnahme ganz allgemein von kollektiven Rechtsbehelfen, verwies darin (2011, 12) aber wiederum auf eine frühere Stellungnahme (BEUC 2008), in der sie für Sammelklagen eingetreten war.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Code
C 13 D Für die verbindliche Ausgestaltung einer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung in vielen Fällen	5
C 17 D Starke Befürwortung der Einführung eines Verbands- /Sammelklagerecht	5
C 17 E Für die deutliche Ausweitung der Regelungen zu Sanktionen und Geldbußen	5

Tabelle 4-22: Überblick der Überzeugungen der Datenschutzbefürworter-Koalition (eigene Erhebung bzw. Berechnung mit SPSS)

Item	DSGVO-E 2011	DSGVO-E 2012	BEUC	DSAB-AUT	DSAB-BEL	DSAB-GER alle	DSAB-LIE	EDRi	Patrick Breyer	PI	VZBV	Art. 29-Datenschutzgruppe	DG JUST	DSAB-CAN	EDPS	Europ. DSBeauftragte	EU-PARL	Häufigkeit d. Nennung
B1 Technologischer Wandel	5	4	5	4			4	5			4	5	5	4	5	5	4	11
B2 Staatl./Private Aktivität	5	5	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	15
B3 Policy-Orientierung im Falle staatlichen Handelns	5	5	5	5	4	5	4	4	5	4	5	5	4	4	5	5	4	15
B8 Globalisierung	5	4	5				4			5	4		5		5	5	4	8
B12 Reformwunsch			5	4	4	4	4	5		5		5				5		9
C 1 B Räuml. Anwendungsbereich	5	4	5	4		4		4		4	4		4		5		4	9
C 1 C Definition personenb. Daten	5	4	5		3			5	5	5	5							6
C 2 C Grundsatz der Datenminimierung	4	4	5		3		4			5				5		4	4	7
C 3 D Einwilligung	5	5	4	3	4		5	5	4	5	5	3	5		4		5	12
C 4 A Besondere Kategorien personenbezogener Daten	4	4	5	4	5	5	4			5	5						4	8
C 4 D Datenschutz bei Kindern	5	5	5	4	5		5	4		5	5				5		5	9
C 5 A Transparenz	4	4	5	4		4	4	5	4	5	5	3			5	4	5	12
C 5 C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	4	4	5	4		4		5	4	5	5				3	4	5	10
C 5 E Recht auf Vergessenwerden	5	4	5	3		4	4		5	4	5				4		5	9
C 5 G Recht auf Datenportabilität	5	5	5				4			4	5				4		5	6
C 5 I Automat. Verarbeitung / Profiling	5	4		4		5					5					4	4	5
C 5 L Benachrichtigung bei Datenschutzverletzungen	5	4	4	3			4	5	4	5	5		4		4		5	10
C 6 A Privacy by Default	4	4	5						5	5	5				5		5	6

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	DSGVO-E 2011	DSGVO-E 2012	BEUC	DSAB-AUT	DSAB-BEL	DSAB-GER alle	DSAB-LIE	EDRi	Patrick Breyer	PI	VZBV	Art. 29-Datenschutzgruppe	DG JUST	DSAB-CAN	EDPS	Europ. DSBeauftragte	EU-PARL	Häufigkeit d. Nennung
C 6 B Privacy by Design	4	4	5	4		4	4		5	5		5	5	5	5	5	5	12
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	4	4	4		4		3	2		4			3		4		3	8
C 6 N Rechenschaftspflicht	5	4	5											5	5	4	5	5
C 7 Übermittlung in Drittstaaten	4	4	4		4	3	4		5	5			4		4		5	9
C 10 D Technologieneutralität	3	3		5				5							5		4	4
C 13 A Verhaltensregeln	4	4	4					5		4							4	4
C 13 B Zertifizierungen/Gütesiegel	3	3	5	4		4		5		5					5		5	7
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	4	4	5	5	5	4	4	5					5		4		5	9
C 13 D Datenschutz-Folgenabschätzung	4	4	5	5	5		4						4	5	5	4	5	9
C 15 B Datenschutzbehörden	4	4	5	5		5	5	5		5		5			5		5	9
C 16 C Art. 29-Datenschutzgruppe	3	3	5		5		4			5		5			5		5	7
C 17 D Verbands- / Sammelklagerecht	4	4	5						5	5	5				5		4	6
C 17 E Sanktionen und Geldbußen	5	4	5				4	5		4	5				4		5	7

Tabelle 4-23: Positionierung der Datenschutzbefürworter zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung)

4.2.1.2.3 Ressourcen der Datenschutzbefürworter-Koalition während der Entwurfsphase

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die Advocacy-Community bzw. Koalition der Datenschutzbefürworter verfügte einen hohen Grad der Einbindung in politische Entscheidungsprozesse, da die für die Ausarbeitung des Datenschutzreformvorschlags zuständige GD JUST bzw. die zuständige Kommissarin Viviane Reding Teil der Advocacy-Koalition der Datenschutzbefürworter war. Erwähnenswert ist auch, dass das Europäische Parlament als Mitgesetzgeber in seiner Stellungnahme die volle Unterstützung für das Gesamtkonzept der Kommission

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zum Ausdruck brachte. Die Position des Ministerrats las sich im Vergleich zur Parlamentsentschließung deutlich zurückhaltender.

Unterstützung durch die Öffentliche Meinung

Wie insbesondere an den Ergebnissen der von der Kommission in Auftrag gegebenen Eurobarometer-Studie aus dem Jahr 2011 deutlich wird, blieb die konstante Befürwortung der EU-Bevölkerung für ein hohes Datenschutzniveau auch in der Entwurfsphase erhalten. Weiterhin äußerten sich viele EU-Bürgerinnen und –Bürger besorgt über die Zunahme von Diensten, die die Preisgabe personenbezogener Daten erfordern. Mit nur 22% brachten die Menschen dabei insbesondere Internet-Unternehmen nur sehr wenig Vertrauen beim Umgang mit personenbezogenen Daten entgegen, während beispielsweise medizinischen Einrichtungen mit 78% sehr viel Vertrauen entgegengebracht wurde. 70% der Befragten zeigten sich zudem besorgt darüber, dass ihre für legitime Zwecke bereitgestellten personenbezogenen Daten für illegitime andere Zwecke genutzt werden könnten (European Commission 2011b, 56 ff.). Weniger klar war hingegen der Wunsch nach einer Regulierung des Datenschutzes auf EU-Ebene: Nur eine relative Mehrheit von 44% war für die Regelung des Datenschutzes auf EU-Ebene, während 40% für nationale Regeln eintraten und weitere 10% regionale oder lokale Gesetze befürworteten (ebd., 184). Zudem demonstrierte die Eurobarometer-Studie auch weitgehende Unterstützung für verschiedene Datenschutz-Maßnahmen, die die Kommission einzuführen beabsichtigte: betriebliche Datenschutzbeauftragte (64% dafür), Sanktionen bei Datenschutzverletzungen (51%), Datenübertragbarkeit (71%), kostenfreie Inanspruchnahme des Auskunftsrechts (28%) (ebd.).

Informationen/Informationshoheit

Die Informationslage der Advocacy-Koalition bzw. Community der Datenschutzbefürworter blieb in der Entwurfsphase unverändert auf hohem Niveau.

Fähigkeit zur politischen Mobilisierung

Auch die Fähigkeit zur politischen Mobilisierung blieb unverändert. So war zwar eine gewisse Fähigkeit zur politischen Mobilisierung gegeben und stärker als bei den Flexibilitätsbefürwortern ausgeprägt, doch spielte diese Ressource in der Entwurfsphase noch keine Rolle.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Finanzielle Ressourcen

Durch die kommissionsinternen Umstrukturierungen (insb. die Schaffung des neuen Justiz-Kommissariats sowie des Generaldirektorats für Justiz) wurden die finanziellen Ressourcen der Advocacy-Koalition seit 2009 stetig ausgebaut und ermöglichten so die Finanzierung mehrerer wichtiger Studien und zahlreicher hochkarätig besuchter Konferenzen, in bzw. auf denen der Diskurs über die Datenschutzreform produktiv fortgesetzt wurde.

Das Vorhandensein einer fähigen Führung

In der Entwurfsphase machte sich das Eintreten Viviane Redings für die Datenschutzreform erstmals bemerkbar. Auf zahlreichen von der Kommission selbst organisierten Veranstaltungen als auch bei ihren öffentlichen Auftritten auf Stakeholder-Konferenzen warb Viviane Reding für die Datenschutzreform und trat durchgehend für die Stärkung des Datenschutzes ein. Redings sehr wohlwollende persönliche Einstellung gegenüber der grundrechtlichen Perspektive auf Datenschutz erklärt auch die intensiven Beziehungen, die die Kommission zu den übrigen Datenschutzbefürwortern unterhielt.

4.2.1.3 Flexibilitätsbefürworter

4.2.1.3.1 Zusammensetzung der Flexibilitätsbefürworter: Von der Advocacy-Community zur Advocacy-Koalition

Auch die Zusammensetzung der Flexibilitätsbefürworter blieb gegenüber der Orientierungsphase weitgehend unverändert. Weiterhin bestand die Community fast ausschließlich aus privatwirtschaftlichen Akteuren. Lediglich die britische Datenschutzaufsichtsbehörde ICO vertrat eine dermaßen wohlwollende Haltung gegenüber den Wünschen der Verantwortlichen, sodass sie als Teil der Community betrachtet werden kann. Bei den übrigen Akteuren war allerdings auch eine Intensivierung der Kooperationsstrukturen zu beobachten. Der deutlichste Ausdruck dessen war das erstmalige Erscheinen der *Industry Coalition for Data Protection* (ICDP) Ende 2011. Diese formelle Koalition vereinigte einige der bedeutendsten Akteure aus der datenverarbeitenden Privatwirtschaft unter einem Dach, darunter ACT, AmCham EU, BSA, Digitaleurope, Emota, EPC, EuroIspa, FEDMA, IAB, TechAmerica Europe sowie WFA, und reifte in der Folgezeit zum zentralen Akteur der Flexibilitätsbefürworter Advocacy-Community heran. Während

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

meiner Recherchen stieß ich schließlich auf ein Schaubild (Fiedler 2013b), welches das Problem des Astro-Turfing und versteckten Lobbyings vor Augen führte. EDRi hatte in dem Schaubild einige der größeren und bekannteren Mitglieder der ICDP aufgeführt. Es verdeutlichte, dass vor allem Microsoft und Intel, aber auch Google, Yahoo, eBay und Nokia Mitglied bei fast jedem der ICDP-Mitgliedsverbände (also von ACT, BSA, FEDMA, usw.) waren. Auf diese Weise konnten diese Unternehmen nicht nur in ihrem eigenen Namen lobbyieren, sondern zugleich auch unter Rückgriff auf multiple Verbände und Dachverbände. Um das weitere Ausmaß dieser Form des Lobbyings zu untersuchen führte ich schließlich eine Recherche durch, in der ich alle Mitgliedsunternehmen aller Verbände, die während der DSGVO-Verhandlungen aktiv und Teil meiner finalen DSGVO-Akteursliste waren, dahingehend untersuchte, ob dasselbe Unternehmen Mitglied bei multiplen Verbänden war.

Wie Abbildung 7 entnommen werden kann, zeigte sich, dass viele der Akteure über Netzwerkbeziehungen zueinander verfügten.

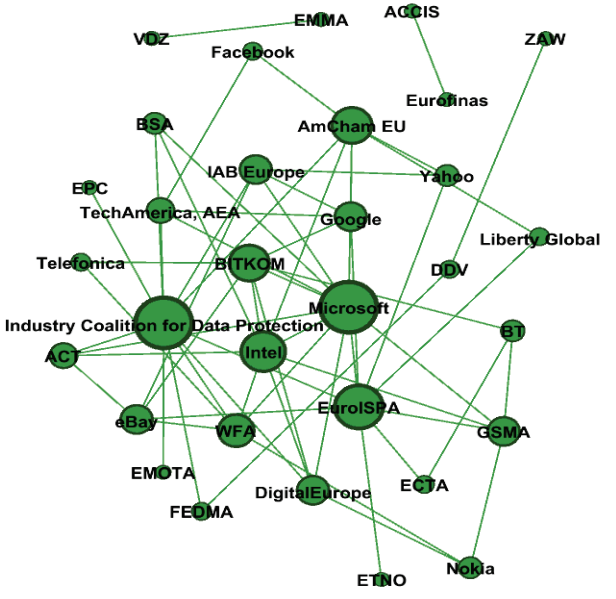

Abbildung 7: Netzwerk der Flexibilitätsbefürworter (eigene Darstellung und Berechnung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Da auf diese Weise einerseits konkrete Kooperationsstrukturen nachgewiesen werden konnten und zum anderen in Form der ICDP auch erstmals eine offizielle Koalition der Flexibilitätsbefürworter die datenschutzpolitische Bühne betrat, werte ich den Kooperationsgrad der beteiligten Akteure als nicht-trivial und betrachte alle genannten Akteure als Teil einer Advocacy-Koalition und nur die übrigen Akteure als Teil der Advocacy-Community.[303] Die genaue Zuordnung der jeweiligen Akteure kann Tabelle 4-24 entnommen werden.

303 So ist es zwar unüblich, dass jede Mitgliedsorganisation eines Verbands zu allen Verbandsaktvitäten aktiv beiträgt. Zugleich ist es aber umso üblicher, dass Organisationen, die ein essentielles Interesse an einem bestimmten politischen Thema haben, umso intensiver an den Verbandsaktivitäten zu dem jeweiligen Thema mitwirken (Reutter 2012, 25 ff.). Da ich nur die auf Basis des ACF-Relevanzkriteriums identifizierten Subsystem-Akteure auf ihre Verbandszugehörigkeit hin untersuchte, kann also davon ausgegangenen werden, dass diese in ausreichend nicht-trivialem Maße zur Entstehung der jeweiligen Verbandsposition beitrugen. Dies zeigte sich, nicht zuletzt, an den vielfachen inhaltlichen Überlappungen, die teils bis hinein in konkrete Formulierungen reichten (vgl. insb. Fn. 310).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Advocacy-Koalition	
Akteur	**Akteursgruppe**
ACCIS	Privatwirtschaft
ACT	Privatwirtschaft
AmCham EU	Privatwirtschaft
BITKOM	Privatwirtschaft
BSA	Privatwirtschaft
BT	Privatwirtschaft
DDV	Privatwirtschaft
DIGITALEUROPE	Privatwirtschaft
eBay	Privatwirtschaft
EMOTA	Privatwirtschaft
EPC	Privatwirtschaft
Eurofinas	Privatwirtschaft
EuroISPA	Privatwirtschaft
Facebook	Privatwirtschaft
FEDMA	Privatwirtschaft
GSMA	Privatwirtschaft
IAB Europe	Privatwirtschaft
Industry Coalition for DP	Privatwirtschaft
Intel	Privatwirtschaft
Liberty Global	Privatwirtschaft
Microsoft	Privatwirtschaft
Nokia	Privatwirtschaft
TechAmerica (formerly AeA)	Privatwirtschaft
Telefonica	Privatwirtschaft
WFA	Privatwirtschaft
Yahoo	Privatwirtschaft
ZAW	Privatwirtschaft

Advocacy-Community	
BDIU	Privatwirtschaft
EBF	Privatwirtschaft
ECTA	Privatwirtschaft
ENPA & FAEP	Privatwirtschaft
ETNO	Privatwirtschaft
FBF	Privatwirtschaft
GDV	Privatwirtschaft
ICC	Privatwirtschaft
ICO	Datenschutzbehörden
UEAPME	Privatwirtschaft
VDZ	Privatwirtschaft

Tabelle 4-24: Advocacy-Koalition sowie Advocacy-Community der Flexibilitätsbefürworter

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.2.1.3.2 Überzeugungssystem der Flexibilitätsbefürworter während der Entwurfsphase

Sowohl die Policy-Kernüberzeugungen als auch die Sekundärüberzeugungen der Flexibilitätsbefürworter blieben gegenüber der Orientierungsphase weitgehend stabil, während viele der zuvor unkonkret formulierten Position deutlich stärker spezifiziert wurden.

Item	Code
B1 Technologischer Wandel birgt Chancen und Risiken	3
B2 Eher für private anstelle von staatlicher Aktivität	2
B3 Eher für marktbasierte Lösungen	2
C1C Für ein kontextbezogenes Verständnis, das dem Verarbeiter die Entscheidung überlässt	2
C 2 C Für die Beibehaltung der Datenminimierung i. S. d. DS-RL	3
C3D Für flexible und kontextabhängige Einwilligungsregelungen	2
C 4 A Für einen engen Katalog besonderer Kategorien personenbezogener Daten	2
C 4 D Befürwortung des Datenschutzes bei Kindern unter Abwägung der Interessen der Verarbeiter	3
C5A Befürwortung von Transparenz bei gleichzeitiger Ablehnung verbindlicher Vorschriften	2
C5C Für die Beibehaltung der bestehenden, unverbindlichen Regelungen im Hinblick auf das Auskunftsrecht bzw. Informationspflichten des Verantwortlichen	3
C 5 E Eher gegen die Einführung eines Rechts auf Vergessenwerden	2
C 5 G Eher gegen die Einführung eines Rechts auf Datenportabilität	2
C 5 L Für flexible Benachrichtigungserfordernisse bei Datenschutzverletzungen	2
C 6 B Gegen verpflichtende Privacy by Design-Vorgaben	2
C 6 C Für die Abschaffung der Meldepflicht bzw. deutliche Vereinfachungen bei der Meldepflicht	2
C 6 N Für eine flexibel ausgestaltete Rechenschaftspflicht	2
C 7 Für vereinfachte Drittstaatentransfers	2
C 13 A Für die flexible Ausarbeitung von Verhaltensregeln	2
C 13 B Für flexible Verfahren zur Erteilung von Zertifizierungen bzw. Gütesiegeln	2
C 13 C Eher gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten	2
C 13 D Für die flexible Ausgestaltung einer möglichen Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung	2

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Code
C 17 D Gegen ein Verbands-/Sammelklagerecht, für flexible alternative Streitschlichtungsverfahren	2
C 17 E Für die Beibehaltung der bestehenden, unverbindlichen Regelungen zu Sanktionen und Geldbußen	2

Tabelle 4-25: Überblick der Überzeugungen der Flexibilitätsbefürworter (eigene Erhebung bzw. Berechnung mit SPSS)

Policy-Kernüberzeugungen

Die Policy-Kernüberzeugungen der Flexibilitätsbefürworter blieben im Vergleich zwischen der Orientierungs- und Entwurfsphase weitgehend unverändert. Weiterhin wurden zwar die Herausforderungen des technologischen Wandels (und in eingeschränkter Weise auch jene der Globalisierung) in gewissem Maße anerkannt. Letztendlich wurde jedoch auf die Potentiale und Chancen der technologischen Entwicklung verwiesen. Selten wurde dagegen die Überzeugung vertreten, dass Datenschutz als Grundrechtsschutz zu begreifen sei. Stattdessen wurde Datenschutz eher als vertrauensbildende Maßnahme dargestellt, die bedeutsam im Hinblick auf die Förderung der Nutzung datenverarbeitender Dienste sei. Stärker als während der ersten Phase pochten die Akteure dabei auf die wirtschaftliche bzw. wettbewerbspolitische und gesellschaftliche Bedeutung der Datenverarbeitung. Besonders anschaulich spiegelt sich das Überzeugungssystem der Flexibilisieurngsbefürworter in der Stellungnahme der ICDP wider:

> *„The revision of the EU legal framework on data protection provides for a great opportunity that will define the competitiveness of the European economy for years to come. We urge the European Commission to balance in a sensible manner the protection of individual rights with the functioning of the Single Market. The ability of the European Information Society to generate innovation and growth, as envisaged in the European Commission's Digital Agenda, depends on creating the necessary trust, but also in the continued use of all kinds of data that are at the heart of the digital economy. Overly strict and bureaucratic data protection rules will have a detrimental impact on Europe's digital economy." (ICDP 2011, 2)*

Nachdem mit der Veröffentlichung des Gesamtkonzepts zum Datenschutz klargeworden war, dass die Kommission in jedem Fall einen neuen Legislativvorschlag unterbreiten und nicht bloß kleinere Anpassungen an der DS-RL vornehmen würde, setzte die Community der Flexibilitätsbefürworter mehrheitlich darauf, den Reformprozess aktiv und konstruktiv zu begleiten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Freilich wurde in diesem Rahmen eine möglichst flexible Ausgestaltung des Reformvorschlags der Kommission befürwortet, indem die verpflichtenden Bestandteile des von der Kommission anvisierten neuen Legislativvorschlags abgelehnt und dafür Maßnahmen der Selbstregulierung in so gut wie allen Bereichen befürwortet wurden. Einig waren sich die Akteure der Flexibilitätsbefürworter weiterhin auch im Hinblick auf die Befürwortung der Harmonisierung der in den 27 EU-Mitgliedstaaten divergierenden Datenschutzvorschriften. Während die Mehrzahl der Akteure, die sich zu diesem Thema äußerten, der Reform des datenschutzrechtlichen Rahmens zwar verhalten, aber nicht ablehnend, gegenüberstanden, beharrten einige wenige Akteure auch weiterhin darauf, dass keinerlei Reformen nötig seien (vgl. Item B12 Reformwunsch in Tabelle 4-26).

Sekundärüberzeugungen

Weiterhin hielt die Community der Flexibilitätsbefürworter an der Befürwortung ihres Konzepts der Rechenschaftspflicht fest. Zwar wurden die während der Orientierungsphase seitens der Flexibilitätsbefürworter erhobenen Kernforderungen (die Reduktion bzw. Abschaffung der Meldepflicht, die Vereinfachung von Drittstaatentransfers und die Förderung von Selbstregulierungsmaßnahmen) erneuert, doch widmeten sich die in die Entwurfsphase eingebrachten Stellungnahmen insbesondere der Ablehnung bzw. Schwächung ausnahmslos aller von der Kommission zur Stärkung des Datenschutzes angekündigten Maßnahmen. Insbesondere die unmissverständliche Ankündigung der Kommission, dass die angestrebten verwaltungstechnischen Erleichterungen nicht zu weniger Verantwortung für die Verantwortlichen führen würden, wurde dabei durchweg abgelehnt.[304] Viele der Akteure forderten in diesem Zusammenhang den Umstieg von einem sog. *verfahrensorientierten* Datenschutz-System zu einem

304 So lautete etwa der Einwand der BSA: "*Others, however, see an accountability principle as imposing additional requirements on data controllers to demonstrate compliance with data protection rules.* While much would depend on the specifics of any such proposal, we are concerned that increasing the administrative obligations of data controllers would prove to be a costly exercise that would simply create more boxes for controllers to tick without meaningfully enhancing the protection of individuals' private data. BSA would have significant concerns with this approach (BSA 2011, 11, Hervorhebung im Original)."

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sog. *ergebnisorientierten* Datenschutz-System.[305] Insbesondere ging es den datenverarbeitenden Akteuren darum, datenschutzrechtliche Vorschriften zu reduzieren und die Wahl der zum Schutz personenbezogener Daten notwendigen Maßnahmen möglichst weitgehend den jeweils verantwortlichen Organisationen zu überlassen. Begründet wurde diese Forderung mit dem Argument, dass zu detaillierte datenschutzrechtlichen Vorschriften dazu neigten, wirkungslos im Hinblick auf den Schutz personenbezogener Daten zu sein:

> *"In an ex post system, organisations (public and private) are accountable for their handling of data, wherever that data travels instead of merely seeking legal compliance. It is, however, broader than only focusing on increasing the data controllers' responsibility, as mentioned in the European Commission's Communication of November 2010. It is a concept that underpins the entire legal framework, on how we look at data protection, on how we enforce and supervise it. An optimised legal framework should encourage and give incentives to organisations to be accountable; to have as a recognised corporate objective the protection of the rights of individuals, while at the same time seeking and obtaining legal compliance. This will enable data protection to become a proactive part of their business instead of a reactive compliance function. Accountability and ex post controls does not mean adding individual new obligations on top of already prescriptive rules, but instead that this term needs to offer a more flexible and effective alternative to the proliferation of complex and potentially conflicting obligations." (ICDP 2011, 8)*[306]

Verknüpft wurde dieses Argument auch weiterhin mit der Forderung nach der verstärkten Beachtung des jeweiligen Kontexts, in dem personenbezogene Daten verarbeitet werden. Auf das Kontext-Argument wurde insbesondere im Rahmen der Zurückweisung der von der Kommission angekündigten Vorgaben zur Transparenz, Einwilligung, Definition personenbezogener Daten, Privacy by Design und DSFA zurückgegriffen. Weiterhin vertraten fast alle Akteure (32) der Flexibilitätsbefürworter-Advocacy-Koalition die Position, dass der Herstellung von Transparenz im Zusammenhang

305 Im englischsprachigen Original beispielsweise: „AmCham calls for the regulatory framework to move from a procedure-based regime to a results-based legal system." (AmCham EU 2011, 15)

306 Näher als in diesem Zitat begründet, wurde die Kritik, dass das verfahrensorientierte Datenschutz-System wirkungslos sei, jedoch nicht.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

mit der Verarbeitung personenbezogener Daten zwar eine zentrale Rolle zukommt, detaillierte staatliche Transparenzvorschriften allerdings nicht hilfreich seien. Insofern wurde die Einführung des von der Kommission angekündigten, allgemeinen Transparenzgrundsatzes begrüßt.[307] Abgelehnt wurden dagegen die Kommissionspläne, die Art der zur Verfügung zu stellenden Information und insbesondere die Modalitäten der Bereitstellung dieser Informationen genauer festzulegen (AmCham EU 2011, 29; DIGITALEUROPE 2011, 32; Telefónica 2011, 4). Begründet wurde die Ablehnung detaillierter Transparenzvorgaben einerseits damit, dass diese im Hinblick auf das Ziel der Herstellung von Transparenz wirkungslos seien, wenn sie nicht die kontextspezifischen Bedingungen auf angemessene Weise berücksichtigten. Im Ergebnis würden Betroffene vielfach überfordert und die dargebotenen Informationen von diesen letztlich nicht zur Kenntnis genommen (BITKOM 2011, 2 f.). Andererseits stellten detaillierte gesetzliche Anforderungen auch eine Belastung der Verantwortlichen dar, da sie den zur bestmöglichen Darstellung der erforderlichen Informationen benötigten Freiraum bzw. Kreativität verlören (AmCham EU 2011, 28 f.). Das einzige Beispiel, das in diesem Kontext seitens der Flexibilitätsbefürworter im Hinblick auf die erfolgreiche Gewährleistung von Transparenz mittels Selbstregulierung genannt wurde, waren die seitens der Datenschutzbefürworter massiv kritisierten und von der Datenschutzgruppe nur wenig später für nicht-konform mit den Vorgaben der ePrivacy-Richtlinie befundenen (vgl. Fn. 300) Transparenzvorgaben der EASA (AmCham EU 2011, 20; ICDP 2011, 7).

Während das Thema Einwilligung in der Orientierungsphase noch nicht von großer Bedeutung war, reagierte ein Großteil (29) der Akteure der Flexibilitätsbefürworter auf die Ankündigung der Kommission, die Einwilligung stärken zu wollen. Die dabei seitens der Flexibilitätsbefürworter verfolgte Strategie strebte nach der Überwindung der Opt-in-/Opt-out-Dichotomie, indem auf die Bedeutung des Kontexts abgestellt wurde, in dessen Rahmen die Erteilung einer Einwilligung erfolgt. Kernelement der Argumentation war der Versuch, Opt-in-Verfahren als wirkungslos darzustellen, da diese einen spezifischen Mechanismus für Situationen vorschreiben würden, in denen – je nach spezifischem Kontext – andere Formen der Einholung der Einwilligung angemessener und wirkungsvoller seien.

307 Die Ausnahme bildeten insbesondere jene Akteure, die jegliche Änderungen an den Richtlinienvorgaben ablehnten (vgl. z. B. ACCIS IVZW 2011, 8).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Entsprechend wurde gefordert, die Entscheidung darüber, ob Opt-in- oder Opt-out-Verfahren zur Einholung der Einwilligung verwendet werden, vollständig den Unternehmen zu überlassen bzw. die Bestimmungen der geltenden DS-RL beizubehalten, da diese den nötigen Freiraum lieferten (AmCham EU 2011, 20; BITKOM 2011, 4; DIGITALEUROPE 2011, 11; NOKIA 2011, 8 f.).[308]

Daneben wurde auf das Kontext-Argument auch im Hinblick auf die Definition personenbezogener Daten zurückgegriffen. Als Grundlage für die Argumentation der Flexibilitätsbefürworter (22 Akteure) diente die Tendenz moderner Datenverarbeitungen Analysen eher auf Basis aggregierter Daten und nicht mittels unmittelbar personenbezogener Daten durchzuführen. Da das Ziel dieser Analysen die Unterscheidung zwischen anonymen Individuen sei (um beispielsweise die Kundenansprache oder die Produktpalette zu verbessern) und die dahinterstehenden natürlichen Personen nicht identifiziert würden, wurde gefordert, derartige Verarbeitungsweisen aus dem datenschutzrechtlichen Anwendungsbereich herauszunehmen. Demnach sollten Daten nur dann als personenbezogen angesehen werden, falls der Verarbeiter auch tatsächlich durch das Heranziehen weiterer Daten eine Identifizierung der natürlichen Person anstrebe. Falls der Verantwortliche die Identifizierung nicht anstrebe oder dazu nicht in der Lage sei, sollten die zur Debatte stehenden Daten nicht als personenbezogen gelten (ICDP 2011, 4 f.).

Auf ähnliche Weise wurden auch detaillierte Privacy by Design- bzw. Default-Vorgaben abgelehnt. Auf die grundsätzliche Begrüßung der Idee eines Privacy by Designs folgte (28 Akteure) die Kritik, dass es keinen Konsens über die Definition gäbe und daher keine Maßnahmen vorgeschlagen werden sollten, bevor alle Stakeholder sich einig über den Inhalt von Privacy by Design seien.[309] Begrüßt wurde Privacy by Design als Prozess bzw. als ein Aspekt der flexiblen Rechenschaftspflicht der Verantwortlichen.

308 Als einer der wenigen Akteure zeigte der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) eine konkrete mögliche Folge des vollständigen Umstiegs auf Opt-in-Verfahren auf. Da durchschnittlich nur 5% der Kundinnen und Kunden auf schriftlich-postalische Opt-in-Anfragen reagierten, wurden erhebliche Störungen des Geschäftsmodells befürchtet (GDV 2011, 11).

309 AmCham EU beispielsweise nahm durchaus zur Kenntnis, dass ein bestimmtes Privacy by Design-Verständnis in der Datenschutz-Community zu einem populären Konzept avanciert sei, verwies allerdings darauf, dass jenes Verständis nicht von allen Stakeholdern (gemeint waren die privatwirtschaftlichen Vertreter) geteilt würde (AmCham EU 2011, 17).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Demnach würde Privacy by Design bereits seitens vieler Organisationen regelmäßig praktisch angewendet, indem während der Entwicklungsphase neuer Dienste und Produkte unter Beachtung des spezifischen Datenverarbeitungskontexts auf den angemessenen Schutz personenbezogener Daten Rücksicht genommen werde. Vehement abgelehnt wurden dagegen jedwede technologiespezifischen Vorgaben im Hinblick auf Dienste und Produkte. Begründet wurde die Ablehnung sowohl mit der Wirkungslosigkeit detaillierter Vorgaben (NOKIA 2011, 18) als auch mit steigenden Kosten für in Entwicklung befindliche Dienste und Produkte, die zu einer Mehrbelastung von insb. KMUs führen und diese vom Markt drängen würden (AmCham EU 2011, 17; GDV 2011, 19; ICDP 2011, 9). Zwar äußerten sich nur wenige (6) Akteure zum Thema Privacy by Default, doch wurde diese Idee mit den soeben genannten Argumenten stets vollständig zurückgewiesen (ETNO 2011, 11; ICDP 2011, 9). Schließlich spielte das Thema Kontext auch bei der Reaktion auf die Ankündigung der Kommission, eine Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen durchzuführen, eine wichtige Rolle. Viele Akteure (20) wiesen darauf hin, dass Datenschutz- bzw. Privatheitsrisiken in Relation zu ihrem jeweiligen spezifischen Kontext und der jeweils genutzten spezifischen Technologie zu bewerten seien, und dass einheitliche gesetzliche Vorgaben die Kontexte nicht auf angemessene Weise berücksichtigen könnten. Überdies wurde darauf hingewiesen, dass kein Industriestandard zur Durchführung einer DSFA existiere, sodass der Erlass gesetzlicher Vorgaben lediglich der Einhaltung von Checklisten Vorschub leisten würde, ohne einen Nutzen im Hinblick auf verbesserten Datenschutz zu bieten (ebd.).[310] Daher wurden gesetzliche Vorgaben auch im Hinblick auf das DSFA-Instrument abgelehnt und stattdessen die möglichst flexible Ausgestaltung der gesetzlichen Vorgaben begrüßt (AmCham EU 2011, 18 f. DIGITALEUROPE 2011, 20; ICDP 2011, 8 f. NOKIA 2011, 18).[311]

310 Die schriftlichen Positionen von Nokia, Digitaleurope und der ICDP glichen sich nicht nur inhaltlich, sondern auch bis aufs Wort. In allen drei Stellungnahmen findet sich die folgende Passage: „Care must be taken, however, to avoid mandating a specific PIA template. Privacy risks are typically contextual and often technology specific. At present, a common and industry approved privacy threat identification model is missing. Without such a threat identification model a policy based PIA methodology runs the risk of being mere 'check list compliance'."(DIGITALEUROPE 2011, 20; ICDP 2011, 8 f. NOKIA 2011, 18)

311 Einige Akteure konnten sich mit einer DSFA-Verpflichtung in Fällen arrangieren, in denen *sehr sensible* personenbezogene Daten– ohne näher zu spezifizieren, was genau damit gemeint sein könnte – verarbeitet werden oder die zugrundeliegende Verarbeitung besondere Risiken beinhaltet (vgl. ACCIS IVZW 2011, 17).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Eine starke Ablehnung äußerten die Flexibilitätsbefürworter auch gegenüber der Ankündigung der Kommission, ein Recht auf Vergessenwerden einführen zu wollen. Das dabei verwendete Hauptargument war die Herausstellung von dessen Redundanz unter Verweis auf die bestehenden Regelungen der DS-RL. So ermögliche die Richtlinie sowohl die Löschung personenbezogener Daten in Art. 12 lit. b und c als auch die Begrenzung der Speicherdauer in Art. 6 (1) f. (AmCham EU 2011, 23 f. ICDP 2011, 11; Telefónica 2011, 5 f.). Entsprechend wurden möglicherweise bestehende Probleme auf die fehlerhafte und divergierende Umsetzung der Richtlinienvorgaben im mitgliedstaatlichen Recht zurückgeführt und die Verbesserung der Rechtsdurchsetzung und die EU-weite Harmonisierung der Vorgaben anstelle der Einführung neuer Vorgaben gefordert (AmCham EU 2011, 23 f. BITKOM 2011, 3). Überdies wurde auf einen Debattenstrang Bezug genommen, der sich in der Zwischenzeit insbesondere auf Ebene einiger Mitgliedstaaten entwickelt hatte und in dessen Rahmen die Schwierigkeit der Löschung von personenbezogenen Daten diskutiert wurde, die zwar zunächst von dem Nutzer eines sozialen Netzwerks geteilt, aber von anderen Nutzerinnen und Nutzern jener Plattform oder im Internet weiterverbreitet worden waren (ICC 2011, 5). Problematisiert wurde in diesem Zusammenhang insbesondere der – von der Community der Datenschutzbefürworter vollkommen unbeachtete – Aspekt, dass die konsequente Durchsetzung eines Rechts auf Vergessenwerden, das die Löschung nicht nur der vom jeweiligen Individuum selbst verbreiteten personenbezogenen Daten, sondern auch die seitens anderer Individuen und/oder Organisationen weiterverbreiteten personenbezogenen Daten desselben Menschen vorsieht, die Überwachung des gesamten Internets erfordern und folglich zu einer massenhaften Zensur des Internets führen würde (AmCham EU 2011, 23 f.). Teilweise äußerten die Stakeholder allerdings auch Verständnis für das Problem der Persistenz digital verbreiteter personenbezogener Daten im Internet und vor allem im Kontext sozialer Medien, das mit dem Recht auf Vergessenwerden adressiert werden sollte. Einige der Akteure – beispielsweise der GDV (2011, 9) und ACCIS (2011, 10) – lehnten ein solches Recht schließlich lediglich im Hinblick auf das eigene Operationsgebiet ab, konnten sich allerdings mit der Regulierung sozialer Netzwerke anfreunden. Die ICDP zeigte trotzdem Dialogbereitschaft im Hinblick auf die Probleme, deren Lösung mit dem Recht auf Vergessenwerden angestrebt wurde (ICDP 2011, 11). Einige Akteure stellten das adressierte Problem bzw. das Regulierungsziel allerdings auch vollständig infrage. Nokia beispielsweise

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

verwies – ohne eine Unterscheidung zwischen verschiedenen Anwendungs- oder Wirtschaftsbereichen zu machen – auf die Bedeutung der Speicherung personenbezogener Daten auch nach Beendigung einer Kundenbeziehung (NOKIA 2011, 9). AmCham dagegen kritisierte die Überlegungen hinsichtlich der Einführung eines automatischen Ablaufdatums für personenbezogene Daten unter Verweis auf die gesellschaftliche und wirtschaftliche Bedeutung der Zweitverwertung von Daten (AmCham EU 2011, 24 f.). Indem AmCham EU auf ein Zitat der Digitalkommissarin Neelie Kroes[312] verwies, wurde der Schutz personenbezogener Daten zudem als Sache des Individuums bezeichnet, die keiner besonderen rechtlichen Regelung bedürfe (ebd., 25). Schließlich verwiesen mehrere Akteure für den Fall der Verabschiedung eines Rechts auf Vergessenwerden auf die Notwendigkeit der Unterscheidung zwischen Daten, die von den Nutzenden selbst eingestellt wurden und Daten, die auf Basis der Analyse der von den Nutzenden eingestellten Daten vom Dienstebetreiber generiert wurden. Letztere Art von Daten sollte von einem Recht auf Vergessenwerden nicht betroffen sein (AmCham EU 2011, 24; ICDP 2011, 11) bzw. sollte jedwede diesbezügliche Verpflichtung möglichst geringe Kosten für die Verantwortlichen mit sich bringen (BSA 2011, 11).

Zum Vorschlag der Kommission hinsichtlich der Einführung eines Rechts auf Datenportabilität äußerte sich ebenfalls ein Großteil (25 an der Zahl) der an der Orientierungsphase beteiligten Akteure der Flexibilitätsbefürworter. Der Vorschlag stieß dabei durchweg auf Ablehnung seitens der Akteure. Einige Akteure machten den Vorschlag, derartige Fragen im Rahmen wettbewerbspolitischer Gesetzesvorhaben zu diskutieren, da die Reform des Datenschutzrechts nicht der richtige Ort dafür sei (DIGITALEUROPE 2011, 31; ICDP 2011, 11). Andere verwiesen darauf, dass die Möglichkeit des Transfers personenbezogener Daten seitens einiger Diensteanbieter bereits als Service angeboten werde, dass aber eine entsprechende gesetzliche Vorgabe Probleme schaffen würde, da die Gewährleistung der Interoperabilität abhängig von vielen verschiedenen Kontextbedingungen sei (BSA 2011, 11; Microsoft Corporation 2011, 11). Dementsprechend wurden gesetzliche Vorgaben zur Gewährleistung der Interoperabilität abgelehnt, da die Gefahr der Be- oder gar Verhinderung von Innovationen bestünde (BITKOM 2011, 4; BSA 2011, 11;

312 Diese hatte sich im Rahmen einer Rede zum Thema Cloud-Computing und Datenschutz folgendermaßen geäußert: „Just like in real life, when you present yourself on the net, you cannot assume no records exist of your past actions." (AmCham EU 2011, 25)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ETNO 2011, 7; ICC 2011, 5 f.). Unter Verweis auf die unbedingte Technologieneutralität und die horizontale Anwendbarkeit der datenschutzrechtlichen Vorgaben wurde auch der Anwendungsbereich des Rechts auf Datenportabilität infrage gestellt. Während klar sei, dass ein solches Recht auf den Online-Bereich abziele, erfordere die Technologieneutralität auch ihre Anwendung auf den offline-Bereich, die allerdings kaum umsetzbar sei (DIGITALEUROPE 2011, 31).[313] Weitere Kritiken bezogen sich sowohl auf das Recht auf Datenportabilität als auch auf das Recht auf Vergessenwerden: So wurde das Argument, dass nur jene vom Nutzenden selbst eingestellten Daten in den Anwendungsbereich eines solchen Rechts fallen sollten, auch im Falle der Datenportabilität geäußert, da andernfalls Wettbewerbsverzerrungen die Folge wären, wenn Konkurrenten über die Datenportabilität Zugriff auf Analyseergebnisse eines Diensteanbieters erhalten würden (AmCham EU 2011, 24; BSA 2011, 11; ICDP 2011, 11). Außerdem wurden beide Rechte auch unter Verweis auf Widersprüche zu bestehenden Gesetzen abgelehnt. Vielfach bestünden gesetzliche Vorgaben zur Vorhaltung von Kopien personenbezogener Daten für Abrechnungs- oder steuerrechtliche Zwecke. Ein Recht auf Datenportabilität bzw. Vergessenwerden schaffe unnötige Schwierigkeiten (ICDP 2011, 11).

Ein weiteres Thema, das bei den meisten Akteuren[314] der Flexibilitätsbefürworter auf Ablehnung stieß, war die Ankündigung der Kommission, die Einführung kollektiver Rechtsbehelfe in Form eines Verbandsklagerechts prüfen zu wollen. Der während der Orientierungsphase vielfach genannte Vorschlag nach der Einführung alternativer Streitschlichtungsverfahren wurde dagegen kaum mehr aufgegriffen (so allerdings z. B. seitens der GDV 2011, 15 f.), da sich die Beiträge meist mit der Ablehnung kollektiver Rechtsbehelfe beschäftigten. Wie bei den Reaktionen zu vielen anderen Vorschlägen auch, wurde statt der Einführung neuer Regeln auf die verbesserte Durchsetzung bzw. Harmonisierung der bestehenden Regeln verwiesen (AmCham EU 2011, 41 f. GSMA 2011, 14). Andere Akteure lehnten kollektive Rechtsbehelfe mit der Begründung ab, dass derartige Befugnisse ausschließlich bei den Datenschutzaufsichtsbehörden verbleiben sollten und dass eine sorgfältige Trennung der Aufgabenbereiche von Verbrau-

313 Unbenommen von derartigen Positionen, konnte sich beispielsweise der GDV mit der Einführung eines auf soziale Online-Netzwerke bezogenen Rechts auf Datenportabilität arrangieren (GDV 2011, 10)

314 Insgesamt äußerten sich 23 Akteure zu der Frage, 20 Akteure standen den Kommissionsvorschlägen ablehnend gegenüber, während 3 Akteure sich nicht klar oder abwägend positionierten (vgl. Tabelle 4-26).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

cherschutzorganisationen und Datenschutzaufsichtsbehörden gewährleistet bleiben sollte (BDZV und VDZ 2011, 8 f. BITKOM 2011, 5; DIGITALEUROPE 2011, 31). Als weiteres Argument diente der Verweis auf die Missbrauchsanfälligkeit kollektiver Rechtsbehelfe: Diese würden häufig nicht die wirklich *bösen* Akteure, die Datenschutzverletzungen bewusst begingen, sondern unbeabsichtigtes Fehlverhalten der guten Player bestrafen (BDZV und VDZ 2011, 8 f. ICC 2011, 6). Der KMU-Verband UEAPME befürchtete zudem, dass der Missbrauch kollektiver Rechtsbehelfe eine existentielle Bedrohung vor allem von KMUs darstellen würde (UEAPME 2011, 2 f.). Einige zentrale Beteiligte verwechselten allerdings die Ankündigung der Kommission, die Einführung eines Verbandsklagerecht überprüfen zu wollen mit der Prüfung der Einführung eines Sammelklagerechts. Sowohl die ICDP als auch die ICC und AmCham EU unterstellten dies der Kommission und verwiesen in ihrer Reaktion auf die negativen Erfahrungen, die in der Vergangenheit in den Vereinigten Staaten mit Sammelklagen gemacht worden seien (AmCham EU 2011, 41 f. ICC 2011, 6; ICDP 2011, 11 f.). Erwähnenswert ist zudem noch die Stellungnahme der ICDP: Während die Koalition bei anderen Themen stets auf die Vereinbarkeit der geplanten datenschutzrechtlichen Regelungen mit internationalen Rechtsnormen – womit wiederum zumeist die US-amerikanische Perspektive auf Datenschutz gemeint war – pochte, lehnte sie kollektive Rechtsbehelfe ausgerechnet unter Verweis auf die westeuropäische Rechtstradition ab, obwohl deren Einführung eine Annäherung an das US-System bedeutet hätte (ICDP 2011, 11 f.). Zudem drängten einige Akteure die Kommission darauf, keine für den Bereich des Datenschutzes spezifischen kollektiven Rechtsbehelfe zu formulieren, ohne den Abschluss der Debatte zu EU-weiten, kollektiven Rechtsbehelfen (vgl. Fn. 186) abzuwarten (AmCham EU 2011, 41 f. ICDP 2011, 11 f. NOKIA 2011, 12 f.).

Im Zusammenhang mit kollektiven Rechtsbehelfen äußerten sich vergleichsweise wenige (15) Akteure auch zu den Plänen der Kommission, die bestehenden Sanktionsregelungen im Falle ernster Datenschutzverletzungen zu verschärfen. Zwar gehört die Möglichkeit der Verhängung hoher und auch strafrechtlicher Sanktionen zu einem Kernbestandteil des von den Flexibilitätsbefürwortern unterstützten Ansatzes der Rechenschaftspflicht (N. Robinson u. a. 2009, 18), doch sprachen sich die Akteure trotzdem dagegen aus. Einige Akteure verwiesen in diesem Zusammenhang darauf, dass die Sanktionsregelungen bereits ausreichend seien (ACCIS IVZW 2011, 13; UEAPME 2011, 2 f.). Andere verwiesen auf die Notwendigkeit der EU-weiten Harmonisierung und Präzisierung der bestehenden

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Regelungen, die eine Erhöhung des Sanktionsniveaus überflüssig machen würden (AmCham EU 2011, 41; NOKIA 2011, 23). Digitaleurope (2011, 19) wandte sich explizit gegen die Einführung strafrechtlicher Sanktionen und Nokia (2011, 23) vertrat die Auffassung, dass nur tatsächlicher Schaden bei Individuen sanktioniert werden sollte, die Nichtbefolgung administrativer Vorgaben dagegen nicht. Die Telekommunikationsbranche äußerte auch in diesem Zusammenhang ihre Unzufriedenheit mit den sektorspezifischen Sanktionsregelungen der ePrivacy-RL, die strenger seien und eine Mehrbelastung für EU-Unternehmen darstellten und zu einem Wettbewerbsnachteil führten. Gefordert wurde daher auch für diesen Bereich die Angleichung der Wettbewerbsbedingungen (GSMA 2011, 14; Telefónica 2011, 8).

Starke Beachtung fanden auch die Themen Verhaltensregeln, Zertifizierungen, betriebliche Datenschutzbeauftragte sowie die Meldepflicht bei Datenschutzverletzungen. In besonderem Maße und seitens aller 26 Akteure, die sich zu diesem Thema äußerten, wurde die Ankündigung der Kommission, Initiativen zur Selbstregulierung verstärkt zu fördern und die Bestimmungen über die Erstellung von Verhaltensregeln zu verbessern, begrüßt. Begründet wurde dies damit, dass Verantwortliche durch die mit Selbstregulierung einhergehende Flexibilität deutlich schneller und effektiver auf gesellschaftspolitische und technische Entwicklungen reagieren könnten, als dies mittels gesetzlicher Vorgaben möglich sei (BDZV und VDZ 2011, 10; GDV 2011, 20 f. NOKIA 2011, 19 f. TechAmerica Europe 2011, 12). Auf diese Weise könnten Rechte besser gewährleistet werden und eine Kultur des Respekts für informationelle Privatheit geschaffen werden, in der *Transparenz, Kontrolle und die dynamischen Privatheitserwartungen* der Nutzenden insgesamt besser gewährleistet werden könnten (GSMA 2011, 9; Telefónica 2011, 12). Als Grund dafür, weshalb nicht stärker auf die bereits im Rahmen der DS-RL bestehende Möglichkeit zum Erlass von Verhaltensregeln zurückgegriffen worden war, wurde das komplizierte und zeitintensive Überprüfungs- und Genehmigungsverfahren der Art. 29-Datenschutzgruppe (NOKIA 2011, 19 f.) und die unzureichende EU-weite Harmonisierung der Regeln angeführt (AmCham EU 2011, 30). Entsprechend wurde vor allem eine Vereinfachung des Verfahrens befürwortet (IAB Europe 2011, 6; Microsoft Corporation 2011, 21 f.). Lediglich AmCham EU schlug vor, das auf der Überprüfung und Genehmigung seitens der Datenschutzaufsichtsbehörden beruhende Verfahren vollständig aufzugeben und die Aufgaben fortan an eine Kommissionsstelle oder neu zu gründende EU-Institution zu übertragen, die die Vorteile der Selbstregulierung zu schätzen wisse (AmCham EU 2011, 30). Einige Akteure forderten mehr Anreize zur Erarbeitung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

von Verhaltensregeln, spezifizierten allerdings nicht näher, was darunter zu verstehen sein könnte (Telefónica 2011, 12). Lediglich AmCham EU brachte in diesem Zusammenhang die Reduktion sonstiger – nicht näher spezifizierter – rechtlicher Pflichten für Unternehmen, die an genehmigten Selbstregulierungssystemen partizipieren, in die Diskussion (AmCham EU 2011, 30).

Während Verhaltensregeln durchweg als positiv begrüßt wurden, reagierten die Flexibilitätsbefürworter deutlich verhaltener auf die Ankündigung der Kommission, dass sie die Möglichkeit der Einführung von EU-Zertifizierungsregeln sondieren würde. Viele Akteure waren insbesondere besorgt darüber, dass die Kommission statt der Einführung einer Möglichkeit der Zertifizierung eine Zertifizierung*spflicht* für datenverarbeitende Dienste und Produkte einführen würde. Entsprechend ablehnend zeigten sich die Akteure gegenüber der Einführung einer solchen Pflicht (BSA 2011, 8 f. ICDP 2011, 12; Microsoft Corporation 2011, 11 f. UEAPME 2011, 3).[315] Als Gründe für die Ablehnung wurde vor allem auf die befürchteten Kosten verwiesen, die zugleich keinen echten Mehrwert im Hinblick auf einen verbesserten Schutz personenbezogener Daten böten (ACCIS IVZW 2011, 16; Microsoft Corporation 2011, 21).[316] Letztlich waren die Flexibilitätsbefürworter ablehnend gegenüber jeder Form von Zertifizierungen eingestellt, die nach der Kenntlichmachung bzw. Übervorteilung von Produkten und Diensten strebten, denen ein absolut festgelegtes Datenschutzniveau attestiert wurde. Der VDZ beispielsweise äußerte die Befürchtung, „dass die etwaige Einführung von EU-Zertifizierungsregeln nicht zu einer faktischen Zertifizierungspflicht für Unternehmen führt, wenn durch solche in der Öffentlichkeit der Eindruck entsteht, nur derart zertifizierte Verfahren, Technologien, Produkte oder Dienste seien datenschutzrechtlich unbedenklich." (BDZV und VDZ 2011, 10) Somit wurde seitens der Flexibilitätsbefürworter genau jene Differenzierung abgelehnt, die von den Datenschutzbefürwortern gefordert worden war, und die es Nutzerinnen und Nutzern ermöglichen sollte, zwischen Produkten mit einem hohen, mitt-

315 Weniger verbreitet war dagegen die beispielsweise von TechAmerica Europe (2011, 12) vertretene Sichtweise, dass Zertifizierungen generell unwirksam seien.

316 Die politische Debatte zum Datenschutz-Audit, die insb. im Rahmen der Reform des deutschen BDSG geführt worden war (Hornung und Hartl 2014), wurde dabei als Beispiel herangezogen, um die Unmöglichkeit der Verabschiedung einer effektiven Zertifizierungspflicht zu belegen (GDV 2011, 21; UEAPME 2011, 3)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

leren oder niedrigen Datenschutzniveau zu unterscheiden.[317] Stattdessen wurde von einer Mehrheit der Akteure gefordert, dass Zertifizierungen und Prüfsiegel freiwillig, bezahlbar,[318] technologieneutral[319] und vom Ansatz her nach weltweiter Gültigkeit streben und keine europäischen Sonderwege einschlagen sollten (AmCham EU 2011, 31; BSA 2011, 8 f. DIGITALEUROPE 2011, 22; ICC 2011, 7; ICDP 2011, 12; Microsoft Corporation 2011, 22). Zudem sei zu befürchten, dass Zertifizierungen auf Basis hoher Kosten vor allem zum Konkurrenzschutz großer und finanzkräftiger Unternehmen gegenüber kleinen und mittelständischen Unternehmen zu werden drohten, da sich diese aufwändige Zertifizierungen nicht leisten könnten (BDZV und VDZ 2011, 10). Nokia wies zudem darauf hin, dass die Kommission regulatorische Anreize für Zertifizierungen schaffen sollte (NOKIA 2011, 3). Überdies forderte der Konzern, dass Zertifizierungen nicht vonseiten der Datenschutzaufsichtsbehörden, sondern seitens unabhängiger Stellen erteilt werden sollten (ebd., 20). Als ein positives Beispiel für ein funktionierendes Zertifizierungssystem, das den genannten Anforderungen entspreche, nannten Nokia, Microsoft und die GSMA das vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein ULD ins Leben gerufene Europäische Datenschutz-Gütesiegel EuroPriSe (GSMA 2011, 9 f. Microsoft Corporation 2011, 9 f. NOKIA 2011, 19 f.)

Ein weiteres Thema, das von vielen (26) Flexibilitätsbefürwortern kommentiert wurde, war die Ankündigung der Kommission, die verpflichtende Benennung eines betrieblichen Datenschutzbeauftragten (bDSB) prüfen zu wollen. Ihren Policy-Kernüberzeugungen entsprechend traten die Akteure auch im Hinblick auf dieses Thema für die Aufweichung verbindlicher Vorgaben und deren Ersetzung durch flexible Vorgaben ein, die den Verant-

317 Lediglich die GSMA EU vertrat die Position, dass Zertifizierungen nützlich im Hinblick auf die Verbesserung des Verantwortungsbewusstseins von Unternehmen seien, insgesamt zu einem ausbalancierten Datenschutz beitragen und sowohl Regulierungsbehörden als auch den Nutzenden gegenüber als eine Form der unabhängigen Bestätigung der Einhaltung der Datenschutzgesetze dienen könnten (GSMA 2011, 9 f.).

318 Die Forderung nach Bezahlbarkeit bezog sich vor allem auf den für den Erhalt einer Zertifizierung benötigten bürokratischen und personellen Aufwand, den ein Verantwortlicher auf sich nehmen musste und nur in zweiter Linie auf die externe Kostendimension.

319 Mit der Forderung nach Technologieneutralität war in diesem Zusammenhang gemeint, dass ähnliche Dienste und Produkte anhand derselben Kriterien gemessen werden und etwaige Prüfungen und Zertifizierungsregeln keine Präferenz für bestimmte Technologien aussprechen sollten, da ansonsten Wettbewerbsschädigungen zu befürchten seien (Microsoft Corporation 2011, 22).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wortlichen einen möglichst großen Spielraum bei der Umsetzung der gesetzlichen Regelungen überlassen. So wurde die Maßnahme der Bestellung eines betrieblichen Datenschutzbeauftragten von allen Akteuren grundsätzlich für wirksam befunden. Allerdings wurde seitens fast aller Akteure zugleich, unter Verweis auf unterschiedliche Kontextbedingungen unter denen unterschiedliche Verantwortliche operieren müssten, gefordert, dass die finale Entscheidung über die Bestellung eines bDSB unter Einbeziehung aller relevanten Faktoren dem jeweiligen Verantwortlichen obliegen und nicht gesetzlich vorgeschrieben werden sollte (ACCIS IVZW 2011, 15; AmCham EU 2011, 16; BSA 2011, 7; DIGITALEUROPE 2011, 19; vgl. ICC 2011, 8; ICDP 2011, 7). Andernfalls sei zu befürchten, dass die Möglichkeit zur Bestellung nicht zu einer Erleichterung der regulatorischen Vorgaben, sondern zu ihrer weiteren Verkomplizierung führen (ETNO 2011, 10) und KMUs negativ belasten würde (IAB Europe 2011, 5). Eine Reihe weiterer Akteure begrüßte die Möglichkeit der freiwilligen Bestellung eines bDSB dagegen unter der Bedingung, dass dem Verantwortlichen Anreize – wie der in Deutschland praktizierte Wegfall der Meldepflicht – geboten werden (BITKOM 2011, 5; ETNO 2011, 10; GDV 2011, 18; ICDP 2011, 7). Eine prominente Forderung war zudem die Einführung der Möglichkeit, einen bDSB für eine ganze Unternehmensgruppe benennen zu können (AmCham EU 2011, 16; ETNO 2011, 10; NOKIA 2011, 19).

Das letzte, von der Mehrheit (24) der Flexibilitätsbefürworter diskutierte Thema war die von der Kommission angekündigte Einführung einer horizontalen, also auf jede Verarbeitung personenbezogener Daten anzuwendenden Meldepflicht bei Datenschutzverletzungen. Die Mehrheit der Akteure, die sich zum Thema äußerten, befürwortete die Einführung einer solchen Meldepflicht grundsätzlich, da Betroffene auf diese Weise in die Lage versetzt würden, Gegenmaßnahmen (Änderung von Passwörtern usw.) zu ergreifen, um die Risiken einer Verletzung zu minimieren.[320] Allerdings verwiesen die Akteure auf die Herausforderung der sog. *Over-Notification*, die zu bewälti-

320 Lediglich einige wenige Akteure äußerten sich ablehnend gegenüber einer Meldepflicht bei Datenschutzverletzungen. Die vehementeste Ablehnung äußerte der VDZ (2011, 6), unter Verweis darauf, dass der bestehende Rechtsrahmen bereits die sachgerechte und effektive Verfolgung und Ahndung von Verstößen gegen das Datenschutzrecht ermögliche. ACCIS (2011, 8), ACT (2011, 3) und BITKOM (2011, 2 f.) waren ebenfalls gegen die Regelung. Der KMU-Verband UEAPME (2011, 2) etwa begründete ihre Ablehnung ganz offen damit, dass die meisten KMU über eine Datenschutzverletzung in der Regel schlicht keine Kenntnis hätten und daher den rechtlichen Vorgaben auch nicht Folge leisten könnten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gen sei, damit die Meldepflicht auf Seiten der Betroffenen die gewünschte Wirkung zeitigt und zu keiner zu großen Belastung der Verantwortlichen führt. So wurde insbesondere befürchtet, dass eine zu hohe Zahl bzw. Frequenz an irrelevanten Meldungen auf Seiten der Betroffenen zu einer Desensibilisierung führen könnte, in deren Folge sie wichtige Meldungen ignorieren und überhaupt keine Gegenmaßnahmen treffen würden (AmCham EU 2011, 21; BSA 2011, 8; GDV 2011, 8; ICC 2011, 4 f. TechAmerica Europe 2011, 4). Während diese Befürchtung in der Regel nicht belegt wurde, verwies die ICC auf negative Erfahrungen, die bei der Umsetzung vergleichbarer Gesetze in den Vereinigten Staaten gemacht worden seien (ICC 2011, 4 f.). Im selben Zusammenhang wurde auch – aber deutlich seltener – auf die aus der Over-Notification resultierende Mehrbelastung, insb. kleinerer Unternehmen verwiesen (UEAPME 2011, 2). Zur Lösung des Over-Notification-Problems schlugen die Flexibilitätsbefürworter Änderungen am Konzept der Meldepflicht vor, so wie sie auch im Rahmen der Novelle der ePrivacy-RL verabschiedet worden war. Diese sah vor, dass eine Meldung an die Datenschutzbehörde in jedem Fall erfolgen musste und dass die Benachrichtigung der Betroffenen dann zu erfolgen hatte, wenn anzunehmen war, dass durch die Verletzung eine Beeinträchtigung der Privatsphäre die Folge sein würde (ePrivacy-RL Art. 4 Abs. 4). Die Änderungsvorschläge der Flexibilitätsbefürworter sahen dagegen vor, dass eine Meldung an den Betroffenen nur noch dann erfolgen sollte, wenn *schwerwiegende* Beeinträchtigungen der Privatheit in Folge einer Datenschutzverletzung drohten (AmCham EU 2011, 21; ICC 2011, 4 f. TechAmerica Europe 2011, 4).[321] Was unter einer *schwerwiegenden* Beeinträchtigung zu verstehen sei, blieb in der Regel offen. Lediglich Microsoft und TechAmerica Europe benannten als mögliche Risiken Identitätsdiebstahl, Betrug und körperliche Verletzung (Microsoft Corporation 2011, 8) bzw. finanzielle Folgen und Rufschädigung (TechAmerica Europe 2011, 3). Wenig beachtet blieb auch die Frage, welche Stelle die Entscheidung darüber fällen sollte, wann Betroffene zu benachrichtigen sind. Während der GDV die Datenschutzaufsichtsbehörden in dieser Rolle sah (GDV 2011, 8), war die Tendenz unter den übrigen Akteuren eher, dass die Entscheidung seitens der verantwortlichen Stelle getroffen werden sollte (vgl. insb. ICC 2011, 4 f.). Schließlich wurde gefordert, dass Betroffene nicht benachrichtigt werden sollten, falls der Verantwortliche durch geeignete technische Schutzmaßnah-

321 Das Konzept des „serious risk of harm" als Benachrichtigungsschwelle war in §42a der BDSG-Novelle von 2009, auf die mehrere Akteure direkt Bezug nahmen (GDV 2011, 8; Microsoft Corporation 2011, 8; NOKIA 2011, 11), festgelegt worden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

men (bspw. Verschlüsselung) sicherstellen konnte, dass keine schwerwiegende Beeinträchtigung der Betroffenen zu erwarten sei (AmCham EU 2011, 22; BSA 2011, 8; DIGITALEUROPE 2011, 33; Microsoft Corporation 2011, 7).[322] Überdies kritisierten einige Akteure, dass die Vorgaben der ePrivacy-RL den Mitgliedstaaten zu viel Raum bei der Umsetzung von Art. 4 Abs. 4 überließen, sodass die Mitgliedstaaten abweichende Vorgaben hinsichtlich der *Umstände unter denen die Benachrichtigung erforderlich ist, sowie bezüglich des Formates und der Verfahrensweise für die Benachrichtigung* verabschiedet hätten. Daher wurden EU-weit einheitliche Vorgaben zur Meldepflicht bei Datenschutzverletzungen begrüßt (ICC 2011, 5; Microsoft Corporation 2011, 9; TechAmerica Europe 2011, 3 f.).

Die Ankündigung der Kommission, das Marktortprinzip einzuführen, indem Präzisierungen bei den Vorschriften über das anwendbare Recht vorgenommen werden, die es erlauben, „den von der Verarbeitung Betroffenen in der EU unabhängig vom geografischen Standort des für die Verarbeitung Verantwortlichen stets ein gleiches Schutzniveau zu garantieren" (EK 2010, 12), stießen auf geteiltes Echo bei den 15 Flexibilitätsbefürwortern, die sich zu dem Thema äußerten. Während die europäischen Akteure die Einführung eines Marktortprinzips begrüßten, standen die US-amerikanischen bzw. US-amerikanisch dominierten internationalen Akteure dem Marktortprinzip stark ablehnend gegenüber. Die europäischen Anbieter verwiesen bei ihrer Unterstützung des Marktortprinzips auf die Angleichung der Wettbewerbsbedingungen. Unter den geltenden Vorgaben der DS-RL seien Anbieter, die zwar personenbezogene Daten von EU-Bürgerinnen und -Bürgern verarbeiteten, dabei allerdings auf Mittel zurückgriffen, die nicht im Hoheitsgebiet eines EU-Mitgliedstaates belegen waren, von der Pflicht zur Befolgung der DS-RL ausgenommen, sodass diese Anbieter einen Wettbewerbsvorteil gegenüber europäischen Konkurrenten erhielten (BITKOM 2011, 6; ECTA 2011, 5; ETNO 2011; GSMA 2011, 5; NOKIA 2011, 2; Telefónica 2011, 10 f. ZAW E.V. 2011, 9). Demgegenüber wandten die US-amerikanischen bzw. US-amerikanisch geprägten internationalen Akteure ein, dass die Einführung eines Marktortprinzips zur Doppelbelastung von Unternehmen führe, die somit der ständigen Gefahr der Befolgung unterschiedlicher Regelsets ausgesetzt würden (EMOTA 2011, 2;

322 Ausnahmen wurden auch für Fälle gefordert, in denen eine Offenlegung personenbezogener Daten sich innerhalb eines Unternehmens ereignet, wenn beispielsweise Mitarbeiter Fehler aufgrund fehlverstandener Unternehmenspolicies begingen (AmCham EU 2011, 22; BSA 2011, 8; TechAmerica Europe 2011, 4).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

vgl. IAB Europe 2011, 5). FEDMA beispielsweise malte das Szenario aus, dass ein Unternehmen in Folge der Einführung des Marktortprinzips die Vorgaben 27 unterschiedlicher Jurisdiktionen zu befolgen hätte (FEDMA 2011, 4 f.). Daher wurde gefordert, dass die Divergenz der mitgliedstaatlichen Vorgaben durch die vollständige Harmonisierung des Herkunftslandsprinzips angegangen werden sollte, sodass ein Unternehmen nicht mehr die Regeln mehrerer Jurisdiktionen befolgen bzw. nicht mehr verschiedenen Datenschutzaufsichtsbehörden unterstellt, sondern lediglich einer Behörde bzw. Jurisdiktion[323] gegenüber verantwortlich sein sollte (AmCham EU 2011, 11; eBay 2011, 6; IAB Europe 2011, 5; ICC 2011, 3; Microsoft Corporation 2011, 18; TechAmerica Europe 2011, 8 f.).[324] Auf das von den europäischen Anbietern angesprochene Problem der Nichtanwendbarkeit der EU-Regeln auf Anbieter, die weder einen Sitz in der EU haben, noch auf Mittel in der EU zurückgreifen, ging allerdings keiner der nichteuropäischen Akteure ein (ebd.).

Die Arbeit der Art. 29-Datenschutzgruppe wurde während der Entwurfsphase insgesamt etwas positiver als noch während der Orientierungsphase bewertet. Viele der 20 Beiträge zum Thema begannen mit dem Hinweis, dass die Arbeit der Datenschutzgruppe zur Präzisierung und harmonisierten Interpretation der Richtlinienvorgaben beigetragen hätte (AmCham EU 2011, 40 f. ETNO 2011, 10; GSMA 2011, 15; IAB Europe 2011, 6). Der Kern der Kritik an der Datenschutzgruppe blieb dagegen gleich: Weiterhin forderten so gut wie alle[325] Wirtschaftsvertreter mehr Transparenz und Konsultation bei der Ausarbeitung der Stellungnahmen der Datenschutzgruppe (AmCham EU 2011, 40 f. ETNO 2011, 10; GSMA 2011, 15; IAB Europe 2011, 6). Lediglich die konkreten Vorschläge in dieser Hinsicht

323 Vorzugsweise gegenüber jener Jurisdiktion, in der sich die Hauptniederlassung des jeweiligen Verantwortlichen befindet (vgl. AmCham EU 2011; ICDP 2011, 4).

324 Dass Verantwortliche bei innereuropäischen grenzüberschreitenden Datenübermittlungen nicht verschiedenen Jurisdiktionen unterliegen sollten, wurde auch seitens europäischer Akteure befürwortet (NOKIA 2011, 2), der Fokus der europäischen Akteure lag allerdings klar auf der Forderung nach Angleichung der Wettbewerbsbedingungen.

325 Die einzige Ausnahme bildet der Beitrag von Liberty Global, der zwar verstärkte Anstrengungen in Richtung mehr Harmonisierung begrüßte, aber ansonsten ungewöhnlich starkes Lob aussprach: „Liberty Global applauds the work of the Article 29 Working Party, which has helped to ensure greater consistency in the application of the Directive. Ensuring a consistent interpretation and application of Directive 95/46/EC by Member States and Data Protection Authorities (DPAs) is key." (Liberty Global 2011, 5)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

variierten gegenüber der Orientierungsphase. Ein Teil der Akteure schlug die Einsetzung einer ständigen Multi-Stakeholder-Beratungsgruppe vor, die die Arbeiten der Datenschutzgruppe begleiten sollte (BSA 2011, 7; DIGITALEUROPE 2011, 27; TechAmerica Europe 2011, 15), ein anderer Teil schlug einen stärkeren Einbezug von Wirtschaftsvertretern in die bestehenden Arbeitsgruppen der Datenschutzgruppe vor (ACCIS IVZW 2011, 19; Microsoft Corporation 2011, 29) während ein weiterer Teil dafür eintrat, dass die Kommission mehr Einfluss[326] auf die Datenschutzgruppe bzw. die Harmonisierung erhalten sollte (AmCham EU 2011, 41; BSA 2011, 7)

Auf die Ankündigung der Verbesserung der Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung reagierten die (19) Flexibilitätsbefürworter eher ablehnend. Zwar waren die entsprechenden Äußerungen der Akteure selten ausführlich, allerdings wurde häufig im Kontext der Ablehnung der Rechte auf Vergessenwerden und Datenportabilität darauf verwiesen, dass der Status Quo der Betroffenenrechte bereits einen angemessenen Schutz gewährleiste (ACCIS IVZW 2011, 9 f. AmCham EU 2011, 23 ff. BITKOM 2011, 3; ICDP 2011, 11). Auch bei diesem Thema wurde vorgeschlagen, statt der Stärkung der Vorgaben die EU-weite Harmonisierung voranzutreiben (Microsoft Corporation 2011, 11; Telefónica 2011, 5). Einige Akteure verwiesen auch explizit auf mögliche Probleme im Kontext der von der Kommission angekündigten Festlegung kostenloser Auskunftsersuchen und Antwortfristen. Befürchtet wurde die Überbelastung der Verantwortlichen in Folge des massenhaften Missbrauchs der Möglichkeit kostenfreier Anfragen. Zudem wurde gefordert, dass bei der Festlegung einer Antwortfrist keine zu strengen Vorgaben gemacht werden, damit Verantwortliche auf spezielle Situationen (etwa zu viele oder zu schwierige Anfragen) angemessen reagieren könnten, ohne Sanktionen befürchten zu müssen (DIGITALEUROPE 2011, 30 f. NOKIA 2011, 10).

Ähnlich ablehnend waren die Flexibilitätsbefürworter auch gegenüber der Stärkung des Grundsatzes der Datenminimierung und der Erweiterung besonderer Kategorien personenbezogener Daten eingestellt. Im Hinblick

326 Der am weitesten gehende Vorschlag in diesem Zusammenhang kam von Microsoft. Demnach sollte das Artikel 31-Komitee deutlich gestärkt und zu einer allgemeinen Kontrollinstanz ausgebaut werden, die die Umsetzung der Richtlinienvorgaben überwacht und verbindliche Empfehlungen ausspricht (Microsoft Corporation 2011, 16).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auf das Thema Datenminimierung[327] wurde vor allem der Erhalt des Status Quo gefordert (ECTA 2011, 1; ENPA und FAEP 2011, 4; EPC 2011, 8), da in Folge einer Stärkung eine noch stärkere Belastung der Verantwortlichen zu befürchten wäre (ACCIS IVZW 2011, 9; GDV 2011, 8). Zudem wurde auch darauf verwiesen, dass gestärkte Datenminimierungsvorgaben unpraktikabel und schwer umsetzbar seien, da das geforderte Minimum schwer zu bestimmen sei (AmCham EU 2011, 4; EUROFINAS 2011, 5). Auf das Argument der verbesserten Durchsetzung wurde auch bei diesem Thema zurückgegriffen (EPC 2011, 8).

Im Kontext besonderer Kategorien personenbezogener Daten (15 äußerten sich insgesamt zum Thema) sprachen sich einige Akteure unter Verweis auf verstärkte Harmonisierungsbestrebungen auf diesem Gebiet gegen jede Veränderung bzw. Erweiterung der Kategorien aus (FBF 2011, 4; GDV 2011, 11 f.). Andere sprachen sich lediglich gegen die Aufnahme genetischer Daten – vor allem, weil diese als Teil von Gesundheitsdaten betrachtet wurden – (vgl. z. B. FEDMA 2011, 3) bzw. gegen die Erweiterung um Finanzdaten aus (vgl. z. B. ACCIS IVZW 2011, 12; EUROFINAS 2011, 7). Das ICO und das britische Justizministerium verwiesen dagegen auf die Notwendigkeit eines generellen Umstiegs vom Konzept besonderer Kategorien personenbezogener Daten auf ein Konzept, das nicht die Kategorie, sondern die konkrete und kontextspezifische Verarbeitung bzw. Nutzung der Daten in den Mittelpunkt rückt (ICO 2011, 6 f. UK Ministry of Justice 2011, 4).

Die geringste Aufmerksamkeit erhielten die Themen Datenschutz bei Kindern (14), Datenschutzbehörden (11) und die automatisierte Verarbeitung/Profiling (6). Die von der Kommission angekündigten besonderen Vorkehrungen zum Datenschutz bei Kindern wurden unter Verweis auf die divergierende Gesetzeslage und Schwierigkeiten bei der Umsetzung in den verschiedenen Mitgliedstaaten eher abgelehnt.[328] Stattdessen wurde auf die Bedeutung von Initiativen der Selbstregulierung verwiesen, die wirksamer seien (BDZV und VDZ 2011, 5; EuroISPA 2011, 3; GSMA 2011, 11). Die Stärkung der Datenschutzaufsichtsbehörden wurde eher begrüßt (DIGITALEUROPE 2011, 27 f. Microsoft Corporation 2011, 28 f.) und Einschränkungen automatisierter Verarbeitungen bzw. des Profilings durchweg abgelehnt. In diesem Zusammenhang wurde insbesondere die seitens der Datenschützer – zwar nicht im Zusammenhang mit dieser Reform,

327 Zu diesem Thema äußerten sich 17 Akteure.

328 Einige Akteure zeigten sich allerdings auch abwägend und nahmen keine klare Position ein (GDV 2011, 13; NOKIA 2011, 12; Telefónica 2011, 4).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

jedoch im Kontext ihrer sonstigen Aktivitäten – geforderte Offenlegung von Scoring-Methoden abgelehnt (EUROFINAS 2011, 6). FEDMA (2011, 5) beispielsweise war sehr bemüht darum, die gesellschaftlichen Vorteile des Profilings zu erläutern. Ebenso ausführlich legte der GDV (2011, 23 f.) die Bedeutung des Profilings für Versicherungszwecke dar.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Häufigkeit d. Nennung	22	39	39	28	12	19	15	22	17	29	15	14
ZAW	2	2	2			2	4	1	3	1	2	2
Yahoo	2	2	2	5	2	4			2	1		2
WFA	1	2	2	4				2	2	3	2	3
VDZ	1	2	2					2		3	3	2
UEAPME	4	2	2	4		4				3		
Telefonica	3	2	1	4	2	4	4	2	3	2		3
TechAmerica (formerly AeA)		2	2	5		4	3	2	2			
Nokia	4	4	1	4		4	4	2	2	1	2	3
Microsoft	5	4	2	4	3	4		1		1	1	
Liberty Global	4	2	1	5	3			3		2		
Intel	4	2	1	4	3							
Industry Coalition for DP		3	2	5				2		2		
ICO		2	2	4				4				1
ICC	4	2	2	5	3	4	2	2		3		
IAB Europe		2	2	5			2	1		1		
GSMA	4	2	2	5	4		4	1		1		3
GDV	4	2	2	4				4	3	2	3	3
FTC	4	3	2		4				4	3		
FEDMA		2	1				2			2	2	2
FBF		2	1					3	3	2	1	
Facebook		2	2	4						2	2	
EuroISPA	3	2	2	5	3		3		3	2		2
Eurofinas		2	2	4		1			2		2	
ETNO		2	2	5			4			2		
EPC	2	2	2	4		2		2	3	2	3	3
ENPA & FAEP		2	2			2	2	3	2	2		3
EMOTA		2	2				2			2		
ECTA		2	1	4		4	4		3	1		
EBF		2	2									
eBay		3	2				3	2				
DIGITALEUROPE	3	2	2	5				1		2		
DDV	2	2	2	5		1		1	3	1	2	2
BT	3	2	2	4	2	4		2		2		
BSA	4	2	2	5	3	4	3	2			2	
BITKOM		3	2	5							4	
BDIU		2	2			4						
AmCham EU	4	1	1	4		4			1	2		
ACT		2	2			2						
ACCIS	4	2	2	4	3	2			2	2	2	
DSGVO-E 2012	4	5	5	5	4		4	4	4	5	4	5
DSGVO-E 2011	5	5	5		5		5	5	4	5	4	5
me	B1 Technologischer Wandel	B2 Staatl./Private Aktivität	B3 Policy-Orientierung im Falle staatlichen Handelns	B6 Harmonisierung	B8 Globalisierung	B12 Reformwunsch	C 1 B Räuml. Anwendungsbereich	C 1 C Definition personenb. Daten	C 2 C Grundsatz der Datenminimierung	C 3 D Einwilligung	C 4 A Besondere Kategorien personenbezogener Daten	C 4 D Datenschutz bei Kindern

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

me	C 5 A Transparenz	C 5 C Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung	C 5 E Recht auf Vergessenwerden	C 5 G Recht auf Datenportabilität	C 5 I Automat. Verarbeitung / Profiling	C 5 L Benachrichtigung bei Datenschutzverletzungen	C 6 A Privacy by Default	C 6 B Privacy by Design	C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	C 6 N Rechenschaftspflicht
DSGVO-E 2011	4	4	5	5	5	5	4	4	4	5
DSGVO-E 2012	4	4	4	5	4	4	4	4	4	4
ACCIS	2	2	3	2		2		2	2	
ACT	2		2			2				
AmCham EU	1		2	2		2	2	2	3	1
BDIU										
BITKOM	2		3	1		2				
BSA			3	2		2		2	2	2
BT	2		2					1	1	
DDV	2	3	3	2				3	2	
DIGITALEUROPE	2	2	2	2		3		1	1	2
eBay			2							
EBF	2					1		2	2	
ECTA			3	2	1	3	1	1	1	
EMOTA		3		3					2	
ENPA & FAEP	2	3	1	2				2	1	
EPC	2		1	2		3		2		
ETNO	2		3	2			1	2	2	
Eurofinas	1	3	2		1	1		2		1
EuroISPA	2		3	2	2	2			2	
Facebook	3		3	2		2			2	2
FBF	3			2		3				2
FEDMA	1		2		2					
FTC	3	2				4	3	4		
GSMA	2		3	2					1	2
GDV	3	3	2	2	2	3		2	2	
FCC	1		2	2		2		2	2	2
ICO		4	2		2	3	3	3	2	2
Industry Coalition for DP	2	3	3	1			1	2	2	2
Intel	2							2	2	2
Liberty Global			2			2		2		1
Microsoft	2	3	1	2		1		2	2	1
Nokia	2	3	1	2		2		1	1	1
TechAmerica (formerly AeA)	1	2	2	2		1		2	2	2
Telefonica	2	3	3	2				2	2	2
UEAPME	2					1			2	2
VDZ	1	3		2		2		1		2
WFA	2	3	2					1	2	2
Yahoo	1	3	2	2				2	1	2
ZAW	2	3	2					2	1	
Häufigkeit d. Nennung	32	19	31	25	6	24	6	28	28	20

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Häufigkeit d. Nennung	28	25	26	21	26	20	11	20
ZAW		1 1	2		1			2
Yahoo	2	1 1	1	1	2	2		1
WFA		1 1	2					
VDZ		1 1	2	1	1			
UEAPME	2 2	2 2	2	2 1	2	2		
Telefonica	2 2	1 2	1	1 2	2	2	4	2
TechAmerica (formerly AeA)	1 1	2 2	2	2 1			4	2 2
Nokia	1 1	2 2	2	2 2	2	2		2 2
Microsoft	1 1	1 1		1 1			4	2 2
Liberty Global	2 2	2 2	1	1 1	2	2		4
Intel	2 2	1 1		1 1	2	2		
Industry Coalition for DP	2 2		1	1 1	2	1		
ICO	2 2	4 4			2	3	4	4
ICC	2 2		2	2 2	2	2		
IAB Europe			2	2 2	2	2		2 2
GSMA	1 1	1 1	2	4 4	2			2 2
GDV	2 2	4 4	2	3 3	3	2		
FTC	3 3						4	
FEDMA	2 2							
FBF	2 2				1 1			
Facebook			2	2 2		2		3 3
EuroISPA	2 2	2 2	1	1 1		2		2 2
Eurofinas						2		
ETNO	2 2	1 1	2		3 3			2 2
EPC		2 2	1	2 2	2	2	3	2 2
ENPA & FAEP		1 1	1		2		3	2 2
EMOTA		2 2	2		2			
ECTA	1 1		1				4	2 2
EBF	2 2	2 2						
eBay	2 2	2 2						
DIGITALEUROPE	2 2	1 1	1	1 1	2	2	4	2 2
DDV	2 2	1 1	1		1 1			
BT	2 2							
BSA	1 1	1 1	2	2 2	2	2		2 2
BITKOM	2 2				3 3	3		
BDIU							2 2	
AmCham EU	1 1	2 2	1	2 2	2	2		2 2
ACT					2 2			
ACCIS	2 2		2	2 2	2	2	2	2 2
DSGVO-E 2012	4 4	3 3	4	3 3	4	4	4	3 3
DSGVO-E 2011	4 4	3 3	4	3 3	4	4	4	3 3
me	C 7 Übermittlung in Drittstaaten	C 10 D Technologieneutralität	C 13 A Verhaltensregeln	C 13 B Zertifizierungen/Gütesiegel	C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	C 13 D Datenschutz-Folgenabschätzung	C 15 B Datenschutzbehörden	C 16 C Art. 29-Datenschutzgruppe

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Häufigkeit d. Nennung	23	15
ZAW	2	2
Yahoo	2	2
WFA	2	
VDZ	2	3
UEAPME	1	1
Telefonica	3	3
TechAmerica (formerly AeA)	1	
Nokia	2	2
Microsoft		3
Liberty Global		
Intel		
Industry Coalition for DP	1	
ICO		2
ICC	2	
IAB Europe		
GSMA	2	3
GDV	1	
FTC		
FEDMA		
FBF	1	
Facebook	2	2
EuroISPA		
Eurofinas		
ETNO		
EPC		
ENPA & FAEP	2	
EMOTA		
ECTA		
EBF	2	2
eBay		
DIGITALEUROPE	2	
DDV	2	2
BT		
BSA	2	2
BITKOM	2	
BDIU		
AmCham EU	2	2
ACT	3	
ACCIS	2	2
DSGVO-E 2012	4	4
DSGVO-E 2011	4	5
me	C 17 D Verbands- / Sammelklagerecht	C 17 E Sanktionen und Geldbußen

Tabelle 4-26: Positionierung der Flexibilitätsbefürworter zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.2.1.3.3 Ressourcen der Flexibilitätsbefürworter während der Entwurfsphase

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die Flexibilitätsbefürworter verfügten während der Entwurfsphase nur über ein geringes Maß an formeller, legaler Einbindung in politische Entscheidungsprozesse. So verfügten die Akteure über keine nennenswerte Einbindung in die Tätigkeiten des für die Datenschutzreform federführend zuständigen Datenschutz-Referats der Kommission oder der übergeordneten Justiz-GD bzw. Justiz-Kommissarin Reding. Demgegenüber bestanden Kontakte insbesondere zum liberalen Handelskommissar Karel de Gucht und der für die Digitale Agenda zuständigen liberalen Neelie Kroes. Diese und weitere Beziehungen wurden seitens der Flexibilitätsbefürworter mit eher geringem Erfolg dazu genutzt, eine Verringerung des Verwaltungsaufwands des Datenschutzreformvorschlags zu erreichen (vgl. 4.2.2.1).

Ein weiterer, seitens der Wirtschaft rege genutzter Lobbying-Kanal war die Kontaktierung der Regierungen jener Mitgliedstaaten, in denen einzelne große Konzerne ihre europäische Hauptniederlassung haben. Dies betraf in erster Linie Facebook in Irland, aber genauso auch europäische Unternehmen mit einem geringen Interesse an strengen Datenschutzregeln (Schildberger 2016, xxxiv, vgl. die Zeilen 54-59).

Unterstützung durch die Öffentliche Meinung

Wie im Unterabschnitt zu den Ressourcen der Datenschutzbefürworter erläutert, sprach sich die EU-Bevölkerung während der Entwurfsphase deutlich gegen die sehr weitreichenden personenbezogenen Datenverarbeitungspraktiken privatwirtschaftlicher (Online-)Anbieter aus.

Allerdings bedienten sich einige Flexibilitätsbefürworter der Lobbying-Strategie des Astro-Turfing. Der Begriff bezeichnet eine Lobbying-Strategie politischer Akteure, die ihr Partikularinteresse als Bürgerinteresse kleiden und so versuchen, größeren Einfluss auf politische Entscheidungsprozesse zu nehmen (Irmisch 2011, 95). So hatte die Gruppe EPA (European Privacy Association) im freiwilligen EU-Lobbying-Register angegeben, ein von Unternehmensinteressen unabhängiger Datenschutz-Think Tank zu sein. In ihren Stellungnahmen während der Orientierungs- und Entwurfsphase hatte die Organisationen schließlich kompromissorientierte Positionen vertreten, die zwar einerseits die Stärkung des Datenschutzes, insb. von Betroffenenrechten, vorsahen, aber andererseits auch mehr Verständnis

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

für die Überbelastung der Verantwortlichen zu schaffen versuchten. Mitte 2013 stellte sich schließlich nach einer Beschwerde von Corporate Europe Observatory heraus, dass die EPA von Google, Facebook, Microsoft und Yahoo finanziert wurde und nicht unabhängig war (Fontanella-Khan 2013a).

Informationen/Informationshoheit

Insbesondere die US-amerikanischen Lobbying-Akteure verfolgten eine bemerkenswert versierte Lobbying-Strategie: Während die europäischen Akteure sich immer wieder in äußert ungeschickter Weise strikt gegen die Vorschläge der Kommission aussprachen,[329] vermochten es die US-Akteure ihre Kritik deutlich geschickter zu präsentieren. Microsoft (2011, 10 f.) beispielsweise führte in ihrer Stellungnahme aus dem Jahr 2011 über eine ganze Seite die Vorzüge des Rechts auf Datenportabilität aus und begrüßte das diesbezügliche Engagement der Kommission. Auf einer weiteren Seite wurde schließlich ausgeführt, welche Gefahren mit dem Recht auf Datenportabilität verbunden seien und welche Vorsichtsmaßnahmen die Kommission treffen müsste, um diese zu verhindern. Inhaltlich stellte auch der Microsoft-Beitrag in letzter Instanz eine Generalablehnung des Kommissionsvorschlags dar, formuliert war er hingegen in einer dialogorientierten Sprache.

Fähigkeit zur politischen Mobilisierung

Die geringe Fähigkeit der Flexibilitätsbefürworter zur politischen Mobilisierung blieb unverändert.

Finanzielle Ressourcen

Das hohe finanzielle Ressourcen-Potential der Flexibilitätsbefürworter blieb ebenfalls unverändert. Genutzt wurden die Ressourcen insbesondere für das Lobbying von Kommissionsangehörigen, indem diese auf Lobbying-Veranstaltungen eingeladen wurden.

Das Vorhandensein einer fähigen Führung

Mit der Gründung der Industry Coalition for Data Protection Ende 2011 zeichnete sich erstmals ein informeller Führungsanspruch innerhalb der Koalition bzw. Community der Flexibilitätsbefürworter ab. Die ICDP ver-

329 Vgl. z. B. die Ausführungen der BITKOM (2011, 2 f.), in denen die Ablehnung der Meldung von Datenschutzverletzungen zum Ausdruck gebracht werden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

einigte erstmals mehrere, seit vielen Jahren auf dem Gebiet der EU-Datenschutzpolitik aktive Verbände unter einem formellen Koalitionsdach.

4.2.1.4 Die Akteursgruppe der Kompromisswilligen

Die Bezeichnung Kompromisswillige trifft auf diese Akteursgruppe insofern zu, als die Überzeugungssysteme der Akteure zwar untereinander durchaus unterschiedlich waren, sie sich jedoch darin überschnitten, dass weder eindeutig eine Stärkung des datenschutzrechtlichen Rahmens, noch eine weitgehende Verringerung des Verwaltungsaufwands bei der Datenverarbeitung gefordert wurde. Den Flexibilitätsbefürwortern grundsätzlich näherstehende Akteure wie der Ministerrat, das britische Justizministerium oder BRAK zeigten sich gegenüber den Positionen der Datenschutzbefürworter deutlich offener als jene Akteure, die der Flexibilitätsbefürworter-Koalition bzw. Community zugeordnet wurden. Auf der anderen Seite äußerten einige Akteure (die Datenschutzbehörden Norwegens, Portugals und Schwedens, aber auch die CDT), die historisch-institutionell eher den Datenschutzbefürwortern näherstanden, verständnisvoll gegenüber den Bedenken der datenverarbeitenden Wirtschaft. Da in dieser Phase noch noch nicht in stärkerem Maße über konkrete Regelungsinhalte diskutiert wurde, drückten zudem einige Akteure (hier sind die Regierungen Österreichs, Deutschlands und Lettlands zu nennen) ihre Positionen in gemäßigterem Tonfall aus, als sie es später während der Verhandlungen taten. Eine Reihe von Akteuren (EPA, FTC, GDD, CDT) vertrat grundsätzlich die Idee, eine Balance zwischen einem starken Grundrechtsschutz und Wirtschaftsinteressen zu finden.

Da die Hauptauseinandersetzung im politischen Aushandlungsprozess der DSGVO zwischen den Datenschutzbefürwortern einerseits und den Flexibilitätsbefürwortern andererseits ausgetragen wurde und die Community der Kompromisswilligen als eigene Gruppe praktisch keine Relevanz hatte, gehe ich an dieser Stelle nicht näher auf die Überzeugungssysteme und Ressourcen dieser Akteure ein. Die ausführliche Übersicht der Positionierung aller Akteure der Community der Kompromisswilligen kann Tabelle Anhang 3 entnommen werden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Akteur	Akteursgruppe
AUT-Regierung	Mitgliedstaaten
BRAK	Privatwirtschaft
CDT	Zivilgesellschaft
DEU-Regierung	Mitgliedstaaten
DSAB-NOR	Datenschutzbehörden
DSAB-PRT	Datenschutzbehörden
DSAB-SWE	Datenschutzbehörden
EPA	Wirtschaft (Astro-Turfing)
FTC	Drittstaat
GDD	Zivilgesellschaft/Wirtschaft
LVA-Regierung	Mitgliedstaaten
Mitgliedstaaten - GBR- Justizministerium	Mitgliedstaaten
Ministerrat	EU-Politik

Tabelle 4-27: Akteure der Community der Kompromisswilligen

4.2.2 Prozessanalyse: Entstehung und Inhalt des DSGVO-Entwurfs der Europäischen Kommission

4.2.2.1 Lobbying der Kommission und Verzögerung des Reformpakets

Nach Ende der zweiten öffentlichen Konsultationsphase am 15. Januar 2011 intensivierte die Kommission ihre Arbeiten an der Datenschutzreform, um noch im selben Jahr einen Legislativvorschlag zu unterbreiten. Obwohl der größte Teil der medialen Berichterstattung erst später auf das enorme Ausmaß des gegen das EU-Parlament gerichteten Lobbyings aufmerksam machen sollte, offenbarte sich bereits zu diesem frühen Stadium das große Interesse der datenverarbeitenden Wirtschaft daran, durch massives Lobbying Einfluss auf die Ausgestaltung der Datenschutzreform zu nehmen. Nachdem die Kommission während der ersten Konsultationsphase 168 Stellungnahmen erhalten hatte, stieg diese Zahl in der zweiten Konsultationsphase auf 305 Einsendungen. Über 200 Stellungnahmen wurden von Wirtschaftsvertretern eingebracht, weitere 54 Einsendungen von Bürgerinnen und Bürgern sowie 31 von öffentlichen Einrichtungen (EU Commission 2012, 68). Der öffentliche Konsultationsprozess war nur einer der Kanäle, die seitens der Stakeholder zur Beeinflussung der Kommissionspolitik genutzt wurden. Daneben wurden sowohl der Leiter bzw. die Mitarbeiter

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des Datenschutz-Referats der Kommission, die Leitung der Direktion, die Leitung der Generaldirektion als auch Kommissarin Reding selbst bzw. ihr Kabinett in Form persönlicher Treffen lobbyiert. Darüber hinaus wurde auch versucht, Einfluss auf Angehörige der Kommission zu nehmen, indem diese zu privaten (Abend-)Veranstaltungen eingeladen wurden, auf denen die Perspektiven der Wirtschaftsvertreter vorgestellt und diskutiert werden (Schildberger 2016, 111 f.). Nachdem Kommissarin Reding und die GD-Mitarbeitenden nur wenig Bereitschaft zeigten, den Forderungen der Flexibilitätsbefürworter entgegenzukommen (Guarascio 2012; Warman 2012c), fokussierten sich das Lobbying auf die thematisch angrenzenden und den Forderungen der Wirtschaft gegenüber offener eingestellten Generaldirektionen bzw. Kommissaren. Insbesondere wurden die für die Digitale Agenda zuständige liberale Kommissarin Neelie Kroes und der ebenfalls liberale Handelskommissar Karel de Gucht dazu gedrängt, den Verordnungsentwurf Redings während des kommissionsinternen dienststellenübergreifenden Abstimmungsprozesses abzuändern (Guarascio 2012).[330]

Ein auf den 29. November 2011 datierter Verordnungsentwurf, der Ende 2011 von Statewatch geleaked wurde, gab Aufschluss über die inhaltlichen Ziele von Reding und ihrem Team und ermöglicht den inhaltlichen Vergleich zwischen Vorfassung und Endfassung des DSGVO-Kommissionsentwurfs. Im Hinblick auf verschiedene Themen (darunter insb. Datenschutz bei Kindern, das Recht auf Datenübertragbarkeit und die mögliche Sanktionshöhe) sah der Entwurf ein sehr hohes Datenschutzniveau vor (EU Commission 2011). Während die Datenschutzbefürworter sich über die Vorschläge erfreut zeigten (EDRi 2011a), führten die Pläne der Kommission zu mehr Beunruhigung auf Seiten insb. der US-amerikanischen Wirtschaft. Als der kommissionsinterne Abstimmungsprozess gegen Ende 2011 kurz vor dem erfolgreichen Abschluss stand, trat schließlich die US-Regierung bzw. das US-Wirtschaftsministerium an die Kommission heran, um einigen zentralen Forderungen der Flexibilitätsbefürworter Nachdruck zu verlei-

330 Die Grundrechteorientierung in Viviane Redings Handeln wurde wenig später auch im Zusammenhang mit der Auseinandersetzung um das Anti-Produktpiraterie-Handelsabkommen ACTA deutlich. Während De Gucht das Abkommen und die Urheberrechtsindustrie in Schutz nahm und keine Konsequenzen für die Meinungsfreiheit befürchtete, sprach sich Reding unter Verweis auf die befürchteten Internetsperren und die Einschränkung der Meinungsfreiheit in aller Deutlichkeit gegen das Abkommen aus (Horten 2012).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

hen.[331] Dazu nahm die US-Seite einerseits direkten Kontakt mit hohen Kommissionspersönlichkeiten auf, andererseits wurde eine sog. informelle Notiz an die Kommission übersandt, mit der auf die aus US-Sicht zentralen Problemfelder hingewiesen wurde (EDRi 2011c; Guarascio 2012; US Administration 2011). In der Folge forderten sechs Generaldirektionen sowie weitere Kommissionsstellen, darunter das Europäische Amt für Betrugsbekämpfung (OLAF) Änderungen am Entwurfstext. Obwohl Kommissarin Reding später selbst bekundete, dass sie sich angesichts des heftigen Lobbysturms unnachgiebig gezeigt habe und der Zeitplan der Reform eingehalten worden sei,[332] verzögerte sich die Veröffentlichung des Verordnungs- bzw. Richtlinienentwurfs im Ergebnis der Auseinandersetzungen auf den 25. Januar 2012 und konnte letztlich erst erfolgen, nachdem Reding einige Änderungen vorgenommen[333] und Innenkommissarin Cecilia Malmström daraufhin ihr Veto zurückgezogen hatte (Euractiv 2012a; Guarascio 2012). Das Ausmaß des gegen die Kommission gerichteten Lobbyings wurde später als vergleichbar oder gar größer als das Lobbying der Wirtschaft gegen die EU-Chemikalienverordnung REACH (Corporate Europe Observatory 2005) bzw. gegen die Lebensmittel-Informationsverordnung (Kluger Dionigi 2017, 75 ff.) bezeichnet (Schildberger 2016, xxxvii, xliv, lxiv).

4.2.2.2 Der Kommissionsvorschlag zur EU-Datenschutz-Grundverordnung

Neben dem *Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (DSGVO-E) (EU-Kommission 2012d) beinhaltete das Ende Januar veröffentlichte Reformpaket den *Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch*

331 Diese Form des Lobbyings stellte eine typische Vorgehensweise der US-Regierung dar und war sowohl in anderen Politikbereichen als auch im Bereich der EU-Datenschutzpolitik in der Vergangenheit bereits praktiziert worden (US FTC 2006).

332 "'The lobbying from all sides has been fierce – absolutely fierce – I have not seen such a heavy lobbying operation,' she said. 'But the legislation was on the table on the 25th January as I wanted to have it. So much to the efficiency of lobbying.'" (Warman 2012c)

333 So hatte der ursprüngliche Kommissionsentwurf aus dem Jahr 2011 noch eine Klausel (vgl. Art. 42 DSGVO-UE) beinhaltet, die eine Weitergabe personenbezogener Daten an öffentliche Stellen in Drittländern unter Strafe stellte (EU Commission 2011). Wie sich erst später im Zuge der Debatten im Kontext der NSA-Enthüllungen herausstellte, war dieser Artikel im finalen Entwurf auf Druck der US-Wirtschaft und der US-Regierung hin ersatzlos gestrichen worden (Fontanella-Khan 2013b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (EU-Kommission 2012c), mit dem die Reform des JI-Rahmenbeschluss angestoßen wurde. In einer weiteren Mitteilung fasste die Kommission ihre Ziele und die Inhalte beider Legislativinstrumente zusammen (EU-Kommission 2012a). Zudem veröffentlichte die Kommission ein weiteres Arbeitsdokument, das die Ergebnisse der Folgenabschätzung enthielt, mit der die Kommission ihren Legislativvorschlag ausführlich begründete (EU Commission 2012; EU-Kommission 2012e). In diesem Dokument wurden die Ergebnisse der zweiten Konsultationsrunde zusammengefasst (EU Commission 2012, 68).

Entgegen den Äußerungen der Kommission, die während der Orientierungs- und der Entwurfsphase gemacht worden waren und die lediglich die Grundrechtsdimension hervorhoben, verwiesen alle Äußerungen der Kommission im Zusammenhang mit der Veröffentlichung des Datenschutzreformpakets auf die Bedeutung sowohl der Grundrechtsdimension als auch der wirtschaftlichen Dimension des Schutzes personenbezogener Daten. So gab die Kommission an, mit der Reform-Initiative zwei[334] Ziele zu verfolgen:

> - *„Stärkung der Wirksamkeit des Grundrechts auf Datenschutz und Übertragung der Kontrolle über die Daten an die Betroffenen, insbesondere vor dem Hintergrund der technologischen Entwicklungen und zunehmenden Globalisierung,*
> - *Vertiefung der Binnenmarktdimension des Datenschutzes durch Abbau der Unterschiede in den Regelungen, Verstärkung der Kohärenz und Vereinfachung des Regelungsumfelds." (EU-Kommission 2012d, 116)*

Gerahmt wurde der Legislativvorschlag als eine binnenmarktrelevante Maßnahme, die durch die bessere Gewährleistung des Grundrechts auf den Schutz personenbezogener Daten das Vertrauen in datenverarbeitende Dienste und Produkte stärkt und auf diese Weise das Wirtschaftswachstum und die Wettbewerbsfähigkeit der EU steigert (EU-Kommission 2012a, 2, 2012b):

334 Ich benenne an dieser Stelle lediglich die auf das allgemeine Datenschutzrecht bezogenen Ziele. Das dritte Ziel, das von der Kommission verfolgt wurde, bezog sich auf den Kontext Datenschutz und Sicherheit und sah die „Einführung einer umfassenden Regelung zum Schutz personenbezogener Daten [vor], die für sämtliche Bereiche gleichermaßen gilt" (EU-Kommission 2012d, 116).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

> *„Fehlendes Vertrauen lässt Verbraucher zögern, online zu kaufen und neue Dienstleistungen in Anspruch zu nehmen. Ein hohes Datenschutzniveau ist daher auch unentbehrlich, um das Vertrauen in Online-Dienste zu stärken, das Potenzial der digitalen Wirtschaft auszuschöpfen und auf diese Weise* ***Wirtschaftswachstum und Wettbewerbsfähigkeit der EU*** *zu steigern." (EU-Kommission 2012a, 2, Hervorhebung im Original)*

Zu diesem Zweck verortete die Kommission die Datenschutzreform im breiteren Kontext der EU-Politiken als Teil des *Stockholmer Programms* (EC 2010), aber darüber hinaus als Teil der *Digitalen Agenda für Europa* (Europäische Kommission 2010) und von Europa 2020, der *Wachstumsstrategie der EU* (EU-Kommission 2010).

In den im Hinblick auf die Grundrechtsdimension gemachten Äußerungen der Kommission dominierte dagegen eine stark individualistische Rahmung der Materie. Häufig war davon die Rede, dass den Nutzerinnen und Nutzern die Kontrolle über ihre personenbezogenen Daten zurückgegeben werden muss. So ließ sich Viviane Reding in der die Veröffentlichung des Legislativvorschlags begleitenden Pressemitteilung folgendermaßen zitieren: „Der Schutz personenbezogener Daten ist zwar ein Grundrecht aller Europäer, aber die EU-Bürger haben nicht immer das Gefühl, dass sie vollständige Kontrolle über ihre personenbezogenen Daten haben." (EU-Kommission 2012b, 2)

Zwar war die Kommission darum bemüht, ihren Legislativvorschlag als Vorteil und Kostenerleichterung für Unternehmen zu bewerben, womit sie den Forderungen der Flexibilitätsbefürworter zumindest rhetorisch entgegenkam, doch wird die folgende Diskussion zeigen, dass die Kommission bei der Mehrheit der Themen bzw. Maßnahmen die Vorschläge der Datenschutzbefürworter aufgriff, während die Positionen der Flexibilitätsbefürworter weitestgehend ignoriert wurden.

4.2.2.3 Inhalte des DSGVO-Kommissionsentwurfs und Einschätzung des Akteurseinflusses

Je nach Dokument wurden die Inhalte des Kommissionsentwurfs der DSGVO unterschiedlich gerahmt: Die Pressemitteilung etwa erwähnte zwar die Grundrechtsdimension, stellte aber ausschließlich jene auf die Binnenmarktperspektive bezogenen Aspekte in den Vordergrund (EU-Kommission 2012b). In der Mitteilung wurden die Maßnahmen-Vorschläge der Kommission in drei inhaltliche Blöcke unterteilt: (1) Den Schutz der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Betroffenen, (2) die Stärkung der Binnenmarktdimension und (3) die Berücksichtigung der Auswirkungen der Globalisierung. Allerdings verortete die Kommission die Mehrzahl ihrer Änderungsvorschläge im Kontext des ersten Themenkomplexes (EU-Kommission 2012a). Die Erläuterungen, die dem eigentlichen Legislativvorschlag vorangestellt waren, folgten der Struktur des DSGVO-Entwurfs, diskutierten die Inhalte Kapitel für Kapitel bzw. Abschnitt für Abschnitt (EU-Kommission 2012d).

Ich beginne die folgende Analyse mit der Diskussion der drei Themen, bei denen die Kommission ganz bis teilweise den sich teils überlappenden Forderungen beider Seiten entgegenkam bzw. die Positionen beider Seiten in gleichem Maße unberücksichtigt lies: Harmonisierung, Datenschutzaufsicht und die Gewährleistung der EU-weiten Kohärenz der aufsichtsbehördlichen Praxis. Daran schließt sich die Diskussion der wenigen Elemente an, bei denen die Kommission den Forderungen der Flexibilitätsbefürworter entsprach. Der Großteil der folgenden Diskussion widmet sich der Darstellung jener Elemente, bei denen die Kommission den Forderungen der Datenschutzbefürworter folgte.

4.2.2.3.1 Konsens-Themen

Als Kernproblem des bestehenden gesetzlichen Rahmens bezeichnete die Kommission deren fragmentierte Umsetzung in den Mitgliedstaaten und die unzureichende Durchsetzung der Vorgaben, die zu Rechtsunsicherheit, erhöhten Kosten und Verwaltungsaufwand sowie zu Behinderungen des grenzüberschreitenden Datenverkehrs führten. Folglich setzte die Kommission die Harmonisierung der mitgliedstaatlichen Datenschutzgesetze in den Mittelpunkt ihrer Strategie und begründete auf diese Weise die Erforderlichkeit des Umstiegs auf das Instrument der Verordnung (EU-Kommission 2012d, 6 f. 2012a, 8). Mit diesem Vorstoß kam die Kommission den Forderungen sowohl der Datenschutzbefürworter als auch der Flexibilitätsbefürworter entgegen, die beide – wenngleich aus unterschiedlichen Gründen – die Harmonisierung der EU-weiten Datenschutzgesetze als Kernthema forciert hatten. Im Zusammenhang mit der Relevanz der Maßnahme für den Binnenmarkt betonte die Kommission zudem, dass die EU-weite Harmonisierung der Datenschutzregelungen auf Seiten der Unternehmen zu einer Reduktion des Verwaltungsaufwands in Höhe von ca. 2,3 Mrd. € jährlich führen werde. Einschränkend sei erwähnt, dass die Kommission die heterogene Haltung der Flexibilitätsbefürworter hinsichtlich der Erfor-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

derlichkeit einer Reform dahingehend verzerrte, dass diesen undifferenziert unterstellt wurde, dass „auch Unternehmen eine umfassende Reform der EU-Datenschutzvorschriften der Kommission wünschten." (EU-Kommission 2012a, 4) Tatsächlich waren sich die Flexibilitätsbefürworter nur dahingehend einig, dass eine Harmonisierung notwendig wäre. Im Hinblick auf eine Reform des Datenschutzrahmens hatten sich einige Beteiligte ablehnend geäußert. Kaum einer der Akteure hatte zudem den Umstieg auf das Instrument einer Verordnung begrüßt. Einige befürworteten eine neue Richtlinie, ein anderer Teil Überarbeitungen an der bestehenden Richtlinie. Die Datenschutzbefürworter waren dagegen geschlossen für die Reform und eine Verordnung eingetreten.

Als Bestandteil der Harmonisierung schlug die Kommission die Stärkung der Unabhängigkeit der Datenschutzaufsichtsbehörden, die Einrichtung eines sog. One-Stop-Shops zur Vereinfachung der Bürokratie sowie die Gewährleistung einer einheitlichen Rechtsanwendung durch die Einführung eines Kohärenz-Verfahrens vor.

Der Kommissionsvorschlag sah die Präzisierung der Bestimmungen zu den Aufsichtsbehörden in den Art. 46 bis 54 DSGVO-E vor, darunter insb. die Stärkung der Unabhängigkeit der Aufsichtsbehörden gemäß der Rechtsprechung des EuGHs in Art. 47 DSGVO-E. Kernelement des Kommissionsvorschlags war die Einführung des sog. One-Stop-Shops, dem *Prinzip einer zentralen Anlaufstelle* für den Datenschutz. Art. 51 DSGVO-E sah vor, dass die Aufsichtsbehörde jenes Mitgliedstaates, in dem ein Verantwortlicher seine Hauptniederlassung hat, die alleinige Zuständigkeit für diesen Verantwortlichen erhält. Die Kommission bezweckte auf diese Weise den Verwaltungsaufwand für Verantwortliche zu reduzieren und Zuständigkeitsfragen über Verantwortliche, die am grenzüberschreitenden Datenverkehr partizipieren und zugleich über Niederlassungen in mehreren Mitgliedstaaten verfügen, abschließend zu klären (EU-Kommission 2012a, 7 ff.).

Den Forderungen der Flexibilitätsbefürworter entsprachen die Vorschläge der Kommission insofern, als sie eine ihrer Kernforderungen erfüllten, nämlich die Orientierung der Regelungen an der Hauptniederlassung. Auf diese Weise hätte sich international operierenden Verantwortlichen die Möglichkeit geboten, ihre Hauptniederlassung in jenem Mitgliedstaat zu wählen, in dem sie die geringsten Hindernisse für ihre Datenverarbeitungstätigkeiten erwarteten. Aufgrund der gesteigerten Unabhängigkeit der einzelnen Aufsichtsbehörden hätten die übrigen Behörden wiederum keine Handhabe gegen die laxe Aufsichtspraxis einer anderen Behörde gehabt. Den Forderungen der Datenschutzbefürworter entsprachen die Kommissi-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

onsvorschläge hingegen deshalb, weil die deutliche Stärkung der einzelnen Datenschutzaufsichtsbehörden im Sinne der Datenschutzbefürworter war – obgleich nicht intendiert worden war, dass Verantwortliche dadurch stärkere Vorgaben vermeiden können würden.

Einen besonderen Fall bildet zudem Art. 3: War die DS-RL auf nicht in der EU niedergelassene Verantwortliche nur dann anwendbar, wenn diese auf Mittel zurückgriffen, die in einem Mitgliedstaat belegen sind, sah die Kommission in den Vorgaben zum räumlichen Anwendungsbereich in Art. 3 DSGVO-E vor, dass die Verordnung künftig auf alle Verarbeitungen eines nicht in der EU niedergelassenen Verantwortlichen Anwendung finden sollte, sofern die entsprechende Verarbeitung dem Angebot von Waren oder Dienstleistungen an Personen in der Union oder der Beobachtung ihres Verhaltens dient. Den Forderungen der europäischen Wirtschaft als auch der Datenschutzbefürworter entsprechend sollte die Einführung des Marktortprinzips künftig vermeiden, dass sich nicht in der Union ansässige Verantwortliche durch die Auslagerung der Verarbeitung in Drittstaaten den Vorgaben der Verordnung entziehen. An diesem Punkt wurde die Intention der Kommission deutlich, mit der Verordnung sowohl die europäische Wirtschaft zu stärken, indem Wettbewerbsverzerrungen vermieden werden, als auch angesichts der durch die Globalisierung bedingten Herausforderungen einen konsequenteren Schutz personenbezogener Daten auch dann zu gewährleisten, wenn der Verantwortliche selbst nicht in der Union ansässig ist und die Datenverarbeitung in einem Drittland stattfindet.

4.2.2.3.2 Von beiden Koalitionen abweichende Positionen der Kommission

In den Artikeln 64 bis 72 DSGVO-E wurde die Einrichtung des Europäischen Datenschutzausschusses (EDSA) geregelt, der an die Stelle der Art. 29-Datenschutzgruppe treten sollte. Art. 55 bis 63 DSGVO-E behandelten dagegen die Zusammenarbeit der Behörden untereinander sowie das Kohärenzverfahren, das zur einheitlichen Rechtsanwendung in einer Vielzahl von Fällen beitragen sollte. Entgegen den Ankündigungen der Kommission hinsichtlich der Stärkung der Datenschutzgruppe, sah der Kommissionsentwurf allerdings die entscheidende Rolle im Rahmen des Kohärenzverfahrens nicht beim EDSA, sondern bei sich selbst vor. So sollten Aufsichtsbehörden im Zweifelsfall der Stellungnahme der Kommission

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

folgen und schließlich sollte die Kommission nach Art. 62 lit. a befähigt werden, Durchführungsrechtsakte[335] zur ordnungsgemäßen Anwendung der DSGVO zu erlassen, womit sie sich selbst in die Rolle einer Meta-Aufsichtsinstanz versetzen wollte (Hornung 2012, 105). Art. 71 DSGVO-E sah schließlich im Hinblick auf die Stärkung der Unabhängigkeit vor, dass das Sekretariat des EDSA vom Europäischen Datenschutzbeauftragten gestellt werden sollte und nicht mehr, wie im Falle der Art. 29 Datenschutzgruppe, von der Kommission selbst bzw. von dessen Datenschutz-Referat.

Mit ihren Vorschlägen entsprach die Kommission weder den Erwartungen der Datenschutzbefürworter, noch jenen der Flexibilitätsbefürworter. Erstere hatten zwar für mehr Kohärenz auf EU-Ebene geworben, jedoch in diesem Zusammenhang eher für die Erweiterung der Macht der Datenschutzgruppe und die Erweiterung ihrer Unabhängigkeit geworben, jedoch zu keinem Zeitpunkt die Übertragung zusätzlicher Befugnisse an die Kommission diskutiert. Letztere dagegen hatten zwar die Harmonisierung der EU-weiten Anwendung der Datenschutzregeln befürwortet, aber ansonsten vor allem auf mehr Transparenz und Einbezug im Hinblick auf die Tätigkeiten der Datenschutzgruppe gedrängt. Weder hätte der Kommissionsvorschlag die Steigerung der Unabhängigkeit der Datenschutzgruppe zur Folge gehabt, noch den verstärkten Einbezug weiterer Stakeholder in die Tätigkeiten der Gruppe. Lediglich im Hinblick auf die Verbesserung der Kohärenz der EU-weiten Vorgaben entsprach die Kommission somit den Wünschen beider Parteien.

Die Vorschläge der Kommission zu Verhaltensregeln und Zertifizierungen waren dermaßen unspezifisch, dass sie weder der einen noch der anderen Community zugerechnet werden können. So sah Art. 38 DSGVO-E zwar – an Art. 27 DS-RL anknüpfend – die Förderung der Ausarbeitung von Verhaltensregeln seitens Mitgliedstaaten, Aufsichtsbehörden und Kommission vor und formulierte beispielhaft Aspekte, auf die sich die Regeln beziehen könnten (Art. 38 Abs. 1 lit. a bis h), formulierte allerdings keine Anreize für Verantwortliche, wie von einigen Akteuren aus der Wirtschaft gefordert worden war. Zudem war weder der von den Datenschutzbefürwortern geforderte datenschutzrechtliche Mehrwert im Kommissionsent-

335 Zwar hatte die Kommission in EG 129 für delegierte Rechtsakte vorgesehen, dass die Kommission *im Rahmen ihrer Vorarbeiten auch auf Sachverständigenebene geeignete Konsultation durchführt*. Für Durchführungsrechtsakte hatte die Kommission allerdings keine vergleichbare Konsultationsankündigung formuliert.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wurf enthalten, noch die von den Flexibilitätsbefürwortern eingeforderte Vereinfachung des Überprüfungs- und Genehmigungsverfahrens.

Ähnlich verhielt es sich mit dem Kommissionsentwurf zur Zertifizierung in Art. 39 DSGVO-E. So formulierte Abs. 1 eine Förderpflicht für Mitgliedstaaten und Kommission, regelte diese allerdings nicht näher. Demnach sollten Betroffene mittels Datenschutzsiegeln und -zeichen in die Lage versetzt werden, das von einem Verantwortlichen gewährleistete Datenschutzniveau in Erfahrung bringen zu können. Keine Aussagen machte der Artikel hingegen zu den Anforderungen und Kriterien des Prüfverfahrens oder zu Zertifizierungsstellen. Zwar sollten die Zertifizierungsverfahren zur ordnungsgemäßen Anwendung der Verordnung beitragen und diese gegenüber potentiellen Betroffenen signalisieren, doch setzte der entsprechende Artikel keine weiteren Anreize. Wie bei vielen anderen Maßnahmen, sollte die nähere Regelung aller relevanten Details seitens der Kommission mittels delegierter bzw. Durchführungsrechtsakte erfolgen. Zum einen waren die Aussagen beider Akteursgruppen hinsichtlich der grundsätzlichen Befürwortung von Zertifizierungen beachtet worden, andererseits ließ die Abstraktheit der vorgesehenen Regelung in Kombination mit den Befugnissen, die der Kommission übertragen werden sollten, vollständig offen, auf welche Weise das Instrument konkret angewendet werden würde.

4.2.2.3.3 Erfüllung der Forderungen der Flexibilitätsbefürworter

Den Forderungen der Flexibilitätsbefürworter entsprach die Kommission vor allem auf zwei Gebieten: Bei der Abschaffung der Meldepflicht einerseits und der Vereinfachung der Übertragung personenbezogener Daten in Drittländer andererseits. Zwar war die Meldepflicht seit längerem als ein überflüssiges Überbleibsel aus der Zeit der Großrechner kritisiert worden, das im Hinblick auf den Schutz personenbezogener Daten in einer Welt allgegenwärtiger Datenverarbeitungen keinen Transparenz-Mehrwert mehr böte. Doch hatten viele Unternehmen und Verbände vor allem Erleichterungen in Form der Ausweitung der Ausnahmeregelungen (bspw. im Falle der Bestellung betrieblicher Datenschutzbeauftragter) bzw. der EU-weiten Harmonisierung der Meldepflicht bspw. durch einheitliche Meldeformulare und -register gefordert und nur ein kleiner Teil der Akteure die vollständige Abschaffung der Meldepflicht gefordert. Insofern kam die Kommission einer zentralen Forderung der Flexibilitätsbefürworter entgegen und tat dies auf eine überraschende Weise, indem sie die vollständige Abschaffung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Meldepflicht vorschlug und die Einwände der Datenschutzbefürworter, die im Hinblick auf die mögliche Reduktion bzw. Abschaffung geäußert worden waren, vollständig ignorierte.

Im Hinblick auf die Übertragung personenbezogener Daten in Drittländer sah der Kommissionsentwurf deutliche Vereinfachungen vor. So sah Art. 41 DSGVO-E vor, dass die Kommission Angemessenheitsbeschlüsse nunmehr nicht nur im Hinblick auf ein Drittland, sondern auch in Bezug auf ein Gebiet oder Verarbeitungssektor des jeweiligen Drittlandes oder einer internationalen Organisation fassen kann. Für den Fall, dass kein Beschluss gemäß Art. 41 DSGVO-E gefasst wurde, sahen die Folgeartikel außerdem die Möglichkeit der Übertragung auf Basis unternehmensinterner Vorschriften (binding corporate rules) und Standarddatenschutz- oder Vertragsklauseln vor. Insbesondere die Möglichkeit der Drittstaatentransfers auf Basis unternehmensinterner Vorschriften wurde gegenüber der DS-RL und den Forderungen der Flexibilitätsbefürworter entsprechend deutlich aufgewertet, indem die Regelung auch für Unternehmensgruppen Anwendung finden sollte. Zudem sah Art. 44 DSGVO-E zahlreiche – teils sehr weitgehende[336] – Ausnahmen vor, auf deren Basis eine internationale Datenübertragung auch in jenen Fällen, in denen die Vorgaben der Art. 41–43 nicht erfüllt sind, möglich sein sollte.

Schließlich blieb die Kommission bei der Präzisierung der Definition personenbezogener Daten grundsätzlich bei der Definition der DS-RL (Art. 4 (1)), ergänzte diese allerdings dahingehend (EG 24 DSGVO-E), dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente zwar unter Hinzuziehung zusätzlicher Informationen zur Identifikation von Betroffenen oder deren Profiling dienen könnten, als solche aber *nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind*. Der ursprüngliche Entwurf von Ende 2011 hatte dagegen noch vorgesehen, dass derartige Daten in den Anwendungsbereich der Verordnung fallen sollten. Indem die Kommission IP-Adressen etc. als nur potentiell personenbezogene Daten definierte, folgte sie tendenziell eher den Forderungen der Flexibilitätsbefürworter, die genau diese Form der Relativierung gefordert hatten. Indem die Kommission zudem nicht näher spezifizierte, unter welchen Umständen derartige Daten als personenbezo-

336 So sah Art. 44 Abs. 1 h) DSGVO-E vor, dass eine Übertragung auch dann zulässig sein sollte, wenn die Übermittlung für die Verwirklichung des berechtigten Interesses eines Verantwortlichen erforderlich ist und *nicht als häufig oder massiv* bezeichnet werden kann.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gen angesehen werden können, schrieb sie letztlich den Status Quo der DS-RL fort.

Ohne, dass dies während der Konsultationsprozesse gefordert worden war, schlug die Kommission zudem in Art. 6 DSGVO-E eine Neuerung gegenüber der DS-RL vor, mit der die Zweckbindung teilweise aufgehoben werden sollte. So sollte eine Weiterverarbeitung für Zwecke, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind, grundsätzlich möglich sein, sofern einer der in Art. 6 Abs. 1 lit. a bis f genannten Gründe[337] auf die fragliche Verarbeitung zutrifft.

Während die meisten datenschutzrechtlichen Belange entweder unmittelbar im Rahmen der DSGVO selbst oder durch die Kommission mittels delegierter oder Durchführungsrechtsakte geregelt werden sollten, eröffnete der Entwurf den Mitgliedstaaten in einigen wenigen Belangen mittels sog. Öffnungsklauseln die Möglichkeit des Erlasses abweichender, mitgliedstaatlicher Regelungen (Hornung 2012, 100; Jaspers 2012, 571). Dies betraf vor allem jene Felder, in denen die Kommission auf Seiten der Mitgliedstaaten Widerstände befürchtete. So sollten Mitgliedstaaten insbesondere die Möglichkeit erhalten, Abweichungen und Ausnahmen für Verarbeitungen zu journalistischen, künstlerischen oder literarischen Zwecken vorzusehen (Art. 80 DSGVO-E) sowie spezifische Regeln im Hinblick auf die Verarbeitung personenbezogener Daten im Beschäftigungskontext zu erlassen (Art. 82 DSGVO-E). Darüber hinaus sahen die Art. 6 Abs. 3 lit. b (Erlaubnistatbestände), Art. 8 Abs. 2 lit. b, g (besondere Kategorien personenbezogener Daten), Art. 17 Abs. 3 lit. d (Ausnahmen vom Recht auf Vergessenwerden), Art. 20 Abs. 2 lit. b (Ausnahmen vom Verbot von auf Profiling basierenden Maßnahmen), Art. 21 (Beschränkungen von Datenschutzrechten und von Pflichten aufgrund eines öffentlichen Interesses), Art. 46 und 48 (die Bestimmung der Aufsichtsbehörde), Art. 73 Abs. 2 (Verbandsklagerecht), Art. 81 (Gesundheitsdaten) und Art. 84 (Geheimhaltungspflichten) Spielräume für nationale Sonderregelungen vor.

Schließlich hatte die Kommission von weiteren, sektor- oder technologiespezifischen Legislativmaßnahmen wieder Abstand genommen, nachdem diese von den Flexibilitätsbefürwortern unter Verweis auf die Notwendigkeit der Technologieneutralität vehement abgelehnt worden waren

337 Diese umfassten neben der Einwilligung in Art. 6 Abs. 1 lit. a, beispielsweise auch die Vertragserfüllung in lit. b oder die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt in lit. e.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

und die Vorschläge auch von Seiten der Datenschutzbefürworter keine nennenswerte Unterstützung erhalten hatten.[338]

4.2.2.3.4 Erfüllung der Forderungen der Datenschutzbefürworter

Im Hinblick auf beinahe alle übrigen Elemente des DSGVO-Entwurfs folgte die Kommission dagegen eher den Positionen der Datenschutzbefürworter. Dies betrifft die Themen: Definition besonderer Kategorien personenbezogener Daten, Grundsatz der Datenminimierung, Einwilligung, Datenschutz bei Kindern, Transparenzvorgaben und Informationspflichten des Verantwortlichen, Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung, Recht auf Vergessenwerden, Recht auf Datenübertragbarkeit, Automatisierte Entscheidungen und Profiling. Privacy by Design und by Default, Dokumentationspflichten des Verantwortlichen, Meldepflicht bei Datenschutzverletzungen, Datenschutzfolgenabschätzung, Benennung eines betrieblichen Datenschutzbeauftragten, kollektive Rechtsbehelfe, Sanktionen und Geldbußen.

So erweiterte die Kommission in Art. 9 DSGVO-E die Definition besonderer Kategorien von personenbezogenen Daten um genetische Daten sowie um Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln. Damit folgte die Kommission eher der Forderung der Datenschutzbefürworter. Zwar kam die Kommission nicht der Forderung nach Einführung eines nicht-abschließenden Katalogs nach, der bei Bedarf erweitert werden kann. Von den Forderungen der Flexibilitätsbefürworter wurde jedoch keine erfüllt.

Im Hinblick auf den Grundsatz der Datenminimierung sah der Kommissionsentwurf in Art. 5 lit. c) zunächst den Richtlinienvorgaben folgend vor, dass personenbezogene Daten *dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein* müssten. Über die DS-RL hinausgehend sah der zweite Halbsatz zudem vor, dass personenbezogene Daten nur verarbeitet werden dürften, *wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogene Daten erreichten werden*

338 Einschränkend sei angefügt, dass Möglichkeiten der sektor- oder technologiespezifischen Regulierung dagegen im Rahmen der zahlreichen delegierten bzw. Durchführungsrechtsakte, die die Kommission im DSGVO-Kommissionsentwurf vorgeschlagen hatte, durchaus vorgesehen waren.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

könnten. Mit diesem Vorstoß ignorierte die Kommission die Forderungen der Flexibilitätsbefürworter nach dem Erhalt des Status Quo und folgte stattdessen den – inhaltlich nicht näher definierten – Forderungen der Datenschutzbefürworter nach einer Stärkung des Grundsatzes.

Eine Stärkung der Datenschutzvorgaben sah die Kommission auch beim Thema Einwilligung vor. Um „eine Verwechslung mit einer ‚ohne jeden Zweifel' erteilten Einwilligung zu vermeiden und sicherzustellen, dass der betroffenen Person bewusst ist, dass sie eine Einwilligung erteilt hat und worin sie eingewilligt hat" (EU-Kommission 2012d, 8), schlug die Kommission die Erweiterung der Definition um das Kriterium „explizit" vor. Auf diese Weise kam die Kommission einer der zentralen Forderungen der Datenschutzbefürworter nach, die für die Ausweitung der ausdrücklichen Einwilligung auf normale personenbezogene Daten eingetreten waren. Zudem schlug die Kommission eine weitere Ergänzung in Art. 7 Abs. 4 vor, wonach die Einwilligung keine gültige Rechtsgrundlage bieten können sollte, wenn *zwischen der Position des Betroffenen und des Verantwortlichen ein erhebliches Ungleichgewicht besteht*. Mit dieser Ergänzung folgte die Kommission klar den Vorschlägen der Datenschutzbefürworter bzw. dem Vorschlag der Datenschutzgruppe (2009, 17). Während die Kommission somit einerseits die Stärkung der Einwilligung für die meisten Datenverarbeitungen vorsah, verfolgte sie mit den Vorgaben zur Rechtmäßigkeit der Verarbeitung in Art. 6 Abs. 1 lit. f wiederum das Ziel, einige Verarbeitungen aus der Pflicht zur Einholung der expliziten Einwilligung auszunehmen. Durch den Rückgriff auf das berechtigte Interesse des Verarbeiters sollte es so insbesondere der Marketing-Branche weiterhin erlaubt sein, Daten zu verarbeiten, solange diese nicht spürbar in die Rechte der Betroffenen eingreift (Reding 2013d, 3).

Den Forderungen der Datenschutzbefürworter kam die Kommission außerdem auch beim Thema Datenschutz bei Kindern entgegen. Zwar waren die weitergehenden Vorgaben des ursprünglichen Kommissionsentwurfs verworfen worden, doch sah der DSGVO-E noch immer vor, dass Kinder, nach Art. 4 alle Personen unter 18 Jahren, bei der Abwägung mit berechtigten Interessen (Art. 6 Abs. 1 lit. f, EG 38), den Transparenzanforderungen (Art. 11 Abs. 2: „adressatengerechte Sprache"; s.a. EG 46), dem Recht auf Vergessenwerden (Art. 17 Abs. 1; EG 53) und der Pflicht zur Datenschutz-Folgenabschätzung (Art. 33 Abs. 2 lit. d) besondere Berücksichtigung erfahren. Nicht mehr enthalten waren dagegen die Vorgaben, dass die Einwilligung eines Kindes nur nach Genehmigung seitens eines Erziehungsberechtigten gültig sein sollte (vgl. Art. 7 Abs. 6 DSGVO-UE) und dass auf Pro-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

filing basierende Maßnahmen im Falle eines Kindes ausnahmslos verboten sein sollten (Art. 18 Abs. 3 DSGVO-UE). Stattdessen sah der neue Art. 8 Abs. 1 DSGVO-E vor, dass die Zustimmung eines Erziehungsberechtigten nur bis zur Vollendung des 13. Lebensjahres notwendig sein sollte. Das Profiling-Verbot wurde dagegen in die Erwägungsgründe verschoben (vgl. EG 58 DSGVO-E).

Beim Thema Transparenz und Informationspflichten des Verantwortlichen gingen die Kommissionsvorschläge über die Vorgaben der DS-RL hinaus und entsprachen somit den Forderungen der Datenschutzbefürworter nach einer Verbesserung der Transparenz. So sah Art. 11 implizit die Einführung eines Transparenz-Grundsatzes vor. Mittels Art. 11 Abs. 2 sollte zudem klargestellt werden, dass alle dem Betroffenen dargestellten Informationen *in verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache* zur Verfügung gestellt werden. Art. 14 DSGVO-E sah zudem die Ausweitung der Informationspflichten des Verantwortlichen bei der Verarbeitung personenbezogener Daten vor. Über die in Art. 10 DS-RL genannten Punkte hinausgehend, sollte dieser dem Betroffenen außerdem mitteilen: Für wie lange die erhobenen personenbezogenen Daten gespeichert werden (Art. 10 Abs. 1 lit. c); ob ein Recht auf Auskunft, Berichtigung, *Löschung* oder *Widerspruch* besteht (Art. 10 Abs. 1 lit. d); dass ein Beschwerderecht bei einer Aufsichtsbehörde besteht sowie deren Kontaktdaten (Art. 10 Abs. 1 lit. e); ob der Transfer der Daten an ein Drittland oder eine internationale Organisation beabsichtigt wird, sowie Informationen über das dort geltende Datenschutzniveau (Art. 10 Abs. 1 lit. g); und sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten (Art. 10 Abs. 1 lit. h).

Eine Stärkung des Datenschutzniveaus sah der Kommissionsentwurf auch im Hinblick auf die Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung vor. So sah Art. 12 Abs. 1 DSGVO-E die Erleichterung der Wahrnehmung der genannten Betroffenenrechte vor, u. a. indem dem Betroffenen ermöglicht wird, dass ein entsprechender Antrag elektronisch gestellt werden kann, sofern es sich bei der jeweiligen Verarbeitung um eine automatisierte Verarbeitung handelt. Art. 12 Abs. 2 sah eine Frist von einem Monat für die Beantwortung des Betroffenen-Anliegens vor, die bei Bedarf um einen Monat verlängert werden können sollte. Art. 12 Abs. 4 sah vor, dass die Auskunft im Regelfall kostenlos zu erfolgen hat, bei offenkundig unverhält-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nismäßigen Anträgen und besonders im Fall ihrer Häufung ein Entgelt verlangt oder die Maßnahme vollständig unterlassen werden kann. Zwar kam die Kommission den Wünschen eines Teils der Flexibilitätsbefürworter insofern entgegen, dass in Sonderfällen die Möglichkeit der Erhebung einer Gebühr beibehalten wurde, doch bildeten die genannten Vorschläge der Kommission insgesamt nicht nur eine deutliche, EU-weite Vereinheitlichung, sondern auch Aufwertung der Modalitäten zur Wahrnehmung der Betroffenenrechte, die den Wünschen der Datenschutzbefürworter deutlich stärker entsprach.

Das in Art. 17 DSGVO-E vorgesehene Recht auf Vergessenwerden und auf Löschung blieb zwar hinter den Erwartungen zurück, sah aber dennoch eine gewisse Stärkung gegenüber den Vorgaben der DS-RL vor. Hatte Art. 12 lit. c DS-RL vorgesehen, dass jeder Löschungswunsch *den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist*, sollte der Verantwortliche nach Art. 17 Abs. 2 DSGVO-E nunmehr *alle vertretbaren Schritte, auch technischer Art* unternehmen, um Dritte über den Löschungswunsch zu informieren. Gestrichen worden war hingegen die in Art. 15 Abs. 2 DSGVO-UE vorgesehene Pflicht, wonach der Verantwortliche nicht nur den Versuch der Mitteilung des Löschungswunsches unternehmen, sondern *sicherstellen sollte*, dass die Löschung aller Links und Kopien auch tatsächlich erfolgt. Hinter den Erwartungen zurück blieb das Recht auf Vergessenwerden deshalb, weil es in seiner im DSGVO-E vorgeschlagenen Fassung letztlich nur eine modifizierte Form des im Rahmen der DS-RL bestehenden Rechts auf Löschung darstellte und nicht die Wünsche der Datenschutzbefürworter nach einer automatisierten Löschung personenbezogener Daten bzw. nach der Einführung eines Verfallsdatums widerspiegelte. Diese Elemente nahm die Kommission vermutlich deshalb nicht auf, da der Grundsatz der Speicherbegrenzung dies teilweise sowohl im Rahmen der DS-RL als auch im Rahmen von Art. 5 lit. f DSGVO-E vorsah.

Dagegen stellte die Einführung des Rechts auf Datenübertragbarkeit in Art. 18 ein Novum dar. Nach Art. 18 Abs. 1 sollten Betroffene eine Kopie der sie betreffenden personenbezogenen Daten, die elektronisch in *strukturierten gängigen elektronischen Formaten* verarbeitet werden, erhalten können. Mit dem zweiten Abs. sollte zudem gewährleistet werden, dass die von einem Betroffenen auf Basis einer Einwilligung oder eines Vertrags zur Verfügung gestellten Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in ein anderes System überführt werden kön-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nen, ohne dabei von dem Verantwortlichen des Ursprungssystems behindert zu werden. Gegenüber dem im DSGVO-UE vorgesehenen Recht auf Datenübertragbarkeit stellte der finale Entwurf eine Schwächung dar. So hatte Art. 16 DSGVO-UE vorgesehen, dass alle personenbezogenen Daten, die *automatisiert verarbeitet* werden, von diesem Recht umfasst sein sollten. Der finale Entwurf beschränkte dies dann letztlich auf jene Daten, die in *strukturierten elektronischen Formaten* verarbeitet werden. Zwar kann die Reduzierung des Anwendungsbereichs den Flexibilitätsbefürwortern angerechnet und als Teilerfolg dieser bewertet werden (Schildberger 2016, 111), doch stellte selbst die abgeschwächte finale Fassung dieses Rechts eine deutliche Stärkung des Datenschutzniveaus gegenüber dem Status Quo der DS-RL dar.

Die Regelung zu automatisierten Entscheidungen erfuhr ebenfalls eine deutliche Stärkung gegenüber den Vorgaben der DS-RL. So sah Art. 20 Abs. 1 DSGVO-E vor, dass jede auf einer automatisierten Verarbeitung basierende *Maßnahme*, die einer *natürlichen Person* gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage ihrer beruflichen Leistungsfähigkeit usw. besteht, unzulässig sein sollte, solange keiner der in Art. 20 Abs. 2 normierten Erlaubnistatbestände greift. Art. 15 DS-RL hatte vorgesehen, dass eine solche Maßnahme eine Entscheidung darstellen muss. Eine Ausweitung stellte der Kommissionsvorschlag deshalb dar, weil eine Entscheidung voraussetzt, dass nach einer gewissen Überlegung eine Schlussfolgerung gezogen wird, während eine Maßnahme jede Vorgehensweise beinhaltet, die ergriffen wird, um zu einem beliebigen Ergebnis zu gelangen, der Anwendungsbereich also deutlich weiterreicht. Da zudem von einer natürlichen Person und nicht von Betroffenen die Rede war, umfasste der Artikel jedes Profiling, unabhängig davon, ob es sich bei einer entsprechenden Verarbeitung um personenbezogene Daten handelt oder nicht. Begrifflich spiegelte sich die Intention der Kommission, das Profiling regulieren und einschränken zu wollen auch im veränderten Titel des Artikels wider, der verändert wurde in „Auf Profiling basierende Maßnahmen". Schließlich definierte der Kommissionsvorschlag in Abs. 2 lit. a Profiling als eines der Regelbeispiele, bei denen eine Datenschutz-Folgenabschätzung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

obligatorisch erfolgen sollte.[339] So hätte der Kommissionsvorschlag, ohne dass ein Individuum selbst tätig werden muss, ein hohes Standard-Datenschutzniveau etabliert, von dem das Individuum jederzeit selbstbestimmt hätte abweichen können.

Stärker hinter den Erwartungen blieben hingegen die Vorschläge der Kommission zu Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design und by Default) zurück. So sah der das Thema Datenschutz durch Technik betreffende Art. 23 Abs. 1 vor, dass der Verantwortliche technische und organisatorische Maßnahmen und Verfahren zur Einhaltung der Verordnung und zur Wahrung der Betroffenenrechte durchzuführen hat. Ähnlich wie im Falle des Rechts auf Vergessenwerden fand das Konzept Privacy by Design auf diese Weise rhetorisch Eingang in die Verordnung. Inhaltlich blieb es aber weit entfernt von den Forderungen nach der Festschreibung eines spezifischen Schutzniveaus, das durch Privacy by Design gewahrt werden sollte. Zudem bezog sich der Kommissionsvorschlag lediglich auf Verantwortliche, definierte aber nicht genauer, ob nur Dienstebetreiber oder, wie seitens einiger Datenschutzbefürworter gefordert, auch Produkthersteller erfasst sein sollten. In ähnlicher Weise schrieb Art. 23 Abs. 2 im Hinblick auf das Thema datenschutzfreundliche Voreinstellungen lediglich die technische Umsetzung der Datenschutz-Grundsätze (insb. der Datensparsamkeit) vor. So sollte der Verantwortliche mittels geeigneter Verfahren sicherstellen, dass nur jene personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der jeweiligen Verarbeitung benötigt werden. Somit blendete dieser Teil des Satzes alle Forderungen nach der Einführung einer normativen Verpflichtung aus, indem sie die Entscheidung darüber, was als datenschutzfreundliche Voreinstellung gilt an den Verarbeitungszweck koppelte, den der jeweilige Verantwortliche selbst bestimmt können sollte. In Anknüpfung an die Debatten über Facebook, deren Standardeinstellungen zeitweilig alle Profile und Beiträge als öffentlich vorgesehen hatten, formulierte der letzte Satz desselben Absatzes allerdings die normative Vorgabe, *dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden*. Mittels delegierter Rechtsakte beabsichtigte die Kommission in Art. 23 Abs. 3 zudem, sich selbst die Befugnis zu erteilen, *etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Ver-*

339 Das in Art. 18 Abs. 3 des DSGVO-UE vorgesehene, vollständige Verbot des Profilings von Kindern schaffte es dagegen nicht mehr in den finalen Entwurf.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

fahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft. In ähnlicher Weise bezweckte die Kommission in Art. 23 Abs. 4, sich selbst die Befugnis zu erteilen, den Erlass von Durchführungsrechtsakten, um technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festzulegen.

Während somit die ersten beiden Absätze (insb. der letzte Satz des Art. 23 Abs. 2) zwar auf Elemente, die im Kontext von Privacy by Design und by Default diskutiert worden waren, Bezug nahmen, blieben die konkreten Vorschläge der Kommission weit hinter den Erwartungen zurück und wurden als entsprechend schwach wahrgenommen (vgl. z. B. Hornung 2012, 103). Allerdings ließen die meisten Analysen die Absätze drei und vier außer Acht. Ausgehend vom generellen, sehr datenschutzfreundlichen Kurs der Kommission kann angenommen werden, dass die Kommission selbst zwar eine stärkere Regelung befürwortete, aber keinen spezifischeren Regelungsvorschlag machen wollte, der zu massiver Kritik auf Seiten der Flexibilitätsbefürworter geführt hätte. So sollte die Verlagerung der Konkretisierung der Privacy by Design- und Default-Vorgaben in die Zukunft nicht nur der Machtsteigerung der Kommission dienen, – davon kann wohl ausgegangen werden – sondern auch der Reduzierung von politischen Streitigkeiten und Hindernissen auf dem Weg zur Verabschiedung ihres Legislativvorschlags dienlich sein.

Wie angekündigt, sah der Kommissionsvorschlag die Ausweitung der im Rahmen der ePrivacy-Novelle von 2009 zunächst für den Bereich der elektronischen Kommunikation erlassenen Meldepflicht auf die Verletzung aller personenbezogenen Daten aus. Die Meldung an die zuständige Aufsichtsbehörde wurde in Art. 31 und die Meldung an den Betroffenen in Art. 32 geregelt. Die in der ePrivacy-Novelle vorgesehen *unverzügliche* Benachrichtigung der zuständigen Aufsichtsbehörde wich im Kommissionsentwurf (Art. 31 Abs. 1, erster Satz) der Vorgabe, die entsprechende Behörde *ohne unangemessene Verzögerung und nach Möglichkeit binnen 24 Stunden nach Feststellung der Verletzung* zu benachrichtigen. Zudem wurde den Verantwortlichen ermöglicht, die Frist zu überschreiten, sofern der verspäteten Meldung eine Begründung beigefügt wird (Art. 31 Abs. 1, zweiter Satz). Nachdem die Aufsichtsbehörde benachrichtigt wurde, sah Art. 32 Abs. 1 vor, dass der Betroffene im Anschluss ohne *unangemessene Verzögerung* ebenfalls zu benachrichtigen ist, *wenn die Wahrscheinlichkeit besteht, dass der Schutz personenbezogener Daten oder der Privatsphäre der betroffenen Person durch eine festgestellte Verletzung des Schutzes perso-*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

nenbezogener Daten beeinträchtigt wird. Dies stellte eine Abschwächung der Vorgabe gegenüber der ePrivacy-Novelle dar. Diese hatte vorgesehen, dass die Benachrichtigung in derartigen Fällen *unverzüglich* zu erfolgen hat. Unverändert von der ePrivacy-RL übernommen wurde dagegen die in Art. 32 Abs. 2 DSGVO-E vorgesehene Möglichkeit, dass keine Benachrichtigung des Betroffenen zu erfolgen hat, falls der Verantwortliche zur Zufriedenheit der Aufsichtsbehörde nachweist, dass er geeignete technische Sicherheitsvorkehrungen getroffen hat. Durch die Einführung einer horizontalen Meldepflicht bei Datenschutzverletzungen erfüllte die Kommission eine weitere Kernforderung der Datenschutzbefürworter. Die in diesem Zusammenhang aufgestellte Kernforderung der Flexibilitätsbefürworter, wonach die Benachrichtigung der Betroffenen nur im Falle einer *drohenden schwerwiegenden Beeinträchtigung* erfolgen sollte, wurde dagegen nicht berücksichtigt. Die Kommission räumte den Verantwortlichen lediglich etwas mehr Zeit bei der Benachrichtigung des Betroffenen ein, indem die *unverzügliche* Benachrichtigung in eine Benachrichtigung *ohne unangemessene Verzögerung* abgeändert worden war.

Die in Art. 20 DS-RL vorhandene Vorabkontrolle, die bei Verarbeitungen, die spezifische Risiken beinhalten können Anwendung finden sollte, wurde im Rahmen des neuen Art. 33 zur Datenschutz-Folgenabschätzung ausgebaut. So sah Art. 33 Abs. 1 vor, dass der Verantwortliche oder der Auftragsverarbeiter bei Verarbeitungsvorgängen, *die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen*, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen hat. Diese allgemeinen Aussagen präzisierte die Kommission in Abs. 4 mittels einiger Regelbeispiele. So sollte eine Datenschutz-Folgenabschätzung insbesondere erforderlich sein: Im Falle von Profiling (lit. a), im Falle der Verarbeitung bestimmter Datenkategorien, die in Maßnahmen oder Entscheidungen resultieren sollen, welche sich auf spezifische Einzelpersonen beziehen (lit. b), bei weiträumiger Überwachung öffentlich zugänglicher Bereiche, insb. mittels Videoüberwachung (lit. c), bei der Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten (lit. d) sowie bei Verarbeitungen, bei denen die Zurateziehung der zuständigen Aufsichtsbehörde nach Art. 34 Abs. 2 erforderlich ist. In den folgenden Absätzen (Art. 33 Abs. 3–5) machte die Kommission grobe Vorgaben hinsichtlich des Inhalts und des Verfahrens, insbesondere verpflichtete Art. 33 Abs. 4 den Verantwortlichen dazu, die Meinung der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

betroffenen Personen oder ihrer Vertreter einzuholen. Art. 34 Abs. 2 sah vor, dass der Verantwortliche, sofern aus einer DSFA hervorgeht, dass *hohe konkrete Risiken* zu erwarten sind, die zuständige Aufsichtsbehörde zurate ziehen muss, damit sichergestellt wird, dass die Vorgaben der DSGVO eingehalten und die Risiken für Betroffene wirksam gemindert werden. Schließlich eröffneten Art. 34 Abs. 4 und 5 Datenschutzaufsichtsbehörden die Möglichkeit, konkrete Listen von Verarbeitungsvorgängen zu erstellen, die Gegenstand der vorherigen Zurateziehung nach Art. 34 Abs 2 sein sollen. Im Rahmen von Art. 33 Abs. 6 schlug die Kommission zudem vor, sich selbst die Ermächtigung zu erteilen, Kriterien und Bedingungen für riskante Verarbeitungsvorgänge zu spezifizieren sowie die Anforderungen an das DSFA-Verfahren gem. Art. 33 Abs. 3 zu spezifizieren. Art. 34 Abs. 8 sah zudem die Festlegung von Kriterien und Anforderungen für die Bestimmung der in Art. 34 Abs. 2 genannten hohen konkreten Risiken vor. Wie im Falle der Vorschläge zu Privacy by Design und by Default versuchte die Kommission beim Thema Datenschutz-Folgenabschätzung eher abstrakte Vorgaben durchzusetzen, die später von ihr konkretisiert werden sollten. Dennoch beinhaltete der Vorschlag der Kommission verbindliche DSFA-Vorgaben für eine Reihe spezifischer Verarbeitungsvorgänge (darunter insb. Profiling), wodurch die Forderung der Flexibilitätsbefürworter nach einer möglichst flexiblen Ausgestaltung der DSFA-Vorgaben weitgehend ignoriert wurde. Die nicht weiter spezifizierte Forderung der Datenschutzbefürworter nach Einführung einer DSFA-Vorgabe wurde somit von der Kommission berücksichtigt.

Ein weiteres Gebiet, auf dem die Kommission den Forderungen der Datenschutzbefürworter entgegenkam, ist das Thema der Bestellung eines betrieblichen Datenschutzbeauftragten. Diese sollte nach Art. 35 Abs. 1 verpflichtend sein für alle Behörden (lit. a), für Unternehmen mit mindestens 250 Beschäftigten (lit. b) und wenn die Kerntätigkeit eines Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, die die regelmäßige und systematische Beobachtung Betroffener erfordern (lit. c). Mittels eines delegierten Rechtsaktes gemäß Abs. 11 beabsichtigte die Kommission zudem für sich selbst die Möglichkeit vorzusehen, Kriterien und Anforderungen für die in lit. c genannte Kerntätigkeit näher zu definieren. In den Folgeabsätzen wurde zudem die Möglichkeit eingeräumt, dass eine Unternehmensgruppe in besonderen Fällen einen gemeinsamen Datenschutzbeauftragten benennen kann (Abs. 2) und dass der betriebliche Datenschutzbeauftragte nicht beim Verantwortlichen selbst beschäftigt sein muss, sondern extern beauftragt werden kann (Abs. 8). Somit kam die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kommission der Forderung der Datenschutzbefürworter nach der Einführung einer Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten weitgehend nach. Durch die Ausnahme für Unternehmen mit weniger als 250 Beschäftigten intendierte die Kommission zugleich die Entlastung von KMUs zu erreichen, während mit Art. 35 Abs. 1 lit. c sichergestellt werden sollte, dass besonders sensible Verarbeitungsvorgänge auch dann in den Anwendungsbereich fallen, wenn diese von KMUs durchgeführt werden. Indem die Bestellung eines betrieblichen Datenschutzbeauftragten somit an verbindliche gesetzliche Vorgaben gekoppelt wurde, ignorierte die Kommission auch bei diesem Thema die Forderung der Flexibilitätsbefürworter, wonach die Verantwortlichen über die Bestellung selbst entscheiden können sollten. Unberücksichtigt blieb auch deren Forderung nach einem Anreizsystem. Indem die Kommission zudem die vollständige und bedingungslose Abschaffung der Meldepflicht angekündigt hatte, raubte sie den einzigen Anreiz, der während der Konsultationen seitens einiger Wirtschaftsvertreter positiv hervorgehoben worden war.

In Art. 73 Abs. 2 DSGVO-E schlug die Kommission schließlich die Einführung eines Verbandsklagerechts vor. Demnach sollten „Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben" das Recht erhalten, im Namen einer oder mehrerer Betroffener Beschwerde bei einer Aufsichtsbehörde einzulegen. Darüber hinaus ermöglichte Abs. 3 denselben Stellen die Beschwerde bei einer Aufsichtsbehörde auch unabhängig von der Beschwerde eines Betroffenen, falls sie der Ansicht waren, dass der Schutz personenbezogener Daten verletzt wurde. Schließlich sah Art. 76 Abs. 1 vor, dass die genannten Einrichtungen, Organisationen oder Verbände im Namen des Betroffenen gegen Aufsichtsbehörden und Verantwortliche klagen konnten. Die Kernforderung der Datenschutzbefürworter nach der Einführung eines Verbandsklagerechts wurde somit erfüllt. Unberücksichtigt blieb lediglich die seitens der Verbraucherschutzorganisationen geforderte Sammelklage. Die ablehnenden Äußerungen der Flexibilitätsbefürworter blieben dagegen auch bei diesem Thema unberücksichtigt.[340]

340 Dass die Kommission nicht die Einführung von Sammelklagen vorschlug kann nicht als Erfolg der Flexibilitätsbefürworter-Community angesehen werden, da die Kommission – zumindest im Zusammenhang mit der Datenschutz-Reform – ohnehin zu keinem Zeitpunkt öffentlich die Einführung eines Rechst auf Sammelklagen diskutiert hatte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Das letzte wichtige Thema, bei dem die Kommission eine deutliche Stärkung des datenschutzrechtlichen Rahmens vorgesehen hatte, bildet das Thema Sanktionen und Geldbußen. So sahen die Art. 78 bzw. Art. 79 die EU-weite Vereinheitlichung und drastische Erhöhung des möglichen Sanktionsrahmens vor, indem Aufsichtsbehörden die Möglichkeit eröffnet werden sollte, Geldbußen bis zu 1 Mio. € oder 2% des weltweiten Jahresumsatzes eines Unternehmens verhängen zu können. Zwar hatte der ursprüngliche Kommissionsentwurf das maximale Sanktionsmaß bei 5% des weltweiten Jahresumsatzes eines Unternehmens angesetzt, sodass der finale Kommissionsentwurf in Relation dazu als deutliche Schwächung zu werten ist. Im Vergleich zu den Vorgaben der DS-RL und deren divergierender Umsetzung in den Mitgliedstaaten stellte dies noch immer eine massive Stärkung der Sanktionsvorgaben dar. Somit folgte die Kommission auch bei diesem Thema den Forderungen der Datenschutzbefürworter und kam nicht dem, seitens der Flexibilitätsbefürworter geforderten, Erhalt des Status Quo der DS-RL nach.

4.2.2.4 Entscheidende Gründe für das Zustandekommen des Kommissionsentwurfs

Die Diskussion der inhaltlichen Überschneidung zwischen den von den Akteuren getragenen Überzeugungen und dem DSGVO-Kommissionsentwurf (vgl. 4.2.2.3) zeigt, dass der DSGVO-Entwurf zahlreiche Elemente enthielt, die von der Advocacy-Koalition der Datenschutzbefürworter gefordert worden waren. Wie schon in der ersten Phase, erfüllen die inhaltlichen Überschneidungen die Anforderungen an einen Hoop-Test. Die Ausführungen zur Datenschutzbefürworter-Advocacy-Koalition in 4.2.1.2 zeigten außerdem, dass während der Entwurfsphase ein reger Austausch zwischen den zuständigen Kommissionsstellen und den übrigen Koalitionsakteuren stattgefunden hat. Schließlich waren die zuständigen Kommissionsstellen und insb. Kommissarin Reding in starkem Maße von der Datenschutzreform und ihren Inhalten überzeugt, folgten also nicht bloß externen Empfehlungen, sondern einer hohen intrinsischen Motivation zur Stärkung des EU-Datenschutzrahmens.

Somit verweisen die Erkenntnisse wieder darauf, dass das Zustandekommen des DSGVO-Entwurfs sowohl auf den inhärenten Überzeugungen der zuständigen Kommissionsstellen als auch auf dem Input der übrigen Datenschutzbefürworter basierte. Dass die Überzeugungen der Flexibilitätsbefür-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

worter nur in geringem Maße Eingang in den Verordnungsvorschlag fanden, hat aber zusätzliche Gründe, die ich im Folgenden darlegen möchte.

Der entscheidendste Grund war wohl die von Kommissarin Reding vertretene Ansicht, dass personenbezogene Daten verarbeitende Unternehmen nicht ausreichend behutsam mit den Daten umgingen. In besonderem Maße kritisierte sie, dass Datenschutzgesetze von den Unternehmen nicht ernst genommen und in zu vielen Fällen keine angemessenen Sicherheitsvorkehrungen getroffen würden, in deren Folge es zu den zahlreichen Datenpannen gekommen sei und dass Datenverarbeitungen in vielen Fällen ohne die Kenntnis der Nutzerinnen und Nutzer bzw. der Betroffenen erfolgten. Dieser sorglose Umgang, so Reding, führe wiederum zur Erosion des gesellschaftlichen Vertrauens in die Informationsgesellschaft und verringere die Bereitschaft der Bevölkerung, datenverarbeitende Dienste zu nutzen, worunter letztlich die europäische Wirtschaft leide. Ich bin zwar durchaus der Ansicht, dass Reding zu jenen Akteuren zählt, die den Grundrechtscharakter des Datenschutzrechts glaubwürdig anerkennen. Allerdings bin ich zugleich der Meinung, dass sie, anders als praktisch alle anderen Akteure aus der Advocacy-Koalition der Datenschutzbefürworter, in ebenso starkem Maße der Ansicht war, dass strengere Datenschutzregelungen nicht alleine oder vor allem aufgrund ihrer grundrechtlichen Bedeutung erlassen werden sollten, sondern im Hinblick auf die Wiederherstellung des Vertrauens in die Informationsgesellschaft, die zu einer verstärkten Nutzung und zu Wirtschaftswachstum führen würden (Euractiv 2011).

Daneben wirkte das 2011 (und damit zu einem relativ frühen Zeitpunkt) praktizierte aggressive Lobbying der Wirtschaftsvertreter eher abschreckend auf die zuständigen Kommissionsstellen. Dies möchte ich anhand von zwei Beispielen verdeutlichen. Zum einen musste das Insistieren der Flexibilitätsbefürworter auf einem in möglichst vielen Bereichen auf Selbstregulierung basierenden Datenschutzrahmen angesichts der schlechten Erfahrungen, die mit Selbstregulierung gesammelt worden waren, befremdlich auf die Kommission wirken. Selbstregulierungsmaßnahmen hatten sich im Zuge der DS-RL etwa unter Rückgriff auf das Mittel nationaler oder EU-weiter Verhaltensregeln im Hinblick auf die Information der Betroffenen, die Einholung der Einwilligung, usw. ergeben, doch war diese Möglichkeit seitens der datenverarbeitenden Wirtschaft so gut wie gar nicht genutzt worden. Trotz vielfacher Bemühungen und Aufrufe seitens der Kommissi-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

on,[341] konnten die Wirtschaftsakteure zu keinen nennenswerten Schritten in diese Richtung bewegt werden. Diese beklagten sich stattdessen – zwar durchaus zu Recht – über das mühselige und EU-weit nicht ausreichend harmonisierte Genehmigungsverfahren (vgl. 4.2.1.3.2), doch äußerte sich der Unwille der Datenverarbeiter zu Selbstregulierungsmaßnahmen auch bei Themen, die über das Instrument der Verhaltensregeln hinausgehen. So hatte die Kommission beispielsweise im Jahr 2009 unter Verzicht auf den Erlass staatlicher Vorschriften mit 17 Webseitenbetreibern die sog. *Safer Social Networking Principles* (EK 2009) ausgehandelt, wonach sich die Betreiber auf Basis von Selbstregulierungsmaßnahmen zur Verbesserung der Sicherheit Minderjähriger verpflichteten. Als die Kommission mehr als zwei Jahre später eine Überprüfung der Einhaltung der Selbstverpflichtung vornahm, hielten nur zwei der Webseiten diese in zufriedenstellendem Maße ein (EK 2011).[342]

Zum anderen musste das Taktieren der Flexibilitätsbefürworter während des Lobbyings auf die Kommission unaufrichtig wirken. Die ICDP beispielsweise gab als Grund für die Ablehnung gesetzlicher DSFA-Vorgaben die Befürchtung an, dass viele Unternehmen und insbesondere KMU mit der Einhaltung 27 national unterschiedlich umgesetzter DSFA-Regeln überfordert sein würden (ICDP 2011, 8 f.). Die darin zum Ausdruck kommende Befürchtung über das unzureichende Harmonisierungsniveau widersprach sowohl den eigenen Forderungen als auch den damaligen politischen Entwicklungen. So hatte die ICDP in ihrer Stellungnahme, wie die allermeisten am politischen Verfahren beteiligten Akteure auch, auf die EU-weite Harmonisierung der datenschutzrechtlichen Regeln gedrängt. Zudem hatte die Kommission bereits in ihrem 2010 veröffentlichten Gesamtkonzept die Harmonisierung als ein Kernziel angegeben. Entsprechend war eher davon auszugehen, dass die Datenschutzregeln harmonisiert würden, sodass die Ablehnung von verpflichtenden DSFA-Vorgaben unter Verweis auf die zu erwartende unterschiedliche Implementierung in den Mitgliedstaaten entweder als inhaltliche Fehleinschätzung zu bewerten ist, oder als bewusstes taktisches Kalkül, mit der eine ungerechtfertigte Diskreditierung der Kommissionspläne angestrebt wurde. Ersteres halte ich, angesichts der datenschutzpolitischen Expertise der beteiligten Organisationen, für unwahr-

341 Vgl. insb. die Kritik in den Berichten über die Durchführung der DS-RL (KOM 2003, 28, 2007, 5).

342 Ähnliche Erfahrungen waren schon länger in den Vereinigten Staaten gesammelt worden (Gellman und Dixon 2016).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

scheinlich.[343] Diese und vergleichbare andere Verzerrungen machten auf die zuständigen Kommissionsstellen den Eindruck, dass „ohne zu zucken Unwahrheiten verbreitet" (Schildberger 2016, xliv) wurden, so lange es den eigenen Zielen dient.

4.2.2.5 Zwischenfazit

Die Prozessanalyse der Entwurfsphase hat gezeigt, dass die Kommission trotz des Versuchs, die DSGVO als Erleichterung für Unternehmen zu bewerben, letztlich eine Maßnahme vorgeschlagen hatte, die die Forderungen der Flexibilitätsbefürworter weitestgehend ignorierte und stattdessen im Hinblick auf viele und die wichtigsten Themen die Forderungen der Datenschutzbefürworter übernahm. Interessanterweise veränderte sich die Argumentationsstrategie der Kommission mit der Veröffentlichung des Kommissionsvorschlags leicht. So hatten Reding und ihr Team zunächst durchaus offen kommuniziert, dass die neuen Datenschutzregeln zu höheren Kosten führen würden. Allerdings war argumentiert worden, dass die höheren Kosten durch höhere Gewinne mehr als ausgeglichen würden, sobald das Vertrauen der Bevölkerung in die datenverarbeitende Wirtschaft wiederhergestellt wird (Euractiv 2011; Reding 2011a).[344] Nach der Veröffentlichung des Kommissionsvorschlags wurde dann in stärkerem Maße auf die konkreten Kostensenkungen verwiesen, die insb. durch den Wegfall der Meldepflicht und die EU-weiten Harmonisierung zu erwarten seien.

Insofern spielte die Kommission nicht mit offenen Karten, sondern versuchte, ihre grundrechtsorientierte Maßnahme als Maßnahme zur Binnenmarktförderung zu tarnen. An dieser Stelle lassen sich zwar nur Mutmaßungen anstellen, doch denke ich, dass das Motiv der Kommission der

343 In ähnlicher Weise waren regulatorische Vorgaben zur Erhöhung der Transparenz unter Verweis auf die damit einhergehende Überforderung der Individuen abgelehnt worden, ohne darauf einzugehen, dass die Kommission sich über diese Diskrepanz im Klaren war und mit ebenjenen Vorgaben zugleich die Verbesserung der Verständlichkeit anstrebte.

344 Ein Teil des Arguments kündigte zudem Wettbewerbsvorteile für EU-Unternehmen an: „Die neuen Vorschriften verschaffen den Unternehmen aus der EU ferner einen Vorteil im globalen Wettbewerb. Aufgrund des neuen Rechtsrahmens werden sie ihren Kunden zusichern können, dass wichtige personenbezogene Informationen mit der notwendigen Sorgfalt behandelt werden. Das Vertrauen in einen kohärenten EU-Rechtsrahmen ist ein entscheidender Vorteil für Diensteanbieter und ein Anreiz für Investoren, die bei der Standortsuche nach optimalen Bedingungen Ausschau halten." (EU-Kommission 2012a, 8)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

(verzweifelte) Versuch war, Widerstand auf Seiten der Wirtschaft gegen die von der Kommission intendierte Stärkung des Datenschutzrechts, die notwendigerweise zu einer Mehrbelastung der Unternehmen führen musste, zu reduzieren. Mehrere Gründe sprechen für die Richtigkeit dieser Sichtweise. Wie ich bereits zuvor mehrfach dargelegt habe, hatte die Kommission – trotz einiger Rückzieher – tendenziell eine stets datenschutzfreundliche Politik betrieben (vgl. 3.5.2.1.1). Diese hatte sich Ende der 2000er-Jahre in einer institutionellen Position manifestiert, die mit Nachdruck auf die Reform und Stärkung des EU-Datenschutzrahmens drängte. Ausschlaggebend in dieser Hinsicht waren die institutionellen und rechtlichen Veränderungen infolge des Inkrafttretens des Lissabon-Vertrags, die weitere Stärkung der Position der Datenschutzbefürworter durch die Übernahme des Justiz-Kommissariats-Postens seitens Viviane Reding und durch die Schaffung einer für Datenschutz federführend zuständigen Justiz-GD und nicht zuletzt der Wandel in der öffentlichen Meinung (vgl. 3.4.2.2) der als ermöglichender Faktor wirkte. In der Summe hatte sich für die Datenschutzbefürworter (inklusive der mit Datenschutz befassten Kommissionsstellen) eine historische Gelegenheit ergeben, die Reform und Stärkung des Datenschutzrechts voranzubringen.

Da im Rahmen der Konsultationen der Wirtschaft klargeworden war, dass eine starke Abneigung dieser gegen eine Stärkung des Datenschutzrechts vorherrschte und aus dem Eigeninteresse der Kommission hinsichtlich der Veröffentlichung eines Legislativvorschlags, der auf möglichst wenig Widerstand stößt und erfolgreich zu Ende verhandelt wird, war die Kommission gezwungen, entweder die vorgesehene Stärkung der datenschutzrechtlichen Vorgaben zurückzufahren oder zu versuchen, den Widerstand der Wirtschaft auf andere Weise möglichst gering zu halten. Ersteres kam nicht infrage, weil die federführenden Akteure in der Kommission auf Basis starker Pro-Datenschutz-Grundüberzeugungen handelten. Entsprechend blieb nur die Möglichkeit, den Reformvorschlag zumindest rhetorisch als eine Maßnahme zur Reduktion von Kosten zu bewerben, damit der Widerstand auf Seiten der Wirtschaft möglichst gering bleibt. Wie die folgende Lobby-Schlacht im Kontext der Erarbeitung und Finalisierung des Parlaments-Berichts zeigen wird, scheiterte dieser Versuch der Kommission.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Flexibilitätsbefürworter	DSGVO-E	Datenschutzbefürworter	Kompromisswillige
B1 Einschätzung des techn. Wandels	3	4	5	4
B2 Grad an erwünschter staatlicher oder privater Aktivität	2	5	5	3
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	2	5	5	3
C1C Definition personenbezogener Daten	2	4	5	3
C 2 C Grundsatz der Datenminimierung	3	4	4	4
C3D Bedingungen für die Einwilligung	2	5	4	3
C 4 A Besondere Kategorien personenbezogener Daten	2	4	5	3
C 4 D Datenschutz bei Kindern	3	5	5	4
C5A Transparenz	2	4	4	4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4	4	3
C 5 E Recht auf Vergessenwerden	2	4	4	3
C 5 G Recht auf Datenportabilität	2	5	5	4
C 5 L Benachrichtigung bei Datenschutzverletzungen	2	4	4	4
C 6 B Privacy by Design	2	4	5	4
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	2	4	4	3
C 6 N Rechenschaftspflicht	2	4	5	4
C 7 Übermittlung in Drittstaaten	2	4	4	3
C 13 A Verhaltensregeln	2	4	4	3
C 13 B Zertifizierungen/Gütesiegel	2	3	4	3
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	2	4	5	3
C 13 D Datenschutz-Folgenabschätzung	2	4	5	3
C 17 D Verbands- /Sammelklagerecht	2	4	5	3
C 17 E Sanktionen und Geldbußen	2	4	5	3

Tabelle 4-28: Die Positionen der beiden Advocacy-Koalitionen bzw. der Community im Vergleich zur Kommissionsposition während der Orientierungsphase (eigene Erhebung, Berechnung der Koalitionspositionen mittels SPSS, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum Kommissionsentwurf)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3 Konfliktphase (2012–2015)

Nachdem das ordentliche Gesetzgebungsverfahren der EU mit der Veröffentlichung des Kommissionsentwurfs zur DSGVO am 25. Januar 2012 initiiert worden war, mussten das EP sowie der Rat Stellung zum Vorschlag der Kommission nehmen und im Anschluss eine interinstitutionelle Einigung erzielen.

Die Parlamentsposition wurde zwischen Februar 2012 und Oktober 2013 im federführenden LIBE-Ausschuss und den mitberatenden Ausschüssen erarbeitet und am 21. Oktober 2013 (bei 48 Für-Stimmen, 1 Gegenstimme und 3 Enthaltungen) zunächst im LIBE-Ausschuss angenommen. Vom Parlamentsplenum verabschiedet wurde der LIBE-Bericht am 12. März 2014 (bei 621 Für-Stimmen, 10 Gegenstimmen und 22 Enthaltungen).

Nachdem partielle allgemeine Ausrichtungen im Hinblick auf mehrere wichtige Kapitel auf verschiedenen Ratssitzungen seit Mitte 2014 gebilligt worden waren, erfolgte die Verabschiedung der endgültigen allgemeinen Ausrichtung[345] des Rates auf der Ministerratssitzung vom 15./16. Juni 2015 (EU-Ministerrat 2015b, 3).

345 Diese allgemeine Ausrichtung des Rates bildete zwar informell die Position des Rates in erster Lesung ab, wurde formell aber nicht als solche verabschiedet. Erst der im Rahmen der informellen Trilog-Verhandlungen vereinbarte Kompromisstext wurde später als offizielle Ratsposition in erster Lesung verabschiedet. Das ordentliche Gesetzgebungsverfahren der EU sieht vor, dass zunächst das Parlament seine formelle Position in erster Lesung verabschiedet. Im Anschluss kann der Ministerrat die Parlamentsposition bestätigen oder einen abweichenden Standpunkt in erster Lesung verabschieden, worauf das Parlament in einer zweiten Lesung reagieren muss. In der Regel dient die Festlegung einer allgemeinen Ausrichtung des Ministerrats der Beschleunigung des Gesetzgebungsverfahrens, indem es in jenen Fällen Anwendung findet, in denen das Parlament noch keinen Standpunkt in erster Lesung festgelegt hat und dadurch die Möglichkeit erhält, auf die Ansichten des Ministerrats zu reagieren und das Verfahren innerhalb einer Lesung abzuschließen (EU-Ministerrat 2018a, 2019). Im Rahmen des Aushandlungsprozesses zur DSGVO wurde die allgemeine Ausrichtung des Ministerrats mehr als ein Jahr nach der in erster Lesung verabschiedeten Parlamentsposition angenommen. Eine Verkürzung des Verfahrens stellte dies dennoch dar, weil eine 2. formelle Lesung im Rat sowie die formelle Stellungnahme der Kommission entfielen. Wenn im Folgenden von der Ministerratsposition die Rede ist, meine ich stets die im Sommer 2015 verabschiedete allgemeine Ausrichtung des Ministerrats. Bevor sich der Ministerrat auf eine allgemeine Ausrichtung einigt, werden im Hinblick auf Teilbereiche enes verhandelten Legislativvorschlags sog. partielle allgemeine Ausrichtungen angenommen, die unter dem Vorbehalt der späteren Veränderbarkeit ein gewisses Maß an Einigung demonstrieren (ebd.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nur eine Woche nach Billigung der Ratsposition wurden die interinstitutionellen Verhandlungen im Rahmen des Trilogs aufgenommen. Die Verhandlungsführer des Parlaments und des Rates berieten unter Beteiligung der Kommission zwischen dem 24. Juni 2015 und dem 15. Dezember 2015 über einen Kompromiss. Der Kompromisstext zur Datenschutz-Grundverordnung und der JI-Richtlinie wurde auf der letzten Trilog-Sitzung am 15. Dezember informell verabschiedet (EU-Kommission 2015), am 17. Dezember zunächst vom LIBE-Ausschuss mit 48 Stimmen (bei 4 Gegenstimmen und 4 Enthaltungen) (EU-Parlament 2015) und einen Tag später am 18. Dezember auch vom AStV bestätigt (EU-Ministerrat 2015c).

Nachdem die Texte durch Rechts- und Sprachsachverständige überarbeitet wurden, verabschiedete der Ministerrat die Kompromisstexte am 8. April 2016 als Standpunkt des Rates in erster Lesung (Council of the EU 2016). Diesem stimmte zunächst der LIBE-Ausschuss am 12. April 2016 fast einstimmig zu (Albrecht 2016b). Im Anschluss billigte das Parlament den Kompromisstext am 14. April 2016 in zweiter Lesung ohne weitere Abstimmung und beauftragte den Parlamentspräsidenten, den Vorschlag final zu unterzeichnen (EU-Parlament 2016, 2).

Am 27. April 2016 unterzeichnete dieser schließlich gemeinsam mit dem Präsidenten des Ministerrats die Datenschutz-Grundverordnung mit der finalen Bezeichnung *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)* (Europäische Union 2018).

4.3.1 Akteursanalyse

4.3.1.1 Cluster-Analyse

Auch für die dritte Phase wurde eine große Zahl an Cluster-Analysen mit Verschiedenen Item-Kombinationen getestet. Nachdem anfangs jene Items mit möglichst wenigen fehlenden Werten verwendet wurden, wurde die Items-Liste nach und nach erweitert, bis zuverlässige Ergebnisse vorlagen. Die Liste der final verwendeten 23 Items kann Tabelle 4-29 entnommen werden. Der Anteil der fehlenden Werte lag in Phase 3 bei durchschnittlich 41,9%. Vollständige Werte lagen in der Konfliktphase lediglich für das Item *B3 Grundlegende Policy-Orientierung im Falle staatlicher Intervention* vor.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Dies lag daran, dass mit der Veröffentlichung des Verordnungsvorschlags die Frage nach dem *ob* einer regulativen, staatlichen Intervention, die zuvor von Item *B2 Grad an erwünschter staatlicher oder privater Aktivität* abgebildet wurde, entschieden war und nur noch das *wie*, das von Item B3 abgebildet wird, zur Debatte stand. Ansonsten betrug der Anteil fehlender Werte beim Item C3D 17,7%, gefolgt von C5E (30,2%) und C17E (32,3%). Die höchsten Anteile fehlender Werte waren bei den Items C13B (66,7%), C13A (58,3%) und C17D (57,3%) anzutreffen.

Item	N	Mean	Std. Deviation	Missing	
				Count	Percent
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventione	96	2,7	1,18	0	0
C1B Räumliche Anwendungsbereich	39	3,51	1,167	57	59,4
C1C Definition personenbezogener Daten	51	3,02	1,273	45	46,9
C 2 C Grundsatz der Datenminimierung	49	3,04	0,735	47	49
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	55	2,36	1,128	41	42,7
C3C Verarbeitung zu anderen Zwecken	45	2,44	1,423	51	53,1
C3D Bedingungen für die Einwilligung	79	2,63	1,283	17	17,7
C 4 A Besondere Kategorien personenbezogener Daten	45	3,2	1,14	51	53,1
C5A Transparenz	63	2,68	1,202	33	34,4
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	60	2,83	1,092	36	37,5
C 5 E Recht auf Vergessenwerden	67	2,69	1,018	29	30,2
C 5 G Recht auf Datenportabilität	56	2,91	1,352	40	41,7
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	58	2,88	1,299	38	39,6
C 5 L Benachrichtigung bei Datenschutzverletzungen	62	2,48	0,954	34	35,4
C6A Privacy by Default	50	2,62	1,338	46	47,9
C 6 B Privacy by Design	55	2,58	1,243	41	42,7
C 7 Übermittlung in Drittstaaten	57	2,65	1,094	39	40,6
C 13 A Verhaltensregeln	40	1,97	1,121	56	58,3
C 13 B Zertifizierungen/Gütesiegel	32	2,81	1,256	64	66,7
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	57	2,88	1,181	39	40,6
C 13 D Datenschutz-Folgenabschätzung	62	2,52	1,225	34	35,4
C 17 D Verbands- /Sammelklagerecht	41	2,8	1,616	55	57,3
C 17 E Sanktionen und Geldbußen	65	2,71	1,195	31	32,3
Durchschnitt					41,9

Tabelle 4-29: Überblick über die verwendeten Items und Missing Value Analysis (Quelle: Eigene Auswertung, berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zur Bestimmung der Cluster-Anzahl begann ich die Analyse erneut mit einem 2-Cluster-Modell und ergänzte dieses im Anschluss um ein 3-Cluster-Modell. Auch in dieser Phase wurde deutlich, dass das 2-Cluster-Modell ungeeignet ist, um die Konfliktfronten akkurat abzubilden. Insbesondere dem Cluster der Datenschutzbefürworter wurden dabei Akteure mit sehr unterschiedlichen Positionen zugeordnet. Beim 3-Cluster-Modell wurden 23 Akteure der Flexibilitätsbefürworter und 9 Akteure der Datenschutzbefürworter dem neuen Cluster zugeordnet (vgl. Cluster 1 in Tabelle 4-30). Auch die Cluster-Zentren aller 3 Cluster waren ausreichend weit voneinander entfernt.

Zur weiteren Erhärtung der Ergebnisse führte ich ergänzend 4- und 5-Cluster-Modell-Analysen durch. Das 4-Cluster-Modell teilte einen Teil der in Cluster 1 zugeordneten Akteure gemeinsam mit weiteren, den Flexibilitätsbefürwortern zugeordneten Akteuren einem neuen, vierten Cluster zu. Die Cluster-Zentren der einzelnen Items des vierten Clusters wichen zwar nur in geringem Maße vom Cluster der Flexibilitätsbefürworter ab, doch wurde so bereits deutlich, dass das neue Cluster jene Akteure zusammenfasste, die eine extrem Flexibilitätsfreundliche Haltung vertreten hatten. Um auszutesten, ob bei einem 5-Cluster-Modell eine ähnliche Aufspaltung der Datenschutzbefürworter erfolgen würde, setzte ich auch diese Variante um. Das Grundgerüst des 4-Cluster-Modells blieb dabei stabil und die Gruppe der Datenschutzbefürworter wurden in zwei Cluster aufgespalten. Der Vergleich der Cluster-Zentren der einzelnen Items des neuen Clusters (vgl. Cluster 4 in Tabelle 4-31) und des Datenschutzbefürworter-Clusters offenbarte, dass im neuen Cluster jene Datenschutzbefürworter zusammengefasst wurden, die etwas weniger extreme Positionen vertreten hatten. Der Vorzug des 5-Cluster-Modells besteht darin, eine Differenzierung zwischen extremen und eher gemäßigten Datenschutz- bzw. Flexibilitätsbefürwortern vornehmen zu können. Da dieses Modell somit eine feingranulare Differenzierung der Akteurspositionen versprach, orientierte ich mich im Folgenden an diesem.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster		
	1	2	3
B3 Grundlegende Policy-Orientierung im Falle staatlicher Intervention	3	5	3
C1B Räumliche Anwendungsbereich	4	5	3
C1C Definition personenbezogener Daten	4	5	3
C 2 C Grundsatz der Datenminimierung	4	4	3
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	3	4	3
C3C Verarbeitung zu anderen Zwecken	3	5	4
C3D Bedingungen für die Einwilligung	4	5	3
C 4 A Besondere Kategorien personenbezogener Daten	4	5	3
C5A Transparenz	3	5	3
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	5	3
C 5 E Recht auf Vergessenwerden	3	3	2
C 5 G Recht auf Datenportabilität	4	5	1
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	3	5	3
C 5 L Benachrichtigung bei Datenschutzverletzungen	3	4	1
C6A Privacy by Default	3	5	2
C 6 B Privacy by Design	3	5	2
C 7 Übermittlung in Drittstaaten	4	5	3
C 13 A Verhaltensregeln	3	4	3
C 13 B Zertifizierungen/Gütesiegel	4	5	1
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	3	5	2
C 13 D Datenschutz-Folgenabschätzung	3	5	1
C 17 D Verbands- /Sammelklagerecht	3	5	1
C 17 E Sanktionen und Geldbußen	5	3	1

Tabelle 4-30: Finale Zentren der K-Means-Clusteranalyse mit 3 Clustern (berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster				
	1	2	3	4	5
B3 Grundlegende Policy-Orientierung im Falle staatlicher Intervention	3	5	2	4	2
C1B Räumliche Anwendungsbereich	3	5	3	4	3
C1C Definition personenbezogener Daten	4	5	3	4	2
C 2 C Grundsatz der Datenminimierung	3	4	3	4	2
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	2	4	2	3	2
C3C Verarbeitung zu anderen Zwecken	3	5	2	2	1
C3D Bedingungen für die Einwilligung	4	5	2	5	1
C 4 A Besondere Kategorien personenbezogener Daten	3	5	3	4	3
C5A Transparenz	3	5	2	4	2
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	5	3	4	2
C 5 E Recht auf Vergessenwerden	3	4	2	4	2
C 5 G Recht auf Datenportabilität	3	5	3	5	2
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	3	5	3	5	2
C 5 L Benachrichtigung bei Datenschutzverletzungen	3	4	2	4	2
C6A Privacy by Default	4	5	2	4	1
C 6 B Privacy by Design	3	4	2	4	1
C 7 Übermittlung in Drittstaaten	3	5	2	4	2
C 13 A Verhaltensregeln	3	4	2	4	1
C 13 B Zertifizierungen/Gütesiegel	4	5	2	4	2
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	3	5	2	4	2
C 13 D Datenschutz-Folgenabschätzung	2	5	2	4	1
C 17 D Verbands- /Sammelklagerecht	3	5	2	5	2
C 17 E Sanktionen und Geldbußen	4	4	3	4	1

Tabelle 4-31: Finale Zentren der K-Means-Clusteranalyse mit 5 Clustern (berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1 Bedingte Datenschutzbefürworter	**Cluster 2 Extreme Datenschutzbefürworter**	**Cluster 3 Gemäßigte Flexibilitätsbefürworter**	**Cluster 4 Gemäßigte Datenschutzbefürworter**	**Cluster 5 Extreme Flexibilitätsbefürworter**
Ver 2016/679	Parlamentsposition	Ratsposition	Gesamtkonzept für DS in EU	BSA
ICO 12-02	VZBV 12-02	DS-RL 95/46/EG	DSGVO-Entwurf 2011	UEAPME 12-04
SWE-Parlament	Art. 29-Datenschutzgruppe	Google	Vorschlag 2012/001 COD	GDV
SWE-Regierung	EDPS 12-01	CDT 12-03	FRA-Parlament	BDIU
CPME	BEUC 12-07	Facebook 12-03	ITA-Parlament	DDV
BRAK 12-11	PI	ACCIS 12-04	GER-Bundesrat	VDZ
ICO 13-02	DSAB-DE-Land	GDD	Europ. DSBeauftragte	ICDP
EMPL-Bericht	EDRi	Microsoft 12-07	EWSA	ENPA 12-09
EL/GR - Ratsvorsitz 2014-1	LIBE-Berichtsentwurf	FBF 12-08	FRA - Grundrechteagentur	ZAW 12-09
FR		IMCO-Bericht		GSMA
IT - Ratsvorsitz 2014-2		Intel		ECTA
CY - Ratsvorsitz 2012-2		FEDMA		ETNO
HU		JURI-Bericht		Nokia 12-09
AT		BE		US-DoC
PL		BG		BITKOM
PT		CZ		EBF
RO		DK - Ratsvorsitz 2012-1		Eurofinas 12-10
SK		DE		DIGITALEUROPE 12-11
Li - Liechtenstein		EE		BT
		IE - Ratsvorsitz 2013-1		Yahoo
		ES		EuroISPA
		HR		Telefonica 12-12
		LV - Ratsvorsitz 2015-1		ICC
		LT - Ratsvorsitz 2013-2		AmCham EU
		LU - Ratsvorsitz 2015-2		ITRE-Bericht
		MT		ADR

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Cluster 1 Bedingte Datenschutzbefürworter	Cluster 2 Extreme Datenschutzbefürworter	Cluster 3 Gemäßigte Flexibilitätsbefürworter	Cluster 4 Gemäßigte Datenschutzbefürworter	Cluster 5 Extreme Flexibilitätsbefürworter
		NL		UK
		Sl		CH - Switzerland
		Fl		
		SE		
		NO - Norway		

Tabelle 4-32: K-Means-Clusteranalyse mit 5 Clustern (berechnet mit SPSS)

Die Ergebnisse aller Cluster-Analysen wurden durchgängig mittels einer Varianzanalyse überprüft und nachjustiert. Tabelle 4-33 zeigt die ANOVA-Ergebnisse für das verwendete 5-Cluster-Modell. Alle Items weisen eine hohe Signifikanz (<0,02) auf. Die Identifizierung der Cluster erfolgte insbesondere auf Grundlage der Items C3D (F-Wert vn 77,7), B3 (76), C13D (71,5).

Item	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
B3 Grundlegende Policy-Orientierung im Falle staatlicher Intervention	25,441	4	0,335	91	75,968	0
C1B Räumliche Anwendungsbereich	4,249	4	1,022	34	4,158	0,008
C1C Definition personenbezogener Daten	16,668	4	0,311	46	53,586	0
C 2 C Grundsatz der Datenminimierung	3,577	4	0,264	44	13,552	0
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	10,368	4	0,545	50	19,02	0
C3C Verarbeitung zu anderen Zwecken	16,645	4	0,563	40	29,551	0
C3D Bedingungen für die Einwilligung	25,917	4	0,334	74	77,685	0
C 4 A Besondere Kategorien personenbezogener Daten	6,471	4	0,783	40	8,265	0
C5A Transparenz	16,949	4	0,377	58	44,982	0
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	12,719	4	0,354	55	35,957	0
C 5 E Recht auf Vergessenwerden	11,118	4	0,386	62	28,784	0
C 5 G Recht auf Datenportabilität	20,253	4	0,383	51	52,852	0
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	18,188	4	0,442	53	41,192	0
C 5 L Benachrichtigung bei Datenschutzverletzungen	8,33	4	0,389	57	21,422	0
C6A Privacy by Default	18,319	4	0,322	45	56,842	0
C 6 B Privacy by Design	15,956	4	0,391	50	40,791	0
C 7 Übermittlung in Drittstaaten	12,551	4	0,323	52	38,895	0
C 13 A Verhaltensregeln	7,627	4	0,528	35	14,456	0

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
C 13 B Zertifizierungen/Gütesiegel	8,698	4	0,522	27	16,675	0
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	13,049	4	0,499	52	26,153	0
C 13 D Datenschutz-Folgenabschätzung	19,069	4	0,267	57	71,468	0
C 17 D Verbands- /Sammelklagerecht	20,931	4	0,575	36	36,377	0
C 17 E Sanktionen und Geldbußen	16,511	4	0,423	60	38,996	0

Tabelle 4-33: ANOVA-Ergebnisse für das 5-Cluster-Modell der dritten Phase (berechnet mit SPSS)

Die Ergebnisse der Cluster-Analyse für die Konfliktphase legen die Differenzierung zwischen drei Akteursgruppen nahe. Das 5-Cluster-Modell bietet gegenüber dem 3-Cluster-Modell den Vorteil, anhand der individuellen Akteurspositionen zwischen je einem extremen und einem eher gemäßigten Cluster der Datenschutzbefürworter als auch der Flexibilitätsbefürworter zu unterscheiden. Das fünfte Cluster bildet schließlich all jene Akteure ab, die in bedingtem Maße für die Stärkung des Datenschutzrahmens eintraten. Die folgenden Unterabschnitte widmen sich nun der Untersuchung der Zusammensetzung, Überzeugungssysteme und Ressourcen dieser drei Akteursgruppen.

4.3.1.2 Datenschutzbefürworter

4.3.1.2.1 Zusammensetzung der Datenschutzbefürworter

Das 5-Cluster-Modell eröffnete für die Konfliktphase die Möglichkeit, zwischen Akteuren mit einer besonders extremen und solchen mit einer eher gemäßigten Befürwortung von Datenschutzregelungen zu unterscheiden. Die Betrachtung der extremeren Community-Akteure zeigt, dass diese sich ausschließlich aus den in der Entwurfsphase als Koalitionsmitglieder identifizierten Akteuren zusammensetzen. Neben der Art. 29-Datenschutzgruppe finden sich hier der EDSB, BEUC, PI, EDRi, VZBV. Zudem können sowohl der LIBE-Berichtsentwurf (fortan: LIBE-BE) als auch die finale Parlamentsposition inhaltlich dem extremeren Datenschutzbefürworter-Cluster zugeordnet werden. Im Kreis der etwas gemäßigteren Datenschutzbefürworter sind die Parlamente einiger EU-Mitgliedstaaten (bspw. Frankreich und Schweden) der deutsche Bundesrat, die Konferenz der europäischen Datenschutzbeauftragten, aber auch der Europäische Wirtschafts- und So-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zialausschuss (EWSA) und die EU-Grundrechteagentur FRA zu finden (vgl. Tabelle 4-34).

Die Akteure, die den extremen Datenschutzbefürwortern zuzuordnen sind, gehören zudem der Advocacy-Koalition der Datenschutzbefürworter an. Lediglich die Konferenz der Europäischen Datenschutzbeauftragten wurde aufgrund ihrer inhaltlichen Positionen den gemäßigten Datenschutzbefürwortern zugeordnet (vgl. grau unterlegte Akteure in Tabelle 4-34).[346]

Extreme Datenschutzbefürworter	
Akteur	**Akteursgruppe**
Parlamentsposition	EU-Politik
VZBV 12-02	Verbraucherschutz
Art. 29-Datenschutz-gruppe	Datenschutzbehörden
EDPS 12-01	Datenschutzbehörden
BEUC 12-07	Verbraucherschutz
PI	Zivilgesellschaft
DSAB-DE-Land	Datenschutzbehörden
EDRi	Zivilgesellschaft
LIBE-Berichtsentwurf	EU-Politik

Gemäßigte Datenschutzbefürworter	
Akteur	**Akteursgruppe**
Gesamtkonzept für DS in EU	EU-Politik
DSGVO-Entwurf 2011	
Vorschlag 2012/001 COD	
FRA-Parlament	Mitgliedstaatl. Parlament
ITA-Parlament	Mitgliedstaatl. Parlament
GER-Bundesrat	Mitgliedstaatl. Parlament
Europ. DSBeauftragte	Datenschutzbehörden
EWSA	EU-Politik
FRA - Grundrechteagentur	EU-Politik

Tabelle 4-34: Akteursliste der Datenschutzbefürworter – Mitglieder der Advocacy-Koalition grau unterlegt (eigene Zusammenstellung)

Auch die Zusammenarbeit der (zivilgesellschaftlichen) Akteure intensivierte sich während der Konfliktphase. Auf zahlreichen thematisch einschlägigen Veranstaltungen tauschten sich die zentralen Akteure aus und koordinierten ihre öffentlichkeitsorientierten Strategien.[347] Zudem intervenierten

346 Diese Zuordnung lässt sich damit erklären, dass die Konferenz, die alle Europäischen Datenschutzbehörden unter einem Dach versammelt, ihre Stellungnahmen im Konsens verabschiedet und somit zwar für die Stärkung des Datenschutzes eintrat, in ihren Stellungnahmen allerdings weniger radikale Positionen vertrat als einige der beteiligten Datenschutzaufsichtsbehörden, die dem radikalen Flügel zuzuordnen sind.

347 Von den zahlreichen öffentlichen Veranstaltungen und Auftritten sei an dieser Stelle eine entscheidende Podiumsdiskussion genannt, auf der Rapporteur Albrecht und Datenschutz-NGOs über gemeinsame Strategien berieten und in deren Ergebnis die NGO-Medienkampagne initiiert wurde (Albrecht, Szymielewicz, und Fiedler 2012).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

die Datenschutz-NGOs mehrmals mit gemeinsamen Schreiben in den politischen Entscheidungsprozess. Die relevantesten dieser Interventionen sind die Briefe an die griechische Ratspräsidentschaft vom Januar 2014 (Civil Rights Organisations 2014) bzw. an den neuen Kommissionspräsidenten Juncker im April 2015 (EDRi und Access (International) 2015).[348] Darüber hinaus partizipierten US-amerikanische Verbraucherschutzgruppen am Diskurs. Nachdem sich die TACD bereits 2011 mit einem Schreiben an die zuständigen Ausschüsse im US-Kongress gewandt und diese zur Unterstützung der EU-Datenschutzreform aufgefordert hatte (TACD 2011), wandte sie sich im September an die Berichterstatter Albrecht und Comi, um diesen, angesichts des massiven Lobbyings von Seiten der US-Unternehmen, die Unterstützung der US-amerikanischen Zivilgesellschaft zu signalisieren (US-Consumer Organizations 2012).[349]

4.3.1.2.2 Überzeugungssystem der Datenschutzbefürworter

Policy-Kernüberzeugungen

Die Policy-Kernüberzeugungen der Datenschutzbefürworter blieben in der Konfliktphase gegenüber beiden vorhergegangenen Phasen stabil. Weiterhin stand die Grundrechtsdimension des Datenschutzes klar im Vordergrund. In den Stellungnahmen aller Koalitionsmitglieder wurde der DSGVO-Entwurf der Kommission begrüßt. Argumentiert wurde, dass die Reform des Datenschutzrahmens überfällig gewesen sei und dass der Vorschlag der Kommission einen ersten wichtigen Schritt in die richtige Richtung darstelle, indem der DSGVO-E auf den Vorgaben der DS-RL aufbauend deren Stärkung vorsehe und den Erlass EU-weit verbindlicher Vorga-

Siehe z. B. auch das öffentliche Pad, das zur Koordinierung genutzt wurde: https://pad.foebud.org/datap29c3

348 Während zu den Unterzeichnern des ersten Briefes neben Access und EDRi vor allem die ohnehin unter dem Dach von EDRi versammelten nationalen NGOs zählten (Civil Rights Organisations 2014), gelang es der Datenschutzbefürworter-Koalition im letzteren Brief erstmals eine breite Unterstützung seitens 66 internationaler Datenschutz- und Bürgerrechtsgruppen zu generieren (EDRi und Access (International) 2015). Vgl. für die vollständige Akteursliste des Schreibens vom Januar 2014 TabelleAnhang 11 und für das Schreiben vom April 2015 TabelleAnhang 12.

349 Vgl. für die vollständige Akteursliste Tabelle Anhang 10.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ben mittels einer Verordnung ermögliche.[350] Im Anschluss an das Eingangslob wurde dann allerdings kritisiert, dass der Kommissionsvorschlag viele gute Konzepte und Ideen nur halbherzig umsetze und daher dringender Verbesserungsbedarf bestehe. Insbesondere wurde die unzureichende Spezifizierung vieler Vorschläge kritisiert, die einen zu großen Interpretationsspielraum bei der Anwendung der entsprechenden Artikel eröffneten und damit die beabsichtigte Stärkung des Grundrechtsschutzes zu untergraben drohten (BEUC 2012, 2–8; EDRi 2012b; EDSB 2012b, 1–8; PI 2012, 2 f. VZBV 2012, 3–6).[351] Teilweise fand aber auch das Binnenmarkt-Argument Erwähnung, von dem zunächst die Kommission, ab Ende 2012 auch zunehmend das EP Gebrauch machte. Bei Parlament und sonstigen Akteuren stand trotzdem die Grundrechtsdimension klar im Vordergrund, während die Binnenmarkt-Perspektive häufig in eher kurzer Form als letzter Aspekt mitbenannt wurde.[352]

350 Sofern dies begründet wurde, wurde auf die technologischen Entwicklungen und die mangelnde Harmonisierung der Datenschutzgesetze der EU-Mitgliedstaaten verwiesen. Allerdings stand der Verweis auf den technologischen Wandel im Vergleich zu den ersten beiden Phasen deutlich weniger im Vordergrund (BEUC 2012, 2–8; EDRi 2012b; EDSB 2012b, 1–8; PI 2012, 2 f. VZBV 2012, 3–6).

351 Deutlich schärfer fiel dagegen die Kritik des EDSB an der Wahl des Rechtsinstruments einer Richtlinie für den JI-Bereich und an den vorgeschlagenen Inhalten aus, die jedoch nicht Gegenstand der vorliegenden Arbeit ist (EDSB 2012a, 2012b, 5 f. vgl. auch: Ermert 2012).

352 Vgl. zum Beispiel die Aussagen der VZBV: „Der Verbraucherzentrale Bundesverband unterstützt die EU-Kommission in ihren Bestrebungen, für einen verbesserten, harmonisierten und modernen Datenschutz in Europa zu sorgen. Der Datenschutz ist vor allem durch die digitale Entwicklung zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Modernisierung ist dringend notwendig, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucher auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken." (VZBV 2012, 3)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item / Akteur	Extreme Datenschutzbefürworter											Gemäßigte Datenschutzbefürworter								
	Ver 2016/679	Parlamentsposition	LIBE-Berichtsentwurf	Art. 29-Datenschutzgruppe	BEUC 12-07	DSAB-DE-Land	EDPS 12-01	EDRi	PI	VZBV 12-02	Häufigkeit d. Nennung	Gesamtkonzept für DS in EU	DSGVO-E 2011	DSGVO-E 2012	Europ. DSBeauftragte	EWSA	FRA-Grundrechteagentur	FRA-Parlament	ITA-Parlament	GER-Bundesrat	Häufigkeit d. Nennung
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	3	5	5	5	5	4	5	5	4	5	9	4	5	4	5	5	5	4	4	6
C1B Räumliche Anwendungsbereich	4	5	5	5	5	4	4			5	7	5	5	4		2				1
C1C Definition personenbezogener Daten	4	5	5	5	4		5	5	5	5	8	4	5	4		4				1
C 2 C Grundsatz der Datenminimierung	4	4	4	4	4		4				5		4	4	4					1
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	3	2	4		5	5		5	5	5	7	4	3	3						0
C3C Verarbeitung zu anderen Zwecken	3	5	5	4			4	5	4	5	7		2	2		1				1
C3D Bedingungen für die Einwilligung	4	5	5	4	5	5	5	5		5	8	4	5	5						0
C 4 A Besondere Kategorien personenbezogener Daten	4	5	5		5		5	5			5	4	4	4		4	4			2
C 4 D Datenschutz bei Kindern	4	5	4	5	5			5		5	6		5	5	4	5	5			3
C5A Transparenz	3	4	5	5	5		4	5	5	5	8	4	4	4	4	5				2
C5C Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung	3	5	5	4	5			5	5	5	7	4	4	4	4					1
C 5 E Recht auf Vergessenwerden	3	5	3	5	4		4	3		5	7	4	5	4	4	4				2
C 5 G Recht auf Datenportabilität	4	5	5	5	5		5	5	5	5	8	5	5	5	5	4				2
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	3	4	5	5	5		4	5	5	5	8		5	4		5	5			2
C 5 L Benachrichtigung bei Datenschutzverletzungen	3	4	4	3	4		3	4	3		7	4	5	4	4	3				2
C6A Privacy by Default	3	4	5	5	4		5	5	4	5	8	4	4	4	3					1
C 6 B Privacy by Design	3	5	5	5	3	4	4	5	4	5	9	4	4	4	3					1
C 6 C Dokumentation	3	3	4	5	4		3				5	4	4	4		5				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item / Akteur	Extreme Datenschutzbefürworter											Gemäßigte Datenschutzbefürworter									
	Ver 2016/679	Parlamentsposition	LIBE-Berichtsentwurf	Art. 29-Datenschutzgruppe	BEUC 12-07	DSAB-DE-Land	EDPS 12-01	EDRi	PI	VZBV 12-02	Häufigkeit d. Nennung	Gesamtkonzept für DS in EU	DSGVO-E 2011	DSGVO-E 2012	Europ. DSBeauftragte	EWSA	FRA-Grundrechteagentur	FRA-Parlament	ITA-Parlament	GER-Bundesrat	Häufigkeit d. Nennung
C 7 Übermittlung in Drittstaaten	4	5	5	4	4		4	5		5	7	3	4	4							0
C 13 A Verhaltensregeln	3	4	4		4						3	3	4	4							0
C 13 B Zertifizierungen/Gütesiegel	4	5	5		5						3	4	3	3		5					1
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	3	5	5	5	5		5			5	6	4	4	4	4	5					2
C 13 D Datenschutz-Folgenabschätzung	3	5	5	5	5		5	5		5	7	4	4	4	4	4					2
C 15 C Datenschutzbehörden	4	5	5	5	5		5	5	5	5	8	4	4	4	4	3	5				3
C 17 D Verbands- /Sammelklagerecht	3	5	5		5		5	5	5	5	7	4	4	4	5	5	5				3
C 17 E Sanktionen und Geldbußen	5	5	3	5	4		4			5	6	4	5	4	4	4	4				3

Tabelle 4-35: Positionen aller Datenschutzbefürworter zu allen relevanten Themen (eigene Zusammenstellung)

Sekundärüberzeugungen

Auch im Bereich der Sekundärüberzeugungen lässt sich eine weitgehende Überlappung mit den vorherigen Phasen feststellen. Erwartungsgemäß waren die Beiträge der Datenschutzbefürworter inhaltlich deutlich spezifischer als in den Phasen zuvor, da darin unmittelbar auf die Regelungsvorschläge der Kommission Bezug genommen werden konnte. Insbesondere ab Ende 2012, als in den zuständigen Parlamentsausschüssen über Änderungsanträge beraten wurde, gingen die Stellungnahmen auch auf konkrete Formulierungsvorschläge ein.

Anders als in den beiden vorherigen Phasen, äußerten sich die Koalitionsakteure zu beinahe jedem Thema (vgl. Tabelle 4-35). Lediglich die Themen Verhaltensregeln und Zertifizierungen blieben weitestgehend unbeachtet (3 Erwähnungen) und auch zur Datenminimierung, zu besonderen Kategorien personenbezogener Daten und zur Dokumentation äußerten sich nur wenige (je 5) Akteure.

Deutlich weniger Äußerungen zu allen Themen finden sich bei den gemäßigten Datenschutzbefürwortern. Hier äußerten sich lediglich die Konferenz der Europ. DSB, der EWSA und FRA in nennenswertem Maße zum DSGVO-E. Das französische und schwedische Parlament und der deutsche

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Bundesrat sprachen sich nur auf Ebene der Policy-Kernüberzeugungen für eine Stärkung des Datenschutzrechts aus, äußerten sich aber nicht zu den als Sekundärüberzeugung identifizierten Aspekten (vgl. Tabelle 4-35).

Im Hinblick auf so gut wie jeden im Kommissionsentwurf enthaltenen Regelungsvorschlag äußerten die Koalitionsakteure ihre Unterstützung, forderten zugleich aber eine weitere Stärkung der entsprechenden Vorschläge.[353] So wurde im Rahmen der Vorgaben zum räumlichen Anwendungsbereich die Einführung des Marktortprinzips durchweg begrüßt. Doch forderte beispielsweise der VZBV, dass die Kommission sich zugleich selbst dazu verpflichten solle, den Abschluss internationaler Abkommen zur Rechtsdurchsetzung zu fördern, damit die Wirksamkeit der Regelung gewährleistet wird (VZBV 2012, 4). Die Art. 29-Datenschutzgruppe und BEUC wiederum traten für eine Klarstellung ein, dass Dienste, für deren Nutzung zwar keine Geldkosten entstehen, jedoch die Preisgabe personenbezogener Daten erforderlich ist, sowie jegliches Online-Tracking und -Profiling in den Anwendungsbereich der Verordnung fallen sollten (Article 29 WP 2012, 9; BEUC 2012, 2).

In Bezug auf die Definition personenbezogener Daten vertraten die Koalitionsakteure die von der Datenschutzgruppe ausgearbeitete Position, wonach ein Datum wie eine Kennnummer immer dann als personenbezogen gelten muss, sofern es mit einer natürlichen Person verknüpft wird und der eindeutigen Bestimmung (*singling out*) dieser Person dient (Article 29 WP 2012, 9 f. BEUC 2012, 11 f. EDSB 2012b, 20 f.).

Kritik erntete bei den Datenschutzbefürwortern der Kommissionsvorschlag, im Rahmen der Vorgaben zur Rechtmäßigkeit der Verarbeitung die Verarbeitung personenbezogener Daten auf Grundlage berechtigter Interesses zu ermöglichen. Privacy International befürchtete, dass Art 6 Abs. 1 lit. f dazu missbraucht werden könnte, die Vorgabe zur expliziten Einwilligung regelmäßig zu umgehen. Um einem solchen Missbrauch vorzubeugen, machte PI (2012, 5) den Vorschlag, Regelbeispiele für Situationen und Fälle vorzugeben, in denen ein berechtigtes Interesse geltend gemacht werden könnte. Zudem traten sowohl PI (ebd.) als auch der Berliner Datenschutzbeauftragte für eine Klarstellung ein, dass Direktmarketing kein berechtigtes Interesse darstellt (Berliner DSB 2012, 1).

353 Einige der Kommissionsvorschläge wurden auch uneingeschränkt begrüßt, etwa die Stärkung des Grundsatzes der Datenminimierung (Article 29 WP 2012, 6; BEUC 2012, 13 f. EDSB 2012b, 23).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

In ähnlicher Weise wurde der Vorschlag der Kommission zur Aufweichung des Zweckbindungsprinzips in Art. 6 Abs. 4 kritisiert. Diesbezüglich forderte ein Teil der Koalitionsakteure die deutliche Einschränkung einer solchen Weiterverarbeitung zu Zwecken, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind (Article 29 WP 2012, 11 f. EDSB 2012b, 23 f.). Ein anderer Teil, darunter EDRi, PI und auch der LIBE-Ausschuss, traten dagegen für die vollständige Streichung des Absatzes und damit für die Beibehaltung der strikten Zweckbindung, wie sie in der DS-RL geregelt war, ein (Albrecht 2013d, 75 Am. 103, 2013a, 113 Am. 100; EDRi 2012b, 53; PI 2012, 6; VZBV 2012, 3). BEUC und der EDSB wiesen zudem darauf hin, dass eine Regelungslücke entstehen könnte, falls der Begriff der Vereinbarkeit nicht in der Verordnung selbst definiert würde (BEUC 2012, 14; EDSB 2012b, 24).

Die Kommissionsvorschläge zur Stärkung der Einwilligung wurden ausdrücklich befürwortet, ohne dass erwähnenswerte Änderungsvorschläge gemacht wurden (Article 29 WP 2012, 4; EDSB 2012b, 22, Rn. 113). Die Vorschläge der Kommission zu besonderen Kategorien personenbezogener Daten in Art. 9 DSGVO-E wurden ebenfalls eher unaufgeregt diskutiert. So schlugen einige Akteure vor, die Liste besonderer Kategorien personenbezogener Daten um weitere Datentypen zu ergänzen. Insbesondere wurde gefordert, dass nicht nur strafrechtliche Verurteilungen, sondern jegliche Verarbeitung von Daten im Zusammenhang mit Straftaten und auch die Verarbeitung von Daten zu Fällen, in denen es zu keiner Verurteilung gekommen ist (wie Verdächtigungen) ebenfalls Teil des Katalogs sein sollten (EDRi 2012b, 54 f., Am. 72; EDSB 2012b, 26 f.). EDRi (ebd.) forderte zudem die Neufassung der Glaubenszugehörigkeit als weltanschauliche Überzeugungen und engere Grenzen für Ausnahmen vom Verarbeitungsverbot. Diese Vorschläge befassten sich einerseits mit den Ausnahmeregelungen in Art. 9 Abs. 2, und andererseits mit EG 42. Gemäß dem Vorschlag von EDRi (ebd., 18, Amd. 22) sollte eine Ausnahme vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nur zur Gewährleistung der öffentlichen Gesundheit oder der sozialen Sicherheit, aber nicht zu historischen, statistischen oder wissenschaftlichen Forschungszwecken erlaubt sein. Diesen letzteren Vorschlag übernahm der LIBE-Berichtsentwurf (Albrecht 2013d, 24, Am. 27), im finalen LIBE-Bericht war er allerdings nicht mehr enthalten. Dagegen sah letzterer die Verschärfung der Ausnahmeregelungen in Art. 9 Abs. 2 vor (Albrecht 2013a, 119, Am. 103). Über die Vorschläge der Koalitionsakteure hinausgehend sah der LIBE-Ausschuss im Berichtsentwurf zudem die Erweiterung der Liste um philosophische bzw. weltanschauliche

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Überzeugungen, um die sexuelle Orientierung und Geschlechtsidentität sowie nicht nur die Mitgliedschaft in einer Gewerkschaft, sondern auch gewerkschaftliche Betätigung vor (Albrecht 2013d, 80, Am. 112). Zu dieser Liste kamen im finalen LIBE-Ausschussbericht biometrische Daten, sowie Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten oder mutmaßliche Straftaten und Verurteilungen hinzu (Albrecht 2013a, 117, Am. 103). Der Vorschlag von BEUC, die Liste um Finanzdaten zu erweitern schaffte es hingegen in keines der LIBE-Berichte (BEUC 2012, 16).

Die Kommissionsvorschläge hinsichtlich der Stärkung der Transparenz in den Art. 11 und 14 DSGVO-E stießen auf breite Unterstützung auf Seiten der Datenschutzbefürworter, während zugleich die weitere Stärkung der Vorgaben gefordert wurde (Article 29 WP 2012, 6; EDSB 2012b, 28, Rn. 142). EDRi und VZBV forderten beispielsweise, dass Verantwortliche bei der Information der Betroffenen auch die spezifischen Zwecke einer Verarbeitung angeben sollten (EDRi 2012b, 57, Am. 78; VZBV 2012, 11). Der EDSB und BEUC befürworteten die Spezifizierung der „sonstigen Informationen", die seitens der Verantwortlichen gemäß Art. 14 bereitgestellt werden sollten, insbesondere wurde mehr Transparenz im Hinblick auf Online-Profiling und Tracking gefordert (BEUC 2012, 18; EDSB 2012b, 28, Rn. 143 f. PI 2012, 6). BEUC (2012, 19) forderte zudem, dass die von der Kommission ursprünglich angedachten, letztlich aber im Rahmen von Durchführungsrechtsakten optional vorgesehenen, Standardvorlagen durch den EDSA unter Beteiligung von Verbrauchervertretern und Wirtschaftsvertretern ausgearbeitet werden sollten. PI befürwortete die Pflicht zur Ausarbeitung von Standardvorlagen zwar ebenfalls, zeigte sich aber auch offen gegenüber der Führungsrolle der Kommission (PI 2012, 6).

Auch die Vorschläge der Kommission zur Stärkung der Modalitäten zur Wahrnehmung der Betroffenenrechte wurden grundsätzlich begrüßt (Article 29 WP 2012, 6; Europäische Datenschutzbeauftragte 2012, 2). Gefordert wurde allerdings, dass die Frist auf einen Monat festgesetzt werden sollte (BEUC 2012, 18) und dass individuelle Anfragen (außer im Falle eines Missbrauchs) immer kostenfrei erfolgen können sollten (BEUC 2012, 18). Der LIBE-BE blieb weitestgehend bei den Formulierungen des Kommissionsvorschlags, schlag aber kleinere Änderungen vor, etwa, dass die Gebühr, die der Verantwortliche bei wiederholten Anfragen erheben darf, angemessen sein sollte (Albrecht 2013d, 84, Am. 120). Der finale LIBE-Bericht legte eine maximale Bearbeitungszeit von 40 Tagen fest (Albrecht 2013a, 125, Am. 107) und sah die grundsätzliche Kostenfreiheit von Anfragen vor (ebd., 122, Am. 107).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Zum sog. Recht auf Vergessenwerden äußerten sich die Datenschutzbefürworter eher ambivalent. Ein Teil der Akteure unterstützte die Kommissionsvorschläge und forderte eine weitere Stärkung von Löschansprüchen (vgl. z. B. Europäische Datenschutzbeauftragte 2012, 2).[354] Gleichzeitig verwiesen andere Datenschutzbefürworter darauf, dass es Probleme im Hinblick auf die wirksame Durchsetzung des Löschanspruchs von. Art. 17 Abs. 2 geben könnte.

Beispielsweise befürchteten BEUC (2012, 19 f.) und EDRi (EDRi 2012b, 24 f., Am. 29), dass die wirksame Umsetzung der rechtlichen Vorgaben zum Vergessenwerden die Durchleuchtung des gesamten Internets erforderlich machen und zu Einschränkungen der Kommunikationsfreiheit führen würde. Während der EDSB (2012b, 28 f.) einen Diskurs mit der Internetwirtschaft zur Erarbeitung von Lösungsmöglichkeiten befürwortete, sah BEUC die Lösung des Problems darin, dass die Vorgabe in Art. 17 Abs. 2 als Verpflichtung zu einem gewissen Bestreben formuliert sein sollte und nicht als eine Ergebnisverpflichtung. Den weitreichendsten Vorschlag machte hingegen EDRi (ebd., 62, Am. 87), indem die Löschung des Absatzes gefordert wurde. Als Begründung führte EDRi sehr allgemein an, dass Betroffene den Datenschutz in die eigenen Hände nehmen müssten, indem sie mehr und einfacher Gebrauch von ihren Betroffenenrechten machten. Im Ergebnis der intensiven Debatten über das Recht auf Vergessenwerden machte Berichterstatter Albrecht im LIBE-Berichtsentwurf den Vorschlag, dass nicht der Verantwortliche zur Benachrichtigung verpflichtet werden sollte, da dies unrealistisch wäre, sondern dass sichergestellt werden sollte, dass jede Verarbeitung sich auf die in Art. 6 angegebenen Gründe beziehen müsste. Dabei wurde das Ziel verfolgt, dass jede weitere Stelle, die personenbezogene Daten verarbeitet, in die Rolle des Verantwortlichen übergehen sollte (Albrecht 2013d, 30, Am. 35). Ansonsten sah der Berichtsentwurf vor, dass der Verantwortliche den Betroffenen über jede bewusste Übertragung der Daten an Dritte informieren sollte (ebd., 86, Am. 124). Zudem sah der Berichtsentwurf eine Ergänzung vor, nach der die Meinungsfreiheit aufgrund des Rechst auf Vergessenwerden nicht eingeschränkt werden dürfe (ebd., 98, Am. 148). Diese Vorschläge schafften es später in den finalen LIBE-Bericht (Albrecht 2013a, 143, Am. 112).

354 „Der Löschwunsch eines Verbrauchers sollte aber durch Unternehmen nicht nur dann an Dritte weitergegeben werden müssen, wenn Daten öffentlich gemacht, sondern auch immer dann, wenn Daten anderweitig an Dritte übermittelt wurden." (VZBV 2012, 4) Der VZBV nahm später allerdings wieder Abstand von dieser Position und trat für die Löschung von Art. 17 Abs. 2 ein (VZBV 2013, 15).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Der Kommissionsvorschlag zur Einführung eines neuen Rechts auf Datenportabilität wurde auf Seiten der Datenschutzbefürworter durchweg positiv aufgenommen (Article 29 WP 2012, 6; BEUC 2012, 20; EDSB 2012b, 29 f.). Einige Akteure (BEUC 2012, 21; PI 2012, 8; VZBV 2012, 5) traten für die regulatorische Festlegung von Datenstandards und Schnittstellen ein, damit das Recht nicht ins Leere läuft. Zudem forderte PI (2012, 8) eine Klarstellung, dass Dienstebetreiber das Portieren von Daten nicht zu einer Bedingungen zur Nutzung ihrer Dienste machen dürften. Beide Vorschläge wurden auch im LIBE-Ausschuss vorgeschlagen. Zudem machte dieser die Vorgabe, dass die Wahrnehmung des Rechts kostenfrei erfolgen können sollte. Deutlich schwächer als von den Koalitionsakteuren gefordert, fiel die Formulierung zur Interoperabilität aus: Der Berichtsentwurf formulierte nur eine Pflicht zur Interoperabilität, machte allerdings keine Verfahrensvorschläge, wie dieses Ziel erreicht werden sollte (Albrecht 2013d, 30, Am. 36). Der finale LIBE-Bericht übernahm alle Elemente des Berichtsentwurfs, führte aber darüber hinaus in EG 55 die Formulierung ein, dass die Verantwortlichen dazu angehalten werden sollten, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen (Albrecht 2013a, 38, Am. 30).

Die Kommissionsvorschläge zum Profiling bzw. zu automatisierten Maßnahmen stießen ebenfalls auf weitgehende Zustimmung (Article 29 WP 2012, 14; EDSB 2012b, 30). Die Änderungsvorschläge bezogen sich einerseits auf die Ausweitung des Anwendungsbereichs und andererseits auf die Herstellung von mehr Transparenz. Die Datenschutzgruppe befürwortete zum Beispiel die Ausweitung des Anwendungsbereichs des Artikels auf teilautomatisierte Verarbeitung personenbezogener Daten. Zudem wurde der Einbezug von Web-Analyse-Tools, von Tracking zur Beurteilung des Nutzerverhaltens, sowie der Erstellung von Bewegungsprofilen durch Apps und SNS-Profiling gefordert (Article 29 WP 2012, 14). BEUC (2012, 21) fordert zudem, dass die *Techniken und Verfahren* der Profilbildung den Betroffenen gegenüber transparent kommuniziert werden sollten. In ähnlicher Weise trat PI (2012, 8) dafür ein, dass Betroffene Informationen über die *Logik und Techniken* des jeweiligen Profilings erhalten sollten. Der LIBE-Bericht (Albrecht 2013a, 151, Am. 115) sah schließlich die Möglichkeit vor, dem Profiling generell zu widersprechen. Zu diesem Zweck sollten Betroffene vor der Durchführung des Profiling über das Recht auf Widerspruch in deutlich sichtbarer Weise unterrichtet werden.

Beim Thema der Meldung von Datenschutzverletzungen nahmen die Datenschutzbefürworter eine von der Kommission abweichende Position

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

ein. Sowohl EDRi, als auch die Datenschutzgruppe, BEUC und der EDSB befürworteten die Ausweitung der 24-Stunden-Frist auf 72 Stunden (Article 29 WP 2012, 16; BEUC 2012, 6; EDRi 2012b, 83, Am. 119; EDSB 2012b, 38). Weitgehende Einigkeit herrschte auch hinsichtlich der Benachrichtigung der Betroffenen. Diese sollte entgegen dem Kommissionsvorschlag nur erfolgen, wenn das Risiko einer konkreten bzw. ernsten Gefahr oder eines Schadens für die Betroffenen besteht. Andernfalls wurde befürchtet, dass eine De-Sensibilisierung der Betroffenen für wichtige Verletzungen die Folge sein könnte (Article 29 WP 2012, 17; BEUC 2012, 6; EDRi 2012b, 84, Am. 121; PI 2012, 10). Auseinander gingen die Meinungen bei der Frage, in welchen Fällen eine Benachrichtigung der Datenschutzbehörden erforderlich sein sollte. Die Datenschutzgruppe (2012, 16) vertrat beispielweise die Auffassung, dass diese nicht immer benachrichtigt werden sollten, da es sonst zu einer Überbelastung der Behörden kommen könnte, falls auch kleinere Verletzungen, die die Rechte der Betroffenen voraussichtlich nicht beeinträchtigen, ebenfalls gemeldet werden müssten. PI (2012, 10) dagegen war der Auffassung, dass die Benachrichtigung der Aufsichtsbehörden immer erfolgen sollte, damit Transparenz gewährleistet bleibt. Der LIBE-BE hielt am zweistufigen Meldesystem fest, sah aber eine Verlängerung der Meldepflicht auf 72 Stunden vor (Albrecht 2013d, 37, Am. 45). Darüber hinaus sah der Berichtsentwurf (ebd., 125, Am. 201) eine Spezifizierung der ernsten Gefahren vor, bei denen die Benachrichtigung der Betroffenen erforderlich sein sollte. Zu diesen zählte der Berichtsentwurf Identitätsdiebstahl oder -betrug, finanziellen Verlust, körperlichen Schaden, erhebliche Demütigung oder Rufschädigung. Der finale LIBE-Bericht hielt an der 72-Stunden-Frist fest, nahm aber die vorgeschlagene Spezifizierung wieder zurück und sah nur vor, dass die Benachrichtigung des Betroffenen erfolgen sollte, wenn die Wahrscheinlichkeit besteht, dass der Schutz personenbezogener Daten, die Privatsphäre, die Rechte oder die berechtigten Interessen der betroffenen Person beeinträchtigt werden (Albrecht 2013a, 180, Am. 126).

Die Vorschläge der Kommission zum Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen wurden zwar grundsätzlich begrüßt (Article 29 WP 2012, 11; BEUC 2012, 23; EDSB 2012b, 34), aber als unterambitioniert kritisiert. Mehrere Akteure befürworteten insbesondere eine stärkere Zielspezifizierung, indem bspw. Anonymisierungs- oder Pseudonymisierungsmaßnahmen vorgeschrieben werden (Article 29 WP 2012, 11; VZBV 2012, 21). Wie genau das mit der Regelung zu erreichende Ziel formuliert sein sollte, blieb eher unkonkret. Der EDSB (2012b, 35)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

machte beispielsweise im Hinblick auf datenschutzfreundliche Voreinstellungen den Vorschlag, dass die Verarbeitung personenbezogener Daten bei einem Produkt oder Dienst anfänglich auf das begrenzt sein sollte, was für dessen *einfache Nutzung* erforderlich ist, während eine *umfangreichere Nutzung* nur auf die Entscheidung des Betroffenen hin erfolgen sollte. Unter anderem übernahm die VZBV den aus vorherigen Debatten bekannten Vorschlag, dass die Voreinstellungen den der DSGVO zugrundeliegenden Prinzipien wie Datenvermeidung und Zweckbindung gerecht werden (BEUC 2012, 23; VZBV 2012, 21). Diesen Ansatz übernahm auch der LIBE-Berichtsentwurf (Albrecht 2013d, 34, Am. 37, 41). Der finale Bericht (Albrecht 2013a, 161, Am. 118) sah darüber hinaus und abweichend vom Kommissionsentwurf zudem vor, dass nicht nur der *Stand der Technik*, sondern auch *neueste technische Errungenschaften* und *bewährte internationale Verfahren* Berücksichtigung bei der Gewährleistung des Datenschutz durch Technik-Prinzips finden sollten. Eine weitere aus der Entwurfsphase bekannte Forderung war, dass die Regelungen sich nicht nur an Verantwortliche, sondern auch an Auftragsverarbeiter (BEUC 2012, 24), Berater, Entwickler und Hersteller von Hardware oder Software (EDRi 2012b, 29 f., Am. 35; EDSB 2012b, 35) richten sollten. Zwar übernahm der LIBE-Berichtsentwurf diesen Vorschlag (Albrecht 2013d, 70 f., Am. 98), im finalen Ausschussbericht wurden hingegen nur Auftragsverarbeiter zusätzlich genannt.

Die Kommissionsvorschläge hinsichtlich des Datentransfers in Drittstaaten wurden insgesamt als zu nachlässig kritisiert, insb. im Hinblick auf die von der Kommission vorgesehenen Ausnahmeregelungen (Article 29 WP 2012, 22; BEUC 2012, 29 f.). Der Europäische Datenschutzbeauftragte (2012b, 43) beispielsweise forderte, dass ein grenzüberschreitender Transfer nur auf Grundlage eines rechtsverbindlichen Instruments erfolgen dürfen sollte und nicht auch dann, wenn, wie von der Kommission in Art. 42 Abs. 5 DSGVO-E vorgeschlagen, nur unverbindliche Vereinbarungen getroffen wurden.[355] Sowohl der LIBE-BE (2013d, 151–55) als auch der finale Bericht (2013a, vgl. Kapitel V) sahen die Verschärfung der Regelungen zu Drittstaatentransfers vor, sodass diese weitestgehend nur noch auf Grundlage rechtsverbindlicher Instrumente erfolgen dürfen sollten.

355 Einige Akteure sprachen sich für den Abschluss von Vereinbarungen zur gegenseitigen Amtshilfe aus, damit im Falle eines Transfers personenbezogener Daten von EU-Bürgerinnen und -Bürgern an die Sicherheitsbehörden von Drittstaaten mehr Rechtssicherheit geschaffen wird (Article 29 WP 2012, 23; Europäische Datenschutzbeauftragte 2012).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Wie schon in den vorherigen Phasen fanden die Themen Verhaltensregeln und Zertifizierung auch in der Konfliktphase kaum Beachtung auf Seiten der Datenschutzbefürworter. Lediglich BEUC (2012, 28) äußerte sich dahingehend, dass Verhaltensregeln nur dann sinnvoll seien, wenn diese nicht von den Unternehmen selbst, sondern bspw. in Kooperation mit Aufsichtsbehörden entwickelt würden und sofern sie dazu dienten, ein höheres Datenschutzniveau für einzelne Bereiche festzuschreiben. Während das Thema im Berichtsentwurf nicht erwähnt wurde, folgte der finale Bericht teilweise der von BEUC vertretenen Linie, indem vorgeschlagen wurde, dass auch Aufsichtsbehörden die Befugnis zur Ausarbeitung von Verhaltensregeln erhalten sollten (Albrecht 2013a, 206, Am. 135).

In ähnlicher Weise wurde seitens BEUC (2012, 28 f.) auch für Zertifizierungen gefordert, dass diese nur dann sinnvoll seien, wenn sie über die Vorgaben der DSGVO hinausgingen. Eine einfache Einhaltung der DSGVO-Vorgaben dürfe nicht Gegenstand von Zertifizierungen sein, da die Einhaltung der Vorgaben ohnehin verpflichtend sei. Zudem forderte BEUC, dass klare Zertifizierungskriterien in der Verordnung selbst festgelegt werden sollten und das Zertifizierungsverfahren einer noch einzurichtenden, unabhängigen Stelle anvertraut werden sollte. Der EWSA (2012, Rn. 4.12) machte in diesem Zusammenhang den Vorschlag, dass die Zertifizierung Aufgabe der Kommission selbst sein sollte. Der LIBE-Bericht setzte schließlich fest, dass der Prüfungsmaßstab die Einhaltung der Verordnung sein sollte, sah aber darüberhinausgehend auch vor, dass der EDSA einen technischen Standard zur Verbesserung des Datenschutzes festlegen können sollte. Verantwortliche, die davon Gebrauch machen, sollten in anderer Hinsicht, etwa bei den Sanktionen, privilegiert werden (Albrecht 2013a, Amd. 295 ff.).

Die Einführung der Vorgabe zu einer verpflichtenden Bestellung eines betrieblichen Datenschutzbeauftragten in festgelegten Fällen wurde seitens der Datenschutzbefürworter positiv aufgenommen (Article 29 WP 2012, 6; EDSB 2012b, 40, Rn. 209). Weniger erfreut zeigten sich diese über das von der Kommission vorgeschlagene Kriterium der 250-Mitarbeiter-Schwelle. Diese wurde dahingehend kritisiert, dass auch ein Unternehmen mit weniger Mitarbeitern viele personenbezogene Daten verarbeiten bzw. riskante Verarbeitungen durchführen könnte. Favorisiert wurde stattdessen, dass die Art oder der Umfang einer Verarbeitung bzw. die Zahl der konkret mit der Verarbeitung personenbezogener Daten betrauten Mitarbeitenden oder die Anzahl der von einer Verarbeitung Betroffenen entscheidend sein sollte (Article 29 WP 2012, 16; BEUC 2012, 28; EDSB 2012b, 40 f., Rn. 211). Der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

VZBV (2012, 23) etwa plädierte dafür, dass jedes Unternehmen, dessen Kerntätigkeit in der Verarbeitung personenbezogener Daten besteht, einen Datenschutzbeauftragten bestellen müssen sollte. Dagegen sollten Unternehmen, bei denen die Datenverarbeitung eine Hilfstätigkeit zur Haupttätigkeit darstellt, von dieser Pflicht ausgenommen sein, sofern der Umfang, die Art der Daten, die Art der Verarbeitung oder eine Kombination der genannten Aspekte nicht die Bestellung eines Datenschutzbeauftragten erforderlich macht.

Der LIBE-Berichtsentwurf sah schließlich vor, dass die Bestellung dann verpflichtend sein sollte, sofern eine juristische Person die Daten von jährlich mehr als 500 Betroffenen verarbeitet (Albrecht 2013d, 136 f., Am. 223). Im finalen LIBE-Bericht wurde dieser Wert auf jährlich 5000 Betroffene angehoben (Albrecht 2013a, 198, Am. 132). Zudem sah der Berichtsentwurf vor, dass nicht nur im Falle der Beobachtung, sondern auch in Fällen des Profilings von Betroffenen und im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten die Bestellung verpflichtend sein sollte (Albrecht 2013d, 137, Am. 224, 225). Während der Verweis auf das Profiling gestrichen wurde, fand die Verarbeitung besonderer Kategorien personenbezogener Daten als Kriterium ihren Weg in den finalen LIBE-Bericht. Zudem wurde der entsprechende Buchstabe um Standortdaten, Daten über Kinder sowie Arbeitnehmerdaten, die in groß angelegten Ablagesystemen bestehen, ergänzt (Albrecht 2013a, 199, Am. 132).

Hinsichtlich des Kommissionsvorschlags zur Einführung des Instruments der DSFA äußerten sich die Akteure überaus positiv. Die Verbesserungsvorschläge sahen vor, dass eine DSFA in mehr Fällen durchgeführt werden sollte als im DSGVO-Entwurf vorgesehen, beispielsweise nicht nur wenn eine Verarbeitung ein konkretes Risiko birgt, sondern auch dann, wenn die Gefahr eines entsprechenden Risikos besteht oder bei jedweden Daten, die unter besondere Kategorien personenbezogener Daten fallen (Article 29 WP 2012, 16; BEUC 2012, 27; EDRi 2012b, 86; EDSB 2012b, 39). Der LIBE-Bericht sah eine deutliche Aufwertung und Spezifizierung des Instruments vor: So sollte nicht nur die Gefährdung des Schutzes personenbezogener Daten, sondern auch die Gefährdung anderer Grundrechte und Grundfreiheiten der Betroffenen ausschlaggebend für die Durchführung einer DSFA sein. Daneben sah der Ausschussbericht eine deutliche Spezifizierung der Regelbeispiele vor, wann eine DSFA durchgeführt werden sollte und schließlich wurden sehr umfassende formale Vorgaben für die Durchführung der Folgenabschätzung, aber auch Erleichterungen gegenüber Start-Ups bzw. KMU formuliert (Albrecht 2013a Amd. 257 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Vorschläge der Kommission zu kollektiven Rechtsbehelfe stießen ebenfalls auf Unterstützung (BEUC 2012, 34; EDSB 2012b, 50). Zur weiteren Stärkung der Vorgaben forderten PI und BEUC die Ausweitung der Verbandsklage auf Schadensersatzklagen (BEUC 2012, 34; PI 2012, 11). Zudem wurde gefordert, dass Schadensersatzklagen auch im Falle nicht-materieller Schäden, wie emotionalem Stress und Zeitverlust, möglich sein sollten (BEUC 2012, 35; PI 2012, 11). Die Ausarbeitung diesbezüglicher Richtlinien solle dem Europäischen Datenschutzausschuss obliegen (ebd.). Zudem forderte PI, dass ein Verband gegen einen Verantwortlichen vor Eintritt eines konkreten Schadens klagen können sollte, wenn dessen datenverarbeitende Systeme nicht den Vorgaben datenschutzfreundlicher Technikgestaltung und Voreinstellungen entsprächen (PI 2012, 11 f.). Das Fehlen der Möglichkeit einer Sammelklage wurde nur vom EDSB (2012b, 50, Rn. 261) beklagt. Der LIBE-Bericht enthielt schließlich die geforderte Ausweitung der Verbandsklage auf Schadensersatzklagen. Außerdem änderte das Parlament die Zielsetzung der in Art. 73 Abs. 2 genannten Organisationen dahingehend, dass diese im öffentlichen Interesse handeln müssten. Hintergrund waren Bedenken, dass eine profitorientierte Abmahnindustrie – ähnlich wie im Bereich des Urheberrechts – entstehen könnte (Albrecht 2013a, Amd. 182 ff.).

Bei den Sanktionen und Geldbußen wurde trotz der generellen Begrüßung des harmonisierten und erhöhten Strafrahmens (Article 29 WP 2012, 23; EDSB 2012b, 53) bedauert, dass der maximal mögliche Bußgeldrahmen im Vergleich zum ursprünglichen DSGVO-Entwurf verringert wurde (VZBV 2012, 14). Der VZBV forderte zudem die Einführung einer – dem deutschen BDSG entsprechenden – Regelung, wonach der Rahmen in Einzelfällen sogar überschritten werden können sollte. Gefordert wurde auch, dass die Einnahmen aus den Sanktionen zumindest teilweise an Organisationen fließen sollten, die die Rechte von Betroffenen schützen (BEUC 2012, 35). Die beiden letztgenannten Vorschläge übernahm der LIBE-Ausschuss zwar nicht, sah jedoch die Erhöhung des maximal möglichen Sanktionsrahmens auf 5 Prozent des weltweiten Jahresumsatzes eines Unternehmens vor (Albrecht 2013a Amd. 188).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3.1.2.3 Ressourcen der Datenschutzbefürworter

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die Einbindung der Datenschutzbefürworter in politische Entscheidungsprozesse blieb auch in der Konfliktphase auf hohem Niveau, da der Koalition neben Datenschutzaufsichtsbehörden, der Zivilgesellschaft bzw. den Verbraucherschützern insbesondere die Kommission und das EP angehörten. Allerdings machte sich auch erstmals das Fehlen eines Zugangs zum Ministerrat negativ bemerkbar, auf deren Positionierung die Datenschutzbefürworter praktisch keinen Einfluss nehmen konnten.

Unterstützung durch die öffentliche Meinung

Die Unterstützung durch die öffentliche Meinung stellte in der Konfliktphase eine wichtige Ressource der Datenschutzbefürworter dar. Sowohl in der ersten Jahreshälfte 2013 noch vor den Snowden-Enthüllungen als auch mit Beginn der Snowden-Enthüllungen im Juni 2013 konnten die Datenschutzbefürworter auf die Unterstützung der Bevölkerung bauen. Allerdings darf die öffentliche Bedeutung des Themas Datenschutz nicht überschätzt werden. So hielten selbst im vergleichsweise datenschutzbewussten Deutschland im August 2013 zwar 26 Prozent der Befragten das Thema für sehr wichtig (ZDF 2013) und einige Monate und Enthüllungen später im November gaben 74 Prozent der Befragten an, dass die Überwachung ein sehr wichtiges oder wichtiges Thema sei (Forschungsgruppe Wahlen 2013). Ähnlich hielt die Mehrheit der Bevölkerung in anderen EU-Mitgliedstaaten die Überwachung durch US-Geheimdienste für inakzeptabel (Pew Research Center 2014). Eine weitere Eurobarometer-Studie zum Datenschutz von Anfang 2015 bestätigte, dass eine große Mehrheit von 69 Prozent weiterhin besorgt über den möglichen Missbrauch ihrer personenbezogenen Daten, insb. seitens privatwirtschaftlicher (Internet-)Anbieter, war (KOM 2015a). Doch ging die öffentliche Aufmerksamkeit für den Themenkomplex Überwachung und Datenschutz nach einigen Monaten wieder deutlich zurück. So rutschte das Thema selbst in der Aufmerksamkeit der deutschen Bevölkerung bereits im Januar 2014 auf Platz 15 ab und war 2015 praktisch nicht mehr präsent (Forschungsgruppe Wahlen 2014; Statista 2015). In der allgemeinen Eurobarometer-Studie aus dem Jahr 2015 tauchte das Thema nicht mehr unter den wichtigsten Problemen auf (EC 2015b, T40).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Wichtig war vor allem die Unterstützung seitens der Medien, die den Datenschutzbefürwortern zuteilwurde. Insb. die Berichterstattung zu den LobbyPlag-Erkenntnissen[356] schaffte es in die weltweit größten Zeitungen (Biermann 2013b; Cáceres 2013; Euronews 2013; Fontanella-Khan 2013a; F. Robinson 2013; Tzschentke 2013). Generell waren die Pressekommentare zu den Positionen der Datenschutzbefürworter tendenziell positiver als zu denen der Flexibilitätsbefürworter.

Informationen/Informationshoheit

Informationen bzw. eine mögliche Informationshoheit spielten zumindest auf Seiten der Datenschutzbefürworter keine nennenswerte Rolle.

Fähigkeit zur politischen Mobilisierung

Im Hinblick auf die Fähigkeiten zur politischen Mobilisierung konnten zwar durchaus Erfolge verzeichnet werden, doch vermochten die Datenschutzbefürworter die Snowden-Enthüllungen und den öffentlichen Aufschrei nicht in stärkerem Maße für sich zu nutzen. Neben kleineren deutschlandweiten Kundgebungen mit wenigen Hundert Teilnehmern konnten selbst zu den größeren Demonstrationen lediglich etwa 10.000 Menschen im Juli 2013 (Breuer und Reißmann 2013), etwa 15.000 Menschen zur Teilnahme an der alljährlichen „Freiheit statt Angst"-Demonstration Anfang September 2013 (Reißmann 2013) und Ende August 2014 nur noch etwa 5.000 Teilnehmer mobilisiert werden (Horchert 2014).[357]

Relevanter als die politische Mobilisierung im Kontext von Demonstrationen waren daher alternative Formen der Mobilisierung, darunter die von BoF, EDRi und PI (BoF, EDRi, und PI 2013) initiierte Unterschriftenkampagne zur *Brüsseler Datenschutz-Erklärung* und insb. die Aktion *Protect Your Data*, bei der die EU-Bevölkerung dazu mobilisiert wurde, ihre Abgeordneten im EU-Parlament zu kontaktieren (Fiedler 2013a; Privacycampaign.eu 2013).

Finanzielle Ressourcen

Zwar blieb die finanzielle Ausstattung der zivilgesellschaftlichen Datenschutzbefürworter auf konstant niedrigem Niveau (Dobusch 2014), doch

356 Die Details zu LobbyPlag werden im Rahmen der der Prozessanalyse ausgeführt.

357 Zum Vergleich: Am *Freiheit statt Angst*-Aktionstag am 11. Oktober 2008 im Rahmen der Anti-Vorratsdatenspeicherungsproteste nahmen allein in Berlin nach Veranstalterangaben 100.000 und nach Polizeiangaben 15.000 bis 50.000 Menschen (DPA 2008)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wurde diese Schwäche durch die gesteigerte grenzübergreifende Zusammenarbeit der nationalen NGOs teilweise ausgeglichen. Die zivilgesellschaftlichen Datenschutzbefürworter setzten ohnehin eher auf Aktionen, die einen geringen finanziellen Ressourcenaufwand erforderten (Unterschriftenkampagne, E-Mail-Aktion, Demonstrationen). Die Ressourcenausstattung auf Seiten der Kommission und des Parlaments blieb zwar ebenfalls konstant, doch hatten die zivilgesellschaftlichen Akteure davon nur einen geringen unmittelbaren Nutzen, da in der Konfliktphase Konferenzen und Treffen zwar weiterhin bedeutsam waren, aber eine Querfinanzierung unmittelbarer zivilgesellschaftlicher Aktivitäten von Seiten der Kommission bzw. des Parlaments ausgeschlossen war.

Das *Vorhandensein einer fähigen Führung*.

Redings Führungsrolle unterlag Fluktuationen. So war die Justiz-Kommissarin insb. im Vorfeld der Veröffentlichung des Kommissionsvorschlags das Gravitationszentrum der Datenschutzbefürworter und auch danach stand sie im Kontext der Vorstellung der Reformvorschläge im Mittelpunkt. Allerdings rückte im weiteren Verlauf der LIBE-Berichterstatter Jan Philipp Albrecht zunehmend in den Fokus. Dieser unterhielt zudem vergleichsweise bessere Beziehungen zu den zivilgesellschaftlichen Datenschutzbefürwortern.[358] Das Verhältnis von Albrecht und Reding lässt sich aber aufgrund der institutionellen Trennung weniger als ein koalitionsinternes Konkurrenzverhältnis, denn als ein symbiotisches Verhältnis auffassen. Beide ergänzten sich und traten im Rahmen ihrer jeweiligen Möglichkeiten für die Stärkung des Datenschutzrahmens ein und hatten auf ihre Weise Erfolg damit, ihre Führungsrolle auszufüllen. Schließlich traten Reding und Albrecht im Kontext der Snowden-Enthüllungen als Policy-Entrepreneure auf und konnten das dadurch entstandene politische Gelegenheitsfenster zum Vorteil der Datenschutzbefürworter erfolgreich nutzen (vgl. die Schilderungen in der folgenden Prozessanalyse insb. in 4.3.2.5). Anerkannt werden muss aber auch die treibende Rolle von EDRi, BoF, PI und Access International, denen die erfolgreiche Koordinierung der internationalen zivilgesellschaftlichen Zusammenarbeit gelang.

358 Beispielhaft sei die Podiumsdiskussion Ende 2012 genannt. Auf dieser forderte Albrecht die zivilgesellschaftlichen Akteure auch explizit dazu auf, sich aktiver in den Entscheidungsprozess einzubringen und Stellungnahmen einzureichen (Albrecht, Szymielewicz, und Fiedler 2012, Min. 39:30 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3.1.3 Flexibilitätsbefürworter

4.3.1.3.1 Zusammensetzung der Flexibilitätsbefürworter

Im Hinblick auf die Zusammensetzung der Flexibilitätsbefürworter-Community erlaubt das 5-Cluster-Modell die Differenzierung zwischen einem extremen und einem gemäßigten Cluster. Die Größe beider Cluster ist ungefähr gleich. Unter den extremen Flexibilitätsbefürwortern finden sich besonders viele Unternehmen bzw. Wirtschaftsverbände, darunter insbesondere die Kernkoalition ICDP, welche die zentralen Akteure wie Digitaleurope, Amcham EU, BSA, EuroISPA, TAE Europe und WFA unter einem Dach vereint. Neben Akteuren aus der Wirtschaft finden sich hier auch das US-Handelsministerium, die Regierung des Vereinigten Königreichs, sowie der ITRE-Ausschuss des Europäischen Parlaments und der Ausschuss der Regionen. Der gemäßigte Flügel setzt sich dagegen überwiegend aus den Mitgliedstaaten zusammen. Hier sind besonders Deutschland, Irland, die tschechische Republik und Schweden zu nennen, die besonders stark für die Abschwächung der DSGVO-Vorgaben eintraten. Wie schon bei den Datenschutzbefürwortern entspricht die Unterteilung in ein extremes bzw. eher gemäßigtes Cluster zudem weitgehend der Unterteilung der Akteure in eine Advocacy-Koalition bzw. Advocacy-Community (vgl. Tabelle 4-36).

Extreme Flexibilitätsbefürworter	
Akteur	**Akteursgruppe**
AmCham EU	Privatwirtschaft
ADR	EU-Politik
BDIU	Privatwirtschaft
BITKOM	Privatwirtschaft
BSA	Privatwirtschaft
BT	Privatwirtschaft
CH - Switzerland	Drittstaat
DDV	Privatwirtschaft
DIGITALEUROPE 12-11	Privatwirtschaft
EBF	Privatwirtschaft
ECTA	Privatwirtschaft
ENPA 12-09	Privatwirtschaft
ETNO	Privatwirtschaft
Eurofinas 12-10	Privatwirtschaft

Gemäßigte Flexibilitätsbefürworter	
Akteur	**Akteursgruppe**
ACCIS 12-04	Privatwirtschaft
BE	Mitgliedstaatl. Regierung
BG	Mitgliedstaatl. Regierung
CDT 12-03	Zivilgesellschaft
CZ	Mitgliedstaatl. Regierung
DE	Mitgliedstaatl. Regierung
DK - Ratsvorsitz 2012-1	Mitgliedstaatl. Regierung
EE	Mitgliedstaatl. Regierung
ES	Mitgliedstaatl. Regierung
Facebook 12-03	Privatwirtschaft
FBF 12-08	Privatwirtschaft
FEDMA	Privatwirtschaft
Fl	Mitgliedstaatl. Regierung
GDD	Zivilgesellschaft/Wirtschaft

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Extreme Flexibilitätsbefürworter	
EuroISPA	Privatwirtschaft
GDV	Privatwirtschaft
GSMA	Privatwirtschaft
ICC	Privatwirtschaft
ICDP	Privatwirtschaft
ITRE-Bericht	EU-Politik
Nokia 12-09	Privatwirtschaft
Telefonica 12-12	Privatwirtschaft
UEAPME 12-04	Privatwirtschaft
UK	Mitgliedstaatl. Regierung
US-DoC	Drittstaat
VDZ	Privatwirtschaft
Yahoo	Privatwirtschaft
ZAW 12-09	Privatwirtschaft

Gemäßigte Flexibilitätsbefürworter	
Google	Privatwirtschaft
HR	Mitgliedstaatl. Regierung
IE - Ratsvorsitz 2013-1	Mitgliedstaatl. Regierung
IMCO-Bericht	EU-Politik
Intel	Privatwirtschaft
JURI-Bericht	EU-Politik
LT - Ratsvorsitz 2013-2	Mitgliedstaatl. Regierung
LU - Ratsvorsitz 2015-2	Mitgliedstaatl. Regierung
LV - Ratsvorsitz 2015-1	Mitgliedstaatl. Regierung
Microsoft 12-07	Privatwirtschaft
MT	Mitgliedstaatl. Regierung
NL	Mitgliedstaatl. Regierung
NO - Norway	EWR-Drittstaat
SE	Mitgliedstaatl. Regierung
Sl	Mitgliedstaatl. Regierung

Tabelle 4-36: Akteursliste der Flexibilitätsbefürworter – Mitglieder der Advocacy-Koalition grau unterlegt (eigene Zusammenstellung)

4.3.1.3.2 Überzeugungssystem der Flexibilitätsbefürworter

Policy-Kernüberzeugungen

Das Überzeugungssystem der Flexibilitätsbefürworter blieb während der Konfliktphase grundsätzlich unverändert gegenüber den beiden vorherigen Phasen. So wurden datenschutzrechtliche Regelungen und die Überarbeitung des bestehenden Rechtsrahmens von den Vertretern der Flexibilitätsbefürworter-Community weiterhin grundsätzlich begrüßt.[359] Zugleich wurde betont, dass jedwede datenschutzrechtliche Vorgaben den freien Fluss personenbezogener Daten nicht behindern, bzw. diesen fördern sollten. Insofern zeigten sich die Flexibilitätsbefürworter erfreut über die Vorschläge der Kommission, die Meldepflicht vollständig abzuschaffen, ein One-Stop-Shop-System auf Basis der Hauptniederlassung des jeweiligen Verantwortlichen einzuführen und die EU-weit divergierenden Daten-

359 Ausnahmen gab es freilich auch während der Konfliktphase. Eine relativ große Zahl an Mitgliedstaaten (insb. BE, CZ, DK, DE, EE, LT, Sl, SE, UK) bevorzugte auch weiterhin eine Richtlinie.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schutzgesetze mittels des Instruments der Verordnung zu harmonisieren (DIGITALEUROPE 2012b, 1; ICDP 2012, 1). Scharf kritisiert wurde dagegen, dass die Kommission zwar einerseits mit den genannten Änderungen das Ziel der Verbesserung des freien Flusses personenbezogener Daten verfolge, zugleich mit ihren weiteren Vorschlägen insgesamt einen administrativen Mehraufwand für alle Datenverarbeiter zu verursachen drohe, der die Unternehmen in ihrer globalen Wettbewerbsfähigkeit einschränken und die Anziehungskraft Europas als Standort verringern würde (BITKOM 2012b, 1; ICC 2013, 1 f. ICDP 2012, 1 f.). Bemerkenswert war zudem eine deutliche Änderung im Tonfall. Während beispielsweise die Industry Coalition for Data Protection Ende 2011 noch Akzeptanz gegenüber der Vorstellung, dass durch ein hohes Schutzniveau gesteigertes Vertrauen in datenverarbeitende Technologien und Anbieter zu Innovation und Wachstum führen könne, geäußert hatte (ICDP 2011, 2), fand das Vertrauensargument in der Stellungnahme vom September 2012 überhaupt keine Erwähnung mehr. Stattdessen setzte die Koalition auf das Ausmalen von Katastrophenszenarien: „If enacted in the present draft form, the Regulation would delay the launch of innovative services in Europe, cause substantial loss in revenues for businesses of all sizes and in a wide range of industries, limit opportunities for ne market entrants, strongly increase administrative costs and create legal uncertainty." (ICDP 2012, 1 f.) Je weiter der Konflikt zudem voranschritt, umso intensiver verwiesen die Flexibilitätsbefürworter darauf, dass die Umsatzeinbußen einzelner Unternehmen oder Branchen der Gesellschaft bzw. Europa insgesamt schaden würden (EDC 2015b; vgl. z. B. ICC 2013, 1). In diesem Zusammenhang wurde immer wieder auf die anhaltende wirtschaftliche Rezession in Folge der globalen Finanzkrise von 2007 verwiesen, aufgrund derer besondere Vorsicht hinsichtlich wettbewerbsschädigender Regeln geboten sei (ICC 2013, 2; UEAPME und HOTREC 2013, 2). Flankiert wurde diese Delegetimierungsstrategie durch das Absprechen der Wirksamkeit strenger Datenschutzvorgaben. Diese würden nicht nur zu einem wirtschaftsschädigenden Mehraufwand für die Unternehmen führen, sondern zugleich nicht einmal den erhofften Datenschutz-Mehrwert mit sich bringen: „In fact, many of these requirements will not enhance the protection of individuals' data but simply lead to inefficient processes, overburden data protection authorities and create false expectations for users." (ICDP 2012, 2)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Sekundärüberzeugungen

Die am häufigsten genannten Themen der Flexibilitätsbefürworter waren Einwilligung (50), Recht auf Vergessenwerden (42), Sanktionen (39), Datenschutz-Folgenabschätzung (37) sowie Benachrichtigung bei Datenschutzverletzungen und Transparenz (je 36). Im Hinblick auf jedes der genannten Themen äußerten die Akteure ihr Unbehagen über den ihrer Meinung nach zu hohen Verwaltungsaufwand, der bei der Umsetzung der vorgeschlagenen Regelungen entstehen würde. Somit können zwar einige Kernthemen der Flexibilitätsbefürworter identifiziert werden, doch wurde letztlich im Hinblick auf jedes Verordnungselement versucht, die regulatorischen Vorgaben und insb. die Verarbeiterpflichten abzuschwächen.

Beim zentralen Thema der Einwilligung lehnten es die Flexibilitätsbefürworter ab, dass eine Einwilligung stets ausdrücklich, also als Opt-in erteilt werden sollte. Weiterhin wurde dabei die Strategie verfolgt, die Möglichkeit des Opt-ins nicht auszuschließen, sondern als eine Möglichkeit darzustellen. Die Verpflichtung zum Opt-in wurde dagegen als ein „one-size-fits-all"-Ansatz kritisiert, der das spezifische Risiko und den spezifischen Kontext einer Verarbeitung unberücksichtigt lasse, sodass die Nutzerinnen und Nutzer mit überflüssigen Opt-in-Anfragen überflutet und dadurch für tatsächlich sensible Verarbeitungen desensibilisiert würden, während Unternehmen die Einführung innovativer Dienste erschwert würde (AmCham EU 2012, 9; BITKOM 2012b, 6; BSA 2012, 10; DIGITALEUROPE 2012b, 3; ICDP 2012, 2; US DoC 2012, 10; VDZ 2012, 6).[360] Ein Teil der Akteure lehnte zudem den Kommissionsvorschlag in Art. 7 Abs. 4 ab, wonach die Einwilligung keine gültige Rechtsgrundlage bieten können sollte, wenn zwischen der Position des Betroffenen und des Verantwortlichen ein *erhebliches Ungleichgewicht* besteht (DDV 2012, 8; ENPA und EMMA 2012, 2). Auf Ebene der Mitgliedstaaten wurden ähnliche Positionen vor allem seitens Belgien, Tschechien, Irland, Luxemburg, den Niederlanden, dem Vereinigten Königreich (Council Presidency 2012, 57, Fn. 140) formuliert.

360 Trotz der an dieser Stelle erfolgenden Zuspitzung der Debatte auf den Begriff der Ausdrücklichkeit, sollte nicht unerwähnt bleiben, dass die Akteure auch gegen andere Elemente der Einwilligungsrelevanten Artikel vorgingen. Ein besonderes Beispiel stellt hier die Stellungnahme des DDV dar. Den Vorschlägen des Verbands gemäß solle jede Verarbeitung personenbezogener Daten als rechtmäßig anzusehen sein, solange *keine schutzwürdigen Interessen im Hinblick auf die Grundrechte und Grundfreiheiten der Betroffenen, die den Schutz personenbezogener Daten erfordern, beeinträchtigt werden* (DDV 2012, 6).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Im Zusammenhang mit den Bedingungen der Rechtmäßigkeit einer Verarbeitung forderten die Flexibilitätsbefürworter zudem die Ausweitung des in Art. 6 Abs. 1 lit. f geregelten berechtigten Interesses und damit den Erhalt des Regelungsniveaus der DS-RL. So sollte eine Verarbeitung zur Wahrung berechtigter Interessen auch im Falle der Wahrnehmung der Interessen Dritter als rechtmäßig gelten (BITKOM 2012b, 3; DIGITALEUROPE 2012b, 26; UEAPME 2012, 3; ZAW 2012, 3).

Im Zusammenhang mit den Vorschlägen der Kommission hinsichtlich der Weiterverarbeitung zu anderen Zwecken traten die Flexibilitätsbefürworter dafür ein, dass diese nicht nur auf Basis der Buchstaben a bis e des Artikels 6 Abs. 1 erlaubt sein sollte, sondern auch auf Basis von Buchstabe f, also auf Grundlage des berechtigten Interesses eines Verarbeiters oder eines Dritten (ACCIS IVZW 2012a, 2; Telefonica 2012b, 12; ZAW 2012, 1). Diese Position übernahmen sowohl der ITRE- (Kelly 2013, 59, Am. 110) als auch der IMCO- (Comi 2013, 49, Am. 77) und JURI-Ausschuss (Gallo 2013, 33, Am. 49) und später, in der Form abweichend aber inhaltlich übereinstimmend, auch der Ministerrat (2015d, 48).

Im Hinblick auf die Änderungsvorschläge der Kommission hinsichtlich des Grundsatzes der Datenminimierung schlugen die Flexibilitätsbefürworter eine Rückkehr zur Formulierung der DS-RL vor. Abgelehnt wurde die vorgesehene Beschränkung auf das Mindestmaß, befürwortet wurde stattdessen die offenere Formulierung, wonach eine Verarbeitung für den Erhebungszweck relevant sein und nicht darüber hinausgehen sollte (DDV 2012, 5; EBF 2012, 11; Eurofinas 2012b, 11).[361]

Bei der Frage der Definition personenbezogener Daten vertraten die Flexibilitätsbefürworter die Position, dass Daten gemäß dem kontext-basierten Ansatz nur dann als personenbezogen angesehen werden sollten, sofern ein Verantwortlicher in der Lage sei, eine natürliche Person zu identifizieren (AmCham EU 2012, 11; BSA 2012, 9; DIGITALEUROPE 2012b, 1; ICDP 2012, 2; Telefonica 2012b, 2). Entsprechend sollten also das Herausgreifen sowie die gesonderte Behandlung einer Person nicht als entscheidende Kriterien zur Bestimmung des personenbezugs angesehen werden, wie es seitens der Datenschutzbefürworter gefordert worden war.

Viele Mitgliedstaaten, (Deutschland, Estland, Frankreich, Italien, Luxemburg, Polen, Slowakei, Vereinigtes Königreich) darunter solche, die ansons-

361 Der Unterschied wird besonders in der englischen Sprachfassung deutlich: Die DS-RL formulierte dies als „not excessive" Art. 6 Abs. 1 lit c) während der Kommissionsentwurf in Art. 5 lit. c) die Stelle abänderte zu „limited to the minimum necessary".

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ten für ein eher höheres Datenschutzniveau eintraten, waren der Auffassung, dass der Definitionsvorschlag der Kommission zu weit gefasst sei, sodass beispielsweise selbst Satellitenbilder unter die Definition fallen würden. Für eine kontextbasierte Definition, wie sie seitens der Wirtschaftsvertreter gefordert wurde, traten dagegen Irland, Luxemburg und das Vereinigtes Königreich ein (Council Presidency 2012, 44, 2013, 64).

Eine weitere, bis zum Ende der DSGVO-Verhandlungen weiterverfolgte Taktik der Flexibilitätsbefürworter war zudem die Forderung nach einer neuen Definitionen für anonyme personenbezogene Daten (kurz anonyme Daten) einerseits und pseudonymisierte personenbezogene Daten (kurz pseudonyme Daten) (BSA 2012, 10). Auf anonyme Daten sollten die Datenschutzgesetze keine Anwendung finden. Auf pseudonyme Daten sollten die Regeln dagegen in abgeschwächter Form anwendbar sein. Diese Forderung war während des Aushandlungsprozess von verschiedenen Akteuren vertreten worden (zu anonymen und pseudonymen Daten: BSA 2011; zu anonymen Daten: GSMA Europe 2009; zu pseudonymen Daten: ICDP 2011), wurde dann aber seitens der Medienberichterstattung (Bergemann 2013b) vor allem einer Stellungnahme von Yahoo (2012) zugerechnet. Dass pseudonyme Daten weniger strengen datenschutzrechtlichen Anforderungen unterliegen sollten, vertraten schließlich auch der ITRE- (Kelly 2013, Am. 77) und der IMCO-Ausschuss (Comi 2013, Am. 4). Der ITRE- (Kelly 2013, Am. 79) und der JURI-Ausschuss (Gallo 2013, Am. 32) forderten zudem die vollständige Herausnahme anonymer Daten aus dem Anwendungsbereich der Verordnung. Der Ministerrat übernahm letztlich jedoch nur die Positionen im Hinblick auf anonyme Daten (EU-Ministerrat 2015d, EG 23). Eine Pseudonymisierung (ebd., EG 23a, 23c) wurde zwar vorgesehen, doch sollten – entgegen den Positionen der Flexibilitätsbefürworter-Koalition – für pseudonyme Daten keine geringeren datenschutzrechtlichen Anforderungen gelten.

Im Bereich der Betroffenenrechte lehnten die Flexibilitätsbefürworter praktisch jede von der Kommission vorgeschlagene Stärkung ab. Im Hinblick auf die Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung wurde sowohl die Verlängerung der vorgesehenen Frist von einem Monat (Eurofinas 2012b, 21; UEAPME 2012, 4) als auch die Möglichkeit der Erhebung einer Gebühr eingefordert (ACCIS IVZW 2012a, 19; Eurofinas 2012b, 6). Im Zusammenhang mit den Transparenzvorgaben in Art. 11 und 14 wurde einerseits die Reduzierung der anzugebenden Informationen (BDIU 2012, 7; Kelly 2013, Am. 72; VDZ 2012, 21) und andererseits die Einführung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

von Ausnahmeregelungen gefordert. Letztere sollten beispielsweise greifen, sofern eine Verarbeitung zu Netzwerksicherheitszwecken oder zum Zwecke der Betrugsverhütung erfolgt (AmCham EU 2013, 15; DIGITALEUROPE 2012a, 31).

In Bezug auf das vorgeschlagene Recht auf Vergessenwerden wurde die Idee, dass Betroffene in der Lage sein sollten, die von ihnen selbst auf einer Plattform veröffentlichten personenbezogenen Daten wieder löschen zu können, grundsätzlich begrüßt. Bemängelt wurde jedoch die Umsetzbarkeit des Regelungsvorschlags der Kommission, da dieser nicht beachte, dass die gegenüber einer unbestimmten Zahl anderer Personen öffentlich gemachten Daten von diesen Dritten und ohne, dass der Verantwortliche dies überblicken könnte, vervielfältigt und auf andere Plattformen übertragen werden könnten. Entsprechend wurde gefordert, dass der entsprechende Artikel zu löschen ist und die Löschpflicht nur den jeweiligen Verantwortlichen, bei dem die Daten hochgeladen wurden, erfassen sollte (BSA 2012, 6; Facebook 2012, 7; Microsoft 2012, 4).[362] Einige Akteure verwiesen in diesem Zusammenhang darauf, dass die Durchsetzung des Rechts eine Dauerüberwachung des gesamten Internets erforderlich machen würde und somit die Meinungsfreiheit in Gefahr brächte (BITKOM 2012a, 13; Google 2012). Verwiesen wurde in diesem Zusammenhang etwa auch auf das Recht auf Erinnern (AmCham EU 2012, 12; Facebook 2012, 7). Die Reaktionen in Bezug auf das Recht auf Datenportabilität waren gespalten. Einerseits forderte eine größere Zahl von Akteuren, dass das Recht nur auf die vom Nutzer selbst erstellten bzw. hochgeladenen Daten Anwendung finden sollte (AmCham EU 2012, 14 f.). Daneben traten viele Akteure gegen verpflichtende Interoperabilitätsvorgaben ein. Diese sollten stattdessen auf dem Wege der Selbstregulierung seitens der Industrie entwickelt werden, damit Innovationsprozesse nicht behindert werden (AmCham EU 2012, 14 f.; DIGITALEUROPE 2012a, 38). Andere Akteure traten dafür ein, dass das Recht nicht auf ihren Sektor angewendet werden sollte, bzw., dass es auf den Bereich sozialer Online-Netzwerke beschränkt bleiben sollte.[363]

Als Begründung führte beispielsweise der Kreditsektor an, dass das Bereitstellen von zu vielen Daten Rückschlüsse auf Geschäftsgeheimnisse

362 Seitens der Akteure, die nicht der Internetwirtschaft hinzuzuzählen sind, wurde vor allem Ausnahmen im Hinblick auf den eigenen Sektor gefordert (vgl. z. B. ACCIS (2012b, 16) für den Kreditbereich; oder EBF (2012, 27) für den Bankensektor).

363 Der GDV (2012a, 12 f.) forderte eine Ausnahme für den Versicherungsbereich, die EBF (2012, 2) für den Bankensektor und der ADR (2012, 3) für öffentliche Verwaltungen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

erlauben bzw. geistige Eigentumsrechte verletzen würde (ACCIS IVZW 2012b, 14; Eurofinas 2012b, 6). Andere, vor allem der europäischen Wirtschaft entstammende Akteure forderten hingegen die vollständige Streichung des Rechts auf Datenportabilität (DDV 2012, 19 f.; ENPA und EMMA 2012, 9; Telefonica 2012a, 4; ZAW 2012, 9). Insbesondere der ITRE-Ausschuss folgte einer Vielzahl dieser Forderungen. So sollten Betroffene das Recht auf Datenportabilität nur dann wahrnehmen können, wenn ein Transfer nach Einschätzung der Unternehmen technisch möglich ist (Kelly 2013, Am. 170). Zudem sah der ITRE-Ausschuss Ausnahmen im Hinblick auf anonyme oder pseudonyme Daten, Geschäftsgeheimnisse und geistige Eigentumsrechte vor (ebd., Am 172, 174). Die Ausarbeitung gemeinsamer Formate sollte der Industrie überlassen bleiben (ebd., 174). Die Position, dass die Interoperabilität seitens des Marktes gewährleistet werden könne, vertrat auch der IMCO-Ausschuss (Comi 2013, Am. 124). Der Ministerrat strich schließlich jegliche Formulierungen hinsichtlich der Förderung der Interoperabilität und lies diese Frage offen, womit die Aufgabe praktisch der Industrie überlassen worden wäre. Zudem sah die Ministerratsposition eine Ausnahme für Verarbeitungen im öffentlichen Interesse und für Situationen vor, in denen die Rechte an geistigem Eigentum verletzt würden (EU-Ministerrat 2015d, Art. 18).

Im Hinblick auf die Thematik des Profilings verfolgten die Flexibilitätsbefürworter die Taktik, die individuellen und gesellschaftlichen Vorteile des Profilings aufzuzeigen und eine Differenzierung zwischen nützlichem Profiling einerseits und schädlichem Profiling andererseits zu etablieren. So diene Profiling der Entwicklung besserer Dienste, die zu einem gesteigerten Nutzen für Betroffene führten (BSA 2012, 7; Microsoft 2012, 5). Daneben ermögliche Profiling eine verbesserte Betrugsbekämpfung (BSA 2012, 7) bzw. Identifikation von Risiken anhand derer die Vergabe von Krediten und Versicherungen verbessert werden könne (ACCIS IVZW 2012b, 14; Eurofinas 2012b, 7). Dementsprechend wurde argumentiert, dass schädliches Profiling durchaus reguliert werden sollte, nützliche Formen des Profilings dagegen weiterhin ohne Vorgaben erlaubt bleiben sollte (Microsoft 2012, 5). Eine weitere Forderung sah vor, dass Profiling auf Grundlage pseudonymer Daten uneingeschränkt erlaubt sein sollte (BITKOM 2012a, 4). Praktisch gingen die Akteure insbesondere gegen den Vorschlag der Kommission vor, die Vorgaben zum Profiling auf *Maßnahmen* auszuweiten. Stattdessen wurde gefordert, dass die Regelungen nach dem Vorbild der DS-RL weiterhin lediglich auf *Entscheidungen* anwendbar sein sollten, die auf Profiling beruhen (BITKOM 2012a, 8; Telefonica 2012b, 24).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Der ITRE-Ausschuss blieb zwar beim Begriff der *Maßnahme*, machte aber Vorschläge für zahlreiche Ausnahmen, etwa für Marketing- und Marktforschungszwecke (Kelly 2013, Am. 182), bei der Verwendung pseudonymer Daten (ebd., Am. 184), für Zwecke der Betrugsprävention (ebd., Am. 191) oder für Profiling, das auf Basis der berechtigten Interessen eines Verantwortlichen durchgeführt wird (ebd., Am. 186). Der IMCO- und JURI-Ausschuss machten dagegen den Vorschlag, zur Formulierung der DS-RL zurückzukehren, wonach nur *Entscheidungen* vom Anwendungsbereich des Artikels erfasst sein sollten. Zudem sollte sich das Recht keiner Entscheidung unterworfen werden zu können nicht mehr an *jede natürliche Person* richten, sondern ausschließlich an *von einer Verarbeitung ihrer personenbezogenen Daten Betroffene*, womit eine des Begrenzung des Anwendungsbereichs angestrebt wurde (Comi 2013, Am. 130; Gallo 2013, Am. 14, 86). Der IMCO-Ausschuss sah vor, dass nur Profiling von der Regelung erfasst sein sollte, das für den Betroffenen negative Effekte hat, etwa Diskriminierung gegen Individuen auf Basis von beispielsweise Rasse oder ethnischer Herkunft, Religion, sexueller Orientierung, o. ä. (Comi 2013, Am. 14). Der IMCO-Ausschuss dagegen spezifizierte den Vorschlag vieler Flexibilitätsbefürworter, dass nur schädliches Profiling reguliert werden sollte, dahingehend, dass Entscheidungen, die auf unlauteren Geschäftspraktiken basieren, wie sie in der EU-Richtlinie 2005/29/EC festgelegt wurden, unter das Verbot fallen sollten (ebd., Am. 130). Der IMCO-Vorschlag wäre somit einer weitgehenden Erlaubnis des Profilings gleichgekommen. Der Ministerrat folgte den Einwänden der Flexibilitätsbefürworter und engte den Anwendungsbereich auf betroffene Personen und Entscheidungen ein, blieb aber bei der Formulierung, dass solche Entscheidungen reguliert sein sollten, die dem Betroffenen gegenüber rechtliche Wirkung entfalten oder sie erheblich beeinträchtigen (EU-Ministerrat 2015d, Art. 20).

Die Pflicht zu Benachrichtigung bei Datenschutzverletzungen wurde von den Akteuren zwar nicht grundsätzlich abgelehnt,[364] doch standen sie dem konkreten Gestaltungsvorschlag der Kommission ablehnend gegenüber. Als besonders problematisch wurde die nach ihrer Einschätzung zu große Zahl an irrelevanten Meldungen an Aufsichtsbehörden und Betroffene bzw.

364 Auch hierbei gab es natürlich Ausnahmen. So forderte EMMA (2012, 12) auch in diesem Zusammenhang unter Verweis auf das Kommissionsziel der Reduktion des administrativen Aufwands die Streichung der vorgesehenen Benachrichtigungspflicht im Falle einer Datenschutzverletzung. Zudem gab es auch bei diesem Thema Bedenken der Vertreter einzelner Sektoren, dass bei den vorgesehenen Pflichten eine sektorspezifische Ausnahme gemacht werden sollte (vgl. EBF 2012, 1).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die daraus resultierende Desensibilisierung der Betroffenen für wichtige Meldungen identifiziert. Gefordert wurde auch weiterhin, dass eine Meldung nur im Falle einer drohenden, schwerwiegenden Beeinträchtigung der Privatheit in Folge einer Datenschutzverletzung erforderlich sein sollte (AmCham EU 2012, 23; Eurofinas 2012a, 8; Microsoft 2012, 25; Telefonica 2012b, 40). Zudem richtete sich die Kritik der Akteure auch auf die von der Kommission vorgesehene 24-Stunden-Frist zur Benachrichtigung der zuständigen Aufsichtsbehörde. Hier wurde eine deutliche Fristverlängerung bzw. die Rückkehr zur Formulierung der ePrivacy-Novelle gefordert (AmCham EU 2012, 23; DIGITALEUROPE 2012a, 14; Microsoft 2012, 6; US DoC 2012, 15). Zudem vertraten die Flexibilitätsbefürworter weiterhin die Position, dass keine Benachrichtigung erforderlich sein sollte, sofern der Missbrauch der entsprechenden Daten seitens des Verantwortlichen durch technische Sicherheitsvorkehrungen ausgeschlossen werden konnte (AmCham EU 2013, 88). Sowohl der ITRE-, als auch der IMCO- und der JURI-Ausschuss schlugen die Streichung der 24-Stunden-Frist vor und befürworteten stattdessen die Formulierung der ePrivacy-Novelle („without undue delay" bzw. „unverzüglich") (Comi 2013, Am. 162; Gallo 2013, Am. 18; Kelly 2013, Am. 246). Der IMCO-Ausschuss (ebd.) schlug zudem vor, dass eine Benachrichtigung nur im Falle drohender erheblicher negativer Auswirkungen erfolgen müssen sollte. Als solche definierte der Ausschuss insb. Identitätsdiebstahl, Betrug, körperlicher Verletzung, erhebliche Erniedrigung oder Rufschädigung (ebd., Am. 167). Der ITRE-Ausschuss folgte einer ähnlichen Linie, sah aber eine zusätzliche Einschränkung vor, indem die entsprechende Vorgabe nicht auf die Verletzung aller personenbezogener Daten, sondern nur auf Kategorien besonderer personenbezogener Daten, auf personenbezogene Daten, die dem Berufsgeheimnis unterliegen, solche, die im Zusammenhang mit Straftaten oder dem Verdacht auf eine Straftat stehen, und personenbezogene Daten im Zusammenhang mit Bank- oder Kreditkartenkonten Anwendung finden sollte (Kelly 2013, Am. 245). Schließlich sahen sowohl der ITRE- (ebd., Am. 253) als auch der IMCO-Ausschuss (Comi 2013, Am. 64) verschiedene Ausnahmen vor, insb. im Falle der Anwendung technischer Sicherheitsvorkehrungen (wie Verschlüsselung) auf die verletzten personenbezogenen Daten. Der Ministerrat folgte den Vorschlägen der Flexibilitätsbefürworter in allen Punkten: Die Meldepflicht sollte lediglich im Falle eines *hohen Risikos* für die persönlichen Rechte und Freiheiten erforderlich sein. Als solche wurden insb. Diskriminierung, Identitätsdiebstahl oder –betrug, finanzielle Verluste, unbefugte Umkehr der Pseudonymisierung, Rufschädigung, Verlust der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile definiert (EU-Ministerrat 2015d, Art. 31 (1)). Die Frist zur Meldung an die Aufsichtsbehörde wurde auf 72 Stunden angehoben (ebd.) und eine Meldung an die Aufsichtsbehörde sollte gar nicht erfolgen müssen, sofern der Verantwortliche angemessene Sicherheitsvorkehrungen getroffen hat oder mittels anderer Maßnahmen sicherstellen konnte, dass kein hohes Risiko mehr besteht (ebd., Art. 31 (2)).

Die Vorschläge der Kommission zu Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen wurden zwar auch kritisch aufgenommen (Eurofinas 2012a, 7), grundsätzlich zeigte sich die Industrie jedoch erfreut darüber, dass der entsprechende Art. 23 eher Zielvorgaben formulierte, statt prozedurale Details vorzuschreiben, wie sie seitens der Datenschutzbefürworter gefordert worden waren (Microsoft 2012, 8). Besonders starke Kritik erntete der Vorschlag der Kommission, prozedurale Details und technische Standards auf dem Wege von Durchführungsrechtsakten festlegen zu können. Daher traten die Akteure für die Streichung der Kommissionsbefugnisse und gegen die Festlegung jeglicher technischen Details in der Verordnung ein. Sofern erforderlich sollten diese seitens der Industrie selbst entwickelt werden können (AmCham EU 2012, 16; BSA 2012, 6; Microsoft 2012, 8; UEAPME 2012, 6).[365] Schließlich standen die Akteure dem Konzept des Datenschutzes durch Technik tendenziell positiver gegenüber als datenschutzfreundlichen Voreinstellungen. Facebook begründete ihre Ablehnung von datenschutzfreundlichen Voreinstellungen damit, dass diese mit dem Ethos sozialer Online-Netzwerke nicht vereinbar seien (Facebook 2012, 5). Auch hier folgte der ITRE-Ausschuss den Vorschlägen der Flexibilitätsbefürworter und trat für die Streichung aller Verweise auf datenschutzfreundliche Voreinstellungen ein. Die übrigen Vorgaben zu Datenschutz durch Technik wiederum versuchte der ITRE-Ausschuss gegen jede technische Spezifizierung zu immunisieren, indem die Befugnisse der Kommission gestrichen und durch weitere Ergänzungen klargestellt wurde, dass die Umsetzung vollständig der Wirtschaft überlassen wird (Kelly 2013, Am. 214–219). Ähnliche Positionen in etwas abgeschwächter Form vertraten auch der IMCO- (Am. 4–6) sowie der JURI-Ausschuss (Am. 95–98). Der Rat (2015d, Art. 23 (1)) folgte ebenfalls dem Wunsch nach der Streichung der vorgesehenen Kommissionsbefugnis-

365 Die European Banking Federation trat auch in diesem Zusammenhang für eine Ausnahmeregelung für den Bankensektor ein (EBF 32).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

se, beließ das von der Kommission vorgeschlagene Grundgerüst der Regelung aber ansonsten intakt. Im Hinblick auf Datenschutz durch Technik ergänzte der Rat beispielsweise Regelbeispiele für angemessene technische und organisatorische Maßnahmen in Form von Datenminimierung und Pseudonymisierung vor.

Die von der Kommission vorgeschlagenen Vereinfachungen von Datenübermittlungen in Drittstaaten wurden begrüßt (BSA 2012, 10; Google 2012, 1), doch forderten die Akteure weitere Vereinfachungen (Microsoft 2012, 2), so unter anderem die weitere Ausweitung der in Art. 44 vorgesehenen Ausnahmen bzw. sogar das vollständige Abrücken vom Prinzip der Regulierung grenzüberschreitender Datentransfers (AmCham EU 2012, 3; ICC 2013, 2; US DoC 2012, 6). Erneut folgte insbesondere der ITRE-Ausschuss weitestgehend den Vorschlägen der Industrie (Am. 301–321). IMCO (Am. 190–193) und JURI (Am. 139–143) sahen ebenfalls – in etwas geringerem Umfang – Vereinfachungen zugunsten der Unternehmen vor. Der Ratsentwurf (vgl. Art. 43 (1) lit. a) sah nur kleinere Änderungen gegenüber dem Kommissionsentwurf vor, etwa die weitere Ausweitung des Anwendungsbereichs von verbindlichen unternehmensinternen Vorschriften auf Unternehmen, die gemeinsam eine wirtschaftliche Tätigkeit ausüben, aber nicht derselben Unternehmensgruppe gehören.

Neben dem Umstand, dass sich nur wenige Akteure der Flexibilitätsbefürworter-Community hinsichtlich der in Art. 38 DSGVO-E vorgesehenen Verhaltensregeln äußerten, blieben die geäußerten Änderungsvorschläge selbst in dieser Phase eher unkonkret. Einige Akteure verwiesen erneut darauf, dass mit dem Instrument mehr Anreize verbunden werden sollten (AmCham EU 2012, 22; ZAW 2012, 3). Grundsätzlich aber befürworteten sie Verhaltensregeln als ein sinnvolles Instrument, mit dem die Konkretisierung der regulatorischen Vorgaben auf Basis von Selbstregulierung möglich würde (AmCham EU 2013, 72 f.; BITKOM 2012b, 11; ZAW 2012, 3). AmCham-EU (2012, 22) machte zum Beispiel den Vorschlag, viele der im Rahmen von delegierten Rechtsakten vorgesehenen Konkretisierungen stattdessen im Rahmen von Verhaltensregeln zu gewährleisten. Weder der ITRE-, noch der IMCO- oder JURI-Ausschuss machten nennenswerte inhaltliche Gestaltungsvorschläge. Der Ministerrat (vgl. Art. 38 Abs. 1ab) legte dagegen großen Wert auf die Konkretisierung des Artikels. Weiterhin sollte die Genehmigung von Verhaltensregeln seitens der Aufsichtsbehörden und – abweichend vom Kommissionsvorschlag – in dem Falle, dass die vorgeschlagenen Verhaltensregeln mehrere Mitgliedstaaten betreffen beim EDSA liegen. Neu waren auch Anreize für Verantwortliche Verhaltensregeln zu er-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

arbeiten, um insb. Erleichterungen bei Datenübertragungen in Drittländer zu erreichen.

Auch das Thema Zertifizierung fand bei den Flexibilitätsbefürwortern wenig Beachtung. Weiterhin tendierten die Akteure dahin, Zertifizierungen unter der Bedingung zu begrüßen, dass diese freiwillig, bezahlbar, technologieneutral und global anschlussfähig sind, sowie auf Grundlage eines transparenten Verfahrens entweder vollständig von der Industrie oder unter Beteiligung der Industrie entwickelt und genehmigt werden (AmCham EU 2013, 81; BITKOM 2012a, 13; DIGITALEUROPE 2012a, 72 f.; Microsoft o. J., 8). Der ITRE-Ausschuss (Am. 295-298) stellte zwar die federführenden Rolle der Aufsichtsbehörden und der Kommission im Zertifizierungsverfahren nicht in Frage, übernahm aber die übrigen Vorschläge der Flexibilitätsbefürworter hinsichtlich Freiwilligkeit, Bezahlbarkeit, Technologieneutralität, globaler Anschlussfähigkeit und eines transparenten Prozesses unter Beteiligung der Industrie. Der Rat (vgl. Art. 39a) schlug schließlich die Aufspaltung des Artikels vor und machte im zweiten der Artikel Vorschläge zur Akkreditierung der Zertifizierungsstellen. Wie von Teilen der Wirtschaft gefordert, sollten Zertifizierungsstellen gleichberechtigt neben den Aufsichtsbehörden für die Durchführung von Zertifizierungen zuständig sein. Als Ziel der Zertifizierung formulierte der Rat (vgl. Art. 39), dass diese dem Nachweis darüber diene, dass die Vorgaben der Verordnung eingehalten werden.

Wie bei anderen Themen, befürworteten die Akteure im Hinblick auf die von der Kommission vorgeschlagene Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten mehr Spielraum. So wurde das Erfordernis einer organisationsinternen Datenschutz-Verantwortlichkeit nicht per se abgelehnt,[366] wohl aber die formelle Verknüpfung der Datenschutz-Aufgaben mit der Position eines betrieblichen Datenschutzbeauftragten. Entsprechend forderten die Akteure, die Änderung der vorgesehenen Verpflichtung in die Form der Möglichkeit der Einberufung eines betrieblichen Datenschutzbeauftragten (AmCham EU 2013, 41 f.; DIGITALEUROPE 2012a, 66 ff.; NOKIA 2012b, 15 ff.). Unterstützt wurden die Wirtschaftsvertreter bei diesem Anliegen von den Ausschüssen ITRE (Am. 277-284), IMCO (Am. 180) und JURI (Am. 123-128). Unterstützung fanden die Wirtschaftsvertreter auf der Ebene der Mitgliedstaaten bei Belgien, Frankreich, Italien,

366 Nur wenige Akteure wie ACCIS standen dem Vorschlag vollends ablehnend gegenüber (157 ACCIS 21). Zudem forderte der EBF auch bei diesem Thema eine Ausnahme für den Bankensektor (192_EBF 32).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

den Niederlanden, Tschechien, dem Vereinigten Königreich, Lettland und Litauen (Presidency of the Council of Ministers 2013, 28, Fn. 113). Der Ministerrat (vgl. Art. 35) machte schließlich den Vorschlag, die Regelung der Materie im Rahmen einer Öffnungsklausel den Mitgliedstaaten zu überlassen und in der Verordnung selbst keine verpflichtenden Vorgaben zu machen.

Besonders umstritten war der Kommissionsvorschlag zur Einführung einer Datenschutz-Folgenabschätzung, da darin eine weitere administrative Belastung der Verantwortlichen gesehen wurde. Ein Teil der Akteure stand dem Vorschlag vollständig ablehnend gegenüber (DIGITALEUROPE 2012b, 1; GDV 2012b, 11; ICC 2013, 3) oder forderte sektorspezifische Ausnahmen (EBF 2012, 32; Eurofinas 2012b, 45; UEAPME 2012, 5). Ein anderer Teil forderte Erleichterungen für Verantwortliche (Microsoft 2012, 6; NOKIA 2012a, 1; Telefonica 2012a, 13). AmCham-EU machte in diesem Zusammenhang den Vorschlag, dass die Pflicht zur Durchführung einer DSFA entfallen sollte, sofern ein Verantwortlicher einen betrieblichen Datenschutzbeauftragten benennt (AmCham EU 2013, 41). Die Ausschüsse ITRE (Amd. 257–265), IMCO (Amd. 172– 178) und JURI (Amd. 115–118) folgten der von der Industrie vertretenen Linie und machten zahlreiche Änderungsvorschläge. So sollten die angegebenen Regelbeispiele fortan eine abgeschlossene Liste bilden, also nicht mehr, wie von der Kommission vorgesehen, um weitere Beispiele ergänzt werden können. Dazu sollten der Kommission jegliche im Rahmen von delegierten und Durchführungsrechtsakten vorgesehene Befugnisse gestrichen werden. Im Falle vergleichbarer Risiken sollte *eine* DSFA für alle Verarbeitungen genügen und das Erfordernis der Einholung der Meinung der Betroffenen sollte gestrichen werden. Eine Stärkung sahen die Ausschüsse ITRE (Am. 260) und IMCO (Am. 174) einzig im Hinblick auf die Ausweitung der Regelung auf alle besonderen Kategorien personenbezogener Daten vor. Unterstützt wurden die Unternehmensvertreter von der Mehrheit der Mitgliedstaaten, darunter insb. Spanien, Frankreich, Portugal, Slowenien und demVereinigten Königreich. Daneben traten aber auch Belgien, Dänemark, Deutschland, Irland, Italien, die Niederlande und Zypern für gewisse wirtschaftsfreundliche Erleichterungen ein (Council Presidency 2013, 133 f.). Der Ratsentwurf (vgl. Art. 33) sah schließlich verschiedene Erleichterungen zu Gunsten der Unternehmen vor. Vergleichbar zu den Änderungsvorschlägen im Hinblick auf die Meldung von Datenschutzverletzungen, sollte eine DSFA nur bei einem hohen Risiko durchgeführt werden müssen. Zudem beschränkte der Rat den bei der Beurteilung des hohen Risikos anzulegenden Maßstab

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auf Diskriminierung, Identitätsdiebstahl oder –betrug, finanzielle Verluste, unbefugte Umkehr der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Ein Thema, bei dem die Vertreter der Wirtschaft nicht nach einer Aufweichung, sondern für die vollständige Herausnahme aus der Verordnung eintraten, bildet die Frage der kollektiven Rechtsbehelfe. Akteure aus den verschiedenen Branchen lehnten die Regelung vollständig ab (ACCIS IVZW 2012b, 20; Eurofinas 2012b, 8; FBF 2012, 3; GDV 2012c, 1). Verwiesen wurde dabei sowohl darauf, dass die Erforderlichkeit eines Verbandsklagerechts nicht erwiesen sei (Eurofinas 2012b, 8), dass die Gefahr des Missbrauchs durch die Entstehung einer Art Datenschutz-Abmahnindustrie bestehe (UEAPME 2012, 7) oder schlicht darauf, dass die aus der Regelung mit aller Wahrscheinlichkeit resultierende höhere Zahl an Klagen zu erhöhten Kosten für Unternehmen führen würde (AmCham EU 2012, 17). Die den Flexibilitätsbefürwortern zuzuordnenden Parlamentsausschüsse folgten den Positionen der übrigen Koalitionsakteure auch bei dieser Frage weitgehend. IMCO (Amd. 198, 201) schlug die Löschung sowohl von Art. 73 (2) als auch von Art. 76 (1) vor. Der ITRE-Ausschuss (Amd. 360) forderte zwar nicht die Löschung des Artikels, aber eine Beschränkung des Klagerechts auf solche Organisationen, die über eine Mindestförderung in Höhe von 80.000 € und eine repräsentative Mitgliedschaft mit einer entsprechenden Mitgliederstruktur verfügen. Damti sollte dem Missbrauch der Regelung vorgebeugt werden. Zudem sah ein ITRE-Vorschlag (Amd. 362) im Hinblick auf Art. 76 Abs. 1 vor, dass die entsprechenden Organisationen im Namen von Betroffenen nur noch gegen Aufsichtsbehörden, aber nicht mehr gegen Verantwortliche klagen können sollten. Der JURI-Ausschuss schlug dagegen die vollständige Streichung sowohl von Art. 76 Abs. 1 (Amd. 174) als auch von Art. 73 Abs. 3 (Amd. 170) vor, sodass Organisationen nicht mehr unabhängig von der Beschwerde eines Betroffenen eine Beschwerde bei einer Aufsichtsbehörde einlegen können sollten. Im Ministerrat traten besonders Tschechien, Estland, Italien, die Niederlande, Slowenien und das Vereinigte Königreich für die Löschung des Verbandsklagerechts ein (Council Presidency 2013, 219, Fn. 528). Der Ministerrat (vgl. Art. 76) folgte in dieser Frage nicht den weitgehenden Forderungen der Flexibilitätsbefürworter-Koalition und behielt das Verbandsklagerecht in leicht abgeänderter Form bei.

Zu den umstrittensten Themen bei den Verhandlungen zur DSGVO zählten Sanktionen und Geldbußen. Obwohl der finale Kommissionsent-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

wurf gegenüber der zuvor öffentlich gewordenen Vorfassung eine deutliche Senkung des maximalen Sanktionsmaßes vorgesehen hatte, wurden verschiedene Elemente des finalen Entwurfs sowie das mögliche Strafmaß enorm kritisiert. Grundsätzlich folgten die Flexibilitätsbefürworter bei diesem Thema weiterhin der Linie, dass die datenverarbeitende Wirtschaft keine schlechten Absichten mit der Datenverarbeitung verfolge und entsprechende Fehltritte nicht oder nicht so stark sanktioniert werden sollten, wie bei kriminellen Akteuren mit kriminellen Absichten, die bspw. Interesse an Identitätsdiebstahl hatten (Microsoft 2012, 9). Kritisiert wurde auch der in Art. 78 den Mitgliedstaaten bei der Festlegung der Sanktionen eröffnete Spielraum. Digitaleurope (2012b, 2) aber auch UEAPME (2012, 7) befürchteten beispielsweise in der Folge *erhebliche Unsicherheiten, die Gefahr der Fragmentierung und mangelnde Verhältnismäßigkeit* (Übersetzung d. Verf.). Andere Forderungen betrafen die Einführung eines Verbots der Doppelbestrafung (AmCham EU 2012, 17), sowie die Änderung der von der Kommission vorgesehenen Sanktions*pflicht* in eine Sanktions*möglichkeit* (Eurofinas 2012a, 8), insb. indem die Ausnahmen ausgeweitet werden (ACCIS IVZW 2012b, 20). Ein Kernpunkt der Kritik war die Höhe der Sanktionen. Diese wurden als zu hoch angesehen und teils vollständig abgelehnt (ACCIS IVZW 2012b, 20; ENPA und EMMA 2012, 12; UEAPME 2012, 7). Insbesondere die multinational agierenden Verbände und Unternehmen traten für die Streichung des Verweises auf den weltweiten Jahresumsatz (BITKOM 2012a, 14; DIGITALEUROPE 2012a, 96 ff.; GSMA u. a. 2012, 4) oder die Deckelung des maximalen Strafmaßes bei zwei Prozent des weltweiten Jahresumsatzes auf zwei Mio. € ein (AmCham EU 2012, 17; Microsoft o. J., 23). Die ICC (2013, 3) äußerte auch bei diesem Thema ihre Befürchtung, dass die vorgesehenen Sanktionen zu einem Rückgang der Investitionen führen und der europäischen Wirtschaft schaden würden. Den extremsten Forderungen der Flexibilitätsbefürworter folgte insbesondere der IMCO-Ausschuss (Amd. 204–211), indem er die vollständige Abschaffung der Sanktionsvorgaben inkl. der Regelung der Sanktionshöhe forderte und zahlreiche weitere Ausnahmen und Erleichterungen für Verantwortliche vorsah. ITRE (Amd. 366–398) schlug neben zahlreichen Ausnahmen und Erleichterungen die Reduktion des maximal möglichen Strafmaßes auf ein Prozent des weltweiten Jahresumsatzes vor und JURI (Amd. 176–180) blieb bei dem von der Kommission vorgeschlagenen Strafmaß, sah aber eine Ausweitung der Ausnahmen vor. Der Rat (vgl. Art. 78–79b) übernahm viele der Vorschläge der Flexibilitätsbefürworter (etwa, dass die Verhängung einer Geldbuße der Aufsichtsbehörde freigestellt sein sollte und

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

andere Erleichterungen für die Verantwortlichen), blieb hinsichtlich der Sanktionshöhe allerdings beim Vorschlag der Kommission. Delegierte und Durchführungsrechtsakte wurden praktisch von allen Flexibilisieurngsbefürwortern dahingehend kritisiert, dass die Kommission dadurch zu viele kritische Bereiche regeln könnte, die besser der Wirtschaft selbst überlassen bleiben sollten (ICC 2013, 1; UEAPME 2012, 2).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	Häufigkeit d. Nennung	29	30	13	21	17	14	26	13	18
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	NO - Norway	2	3						4	5
	SE	1	3	4	3	2	1	2		
	Fl	3			3			2		
	Sl	2		4	3		1	2	3	1
	NL	3			3	2	1	2	4	
	MT	2			3		3	2		
	LU - Ratsvorsitz 2015-2	2		2	4			3	4	
	LT - Ratsvorsitz 2013-2	2	3		3	4	3	2	2	
	LV - Ratsvorsitz 2015-1	3			3			2		
	HR	3			3			2		
	ES	2		3	3	2	3	2		
	IE - Ratsvorsitz 2013-1	2	3	2	3	2		2	3	
	EE	2		3	3			2	2	
	DE	1	4	3	3	2	1	2	2	3
	DK - Ratsvorsitz 2012-1	1			3			2		
	CZ	2	2		3	2		2	1	
	BG	2			3	2	3	2		
	BE	2	2	3	3	1	3	2	2	
	JURI-Bericht	3		3	2	1	1	4	2	3
	FEDMA	2				3	2			
	Intel	2				2				
	IMCO-Bericht	2	3	3	2	1	1	2	4	3
	FBF 12-08	2	4		1	2		2	2	
	Microsoft 12-07	2				2		2		
	GDD	3		3		2	1	3		
	ACCIS 12-04	2			2	2	1	2		
	Facebook 12-03	2				2		2		
	CDT 12-03	3		3		3		3		4
	Google	2	4	2		2		2		
DS-RL 95/46/EG		3	3	3	3	3	4	3	3	3
Vorschlag 2012/001 COD		4	4	4	4	3	2	5	4	4
Ratsposition		2	4	3	3	4	1	3	3	4
Parlamentsposition		5	5	5	5	2	5	5	5	4
Gesamtkonzept für DS in EU		4	5	4		4		4	5	
Ver 2016/679		3	4	4	4	4	3	4	5	4

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	C5C Modalitäten für die Wahrnehmung von Betroffenenrechten	C 5 E Recht auf Vergessenwerden	C 5 G Recht auf Datenportabilität	C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	C5L Benachrichtigung bei Datenschutzverletzungen	C6A Privacy by Default	C 6 B Privacy by Design	C 6 C Dokumentation	C 7 Übermittlung in Drittstaaten	C 13 A Verhaltensregeln
Häufigkeit d. Nennung	20	24	19	21	18	16	16	16	17	15
NO - Norway	3	3	3						2	
SE	2	2	2	3	2	3	3	2	2	2
FI	3	3		2				4	2	1
SI	3	1		2	3			3	3	2
NL	2	2	2	4	2	3	3	1	2	2
MT					2	2	2			
LU - Ratsvorsitz 2015-2	2	2	3	2	3	2	2	2	2	1
LT - Ratsvorsitz 2013-2	2	3	2	4	2	3	3	2	2	
LV - Ratsvorsitz 2015-1	3	3			3					1
HR										
ES	3	2	3	2	3	2	2	1	1	1
IE - Ratsvorsitz 2013-1	2	3	3	2		2	2			2 1
EE	3	2	2							1 1
DE	3	3	2	3	2	4	2	2	3	1 1
DK - Ratsvorsitz 2012-1	2	2	2	2		3	3			1 1
CZ	3	3		3	3			2	2	1
BG	2	2	2	2				4		2 2
BE	2	2	2	2	2	3	3	2	2	2
JURI-Bericht	2	2	3	1	2	2	2	2	2	
FEDMA				3						
Intel										
IMCO-Bericht	3	3	3	2	1	2	2	1	2	
FBF 12-08				3	2			2		
Microsoft 12-07		2	3	3	3	2	2		2	
GDD	4	3	3		2	2	2	3		
ACCIS 12-04	2	2	3	2				2		
Facebook 12-03		2			3	2	2		2	
CDT 12-03		3	3	3	3	2	2		3	2
Google		2	4	3					3	
DS-RL 95/46/EG	3	2	1	3	1	2	2	5	3	3
Vorschlag 2012/001 COD	4	4	5	4	4	4	4	4	4	4
Ratsposition	3	3	3	3	2	2	2	2	2	2
Parlamentsposition	5	5	5	4	4	4	5	3	5	4
Gesamtkonzept für DS in EU	4	4	5		4	4	4	4	3	3
Ver 2016/679	3	3	4	3	3	3	3	3	4	3

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Name	Ver 2016/679	Gesamtkonzept für DS in EU	Parlamentsposition	Ratsposition	Vorschlag 2012/001 COD	DS-RL 95/46/EG	Google	CDT 12-03	Facebook 12-03	ACCIS 12-04	GDD	Microsoft 12-07	FBF 12-08	IMCO-Bericht	Intel	FEDMA	JURI-Bericht	BE	BG	CZ	DK - Ratsvorsitz 2012-1	DE	EE	IE - Ratsvorsitz 2013-1	ES	HR	LV - Ratsvorsitz 2015-1	LT - Ratsvorsitz 2013-2	LU - Ratsvorsitz 2015-2	MT	NL	Sl	Fl	SE	NO - Norway	Häufigkeit d. Nennung
C 13 B Zertifizierungen/Gütesiegel	4	4	5	2	3	1						2					3	2		1		2		3	2						2	2				9
C 13 C Bestellung eines bDSB	3	4	5	2	4	2		2		2	3		3	2			2	2	4	3	2	4	2	2	2		2	2	3		2	2	1	2	3	2 2
C 13 D Datenschutz-Folgenabschätzung	3	4	5	2	4	1		2		2	2	2	2	3			2	2		2	3	3	2	2	2		4		2		3	2	2	3		2 0
C 15 C Datenschutzbehörden	4	4	5		4	3			3									3		2		4	3	2					2		2	2		2	3	1 1
C 17 D Verbands- /Sammelklagerecht	3	4	5	2	4	1				1			1	1			2			1		3	1		3						1	1		2	3	1 2
C 17 E Sanktionen und Geldbußen	5	4	5	3	4	1		3	2	2		2	2	2			3	3			3	3	2	3	3		3		3	3		2	3	2	2	2 0

Tabelle 4-37: Positionierung der gemäßigten Flexibilitätsbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Name	BSA	UEAPME 12-04	GDV	BDIU	DDV	VDZ	ICDP	ENPA 12-09	ZAW 12-09	GSMA	ECTA	ETNO	Nokia 12-09	US-DoC	BITKOM	EBF	Eurofinas 12-10	DIGITALEUROPE 12-11	BT	Yahoo	EuroISPA	Telefonica 12-12	ICC	AmCham EU	ITRE-Bericht	Ausschuss der Regionen	UK	CH - Switzerland	Häufigkeit d. Nennung
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	1	2	2	2	2	2	1	2	1	2	2	2	2	2	2	2	2	2	2	2	1	2	1	1	2	3	1	2	28
C1B Räumliche Anwendungsbereich										4	4	4									3			2		1	1		7
C1C Definition personenbezogener Daten	2	2			2	1	2	2							2			1	2	1	1	1		1	3	2	1		16
C 2 C Grundsatz der Datenminimierung					2											1	2								2		3		5
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	2	2	2	2	1	2		2	2					1	2	2	2	2						2	1	1	1		17
C3C Verarbeitung zu anderen Zwecken			1	1	1	1		1	1							1						1			1				9
C3D Bedingungen für die Einwilligung	2		2	2	1	1	1	1	1	2	2	2	1	1	2	2	1	2	1		2	1		1	2	1	1		24
C4A Besondere Kategorien personenbezogener Daten					4								2			2	3							3	3		1	2	8
C 4 D Datenschutz bei Kindern		2			2			2					3	2	2			2				2		2	4		1		11
C5A Transparenz		2	1	2	1	1		1	2				2		2	2	2	2						2	2		1		15
C5C Modalitäten für die Wahrnehmung von Betroffenenrechten		2	1		1	2		1					3						2			2		1	2	2			14
C 5 E Recht auf Vergessenwerden	2	2	2	2	1			2	1				1	2	2		3	2	2		2	3		1	2	1			18
C 5 G Recht auf Datenportabilität	3	2			1			2	1				2		2	1	1	2	2			1			2	1	1		15
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	2		2		1	2		2	2						1	2	1	1				1		1	1	2			14
C5L Benachrichtigung bei Datenschutzverletzungen	2	2	2		2			1	2	1	1	1	2	3	2	1	1	2				2		1	2	2			18

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Name	BSA	UEAPME 12-04	GDV	BDIU	DDV	VDZ	ICDP	ENPA 12-09	ZAW 12-09	GSMA	ECTA	ETNO	Nokia 12-09	US-DoC	BITKOM	EBF	Eurofinas 12-10	DIGITALEUROPE 12-11	BT	Yahoo	EuroISPA	Telefonica 12-12	ICC	AmCham EU	ITRE-Bericht	Ausschuss der Regionen	UK	CH - Switzerland	Häufigkeit d. Nennung
C6A Privacy by Default	1	2	2					1	2				1		1	1	1	1	1		1			1	1		1		15
C 6 B Privacy by Design	2	2	2				2	2	2				1		1	1	1	1			2		1	1	1		1		17
C 6 C Dokumentation		1	2					1	2		2	2	1		1	1		1				1	1	1	1		1		16
C 7 Übermittlung in Drittstaaten	2		2							2	2	2		1	2	1	2	2	3			2	1	1	2		1	2	17
C 13 A Verhaltensregeln			2						1	1	1	1		1	1									1	2	2	1		11
C 13 B Zertifizierungen/Gütesiegel	2		2					1							2									2	2	3	2		8
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten		2	4										2		2	1		2							1	2	1		9
C 13 D Datenschutz-Folgenabschätzung		1	1					1		1	1	1			2	1	1	2			2	2	1	1	2	2	2		17
C 15 C Datenschutzbehörden																							5			2	2		3
C 17 D Verbands- /Sammelklagerecht		3	1					1								1	1							2	2		1		8
C 17 E Sanktionen und Geldbußen	2	2	1				2	1		1	1	1			2	1	3	1			1	1	2	2	1	2	1		19

Tabelle 4-38: Positionierung der extremen Flexibilitätsbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3.1.3.3 Ressourcen der Flexibilitätsbefürworter

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die guten Verbindungen der datenverarbeitenden Wirtschaft zu den Mitgliedstaaten erwiesen sich besonders in der Konfliktphase als Vorteil, da der Ministerrat dazu bewegt werden konnte, viele der Kritikpunkte in die Ratsposition aufzunehmen. Auf Seiten des Parlaments herrschte eine gute Einbindung in die Arbeiten der Ausschüsse ITRE, IMCO und JURI, sodass die Berichte aller drei Ausschüsse und insb. des ITRE-Ausschusses sehr Flexibilitätsfreundlich ausfielen.

Unterstützung durch die Öffentliche Meinung

Von einer Unterstützung durch *die* Öffentliche Meinung, i. S. der Bevölkerungsmehrheit, kann bei den Flexibilitätsbefürwortern zwar nicht die Rede sein. Allerdings wurden die datenverarbeitenden Akteure seitens der eher wirtschaftsnahen Medien (wie z. B. dem Handelsblatt) unterstützt.

Informationen/Informationshoheit

Die Flexibilitätsbefürworter verfügten über anwendungsorientiertes Wissen zum Datenschutzrecht. Hiervon machten sie auch rege Gebrauch, indem immer wieder auf die zu befürchtende administrative Überbelastung hingewiesen wurde. Ein Problem, das bereits in der Vorphase angesprochen wurde, seine Relevanz aber auch in der Konfliktphase behielt, war die Glaubwürdigkeit der Flexibilitätsbefürworter. Lobbying-Strategien wie Astro-Turfing, die Überschwemmung von Abgeordneten mit Stellungnahmen oder Einladungen zu Gesprächen, Veranstaltungen usw. wurden in der Reformdebatte eher negativ aufgefasst. Ein Problem war insbesondere, dass in der öffentlichen Debatte weniger die Meinungen der europäischen Datenverarbeiter gehört wurden, sondern die der US-amerikanischen Konzerne (Beuth 2013b). Ich gehe davon aus, dass einige der Positionen der Flexibilitätsbefürworter auf offenere Ohren gestoßen wären, wenn nicht die US-Industrie hinter dem Lobbying nicht dermaßen sichtbar gewesen wären. Denn letztlich vertraten europäische und außereuropäische Akteure überwiegend dieselben Positionen, waren in der Medienberichterstattung aber deutlich weniger präsent. Interessant und auffällig in dieser Hinsicht war etwa auch, dass sowohl Intel, als auch Google, Microsoft und Facebook dort, wo sie als einzelne Akteure lobbyierten, eher gemäßigte Positionen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

vertraten. Die Vertretung der extremsten Positionen erfolgte hingegen seitens der (Dach-)Verbände wie AmCham bzw. der ICDP.

Fähigkeit zur politischen Mobilisierung

Die politische Mobilisierung spielte auf Seiten der Flexibilitätsbefürworter keine nennenswerte Rolle.

Finanzielle Ressourcen

Das massive Lobbying der Entscheidungsträger seitens der Flexibilitätsbefürworter war nur auf Grundlage enormer finanzieller Ressourcen möglich. Darunter fallen einerseits die zahlreichen Veranstaltungen und Treffen, die durchgeführt wurden, um den eigenen Positionen Gehör zu verschaffen (Schildberger 2016, 113 ff.), aber andererseits natürlich auch die Personalkosten der Lobbyisten selbst. So beschäftigte Berichten zufolge allein AmCham EU zum Thema der Datenschutzreform 50 Mitarbeiter/innen (Thomas Brewster 2012).

Das *Vorhandensein einer fähigen Führung*

Über eine mit der Rolle von Reding oder Albrecht vergleichbare, in besonderem Maße fähige und öffentlich sichtbare Galionsfigur verfügten die Flexibilitätsbefürworter nicht. Auf Ebene der datenverarbeitenden Wirtschaft kam auch weiterhin der ICDP eine wichtige Rolle zu, da sie große und wichtige (Dach-)Verbände unter einem noch größeren Dach vereinte. Ab 2015 auch die European Data Coalition (EDC) eine ähnliche Rolle ein.

Auf Ebene der Mitgliedstaaten übernahmen insbesondere die jeweiligen Ratspräsidentschaften eine relevante Führungsrolle. Dabei wurden sie von den Gegnern der Datenschutzreform, allen voran durch die Bundesrepublik und das Vereinigte Königreich unterstützt.

4.3.1.4 Die Akteursgruppe der bedingten Datenschutzbefürworter

Deutlich schwieriger im Vergleich zu den anderen Gruppen zu fassen ist das Wirken der Gruppe der bedingten Datenschutzbefürworter. Diese Akteursgruppe stellt deshalb eine Ansammlung von Akteuren dar, die tendenziell eher für die Stärkung der datenschutzrechtlichen Vorgaben eintraten, weil sie dazu tendierten, die Regelungsvorschläge der Kommission zu unterstützen, also weder für die Abschwächung noch für die Stärkung dieser eintraten. Die Zuordnung zu einer Community halte ich allerdings

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

für grundsätzlich problematisch: So kann bei einem Teil der Akteure, den Mitgliedstaaten, womöglich durchaus von einem zumindest geringen Grad an Abstimmung die Rede sein. Doch, dass so unterschiedliche Akteure wie BRAK, ICO, CPME und EMPL sich in einem Maße abstimmten, dass von einer Community gesprochen werden könnte, kann bezweifelt werden.[367] Nichtsdestotrotz wäre die Zuordnung dieser Akteure zu den Datenschutz- bzw. Flexibilitätsbefürwortern noch problematischer gewesen, da dann beispielsweise Frankreich oder Ungarn der Community der Datenschutzbefürworter zugeordnet worden wären, obwohl m. W. n. keine (nicht-)trivialen Verbindungen zwischen diesen Akteuren vorhanden waren. Der Namenszusatz „bedingte" Datenschutzbefürworter wiederum ist daher gerechtfertigt, da die Akteure (teilweise ausgehend von Policy-Kernüberzeugungen, die den Flexibilitätsbefürwortern näherstehen) für eine Form der Ausgestaltung der datenschutzrechtlichen Vorgaben eintraten, die eher den Vorschlägen der Datenschutzbefürworter näherstanden (vgl. Tabelle 4-31). In dieser Gruppe finden sich einige Mitgliedstaaten (Frankreich, Polen, Ungarn und Österreich sowie Italien, Griechenland und Zypern, die im Laufe dieser Phase die Ratspräsidentschaft innehatten), die im Aushandlungsprozess als relative Befürworter eines – im Vergleich zu den Positionen der übrigen Mitgliedstaaten – hohen Datenschutzniveaus aufgetreten waren. Daneben finden sich auch die Slowakei, Rumänien und Liechtenstein.

Von Bedeutung ist die Positionierung dieser Akteure daher, weil die Cluster-Analyse demonstriert, dass der finale DSGVO-Kompromiss am ehesten den Forderungen dieser Akteursgruppe entspricht (vgl. Tabelle Anhang 4). Die Existenz dieser Gruppe ist der Grund dafür, dass die DSGVO-Gegner im Ministerrat sich nicht vollständig durchsetzen konnten (Jančiūtė 2018, 165 ff.). Da die Gruppe der bedingten Datenschutzbefürworter während des Aushandlungsprozesses allerdings weder als Advocacy-Community noch als Advocacy-Koalition agierte, führte ich, anders als bei den anderen Gruppen, keine vertiefte Akteursanalyse durch. Die ausführliche Übersicht der Positionierung aller Akteure der Community der Kompromisswilligen kann dem Anhang (vgl. Tabelle Anhang 4) entnommen werden.

367 Zudem sei erwähnt, dass die Zuteilung zumindest von einigen der Akteure zu dieser Community durchaus auch auf den enormen Anteil an fehlenden Werten zurückgeführt werden könnte. Vgl. insbesondere das Auftauchen der schwedischen Regierung und des schwedischen Parlaments, die auf nur einem bzw. drei Werten basierte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bedingte Datenschutzbefürworter	
Akteur	**Akteursgruppe**
Schwedisches Parlament	Mitgliedstaatl. Parlament
Schweden	Mitgliedstaatl. Regierung
CPME	Verband Ärzteschaft
BRAK	Privatwirtschaft
ICO	Datenschutzbehörden
EMPL-Bericht	EU-Politik
Griechenland - Ratsvorsitz 2014-1	Mitgliedstaatl. Regierung
Frankreich	Mitgliedstaatl. Regierung
Italien - Ratsvorsitz 2014-2	Mitgliedstaatl. Regierung
Zypern - Ratsvorsitz 2012-2	Mitgliedstaatl. Regierung
Ungarn	Mitgliedstaatl. Regierung
Österreich	Mitgliedstaatl. Regierung
Polen	Mitgliedstaatl. Regierung
Portugal	Mitgliedstaatl. Regierung
Rumänien	Mitgliedstaatl. Regierung
Slowakei	Mitgliedstaatl. Regierung
Liechtenstein	EWR-Drittstaat

Tabelle 4-39: Akteursliste der bedingten Datenschutzbefürworter (eigene Zusammenstellung)

4.3.2 Prozessanalyse: Das Zustandekommen der DSGVO

4.3.2.1 Erste Reaktionen auf den Kommissionsentwurf

Obwohl die Kommission darum bemüht war, die Vorteile der Reform für die (datenverarbeitende) Wirtschaft hervorzuheben, wurde der Kommissionsentwurf von Wirtschaftsvertretern durchweg negativ aufgenommen. Wie die Darstellung des Überzeugungssystems der Flexibilitätsbefürworter zeigte, äußerten sich die Flexibilitätsbefürworter kaum zu den Aspekten des Vorschlags, in denen die Kommission ihren Forderungen entgegengekommen war.[368] Stattdessen fokussierte die Debatte auf die, aus der Perspektive der datenverarbeitenden Wirtschaft aus betrachtet, negativen Elemente

368 Dies betraf die Harmonisierung des Datenschutzrechts im Allgemeinen, die Einführung eines One-Stop-Shops, die Abschaffung der Meldepflicht, die Erleichterung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des Kommissionsvorschlags. Insbesondere richtete sich die Kritik zunächst gegen den Vorschlag der Einführung einer *ausdrücklichen Einwilligung*. Zugleich wurde der Entwurf auf allgemeiner Ebene dahingehend kritisiert, dass der *administrative Mehraufwand* zur Befolgung der neuen Elemente des Reformvorschlags[369] die von der Kommission vorgesehenen Erleichterungen für Unternehmen dermaßen überwiegen würden, dass am Ende die Wirtschaft mit einem unverhältnismäßigen Mehraufwand im Vergleich zur DS-RL konfrontiert würde (Euractiv 2012b, 2012c; Krempl 2012d; Warman 2012b). Daneben stand auch das sog. *Recht auf Vergessenwerden* im Fokus der Kritik. Nachdem bereits der bei Google für Datenschutzfragen zuständige Peter Fleischer (2011) harsche Kritik an den französischen Plänen für ein solches Recht geübt hatte, wandte sich Anfang 2012 auch Vinton Cerf, einer der Erfinder des Internets, der seit 2005 bei Google beschäftigt war, gegen die Pläne der EU-Kommission. Demnach würde sich die EU mit ihren Plänen zur weltweiten Internet-Polizei aufschwingen, Geldbußen in Höhe von bis zu 2% des weltweiten Jahresumsatzes eines Konzerns verhängen und letzten Endes die weltweite Zensur des Internets und das Ende der Meinungsfreiheit bedeuten (Warman 2012a, 2012d). Nichtsdestotrotz waren diese ersten Reaktionen, verglichen mit dem späteren Ausmaß des Lobbyings, eher verhalten und abwartend. Abwartend insbesondere im Hinblick darauf, wie das Parlament sich des Entwurfs annehmen würde.

Parallel zur Wirtschaft äußerten sich auch der EDSB und die Datenschutzgruppe zeitnah zum Kommissionsvorschlag. Im Gegensatz zu den Positionen der Industrievertreter wurde der Vorschlag dabei grundsätzlich begrüßt, im Detail wurden jedoch auch Kritikpunkte formuliert (Article 29 WP 2012; EDSB 2012b; Ermert 2012). Auch die zivilgesellschaftlichen Datenschutzbefürworter äußerten sich zeitnah zum Kommissionsvorschlag (EDRi 2012b; VZBV 2012), ihre Positionen blieben aber in den – ohnehin nicht besonders zahlreichen – einschlägigen medialen Berichten zunächst weitestgehend unerwähnt.[370]

---

grenzüberschreitender Datentransfers und die Ausweitung des räumlichen Anwendungsbereichs.

369 Darunter insb. das Recht auf Datenportabilität, die Meldepflicht bei Datenschutzverletzungen, die Einführung von Privacy by Design und Default, die Verpflichtung zur Bestellung betrieblicher Datenschutzbeauftragter sowie zur Durchführung einer Datenschutz-Folgenabschätzung und die neuen Sanktionsvorgaben.

370 Diese Aussage fußt auf einer eigenen Recherche zur Medienberichterstattung über die Datenschutzreform. Dazu wurden die Archive mehrerer europäischer Tageszeitigen und IT-News-Webseiten (Heise.de, Euractiv.de, Telegraph, Spiegel, Zeit, Go-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ein weiterer Akteur, der Mitsprache bei den Verhandlungen beanspruchte, waren die Vereinigten Staaten. Nachdem die US-Regierung im Februar 2012 selbst einen Entwurf für ein US Consumer Privacy Bill of Rights (The White House 2012) vorgelegt hatte, reiste Cameron F. Kerry, oberster Jurist im US-Handelsministerium, in die EU und traf mit Vertretern des Europäischen Parlaments, der Kommission und Vertretern aus Mitgliedstaaten zusammen. In diesem Zusammenhang forderte er ein informelles Mitspracherecht an der Reform ein und wies zugleich Bedenken hinsichtlich des Zugriffs auf Daten von EU-Bürgerinnen und Bürgern durch US-Behörden zurück (Lüke 2012).

4.3.2.2 Diskussion des Kommissionsentwurfs in den Parlamentsausschüssen

Bei der Plenumssitzung des EU-Parlaments am 16. Februar 2012 wurde der LIBE-Ausschuss federführend mit der Erarbeitung der Parlamentsposition betraut. Als mitberatende Ausschüsse wurden ITRE, ECON[371] und IMCO festgelegt. Außerdem wurde auf dieser Sitzung die Konsultation des EWSA beschlossen (EU-Parlament 2012d, 4). Die Zuständigkeit des LIBE-Ausschusses wurde allerdings von Anfang an infrage gestellt. So versuchten die konservative Vorsitzende des ITRE-Ausschusses, Amalia Sartori (Italien, Il Popolo della Libertà / EVP) sowie der konservative, EU-skeptische Vorsitzende des IMCO-Ausschusses, Malcom Harbour (Vereinigtes Königreich, Conservative Party / EKR) mehr Einfluss auf die Gestaltung der Parlamentsposition zu nehmen, indem sie im März 2012 im Rahmen der Konferenz der Ausschussvorsitzenden die Anwendung des *Verfahrens mit assoziierten Ausschüssen* beantragten (EU-Parlament 2012a, 11 f.). Nachdem sich dieser Konflikt einige Monate hinzog (EU-Parlament 2012b, 10), konnten sich die mitberatenden Ausschüsse letztlich nicht durchsetzen und der LIBE-Ausschuss unter dem sozialdemokratischen Vorsitzenden Juan Fernando López Aguilar (Spanien, PSOE / S&D) behielt die alleinige Federführung. Allerdings kamen am 24. Mai 2012 zunächst der EMPL-Ausschuss (EU-Parlament 2012e, 17) und am 14. Juni 2012 der JURI-Ausschuss (EU-Parlament 2012c, 18) als weitere mitberatende Ausschüsse hinzu.

lem) insb. auf die Stichwörter „Datenschutz", „Datenschutzreform", „Datenschutz-Grundverordnung", „Data Protection", „Data Protection Reform", „General Data Protection Regulation", „GDPR" hin durchsucht.

371 Der ECON-Ausschuss entschied sich später gegen die Abgabe einer Stellungnahme (Albrecht 2013g, 720).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nachdem die EVP, die mit Axel Voss bereits den Berichterstatter der Parlamentsresolution zum Datenschutz-Gesamtkonzept gestellt hatte, zunächst versuchte, den Posten des federführenden Berichterstatters zur DSGVO für sich zu beanspruchen, ging diese Funktion aufgrund der Kräftekonstellation und der Vergabe der weiteren Berichterstatter-Posten letztlich doch an die Grünen (Jančiūtė 2018, 161). Die Ernennung des grünen Abgeordneten Jan Philipp Albrecht (Deutschland, Bündnis 90/Die Grünen / Grüne/EFA) zum Berichterstatter des federführenden LIBE-Ausschusses erfolgte am 12. April 2012 (LIBE-Ausschuss 2012d, ab 10:19:35). Die Positionen der für den Aushandlungsprozess sehr wichtigen Schattenberichterstatter der Fraktionen übernahmen Axel Voss für die EVP, Marju Lauristin für die S&D, Sophia in't Veld für ALDE, Timothy Kirkhope für die EKR, Cornelia Ernst für die GUE/NGL sowie Kristina Winberg für die EFD (Legislative Observatory European Parliament 2019). Die Berichterstatter-Posten der mitberatenden Ausschüsse gingen an die konservative Lara Comi (Italien, Il Popolo della Libertà, EVP) für den IMCO-Ausschuss am 29. Februar 2012, an den konservativen Seán Kelly (Irland, Fine Gael Party / EVP) für den ITRE-Ausschuss am 14. März 2012, an die liberale Nadja Hirsch (Germany, FDP / ALDE) für den EMPL-Ausschuss am 20. April 2012 sowie an die konservative Marielle Gallo (Frankreich, La Gauche moderne / EVP) für den JURI-Ausschuss am 14. Juni 2012 (Comi 2013, 120; Gallo 2013, 106; Hirsch 2013, 19; Kelly 2013, 180).

Die Ernennung Jan Philipp Albrechts zum Berichterstatter wurde vor allem seitens der konservativen Abgeordneten mit Skepsis und Sorge aufgenommen, da die Grüne Fraktion bereits in der Vergangenheit stets für stärkere Datenschutzgesetze eingetreten war (Bernet 2015, Min. 10:30 ff.). In der Folgezeit konzentrierten sich die Wirtschaftsvertreter darauf, den federführenden Berichterstatter, aber auch die Schattenberichterstatter des LIBE-Ausschuss und die Berichterstatter der mitberatenden Ausschüsse ITRE, IMCO, EMPL und JURI möglichst häufig und intensiv im Rahmen von Veranstaltungen, persönlichen Gesprächen und des Versands schriftlicher Stellungnahmen von den eigenen Perspektiven auf die Reform zu überzeugen (Schildberger 2016, 113 ff.).[372] Während der Entwurfsphase der

372 Einen ausführlichen Einblick in das von allen Seiten betriebene Lobbying bieten zwei Excel-Tabellen, die von Jan Philipp Albrechts Team zum Zwecke der Transparenz erstellt wurden. Eine der Dateien bietet einen Überblick über alle direkten Treffen mit Vertretern und die andere Datei listet die Veranstaltungsteilnahmen Albrechts von Anfang 2012 bis Mitte 2013 auf (Albrecht 2013f, 2013e).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Ausschusspositionen im Zeitraum zwischen Frühjahr 2012 und Anfang 2013 führten die Ausschüsse aber auch eigene Veranstaltungen in Form formeller Anhörungen und weiterer, informeller Treffen durch, zu denen Interessenvertreter eingeladen wurden. Während der LIBE-Berichterstatter Albrecht bei diesen Treffen Wert auf Meinungspluralismus legte und daher Vertreter sowohl der Flexibilitätsbefürworter als auch der Datenschutzbefürworter eingeladen waren,[373] zeigte sich bei den übrigen Ausschüssen ein deutlich einseitigeres Bild. So beklagten Verbraucherschutzorganisationen, dass sich die konservative Lara Comi, Berichterstatterin des für Binnenmarkt und Verbraucherschutz zuständigen IMCO-Ausschusses, weder mit Vertretern nationaler Verbraucherschutzorganisationen, noch mit Vertretern der europäischen Dachorganisationen BEUC getroffen hätte (Albrecht 2013h). In ähnlicher Weise dominierten die Stimmen der Industrie die Ende 2012 durchgeführte ITRE-Mini-Anhörung zum Thema „Perspektiven der Datenschutz-Grundverordnung für die Bereiche Industrie und Forschung" (ITRE-Ausschuss 2012, vgl. TOP 4).

Weiterhin traten die Flexibilitätsbefürworter für die Reduktion der Datenschutz-Vorschriften und die Ausweitung des Spielraums der Verantwortlichen bei der Befolgung der Datenschutzregeln ein (Krempl 2012e). Zugleich wurden die Änderungsvorschläge aller Interessenvertreter immer konkreter. Waren die unmittelbar nach der Veröffentlichung des Kommissionsvorschlags geäußerten Meinungen noch eher allgemein im Hinblick auf einzelne Aspekte des Vorschlags formuliert, gingen die Akteure, nachdem die Einreichung konkreter Änderungsanträge in den Ausschüssen möglich wurde,[374] zunehmend dazu über, den Mitgliedern der beteiligten Ausschüsse sehr detaillierte Änderungs- und konkrete Formulierungsvorschläge zu unterbreiten. Die mitberatenden Parlamentsausschüsse legten ihre Berichtsentwürfe zwischen September und November 2012 vor.[375] Nach Ablauf der letzten Frist zur Einreichung von Änderungsanträgen Mitte Dezember wurde schließlich in den mitberatenden Ausschüssen die

373 Vergleiche hierzu insb. die Zusammensetzung der Teilnehmer des LIBE *Workshop on the proposed Data Protection Regulation* (LIBE Committee 2012), aber auch die weiteren Treffen des federführenden Berichterstatters Albrecht (Albrecht 2013f, 2013e).

374 Sofern dem keine Ausschussinternen Fristen oder andere Gründe entgegenstehen, kann jedes Mitglied des Europaparlaments (MEP) bis zur Abstimmung im Parlamentsplenum einen Legislativvorschlag betreffende Änderungsvorschläge einbringen (Greenwood 2011, 40 f.).

375 IMCO (25.09.2012), JURI (18.10.2012), ITRE (8.11.2012), EMPL (8.11.2012) (EDRi 2012a).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Arbeit an den finalen Berichtsfassungen aufgenommen (EDRi 2012a). Die finalen Abstimmungen verzögerten sich gegenüber dem ursprünglichen Zeitplan um einen Monat, da die Konsens- bzw. Entscheidungsfindung wegen der verhärteten Fronten schwierig war.

Parallel dazu wurde der Vorschlag im LIBE-Ausschuss neben zahlreichen informellen Besprechungen der (Schatten-)Berichterstatter auf mehr als zehn formellen Sitzungen und auf Basis von drei Arbeitsdokumenten ausführlich diskutiert (LIBE-Ausschuss 2012c, 2012a, 2012b).[376] Eine erste Vorfassung des LIBE-Berichtsentwurfs wurde Mitte Dezember 2012, der offizielle Berichtsentwurf schließlich am 16. Januar 2013 veröffentlicht. Nachdem mit der Veröffentlichung des offiziellen Berichtsentwurfs klar wurde, dass Albrecht anders als die Berichterstatter der übrigen Ausschüsse nur wenig Kompromissbereitschaft gegenüber den weitgehenden Forderungen der Flexibilitätsbefürworter zeigte, erreichte der Streit und der Lobbyansturm um die DSGVO schließlich ihren Höhepunkt und führte zu einer Pattsituation im Parlament. Bevor jedoch dargelegt wird, wie genau es dazu kam und wie diese schließlich überwunden wurde, werden im Folgenden zunächst noch die parallelen Entwicklungen im Ministerrat untersucht.

4.3.2.3 Diskussion des Legislativvorschlags im EU-Ministerrat

Unmittelbar nachdem der Kommissionsentwurf an den Ministerrat übermittelt worden war, setzte sich die für Datenschutzfragen zuständige Ratsarbeitsgruppe DAPIX „Informationsaustausch und Datenschutz" am 23. Februar 2012 erstmals mit dem Vorschlag auseinander.

Die Zuständigkeit von DAPIX für die DSGVO war ebenfalls nicht unumstritten. Eine nicht näher spezifizierte Ratsdelegation unternahm auf der ersten DAPIX-Sitzung zur DSGVO den Versuch der Übertragung der Zuständigkeit in eine Binnenmarktarbeitsgruppe mit der Begründung, dass der Verordnungsentwurf sich auch auf Art. 114 AEUV zur Errichtung und zum Funktionieren des Binnenmarktes stützte (DAPIX 2012). Dieser Vorstoß wurde jedoch vom Generalsekretariat unter Verweis auf eine Entscheidung des Ausschusses der Ständigen Vertreter (AStV) abgelehnt, wonach DAPIX nach Inkrafttreten des Lissabon-Vertrags für alle Datenschutzfragen zuständig sein sollte (Presidency of the Council of the European Union 2009). In den Folgejahren setzte sich DAPIX auf mehreren Dutzend Sit-

376 Vgl. die Liste aller mit der DSGVO befassten LIBE-Sitzungen in Tabelle Anhang 5.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

zungen mit dem DSGVO-E auseinander. Aufgrund der Schengen-Relevanz der Materie wurden seit März 2013 auch Island, Norwegen, die Schweiz und Liechtenstein im Rahmen der DAPIX-Mixed-Committee-Sitzungen in die Verhandlungen miteinbezogen (vgl. Tabelle Anhang 8). Parallel zu den Beratungen auf Ebene von DAPIX setzte sich auch der AStV auf knapp drei Dutzend Sitzungen mit dem DSGVO-E auseinander (vgl. Tabelle Anhang 7). Gerade zu Beginn fanden nur wenige Sitzungen statt. So folgte auf die ersten beiden DAPIX-Sitzungen, die zwischen Februar und März 2012 stattfanden, keine weitere Sitzung innerhalb der darauffolgenden 3 Monate. Der AStV tagte sogar mehr als sieben Monate nicht zu dem Verordnungsvorschlag, wobei dies weniger überraschend war, da die AStV-Sitzungen üblicherweise auf den Sitzungen der Arbeitsgruppen aufbauen bzw. als Vorbereitung für die Sitzungen des Ministerrates dienen (Fouilleux, Maillard, und Smith 2005). Anders als die Diskussion des Kommissionsvorschlags in den Parlamentsgremien kamen die Diskussionen im Ministerrat somit zunächst nur sehr schleppend voran. Begründet wurde dies damit, dass der Kommissionsentwurf zunächst noch durch die Datenschutzexperten aller Mitgliedstaaten geprüft werden musste.[377] Dementsprechend war die erste Lesung des Kommissionsentwurfs im Rat Ende 2012 noch nicht abgeschlossen (Zyprische Ratspräsidentschaft 2012).

Während der Debatten auf Arbeitsgruppenebene wurden schließlich als die drei hervorstechendsten Themen bzw. Problemkomplexe des Verordnungsentwurfs die *hohe Zahl von delegierten Rechtsakten und von Durchführungsrechtsakten*, die *Eindämmung des Verwaltungsaufwands für Verantwortliche* sowie der *Sonderbehandlung des öffentlichen Sektors* identifiziert (EU-Ministerrat 2012, 3). Auf einem informellen Treffen der Justizminister der Mitgliedstaaten Ende Juli 2012 wurden diese drei Problemkomplexe auf Drängen der zyprischen Ratspräsidentschaft erstmals auf Ministerebene thematisiert und priorisiert (Zyprische Ratspräsidentschaft 2012). Eine Reihe von Mitgliedstaaten (Belgien, Tschechien, Irland, Luxemburg, die Niederlande, das Vereinigte Königreich) war insbesondere der Einführung neuer Datenschutz-Instrumente wie der Datenschutz-Folgenabschätzung oder der Verpflichtung zur Einberufung betrieblicher Datenschutzbeauftragter gegenüber stark ablehnend eingestellt, während ein anderer Teil der Mitgliedstaaten sich mit den Vorschlägen arrangieren konnte oder diese befürwortete (vgl. auch die entsprechenden Diskussionen der Akteurspo-

377 „Die Prüfung durch Datenschutzexperten aus 27 Mitgliedstaaten […] ist ein langer, mühsamer und zeitraubender Prozess." (EU-Ministerrat 2012, 2)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

sitionen in den vorangegangenen Unterabschnitten). Nachdem der Kommissionsentwurf in den darauffolgenden DAPIX- und AStV-Sitzungen im Hinblick auf die drei priorisierten Themen näher diskutiert wurde, deutete sich gegen Ende 2012 schließlich als Kompromiss zwischen den Mitgliedstaaten die Befürwortung des sog. risikoorientierten Ansatzes heraus, „bei dem die Verpflichtungen der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter insbesondere auf die Art der Verarbeitung und der verarbeiteten Daten sowie auf ihre Auswirkungen auf die Rechte und Freiheiten des Einzelnen [insb. im Hinblick auf Rufschädigung, Diskriminierung, finanzielle Verluste und Identitätsdiebstahl] abgestimmt werden." (EU-Ministerrat 2012, 8)

Derweil lobbyierten die Vertreter der Wirtschaft nicht nur im Rahmen des Europäischen Parlaments, sondern auch auf Ebene der Mitgliedstaaten (Jančiūtė 2018, 165–72, 184–91; Schildberger 2016, 118–25). Da Ratsarbeitsgruppen bzw. die Ratsdelegationen intransparent operieren, können hierzu nur anekdotische Informationen geliefert werden. So etwa hinsichtlich der Versuche von Facebook, unter Androhung der Einschränkung ihrer Kooperation mit der irischen Datenschutzbehörde, der irischen Regierung Zugeständnisse abzuringen (Beuth 2012). Da die Datenlage zum Lobbying auf Ebene der Mitgliedstaaten nur fragmentiert vorliegt, möchte ich im Folgenden exemplarisch etwas näher auf das Lobbying im Hinblick auf das deutsche Innenministerium eingehen, für das etwas mehr Informationen vorliegen.

In der öffentlichen Debatte war in dieser Phase zunächst insbesondere die Rolle der Bundesrepublik höchst ambivalent. So hatte sich die damalige Justizministerin Ilse Aigner (CSU) in einer gemeinsamen Pressemitteilung mit der EU-Justizkommissarin Reding Anfang November 2011 explizit für einen stärkeren Datenschutz auf EU-Ebene ausgesprochen (Europäische Kommission 2011).[378] Die Federführung für die Verhandlungen zur DSGVO hatte allerdings Bundesinnenminister Hans-Peter Friedrich (CSU) inne, der die Datenschutzreform weitgehend ablehnte. Ausgangspunkt der

378 Allerdings sei an dieser Stelle noch klargestellt, dass von den drei Themen, auf die sich Aigner und Reding geeinigt hatten, lediglich die ausdrückliche Einwilligung zu den umstritteneren Themen zählte, während die Ausweitung des Anwendungsbereichs der Datenschutzregeln auf außereuropäische Unternehmen, die ihre personenbezogene Daten verarbeitenden Dienste an EU-Bürgerinnen und -Bürger richten, praktisch unumstritten war und die Ausführungen zur Löschung selbst ins Internet gestellter Daten so abstrakt waren, dass diese kaum als Positionierung gedeutet werden können (Europäische Kommission 2011).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Debatte war die Entscheidung von Facebook im Jahr 2011, deutsches Datenschutzrecht nicht einhalten zu wollen. Dabei hatte sich das Unternehmen darauf berufen, nur irisches Datenschutzrecht einhalten zu müssen, da der europäische Hauptsitz des Konzerns in Dublin gelegen ist. Während die Community der Datenschutzbefürworter diese Haltung massiv kritisierte und Gegenmaßnahmen forderte, erklärte Innenminister Friedrich den Streit überraschenderweise für entschärft, nachdem er eine informelle Absprache mit dem damaligen Facebook-Cheflobbyisten Richard Allan im September 2011 getroffen hatte. So verwies Friedrich darauf, dass derartige Fragen am besten auf EU-Ebene im Rahmen einer Reform des Datenschutzrechts geklärt werden sollten und, dass er bis zur Verabschiedung EU-weiter Regeln mit Facebook an einer freiwilligen Selbstverpflichtung arbeiten werde, der sich zu unterwerfen das Unternehmen grundsätzlich bereit erklärt habe (Beuth 2011).[379] Nachdem die Kommission die Datenschutzreform initiiert hatte, intervenierte das Innenministerium jedoch und ging gegen den Kommissionsvorschlag vor. Vor allem stand das Bundesinnenministerium der Anwendung der Verordnung auf den öffentlichen Bereich[380] ablehnend gegenüber, beklagte daneben aber auch, dass die Vorschläge der Kommission nicht internettauglich seien und statt regulatorischer Vorschriften Anreize für eine gesteigerte Selbstkontrolle der Wirtschaft geliefert werden müssten, damit bei potentiell riskanten Verarbeitungen freiwillig angemessene Schutzmaßnahmen getroffen werden (Krempl 2012b). Schließlich gingen einige Äußerungen, etwa die von Cornelia Rogall-Grothe, Staatssekretärin im BMI, oder von Ulrich Würmeling, Berater beim US-amerikanischen Anwaltsbüro Latham & Watkins und Sprecher auf einer vom BMI mitorganisierten Tagung, in die Richtung der Abschaffung des Verbots mit Erlaubnisvorbehalt. Demnach sollten staatliche Verarbeitungen zwar weiterhin auf diesem Prinzip basieren, für unternehmerische Verarbeitungen sollte es allerdings umgekehrt werden, sodass Verarbeitungen grundsätzlich erlaubt und – wie im US-amerikanischen Datenschutzrecht – nur einzelne, problematische Verarbeitungen

379 Der Vorstoß Friedrichs scheiterte Mitte 2013, als Vertreter von Facebook und Google zu Verstehen gaben, dass sie sich nicht an nationalen Regelungen beteiligen würden (Briegleb 2013).

380 Einschränkend sei erwähnt, dass Friedrich seine Ablehnung – neben dem Argument, dass Brüssel sich in nationale Fragen durch die Einführung *zusätzlicher Brüsseler Bürokratie* nicht einmischen solle – formell auch mit dem hohen Schutzniveau in Deutschland, das durch die Verordnung bedroht werde (Birnbaum und Jansen 2012; Gerber 2012).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gesetzlich verboten sein sollten (Hülsmann 2012; Motejl 2012; Spiekermann 2012). Während die Ablehnung weitergehender regulatorischer Vorgaben durch Mitgliedstaaten wie dem Vereinigten Königreich oder Irland erwartet worden war,[381] überraschte die ablehnende deutsche Haltung, da die Bundesrepublik international eher als Vorreiter bei Datenschutzfragen wahrgenommen wurde. Dies erklärt auch, weshalb sich im Ministerrat letztlich der Fokus auf die Reduzierung des administrativen Aufwands für Verantwortliche in Gestalt des risikobasierten Ansatzes durchsetzen konnte.[382]

4.3.2.4 Höhepunkt der Debatte und Stillstand der Verhandlungen – Blockade in Parlament und Ministerrat

Den Höhepunkt erreichte die öffentliche DSGVO-Debatte schließlich im Zeitraum zwischen der Veröffentlichung des LIBE-Berichtsentwurfs Anfang Januar 2013 bis Mitte des Jahres 2013. Fokussierte sich das Lobbying bis dahin primär auf die Ansprache der zuständigen Politiker(innen), wurde ab dem Zeitpunkt der Veröffentlichung des LIBE-Berichtsentwurfs, an dem klar wurde, dass Albrecht nicht den von der Flexibilitätsbefürworter-Community gewünschten extremen Positionswechsel vollziehen würde, die Debatte verstärkt in die Öffentlichkeit getragen. In seinem Berichtsentwurf vertrat Albrecht (vgl. insb. die Diskussion in 4.3.1.2.2) Positionen, die weitgehend denen des extremen Flügels der Datenschutzbefürworter-Advocacy-Koalition entsprachen. Trotz seiner verbalen Versuche, strengere Regeln gleichsam als Vorteil für die Wirtschaft darzustellen (Albrecht 2013b), wurde der Bericht nur von Kommissarin Reding (European Commission 2013), dem EDSB (EDPS 2013), sowie von EDRi positiv aufgenommen (EDRi 2013a). Seitens der Wirtschaft und der mitberatenden Parlamentsausschüsse kam hingegen massive Kritik (Beuth 2013c; Singer 2013; Steiner 2013a, 2013b). Der liberale Schattenberichterstatter Alvaro etwa beklagte die fehlende Balance des Berichtsentwurfs. Während Albrecht Vorschläge von Datenschutz-NGOs wörtlich übernommen habe, sei er nicht auf die Kritikpunkte der Wirtschaft eingegangen (A. Alvaro 2013). Seitens der

381 Das britische Justizministerium war Mitte 2012 für die komplette Neuauflage der Reform eingetreten. Diese sollte auf einer Richtlinie fußen und der Wirtschaft größtmöglichen Raum bei ihren Datenverarbeitungstätigkeiten überlassen (Tom Brewster 2012; UK Ministry of Justice 2012).

382 Sehr instruktive Einblicke in das Ministerrats- bzw. deutsche Verständnis des risikobasierten Ansatzes bietet der Aufsatz des Mitglieds der deutschen Ministerratsdelegation Veil (2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Wirtschaft, allen voran der ICDP, aber auch von Microsoft und Facebook, war zu vernehmen, dass der Bericht keine Balance zwischen Datenschutz- und Wirtschaftsinteressen erziele (Clark 2013a; ICDP 2013a). In den darauffolgenden Wochen und Monaten erschienen weltweit in verschiedenen Zeitungen sowie auf verschiedenen Online-Nachrichtenportalen Berichte über die aus der Sicht der Wirtschaft zu erwartenden negativen Folgen der DSGVO. Ein erster zentraler Strang der Kritik, der nicht nur seitens der Wirtschaft, sondern auch seitens Axel Voss, dem Schattenberichterstatter der EVP-Fraktion sowie ehemaligen LIBE-Berichterstatter für die Stellungnahme des Parlaments zur Konsultation der Europäischen Kommission, vertreten wurde, zeichnete das Bild erodierender Internet-Dienste. Die weitgehenden Vorschläge Albrechts zur Einwilligung, zu Profiling, die Einschränkungen der berechtigten Interessen der Verantwortlichen und Einschränkungen hinsichtlich der Weitergabe von Daten an Dritte würden die auf personenbezogenen Daten basierenden Gewinne der Konzerne dermaßen einschränken, dass bislang kostenfreie Dienste entweder eine Gebühr erheben müssten oder die in der EU ansässigen Nutzerinnen und Nutzer diese nicht mehr nutzen könnten. Zudem vertrat Voss die Ansicht, dass es dann auch keine kostenlosen E-Mail-Accounts oder Online-Newsportale mehr geben könne, da diese ihre Gewinne aus werbebasierten Finanzierungsmodellen auf Basis personenbezogener Daten bezögen (Beuth 2013b; Heath 2013; Koch 2013). Ein zweiter zentraler Strang der Kritik verwies auf die wirtschaftlichen Schäden, die der Europäischen Union in Folge eines zu hohen Datenschutzniveaus drohten (Landes 2013). Diese Kritik wurde fortan insbesondere von einigen Mitgliedstaaten, aber auch von den wirtschaftsnahen Parlamentsausschüssen aufgegriffen.

Es war Teil der Strategie von Albrecht und seinem Team, mit einem Entwurf in die Debatte zu gehen, der einseitig die Datenschutzperspektive übernahm. Die Vertretung einer extrem datenschutzbefürwortenden Position wurde als erforderlich erachtet, weil damit gerechnet wurde, dass im Laufe der Diskussionen mit den Schattenberichterstattern, den anderen Ausschüssen und dem Ministerrat Kompromisse zu Lasten des Datenschutzniveaus abgerungen würden. Indem der Entwurf stark in eine Richtung geht, sollte gewährleistet werden, dass der finale Ausschussbericht bzw. die finale Verordnung aus Datenschutzperspektive trotz der Kompromisse ein akzeptables Datenschutzniveau festlegen (Bernet 2015, Min. 49:30 ff.). Die harschen Reaktionen der Wirtschaft auf den Berichtsentwurf

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

wurden von den Datenschutzbefürwortern erwartet[383] und zeitnah mit einer Gegenkampagne beantwortet.

Eine Koalition aus zivilgesellschaftlichen Organisationen unter der Führung von BoF, EDRi und PI[384] veröffentlichten Ende Januar 2013 die sogenannte „Brüsseler Datenschutz-Erklärung", eine offene Unterschriftenkampagne, in der sie Europaparlamentarier und die Regierungen der Mitgliedstaaten dazu aufforderten, stärkere Datenschutzrechte für die Bürgerinnen und Bürger der EU zu verabschieden. Als Kernpunkte eines starken Datenschutzes benannten die Verfasser der Erklärung die Anerkennung von IP-Adressen etc. als personenbezogenes Datum, die Klarstellung, dass eine Einwilligung ausdrücklich erteilt werden muss, die Einführung des Kopplungsverbots, Verbesserung der Transparenz, die Einführung *echter* Datenportabilitätsvorgaben, einen starken Schutz gegen Profiling sowie die Einführung wirksamer Rechtsbehelfe und Sanktionen (BoF, EDRi, und PI 2013). Neben den Fachportalen, die ohnehin regelmäßig über den Stand der Verhandlungen berichteten (Krempl 2013a), erreichten die zivilgesellschaftlichen Datenschutzbefürworter auf diese Weise auch die großen Tageszeitungen. Die *Zeit* verknüpfte beispielsweise den Hinweis auf die Brüsseler Datenschutz-Erklärung mit einem Einblick in die Ausmaße der Lobby-Maschinerie der US-amerikanischen Datenindustrie (Beuth 2013b).

Nur wenige Tage nach Veröffentlichung der Brüsseler Datenschutz-Erklärung startete EDRi, gemeinsam mit PI, la quadrature du net, Access International, der Panoptykon Foundation sowie der Open Rights Group, die öffentlichkeitsorientierte Kampagne „Protect My Data" als Gegengewicht gegen das massive Lobbying der Unternehmen. Weil befürchtet wurde, dass sich die mitberatenden Ausschüsse, in denen die Federführung zum

383 So hatten Vertreter der Zivilgesellschaft sowie Berichterstatter Albrecht bereits auf dem jährlichen CCC-Kongress Ende Dezember 2012, aufgrund der anhaltenden Lobbyschlacht und der sich anbahnenden Auseinandersetzungen mit dem Ministerrat, ihre Besorgnis über den Erfolg der Datenschutzreform geäußert (Albrecht, Szymielewicz, und Fiedler 2012; Krempl 2012a). Zudem befürchtete auch der Beraterstab Albrechts, dass der Bericht seitens Wirtschaftsvertretern stark kritisiert würde. Entsprechend empfahlen sie dem Berichterstatter lieber in die Offensive zu gehen und den Bericht publikumswirksam vorzustellen (Bernet 2015, Min. 42:45 ff.).

384 Weitere Organisationen, die sich an dem Vorhaben beteiligten, sind: Access (International), Consumer Federation of America (United States), Panoptykon Foundation (Poland), Vrijschrift, the Netherlands), Initiative für Netzfreiheit, Austria), La Quadrature du Net (France), The Julia Group (Sweden), TagMeNot.info (Italy), Association for Technology and Internet (Romania), Abine, Inc. (United States) (BoF, EDRi, und PI 2013).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

DSGVO-Bericht bei konservativen Abgeordneten lag, in den bevorstehenden Abstimmungen gegen ein hohes Datenschutzniveau aussprechen würden (Bergemann 2013c), wurde mit der Kampagne das Ziel verfolgt, auf die Berichterstatter aber auch auf weitere Mitglieder der Ausschüsse öffentlichen Druck aufzubauen. Zu diesem Zweck wurde eine Webseite aufgesetzt, auf der Bürgerinnen und Bürger über die Reform informiert und dazu aufgerufen wurden, die in den Parlamentsausschüssen sitzenden MEPs zu kontaktieren und ihnen die Wichtigkeit der Verabschiedung eines hohen Datenschutzniveaus nahe zu legen (Fiedler 2013a; Privacycampaign.eu 2013).[385]

Daneben initiierten die sechs Wissenschaftlerinnen und Wissenschaftler Oliver Günther, Gerrit Hornung, Kai Rannenberg, Alexander Roßnagel, Sarah Spiekermann und Michael Waidner Mitte Februar einen Aufruf an die Politik, die Datenschutz-Grundverordnung nicht zu verwässern. Darin verteidigten sie die Ambitionen des Reformvorhabens gegen die Kritik, dass Innovationen verhindert würden. Zudem sprachen sie ihre Unterstützung für die ausdrückliche Einwilligung, die Begrenzung und Spezifizierung des berechtigten Interesses, eine weite Definition personenbezogener Daten sowie für die Löschung eines Großteils der vorgesehenen delegierten und Durchführungsrechtsakte aus und forderten die Festlegung der wichtigen Regeln im Rahmen der Verordnung selbst (Günther u. a. 2013). In den folgenden Wochen und Monaten schlossen sich dem Aufruf mehr als 100 weitere namhafte Wissenschaftlerinnen und Wissenschaftler aus verschiedenen EU-Mitgliedstaaten an, sodass der öffentliche Druck weiter gesteigert wurde (Europäische Wissenschaftlerinnen und Wissenschaftler 2013; European Academics 2013).

Parallel zum Lobbying seitens der Wirtschaft setzte auch die US-Regierung ihre Intervention in den politischen Aushandlungsprozess fort. Mitte Januar wurde von Statewatch ein sog. Non-Paper[386] veröffentlicht, das die US-Regierung an die EU-Verhandlungsführer versandt hatte. Darin betonte

385 Access teilte später mit, dass mehr als 400.000 E-Mails versendet wurden (MacDonald 2013).

386 Non-Paper sind Stellungnahmen, die über keinen offiziellen Briefkopf verfügen. Sie werden üblicherweise in den heißen Phasen umstrittener Verhandlungen ausgetauscht: „Sie fassen noch einmal alle Positionen der eigenen Seite zusammen und sind in einem weitaus härteren Tonfall gehalten, als außerhalb dieser heißen Phasen üblich ist. Man hält sich dadurch die Türen für künftige Gespräche offen, weil diese „Non-Papers" nach Abschluss der Verhandlungen offiziell gar nicht existiert haben. Zugleich soll die dabei verwendete Tonart Indikator für den jeweiligen Grad der Verstimmung sein." (Möchel 2013b)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

die US-Regierung die Notwendigkeit flexibler Regeln, da ansonsten das globale Handelsregime gefährdet würde (US Administration 2013). Ende Januar 2013 warnte schließlich John Rodgers, US-Botschaftsrat für Wirtschaft in Berlin, gar davor, durch die Verabschiedung zu starker Datenschutzregeln, die eine zu starke Einschränkung für die US-amerikanische datenverarbeitende Wirtschaft mit sich brächten, einen Handelskrieg anzuzetteln. Statt des Einschlagens eines europäischen Sonderweges und der Befürwortung konfliktträchtiger Konzepte, wie das Recht auf Vergessenwerden, legte Rodgers den EU-Entscheidern nahe, die Passfähigkeit ihrer Regeln an globale Datenschutzstandards zu beherzigen (Krempl 2013d). In Folge des anhaltenden Lobbyings seitens der US-Regierung solidarisierten sich schließlich mehrere US-Datenschutz- und Menschenrechtsorganisationen – The American Civil Liberties Union (ACLU), Center for Digital Democracy (CDD) und Consumer Federation of America (CFA) – mit der Datenschutzreform sowie mit Berichterstatter Albrecht. Dabei sprachen sich die Beteiligten in harschen Worten gegen die von der US-Regierung vertretenen Argumente aus und klagten den übermächtigen Einfluss von US-Konzernen auf politische Entscheidungsprozesse und die Darstellung der Partikularinteressen der US-Wirtschaft als Gemeinwohlinteressen seitens der zuständigen US-Stellen an (Clark 2013b; O'Brien 2013; Stanley 2013).

Nachdem der IMCO-Ausschuss Ende Januar für die Absenkung des Datenschutzniveaus gestimmt hatte, stimmten im Februar ITRE und EMPL und schließlich im März auch JURI ebenfalls für die Absenkung des Schutzniveaus des Kommissionsvorschlags (vgl. für die ausführliche Diskussion der Standpunkte 4.3.1.3.2). Im LIBE-Ausschuss zeichnete sich dagegen ab, dass der Berichterstatter gegen jeden Widerstand seitens anderer Ausschussmitglieder und der Wirtschaftslobby einen Bericht mit einem möglichst hohen Datenschutzniveau abliefern und nur kleinere Zugeständnisse an die Gegner machen würde (Albrecht, Szymielewicz, und Fiedler 2012).

Bei den Änderungsanträgen, die von den Europaparlamentarier(-inne)n eingebracht wurden, zeigte sich schließlich, dass beide Koalitionen bzw. Communities enormen Erfolg mit ihrer Strategie des direkten Lobbyings einzelner Parlamentarier hatten. Wie insbesondere die Recherchen von LobbyPlag offenbarten, zielte die Mehrzahl der von den Parlamentariern eingebrachten Änderungsanträge auf die Abschwächung des von der Kommission vorgeschlagenen Datenschutzniveaus ab (Gutjahr 2013; LobbyPlag 2013, siehe unter dem Reiter „Amendments>Overview"). Wie die

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Recherchen außerdem zeigten, waren Änderungsvorschläge, die seitens verschiedener Interessengruppen gemacht worden waren, von den entsprechenden Europaabgeordneten teilweise unverändert übernommen worden. Eher wirtschaftsfreundliche Abgeordnete, darunter der ITRE-Berichterstatter Seán Kelly sowie JURI-Berichterstatterin Marielle Gallo, aber auch der Vorsitzende des ITRE-Ausschusses Malcolm Harbour, übernahmen insbesondere die Positionen von AmCham, Digitaleurope, eurofinas, Amazon und der EBF, in etwas geringerem Maße von ACCIS und eBay. Das von Datenschutzbefürwortern ins Leben gerufene Projekt LobbyPlag[387] diente somit als zusätzliche und sehr erfolgreiche öffentlichkeitswirksame Maßnahme, um der Datenschutzreform mehr öffentliche Aufmerksamkeit zukommen zu lassen. Die Berichterstattung zum sogenannten Copy&Paste-Lobbyismus schaffte es international in zahlreiche Zeitungen (Biermann 2013b; Cáceres 2013; Euronews 2013; Fontanella-Khan 2013a; F. Robinson 2013; Tzschentke 2013).[388]

Nachdem die mitberatenden Ausschüsse ihre Positionen verabschiedet hatten,[389] war es am federführenden Berichterstatter Albrecht, einen Kompromiss zwischen den Ausschüssen auszuhandeln, der sowohl im LIBE-Ausschuss als auch später im Parlamentsplenum mehrheitsfähig sein würde. Dies gestaltete sich aus zwei Gründen als schwierig. Während die Linken, Grünen und Sozialdemokraten Albrechts Vorschlag gegenüber wohlgesonnen waren, stellten sich insbesondere die konservativen Fraktionen EVP und EKR gegen die vorgesehene Stärkung des Datenschutzes. Aufgrund der Mehrheitsverhältnisse im Europäischen Parlament kam somit der liberalen ALDE-Fraktion die Rolle des Züngleins an der Waage zu.[390] Andererseits wuchs die Zahl der eingebrachten Änderungsanträge im

387 LobbyPlag war das Ergebnis einer Kooperation des Datenvisualisierungsunternehmens OpenDataCity und des Datenschutz-Projekts europe vs. facebook, das nach einer Kontaktaufnahme des Datenschutz-Aktivisten Max Schrems mit dem Journalisten Richard Gutjahr entstanden war (Gutjahr 2013).

388 An dieser Stelle sei allerdings erwähnt, dass auch die datenschutzfreundlichen grünen Schattenberichterstatterinnen Eva Lichtenberger, Christina Engström sowie Amelia Andersdotter ebenfalls Positionen, allerdings jene der zivilgesellschaftlichen Datenschützer EDRi und Bo,F eins zu eins übernahmen (LobbyPlag 2013, siehe unter dem Reiter „Influence").

389 Die finalen Stellungnahmen der mitberatenden Ausschüsse lagen zwischen Januar und März 2013 vor: IMCO (23. Januar 2013), ITRE (20. Februar 2013), EMPL (21. Februar 2013), JURI (19. März 2013) (EDRi 2012a).

390 Das Europäische Parlament umfasste in der siebten Legislaturperiode (2009-2014) insgesamt 736 Sitze. Die GUE/NGL (35), Grünen/EFA (55) und die S&D (184) ka-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Laufe der Monate auf beinahe 4000 an, sodass sich die Herausbildung eines Kompromisses als äußert schwierig gestaltete.[391] Im Kern ging es dabei darum, jene Änderungsanträge herauszupicken, denen die größte Chance auf das Erreichen einer Mehrheit in Ausschuss und Plenum zugerechnet wurde und die der Position Albrechts gleichzeitig am nächsten kamen. Zugleich galt es aus den dann infrage kommenden Änderungsanträgen jene auszuwählen, die zu keinen Widersprüchen mit anderen Artikeln bzw. Änderungsanträgen führten (D. Marshall 2012).

Nachdem der in der ALDE-Fraktion für Datenschutzfragen hauptverantwortliche LIBE-Schattenberichterstatter Alexander Alvaro mit einer ambivalenten Position[392] im Hinblick auf die von der Kommission und Albrecht angestrebte Stärkung des Datenschutzniveaus aufgefallen war, verhärteten sich die Fronten nach seiner Ablösung[393] durch die britische Sarah Baroness Ludford noch weiter. Nachdem Anfang März 2013 ein Artikel in der Financial Times erschienen war, in der die Meinung vertreten wurde, dass Unternehmen wie Google und Facebook mit aller Lobby-Macht und mit der Unterstützung der US-Regierung an einer Aufweichung des von der Kommission vorgeschlagenen Datenschutzniveaus arbeiteten und dabei insbesondere vom Ministerrat unterstützt würden (Fontanella-Khan und McCarthy 2013), verfasste Ludford einen Antwortbrief. In ihrer Antwort, die in der Financial Times veröffentlicht wurde, vertrat Ludford die Ansicht, dass die Darstellung der Datenschutzreformdebatten als ein Kampf zwischen dem Goliath in Form der US-Technologie-Riesen einerseits und

men gemeinsam nur auf insgesamt 274 der zum Erreichen der absoluten Mehrheit benötigten 369 Stimmen. Die EVP alleine hatte dagegen 265 Sitze, die EKR kam auf 55 Sitze, die EFD auf 32, Fraktionslose auf 26 und ALDE auf 84 Stimmen. EVP und EKR erreichten gemeinsam 330 Stimmen und waren somit ebenfalls auf die Unterstützung von ALDE angewiesen, mit der sie theoretisch 404 Stimmen erhalten und somit die absolute Mehrheit erringt hätten. Selbst mit den Stimmen von ALDE kam der linke Block gleichzeitig jedoch auf nur 358 Stimmen und war somit immer noch auf die Unterstützung aus den Reihen der übrigen Fraktionen angewiesen.

391 Laut Corporate Europe Observatory wurden im Rahmen eines Legislativvorschlags ansonsten durchschnittlich nur 50 bis 100 Änderungsanträge eingebracht (CEO, 2013a).

392 So hatte er den Albrecht-Berichtsentwurf für dessen Unausgeglichenheit kritisiert und später Abgeordnete gegen die im Kontext der LobbyPlag-Enthüllungen geäußerten Vorwürfe, sie würden zum Spielball der Industrie werden, in Schutz genommen (A. Alvaro 2013; Beuth 2013a).

393 Ende Februar 2013 geriet Alvaro in einen Autounfall und wurde so schwer verletzt, dass er die Rolle des Schattenberichterstatters nicht mehr einnehmen konnte. An seine Stelle trat unverhoffter weise Sarah Baroness Ludford (Ludford 2013c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

dem David in Gestalt der europäischen Bürgerrechtler andererseits eine unzutreffende Stereotypisierung und Verkürzung der Debatte sei. Tatsächlich würden nicht nur US-amerikanische Unternehmen, sondern auch Europäische Unternehmen die Einführung strengerer Datenschutz-Vorgaben ablehnen, darunter Vertreterinnen und Vertreter der medizinischen Forschung, des B2B-Handels, Marktforschungsunternehmen, Telekommunikationsanbieter, Versicherungen, Banken und KMUs im Allgemeinen. Wie den Analysen zur Zusammensetzung der Flexibilitätsbefürworter entnommen werden kann, hatte Baroness Ludford mit ihrer Aussage recht. Darüber hinaus vertrat sie die Auffassung, dass ein vernünftiger Kompromiss zwischen Wirtschaftsinteressen und Datenschutzinteressen möglich sei und dass auf Grundlage eines solchen Kompromisses weder die eine noch die andere Seite notwendigerweise leer ausgehen müsse, sondern eine Win-Win-Situation möglich sei (Ludford 2013b). Eine erste Folge war, dass die zunächst für Ende April 2013 (EDRi 2012a) angesetzte Orientierungsabstimmung im Parlament aufgrund der laufenden Verhandlungen nicht durchgeführt werden konnte. Nachdem auch auf der darauffolgenden LIBE-Sitzung Anfang Mai keine Einigung gefunden werden konnte (O'Connor 2013), wendete sich Berichterstatter Albrecht einmal mehr an die Öffentlichkeit. In einem Beitrag im EU Observer klagte er in deutlich schärferer Tonart als zuvor über die Gefahr, dass die Diskussionen auf Ausschussebene dahin tendierten, die vorgesehene und seitens des Parlaments im Voss-Bericht angekündigte Stärkung des Datenschutzrahmens möglichst weit zurückzufahren und damit hinter das Schutzniveau der DS-RL zurückzufallen. Schließlich kündigte Albrecht an, dass der sich anbahnende Wortbruch der Europaparlamentarier letztlich bei den Bürgerinnen und Bürgern der EU dazu führen würde, das letzte Vertrauen in das Europäische Parlament und die Europäische Union als Ganzes zu verlieren (Nielsen 2013). Daraufhin antwortete Ludford in einem Blogposting in ebenso scharfer Tonart auf die von Albrecht erhobenen Vorwürfe und beschuldigte diesen der Inkompetenz sowie der Verbreitung von Unwahrheiten. Sie würde nicht für eine Absenkung des Schutzniveaus plädieren, sondern durch Präzisierungen Rechtssicherheit schaffen wollen (Ludford 2013a).[394]

394 Ludfords Position war zuvor auch seitens der liberalen Open Rights Group und PI dahingehend kritisiert worden, dass sie die Meinung der Bevölkerung nicht berücksichtigen würde (Bradwell 2013), was Ludford freilich unter Verweis auf den von ihr angestrebten Kompromiss zwischen Wirtschafts- und Bürgerrechtsinteressen von sich wies (Ludford 2013c).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

In der Folge verhärteten sich die Fronten zwischen den Konfliktparteien: Auf der einen Seite der linke Block des Europaparlaments, der stärkere Datenschutzregeln befürwortete, aber nicht über die notwendigen Mehrheiten in Ausschüssen und Plenum verfügte und auf der anderen Seite der konservative Block, der für eine sehr weitgehende Flexibilisierung der Datenschutzvorgaben plädierte, aber weder die Rolle des Berichterstatters im entscheidenden LIBE-Ausschuss inne hatte und ebenfalls nicht über die erforderliche Stimmenmehrheit verfügte. Unterstützt wurde die Parlamentskoalition der Datenschutzbefürworter von zivilgesellschaftlichen Datenschützern, der Art. 29 Datenschutzgruppe, der Konferenz der Europäischen Datenschutzbeauftragten (European Data Protection Authorities 2013), dem EDSB (Fleming 2013) sowie der EU-Grundrechteagentur FRA. Die Positionen des konservativen Blocks im Parlament wurden dagegen seitens des Ministerrats und der datenverarbeitenden Wirtschaft in der EU und aus den USA sowie der US-amerikanischen Administration befürwortet. Die ALDE-Parlamentarier wiederum tendierten inhaltlich in die Richtung des konservativen Blocks und drohten die Pläne von Albrecht hinsichtlich der weiteren Stärkung des von der Kommission vorgeschlagenen Datenschutzniveaus zu unterminieren. Somit war im Mai 2013 im Parlament eine *Pattsituation* eingetreten, die zunächst nur schwer überwindbar schien (Burn-Murdoch 2013).[395] Da sich die Verabschiedung der Parlamentsposition dermaßen verzögerte und kein Kompromiss in Sicht war, verzögerte sich auch die von der Ratspräsidentschaft angestrebte Verabschiedung der Ratsposition vor dem 1. Juli 2013 (O'Connor 2013).

Derweil hatte Anfang 2013 die irische Regierung die Ratspräsidentschaft übernommen und ihre Entschlossenheit zum Ausdruck gebracht, das Datenschutz-Dossier voranzubringen um bis zum Ende ihrer Präsidentschaft eine *Einigung über Schlüsselelemente des Datenschutzpakets zu erzielen, damit das Vertrauen der Bürgerinnen und Bürger in die digitale Wirtschaft gestärkt und so das Wachstum des digitalen Marktes gefördert wird* (Irische Ratspräsidentschaft 2013, 26). In den folgenden Monaten wurden im Rahmen der Ratsarbeitsgruppensitzungen verschiedene Möglichkeiten der Implementierung, des Ende 2012 auf Ministerebene beschlossenen risikoorientierten Ansatzes diskutiert. Auf der ersten Ministerratssitzung im März 2013 wurde beschlossen, dass die Ernennung betrieblicher Datenschutzbe-

395 Einen guten Einblick in die aufgeheizte Stimmung im Parlament liefert insbesondere die Dokumentation Democracy (Bernet 2015, ab Min. 1:02:00).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auftragter fakultativ sein und die freiwillige Benennung eines solchen zu Erleichterungen bei den sonstigen Verpflichtungen, denen Verantwortliche unterliegen, führen sollte. Zudem äußerte sich der Ministerrat erstmals positiv im Hinblick darauf, pseudonymen Daten gesondert zu behandeln (EU-Ministerrat 2013b, 11 f.). Die inhaltlichen Vorstöße der irischen Ratspräsidentschaft wurden sowohl seitens der Medienberichterstattung als auch seitens der Datenschutz-Community als Untergrabung des Datenschutzniveaus bewertet. Berichterstatter Albrecht drückte beispielsweise angesichts der Ministerratspläne im Hinblick auf den risikobasierten Ansatz seine Besorgnis aus, dass die Rechte der Betroffenen beschnitten und die Pflichten für Unternehmen und Behörden reduziert würden (Albrecht 2013c). Die Pläne der irischen Ratspräsidentschaft, das Sanktionsniveau zu reduzieren (Möchel 2013a), die von der Kommission vorgeschlagene explizite Einwilligung durch eine sog. unzweideutige Einwilligung zu ersetzen (Krempl 2013b) oder durch die Verwendung pseudonymer Daten Schutzverpflichtungen zu umgehen (Bergemann 2013b) wurden in der Medienberichterstattung als Verwässerung des Schutzniveaus bewertet. Unterstützung fanden die Vorschläge hingegen auf Seiten der Flexibilitätsbefürworter (Fontanella-Khan und McCarthy 2013; Härting und Lübben 2013). Zwar trat Reding weiterhin für ein hohes Schutzniveau ein (EU-Kommission 2013), veröffentlichte allerdings im März 2013 eine gemeinsame Pressemitteilung mit Innenminister Friedrich, in der sie sich offen gegenüber dem risikobasierten Ansatz zeigte (BMI 2013). Zudem äußerte sie sich nicht kritisch gegenüber den irischen Vorstößen, sondern zeigte sich dankbar für die *gewaltigen Anstrengungen* der Ratspräsidentschaft[396] im Hinblick auf die Erzielung einer Ratsposition (Reding 2013e). Tatsächlich gelang es der irischen Ratspräsidentschaft trotz einiger Fortschritte während ihrer Amtszeit letztlich weder eine allgemeine Ausrichtung des Ministerrats noch eine finale Einigung im Hinblick auf die Kapitel I-IV zu erzielen. Stattdessen wurde auf der letzten Ratssitzung vor Ende des irischen Mandats im Juni 2013 erneut das Interesse an flexiblen Datenschutzregelungen bekräftigt und alle erzielten Fortschritte im Hinblick auf die Kapitel I-IV unter den

396 Insbesondere hob Reding hervor, dass die irische Ratspräsidentschaft 25 Sitzungen auf Ratsarbeitsgruppenebene sowie 5 Sitzungen auf AStV-Ebene forciert hätte, um ein Vorankommen zu garantieren. Aufgrund dieser Anstrengungen sei es möglich gewesen, die Diskussion der ersten vier Kapitel des DSGVO-Entwurfs voranzubringen und damit die aus ihrer Perspektive wichtigsten Punkte Datenschutzgrundsätze (Kapitel II), Betroffenenrechte (Kapitel III) sowie Verarbeiterpflichten (Kapitel IV) zu adressieren (Reding 2013e).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Vorbehalt der Möglichkeit weiterer Änderungen im Laufe des Diskussionsprozesses gestellt. Daneben einigten sich die zuständigen Minister auch darauf, dass das Datenschutzniveau im Rahmen der DSGVO gleichwertig und möglicherweise höher als das der DS-RL sein sollte (EU-Ministerrat 2013a, 9 f.). Während das Parlament in der Zwischenzeit in einer Pattsituation feststeckte, gelangen dem Ministerrat in der Zwischenzeit somit nur kleinere Fortschritte.

4.3.2.5 Überwindung der Pattsituation: Der Einfluss der Snowden-Enthüllungen, die Aufarbeitung des Überwachungsskandals und die Verabschiedung der Parlamentsposition

Die Pattsituation, in der sich die Verhandlungen befanden, drohte zeitweilig sogar die Verhandlungen als Ganzes scheitern zu lassen. Erst ein externer Schock in Form der Snowden-Enthüllungen konnte dem Überzeugungssystem der Datenschutzbefürworter so viel Auftrieb verschaffen, dass unter dem Policy Entrepreneurship von Berichterstatter Albrecht und von Justiz-Kommissarin Reding die Kompromissvorschläge Albrechts, die allerdings nur ein geringfügig schwächeres Datenschutzniveau als der Berichtsentwurf vorwiesen, durchsetzen konnten.

Mitten auf dem Höhepunkt des Streits um die DSGVO, führte eine Reihe von Artikeln, deren Anfang die am 6. Juni 2013 von Barton Gellman und Laura Poitras in der Washington Post sowie von Glenn Greenwald im Guardian veröffentlichten Beiträge bildeten, der Welt die bis dahin kaum möglich erscheinenden Ausmaße einer weltweiten Überwachungsmaschinerie vor Augen. Als Spitze des Eisbergs entpuppten sich dabei die Überwachungsprogramme PRISM und TEMPORA: Während PRISM Aufschluss über die enge Kooperation der National Security Agency (NSA) mit amerikanischen IT Unternehmen wie Apple und Google gab und somit verdeutlichte, dass die Grenzen zwischen privatwirtschaftlicher Datenerhebung und staatlicher Nachrichtendienstüberwachung verschwimmen (The Washington Post 2013), verwies Tempora – ein Überwachungsprogramm in Kooperation mit dem britischen Nachrichtendienst *Government Communications Headquarter* (GCHQ) – auf die technische Machbarkeit eines kompletten Abschöpfens der Verkehrs- und Inhaltsdaten durch das Anzapfen von Internetknotenpunkten und transatlantischen Glasfaserkabeln (MacAskill u. a. 2013). Auf diese ersten Enthüllungen folgen zahlreiche weitere Berichte über die Überwachungspraktiken des, NSA, des GCHQ, im

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Rahmen der Five Eyes (Cox 2012) als auch des deutschen Bundesnachrichtendienstes (Kazim 2014), die immer wieder die Schlagzeilen der größten Medien füllten und der Thematik des Datenschutzes somit einen enormen öffentlichen Auftrieb brachten (Weitkamp, Kimpeler, und Friedewald 2014, 83 ff.).[397]

Für die Koalition der Datenschutzbefürworter waren diese Enthüllungen eine einmalige Gelegenheit, ihr Überzeugungssystem, das die Stärkung des EU-Datenschutzrechts vorsieht, mit Nachdruck zu vertreten. Während aus den Hauptstädten der Mitgliedstaaten zunächst keine Reaktionen auf die Enthüllungen folgten (im Falle Frankreichs und insb. des Vereinigten Königreichs sollte dies auch so bleiben), ergriffen die EU-Kommission als auch das EU-Parlament die Initiative. Kommissarin Reding wandte sich am 10. Juni mit einem Brief an den Generalbundesanwalt der Vereinigten Staaten, Eric Holder, und bat diesen um Aufklärung über die in den Medien bekannt gewordenen Vorwürfe (EU Commission 2013b, 2013c). Dabei stellte Reding die Enthüllungen von Anfang an in einen direkten Zusammenhang mit einem hohen Datenschutzniveau und der zügigen Verabschiedung der Datenschutz-Grundverordnung als europäische Antwort auf den Überwachungsskandal (Euractiv 2013; Gallagher 2013; Watt 2013). Zeitweise hatte sie die Datenschutzreform sogar als „Europas Unabhängigkeitserklärung" bezeichnet (Eder 2013).

Das Parlament befasste sich auf seiner Plenarsitzung vom 11. Juni 2013 mit den ersten bekanntgewordenen Details der Massenüberwachung. Die Abgeordneten der GUE/NGL, Grünen/EFA, S&D sowie von ALDE sprachen sich, wie schon zuvor (vgl. die Abschnitt 3.3.4), mit deutlichen Worten gegen die Massenüberwachung der Bevölkerung aus.[398] Überraschend waren dabei die Wortbeiträge konservativer Politiker (z. B. von Manfred Weber (EVP/CSU)), die ebenfalls für hohe und moderne Datenschutzstandards in der EU und die schnelle Verabschiedung der DSGVO warben (EU-Parlament 2013d).

Während im Frühsommer 2013 fast täglich neue Details der Massenüberwachung bekannt wurden, formierte sich immer stärkerer Widerstand im Europäischen Parlament (EU Parliament 2013b), bis die Abgeordneten auf

397 Siehe für eine ausführliche Chronologie der Enthüllungen beispielsweise: (Greis, Ernst, und Thoma 2013).

398 Auch der für die JI-Richtlinie zuständige LIBE-Berichterstatter Droutsas forderte die Wahrung der Datenschutzstandards bzw. deren Stärkung (EU-Parlament 2013a).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Plenarsitzung vom 4. Juli 2013 mit großer Mehrheit[399] eine Entschließung verabschiedeten, in der sie die Überwachungspraktiken der NSA verurteilten, Kommission, Rat und Mitgliedstaaten dazu aufforderten, das SWIFT- und das PNR-Abkommen auszusetzen, den LIBE-Ausschuss mit der Einsetzung eines Untersuchungsausschusses beauftragten[400] sowie den Rat zur Beschleunigung der Arbeiten am Datenschutzpaket aufforderten (EU-Parlament 2013b). Zudem setzte sich sowohl auf dieser Sitzung als auch bei Folgesitzungen[401] fraktionsübergreifend die Tendenz unter Parlamentariern durch, dass die zügige Verabschiedung der Datenschutz-Reform eine angemessene Reaktion auf die Enthüllungen darstellen würde (EU-Parlament 2013e, vgl. insb. die Aussagen des konservativen Axel Voss und der liberalen Ludford).

Am 21. Oktober 2013 wurde der Albrecht-Bericht zunächst im LIBE-Ausschuss mit 48 Stimmen (bei 1 Gegenstimme und 3 Enthaltungen) angenommen (Albrecht 2013a, 720). Die Abstimmung im Parlamentsplenum erfolgte einige Monate später am 12. März 2014 gemeinsam mit den Berichten zur JI-Richtlinie[402] und den Ergebnissen des LIBE-NSA-Untersu-

399 Bei 483 Stimmen dafür, 98 Gegenstimmen und 65 Enthaltungen. Für die Entschließung stimmten ALDE, EVP, S&D und Grüne/EFA beinahe geschlossen. Zudem noch die halbe GUE/NGL-Fraktion, mehr als die Hälfte der Fraktionslosen sowie einige Abgeordnete der EFD. Fast die gesamte EKR-Fraktion stimmte gegen die Entschließung und erhielt dabei Unterstützung von einigen Abgeordneten der EFD, EVP, Grünen/EFA, GUE/NGL sowie einigen fraktionslosen Abgeordneten. Die Enthaltungen setzten sich vor allem aus Stimmen der EVP zusammen. Auch einige Abgeordnete der S&D sowie der GUE/NGL enthielten sich, sowie auch einzelne Abgeordnete aller übrigen Fraktionen (EU-Parlament 2013g, 25 f.).

400 In der Folge setzte sich der LIBE-Untersuchungsausschuss zwischen September und Dezember 2013 auf insgesamt 15 Sitzungen mit dem Thema der elektronischen Massenüberwachung der EU-Bürger auseinander und legte seinen Abschlussbericht schließlich Anfang 2014 vor (Moraes 2014). Für eine ausführliche Auflistung aller Sitzungen und für einen Überblick über die Sitzungsinhalte, siehe: (EU Parliament 2014).

401 Weitere Plenardebatten, in denen Bezüge zur Datenschutzreform hergestellt wurden, fanden am 10. September zum Thema der EU-Cyber-Security-Strategie (EU-Parlament 2013c) sowie am 9. Oktober zum Thema der Aussetzung des SWIFT-Abkommens infolge der Überwachung durch die NSA (EU-Parlament 2013f) statt.

402 Der Droutsas-Bericht zur JI-Richtlinie wurde mit nur 371 Stimmen angenommen und erreichte somit nur knapp die benötigte Mehrheit von 369 Stimmen. 276 Abgeordnete stimmten gegen den Bericht und 30 enthielten sich. Die Für-Stimmen setzten sich aus den Stimmen von ALDE, GUE/NGL, S&D sowie Grünen/EFA zusammen. Die Gegenstimmen kamen dagegen von den Fraktionen EKR, EFD und EVP (EU-Parlament 2014b, 22 f.), die auch schon zuvor ein vergleichsweise geringes

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

chungsausschusses.[403] Der Albrecht-Bericht wurde dabei mit 621 Stimmen (bei 10 Gegenstimmen und 22 Enthaltungen) und somit fast einstimmig[404] angenommen (EU-Parlament 2014b, 14 f.).[405]

Überraschend an der Befürwortung des finalen Albrecht-Berichts waren zwei Punkte: *Erstens* hatten die Parlamentarier für einen Bericht gestimmt, der weiterhin für ein sehr hohes Datenschutzniveau eintrat. Zwar stellte der Bericht insofern einen Kompromiss dar, dass die extremsten Positionen, die noch im Berichtsentwurf enthalten waren, herausgenommen wurden (vgl. die Analyse des Überzeugungssystems der Datenschutzbefürworter in 4.3.1.2.2). Andererseits sah der Bericht trotz einiger Kompromisse immer noch eine deutliche Steigerung des von der Kommission vorgeschlagenen Datenschutzniveaus dar, ohne dass die zahlreichen Bedenken der Flexibilitätsbefürworter berücksichtigt worden waren. *Zweitens* war überraschend, dass dieser Bericht, der eine dermaßen deutliche Stärkung des Datenschutzniveaus vorsah, beinahe einstimmig auch von jenen Parlamentariern angenommen wurde, die zuvor deutlich offener gegenüber den Kritikpunkten der Flexibilitätsbefürworter eingestellt waren.

Interesse an einer EU-weiten Datenschutz-Lösung für den JI-Bereich gezeigt hatten (vgl. 3.3.4).

403 Der unter der Federführung von Claude Moraes erstellte Bericht über die Ergebnisse NSA-Untersuchungsausschusses wurde mit 544 Stimmen (bei 78 Gegenstimmen und 60 Enthaltungen) angenommen. ALDE, GUE/NGL, EVP, S&D sowie die Grünen/EFA stimmten fast geschlossen für den Bericht. Lediglich die EKR und die EFD stimmten dagegen, während die meisten Enthaltungen aus den Reihen der EVP kamen (EU-Parlament 2014b, 92 f.).

404 Die Gegenstimmen setzten sich fast vollständig aus den Stimmen der EFD zusammen. Neben einzelnen Abgeordneten verschiedener Parteien enthielten sich 7 fraktionslose Abgeordnete sowie bemerkenswerter 10 – überwiegend aus dem skandinavischen Raum stammende – Abgeordnete der S&D-Fraktion (EU-Parlament 2014b, 14 f.).

405 Am 12. März 2014 stimmte das Parlament zudem für einen Entschließungsantrag, in dem die Parlamentarier die Kommission zur Aussetzung des Safe Harbor-Abkommens aufforderten (EU-Parlament 2014a). Zuvor hatte auch die EU-Kommission im Herbst 2013 signalisiert, dass sie Verhandlungen über ein neues Safe Harbor-Abkommen mit den USA aufgenommen hatte. Diese erwiesen sich jedoch als sehr zäh (BfDI 2015) und konnten erst nach dem Safe Harbor-Urteil des EuGH erfolgreich abgeschlossen werden. Auf die Klage von Max Schrems hin hatte der EuGH das Abkommen im Oktober 2015 annuliert (EuGH 2015). Ein Folgeabkommen mit dem Namen EU-US Privacy Shield, das einen besseren Datenschutz garantieren soll, jedoch ebenfalls in der Kritik steht, wurde daraufhin im Juli 2016 von der EU-Kommission beschlossen (Krempl 2017).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Die Enthüllungen Snowdens fungierten somit als externer Schock und erhöhten die Bereitschaft der Gegner eines hohen Schutzniveaus im Europäischen Parlament in signifikantem Maße, einem solch hohen Schutzniveau im Rahmen der DSGVO dennoch zuzustimmen, indem dieses als die angemessene Antwort auf die Massenüberwachung gerahmt wurde. Dabei vermochten es Jan Philipp Albrecht und Viviane Reding, in diesem spezifischen Gelegenheitsfenster als Policy-Entrepreneure aufzutreten und den externen Schock zu ihren politischen Gunsten zu nutzen.[406]

Der Snowden-Shock bewirkte horizontal, also über alle Elemente des Verordnungsvorschlags hinweg, eine Stärkung der Vorgaben gegenüber dem Kommissionsentwurf. So war den Parlamentariern zwar bewusst, dass sie formell über keinerlei Entscheidungskompetenz im Hinblick auf die Regulierung nachrichtendienstlicher Tätigkeiten verfügten. Auf der anderen Seite war jedoch zugleich klar, dass der Regulierung der Verarbeitung personenbezogener Daten eine Schlüsselrolle zukommt, da – wie insb. PRISM gezeigt hat – ein wichtiger Anteil der nachrichtendienstlichen Informationen aus den Datenbeständen privater Anbieter bezogen wurde, die auf Grundlage der geltenden europäischen Datenschutzgesetze erhoben worden waren. Neben der horizontalen Stärkung aller Datenschutzvorgaben waren die Parlamentarier zudem in besonderem Maße an der Wiederaufnahme der sogenannten Anti-FISA-Klausel interessiert. Nachdem die zivilgesellschaftlichen Datenschützer bereits auf dieses Schlupfloch aufmerksam gemacht hatten und auch die Europaparlamentarier dies in Erwägung gezogen hatten, wurde die Anti-FISA-Klausel im Nachgang der Snowden-Enthüllungen in der Position des Parlaments in Form von Art. 43a wieder aufgenommen (Albrecht 2013a).

Wie zu erwarten war, reagierten die Flexibilitätsbefürworter ablehnend gegenüber der Position des Parlaments und riefen den Ministerrat dazu auf, Nachbesserungen (insb. mehr Flexibilität für Verarbeiter in Form der Definition personenbezogener Daten, mehr Anreize zur Pseudonymisierung und die Rücknahme der zentralen Stellung der Einwilligung) vorzunehmen (Härting 2013; ICDP 2013b, 2013). Demgegenüber kann die Reaktion der Datenschutzbefürworter-Koalition am besten als Erleichterung beschrieben werden. Das Datenschutzniveau des LIBE-Vorschlags wurde dabei be-

406 Den signifikanten Effekt der Snowden-Enthüllungen bestätigten alle zentralen Akteure: Sowohl Albrecht selbst (EU Parliament 2013a, 4:12-4:20; Kayali 2015), als auch Voss (CPDP 2015 vgl. die Ausführungen Voss', insb. ab 43:39) und Reding (2013b). Auch Medienberichte (Bergemann 2014; Biermann 2013a) und weitere Beobachter (Rossi 2018) machten dieselbe Feststellung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

grüßt und der Ministerrat dazu aufgerufen, seine Position schnellstmöglich zu verabschieden, damit die Reform noch vor den Europawahlen 2014 erfolgreich beendet werden könnte (Article 29 WP 2013; EDSB 2013).

4.3.2.6 Der lange Weg bis zur Überwindung des Stillstands im Ministerrat

Einen deutlich geringeren unmittelbaren Einfluss hatten die Snowden-Enthüllungen auf die Verabschiedung der Ministerratsposition. Während sich das Europäische Parlament in Anknüpfung an seine Tradition der Grundrechteorientierung, trotz fehlender formaler Kompetenzen, geschlossen gegen die bekannt gewordene Massenüberwachung positionierte, verhielten sich die Mitgliedstaaten deutlich ambivalenter. So reagierten die Regierungen der drei größten Mitgliedstaaten, Deutschlands, Frankreichs und des Vereinigten Königreichs zögerlicher auf den Überwachungsskandal. Wie sich im Laufe weiterer Enthüllungen zunehmend herausstellte, kooperierten europäische Regierungen zum einen mit der US-amerikanischen Regierung und duldeten deren Überwachungsmaßnahmen, um an wichtige nachrichtendienstliche Informationen zu gelangen. Zum anderen praktizierten die EU-Mitgliedstaaten, insbesondere Großbritannien, aber auch Frankreich (Thoma 2013) und Deutschland (Kazim 2014; Leisegang 2013b, 20) selbst ähnlich fragwürdige Überwachungspraktiken, solange es eben den eigenen strategischen Interessen entsprach. Entsprechend vorsichtig waren die europäischen Regierungschefs in Bezug auf Aussagen mit erhobenem Zeigefinger. Hinzu kam, dass der Überwachungsskandal zwar von den französischen und britischen Medien durchaus thematisiert wurde. Zu einer größeren öffentlichen Debatte, wie in Deutschland, kam es in diesen Ländern zu keinem Zeitpunkt (Weitkamp, Kimpeler, und Friedewald 2014, 83 ff.; Tréguer 2017, 4 f.). Bundeskanzlerin Merkel kündigte dagegen während des ARD-Sommerinterviews Mitte Juli als Reaktion auf die jüngsten Enthüllungen – darunter insbesondere das Bekanntwerden der Überwachung diplomatischer Vertretungen der EU sowie einzelner europäischer Länder (Süddeutsche Zeitung 2013) – an, dass die Bundesrepublik bei den Verhandlungen zur DSGVO eine *sehr strikte Position*[407] einnehmen

407 Unter anderem aufgrund dieser Wortwahl waren Merkels Äußerungen in der darauffolgenden Berichterstattung dahingehend gedeutet worden, dass Deutschland fortan generell für eine DSGVO mit einem hohen Schutzniveau eintreten würde (Bergemann 2013d; Schmitz 2013). Tatsächlich hatte Merkel in den darauffolgenden Sätzen klargestellt, dass sie mit der Ankündigung, eine *sehr strikte Position*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

werde (Das Erste 2013, ab Minute: 3:50). Während EU-Justizkommissarin Reding die Regierungschefs der anderen EU-Mitgliedstaaten dazu aufforderte dem Beispiel Angela Merkels in Bezug auf die Befürwortung der DSGVO zu folgen (Travis 2013), blieben konkrete Reaktionen zunächst aus. Erst die europäischen Justiz- und Innenminister sprachen sich auf ihrem informellen Ratstreffen Mitte Juli für ein hohes Datenschutzniveau und den schnellen Abschluss der Verhandlungen aus, trafen aber weder konkrete inhaltliche Vereinbarungen, noch wurde ein verbindlicher Zeitplan festgelegt (EU Commission 2013a). Trotz dieser Ankündigungen und trotz des anhaltenden Drängens der Justizkommissarin, bis Ende des Jahres eine Einigung im Ministerrat zu erzielen (EU Commission 2013d), erreichten die Minister auf dem ersten formellen Treffen des JI-Rates Anfang Oktober lediglich eine erste Annäherung zum Prinzip der zentralen Anlaufstelle (one-stop-shop) (Council of the EU 2013a, 7).

Eine weitere Gelegenheit zur Intervention in den Reformprozess bot sich im Zusammenhang des Gipfels der Europäischen Staats- und Regierungschefs am 24. und 25. Oktober 2013. Aufgrund der gestiegenen öffentlichen Relevanz der Materie als Folge der Snowden-Enthüllungen war erwartet worden, dass sich der Europäische Rat zur Datenschutzreform äußern und die weiteren Verhandlungen in entscheidendem Maße beeinflussen würde. Besonders nachdem einige Tage vor dem Gipfeltreffen bekannt geworden war, dass die NSA das Telefon von Angela Merkel abgehört hatte, war eine starke und einheitliche europäische Antwort auf die Enthüllungen erwartet worden. In diesem Kontext bezeichnete Justizkommissarin Reding die Datenschutz-Grundverordnung als „Europas Unabhängigkeitserklärung" und forderte die im Europäischen Rat versammelten Staats- und Regierungschefs zur schnellen Verabschiedung strenger Datenschutzregeln noch vor den Europawahlen im Jahr 2014 auf. Allerdings wurde die von Frankreich, Italien und Polen ausgehende Initiative zur Verabschiedung der Datenschutzreform im Laufe des Jahres 2014 ausgerechnet von Deutschland torpediert. So wandte sich Merkel gegen die Formulierung der *Verabschiedung im nächsten Jahr* und schlug sich auf die Seite des Vereinigten Königreichs und der anderen DSGVO-Gegner, die lediglich für eine *rasche*

einnehmen zu wollen, lediglich die Haltung Deutschlands gegenüber der Wiedereinführung einer Anti-FISA-Klausel bezeichnet hatte, und nicht das allgemeine Schutzniveau des Verordnungsvorschlags (Das Erste 2013, ab Minute: 3:50).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Verabschiedung eintraten (Schmitz 2013).[408] Dementsprechend hieß es in der offiziellen Abschlusserklärung des Europäischen Rats lediglich:

> *„Das Vertrauen der Bürger und Unternehmen in die digitale Wirtschaft muss gefördert werden. Die rasche Verabschiedung eines soliden allgemeinen Rahmens für den Datenschutz in der EU und der Cybersicherheitsrichtlinie ist für die Vollendung des digitalen Binnenmarkts bis 2015 von entscheidender Bedeutung." (Europäischer Rat 2013, 4).*

Dieses Vorgehen Deutschlands,[409] des Vereinigten Königreichs und ihrer Verbündeten muss als Verschleppungstaktik bewertet werden: Würde nur ausreichend viel Zeit vergehen, in der keine weiteren Enthüllungen folgen, würden der öffentliche Ärger und die öffentliche Aufregung um den Überwachungsskandal verfliegen und sich ein neues Gelegenheitsfenster öffnen, sodass wieder über eine Absenkung des Schutzniveaus diskutiert werden könnte, ohne einen größeren öffentlichen Aufschrei zu befürchten, wie dies während der Hochphase der Snowden-Enthüllungen der Fall war (Schmitz 2013). Die Taktik sollte im Hinblick auf die Ministerratsposition auch Erfolg haben. Interessant war die Stellungnahme des Europäischen Rates aber auch, weil das Vertrauensargument, das zwar von Kommissarin Reding und vom EP vertreten worden war, aber vom Ministerrat vernachlässigt wurde, ausgerechnet von der höchsten politischen Instanz der EU aufgegriffen wurde.

Nachdem der Juristische Dienst des Ministerrats Ende 2013 das von der Kommission vorgeschlagenen Prinzip der zentralen Anlaufstelle in Bezug auf die Verfassungskonformität, insb. im Hinblick auf die Wahrnehmung

408 Jahre später äußerte Ben Rhodes, der damalige Vizesicherheitsberater von Obama, dass Merkel tatsächlich eher über die Meldungen verärgert gewesen sei, und nicht über die in den Meldungen beschriebenen Abhörpraktiken. So habe die deutsche Regierung von den Abhörmaßnahmen ohnehin gewusst oder sie hätte es wissen müssen. Insofern habe Merkel in der ganzen Sache ein PR-Problem gesehen und sich lediglich aus Image-Gründen heraus dazu verleiten lassen, die Abhörmaßnahmen öffentlich zu verurteilen (Zeit Online 2019).

409 Als weiteres, denkbares Motiv (neben dem Argument, dass Merkel ohnehin nichts an den Überwachungspraktiken auszusetzen hatte) der Bundeskanzlerin kommt infrage, dass sie im Hinblick auf den Abschluss eines No-Spy-Abkommens mit der US-Regierung auf die Unterstützung des Vereinigten Königreichs angewiesen war und deshalb vor den britischen Forderungen einknickte (Hecking 2013). Auch dieses Motiv ändert aber nichts an der grundsätzlichen Intention der Verordnungsgegner, eine Verabschiedung zur Hochphase der Snowden-Enthüllungen um jeden Preis vermeiden zu wollen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

individueller Rechtsbehelfe, grundsätzlich infrage gestellt hatte (Jur. Dienst d. Rats 2013), befasste sich der Ministerrat in der Folgezeit weiterhin mit derselben Materie (Krempl 2013c).[410] Reding beklagte – u. a. auch unter Verweis auf das Gutachten des Juristischen Dienstes der Kommission – bereits im Vorfeld der Ministerratstagung, dass das Wiederaufrollen der Diskussion des Prinzips der zentralen Anlaufstelle eine politische Entscheidung unter dem Deckmantel einer juristischen Prüfung sei (Reding 2013a). Nichtsdestotrotz konnten sich die Minister auch auf der Dezember-Sitzung des JI-Rates nicht abschließend zu diesem Thema einigen, sodass die Möglichkeit der Erzielung einer allgemeinen Ausrichtung des Ministerrats bis zu den Europawahlen 2014 zunehmend unwahrscheinlicher wurde (Council of the EU 2013b, 2, 12). In deutlich harscheren Worten als bis dahin kritisierte daraufhin Kommissarin Reding den Ministerrat und beklagte die *verpasste Gelegenheit* (Reding 2013c). Auch Berichterstatter Albrecht kritisierte den Ministerrat und hielt zu diesem Zeitpunkt die Verabschiedung vor den Europawahlen für zunehmend unwahrscheinlicher (Feld 2013).

Reding, Albrecht und weitere Datenschutzbefürworter vertraten dabei die Position, dass die Debatten im Ministerrat an einem Punkt angelangt seien, an dem die Mitgliedstaaten sich bereits zu allen relevanten Elementen geäußert hatten und auf dieser Grundlage, sofern der politische Wille vorhanden gewesen wäre, eine erste allgemeine Ausrichtung des Rates hätten verabschieden können. Dass noch nicht für jedes im Ministerrat identifizierte Problem im Hinblick auf den Verordnungsvorschlag eine *perfekte* Lösung gefunden worden war, stellte für sie kein Hindernis dar, sondern die Möglichkeit, diese noch offenen Punkte während des Trilogs gemeinsam mit Parlament und Kommission zu lösen. Zudem wurde die Meinung vertreten, dass eine perfekte Lösung aller juristischen Herausforderungen bei einem Moving Target wie dem Thema Datenschutz ohnehin nicht möglich sei. Entsprechend unterstellten sie dem Ministerrat fehlenden Willen, in die finalen Verhandlungen mit Parlament und Kommission zu treten (für die Kommissionsposition, siehe: CPDP 2014, Min. 8:00 ff., für die

410 Der Kommissionsvorschlag, der in Bezug auf die Errichtung des Prinzips einer zentralen Anlaufstelle die drastische Aufwertung der Kompetenzen der Kommission vorgesehen hatte, war auf den Widerstand der Mitgliedstaat (insb. von Deutschland, Frankreich, dem Vereinigten Königreich und Irland) gestoßen. Da die diesbezüglichen Diskussionen allerdings eher auf einem technischen Level verblieben und bereits in bestehenden Analysen ausführlich thematisiert wurden, möchte ich nicht weiter ins Detail gehen und nur auf den detaillierten Debattenüberblick in Jančiūtė (2018, 145–50) verweisen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Parlamentsposition, vgl.: 2015, Min. 21:00 ff.). Der Ministerrat dagegen äußerte sich öffentlich dahingehend, einen Kompromiss aushandeln zu wollen, der möglichst viele Detailfragen auf möglichst präzise und Rechtssicherheit schaffende Weise klären würde. Eine schnelle Verabschiedung der Reform oder der Ministerratsposition sei problematisch im Hinblick auf dieses Ziel. Eine Verabschiedung des laufenden Diskussionsstands kam zudem nicht infrage, da die Ministerratsdelegationen bzw. Minister keinesfalls ohne einen ausreichend gut ausdiskutierten Ministerratskompromiss in die Trilog-Verhandlungen gehen wollten, da Uneinigkeit im Rat die Verhandlungsposition des Ministerrats geschwächt hätte (Hecking 2013). Unterstützung fand der Ministerrat dabei sowohl auf Seiten der Wirtschaft[411] als auch einiger Wissenschaftler.[412]

Auf der informellen Ministerratssitzung in Athen Ende Januar 2014 diskutierten die anwesenden Minister,[413] trotz der Bemühungen der griechischen Ratspräsidentschaft (Ermert 2014), schließlich nur über die Wiedereinführung der Anti-FISA-Klausel (Ziedler 2014). Reding, die noch bis zu diesem Treffen Druck gemacht hatte, die Reform vor den Europawahlen abzuschließen, räumte erstmals auf der informellen Ministerratstagung ein, dass die Reform bis zu den Wahlen nicht mehr abgeschlossen werden könne (EU Commission 2014). Dennoch blieb Reding bei ihrer Strategie, weiterhin Druck auf den Ministerrat auszuüben, um mit der Reform voranzukommen.[414] So hatte sich die Justizkommissarin – ohne die übrigen Mit-

411 Googles Datenschutz-Sprecher Fleischer interpretierte die Nicht-Verabschiedung der DSGVO im Vorfeld der Europaparlamentswahlen dahingehend, dass der DSGVO-Entwurf tot sei und dass sich *aus dessen Asche hoffentlich ein besseres, modernes und ausgeglicheneres* Datenschutzgesetz erheben würde (Fleischer 2014).

412 So sah etwa Nikolaus Forgó in einem im Editorial der *Zeitschrift Datenschutz* erschienen Beitrag die Verschiebungen als willkomenen Anlass, „endlich die Grundfragen erneut zu diskutieren: wozu Datenschutzrecht eigentlich dient, was es schützt, ob dieser Schutz gelingt." (Forgó 2014)

413 Der neue deutsche Innenminister Thomas de Maizière, dessen positive Äußerungen zur DSGVO bereits zuvor als Lippenbekenntnisse eingeordnet worden waren (Bergemann 2013a), nahm erst nach Ende der Datenschutzdebatte an der Ministerratssitzung teil, „[w]ie zum Beweis, dass auch Deutschland kein gesteigertes Interesse an der Reform hat." (Ziedler 2014) Weitere Berichte bestätigten die Vermutung, dass Deutschland sich auch weiterhin auf die Seite der Blockierer schlug (Diedrich 2013).

414 Unterstützung erhielten Reding und Albrecht auch weiterhin von der Koalition der Datenschutzbefürworter. Ein Bündnis mehrerer zivilgesellschaftlicher Datenschutz-Organisationen verschickte einen Brief an die griechische Ratspräsidentschaft, worin es für die zügige Fertigstellung der Reform eintrat und die Ratspräsidentschaft um Unterstützung bat (Civil Rights Organisations 2014).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

gliedstaaten einzubeziehen – am Vortag des Treffens mit der amtierenden griechischen und der darauffolgenden italienischen Ratspräsidentschaft und den Parlamentsberichterstattern getroffen und einen informellen Aktionsplan erarbeitet, bis zum Sommer 2014 eine Einigung im Ministerrat zu erzielen, sodass die Trilog-Verhandlungen mit dem neuen Europäischen Parlament im Spätsommer beginnen könnten. Der informelle Aktionsplan stieß jedoch auf den vehementen Widerstand der Mehrheit der übrigen, nicht eingebundenen Mitgliedstaaten, die sich weiterhin weigerten, feste Zusagen im Hinblick auf den weiteren Aushandlungsprozess der DSGVO zu treffen (Ermert 2014).

Somit war ein neuer Stillstand der Verhandlungen erreicht. Ende Januar 2014 befürchtete beispielsweise Wojciech Wiewiórowski, Beauftragter der polnischen Datenschutzbehörde (und ab 2014 stv. EDSB), dass der Stillstand im Ministerrat das neue Europäische Parlament im schlimmsten Falle dazu drängen könnte, die im LIBE-Ausschuss verabschiedete Position des Parlaments neu aufzuschnüren und zu einer Grundsatzdebatte zurückzukehren, in deren Ergebnis der Abschluss der Verhandlungen bis zu den nächsten Europawahlen 2019 verzögert werden könnte (CPDP 2014 ab Min. 29:52).[415]

Auf der Ministerratssitzung vom März 2014 wurde immerhin eine erste Annäherung hinsichtlich des räumlichen Anwendungsbereichs sowie der Regeln zu grenzüberschreitenden Datentransfers erzielt, wobei die Mitgliedstaaten die Linie des Kommissionsvorschlags grundsätzliche begrüßten, jedoch für mehr Freiräume für die Mitgliedstaaten eintraten, von den Verordnungsvorgaben abzuweichen (Council of Ministers 2014, 15). Auf der Sitzung wurde auch über Pseudonymisierung, das Recht auf Datenportabilität, das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern und über Profiling gesprochen, jedoch keine Einigung erzielt (Council of Ministers 2014, 15; Reding 2014a).

Eine Einigung[416] zum räumlichen Anwendungsbereich der DSGVO (Art. 3 (2) DSGVO-E), zu den Definitionen von unternehmensinternen

415 Die Verabschiedung der LIBE-Position im Plenum des Europäischen Parlaments vor den Parlamentswahlen ist daher als Reaktion auf die u. a. von Wiewiórowski angesprochene – zwar unwahrscheinlich, aber doch vorhandene – Gefahr zu deuten, dass ein neues Parlament die Parlamentsposition neu aufrollen und abschwächen könnte.

416 Einigung meint in diesem und in den folgenden Fällen eine sog. „partielle allgemeine Ausrichtung". Eine derartige Einigung kann jedwede Elemente eines Legislativvorschlags betreffen. Partielle allgemeine Ausrichtungen wurden stets unter der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datenschutzvorschriften (Art. 4, 17) und internationalen Organisationen (Art. 4, 21) sowie zu Kapitel V (Datenübermittlungen in Drittstaaten) erzielten die Minister schließlich auf dem JI-Ratstreffen im Juni 2014. Entsprechend euphorisch begrüßte die scheidende Justizkommissarin Reding die Ergebnisse des Ratstreffens und plädierte erneut dafür, die den Abschluss der Datenschutzreform und damit die Vollendung des digitalen Binnenmarktes noch vor 2015 zu erreichen (Reding 2014b, 2). Auch die Datenschutzgruppe begrüßte die Einigung als wichtige Etappe auf dem Weg zu einem neuen Datenschutzrahmen (Artikel 29-Datenschutzgruppe 2014). Ende Juni 2014 folgte eine weitere Äußerung des Europäischen Rates: Die Staats- und Regierungschefs legten erstmals einen Termin für die Verabschiedung des Datenschutzrahmens (also der DSGVO und der JI-Richtlinie) vor. Im Kontext der weiteren Entwicklung des „Raums der Freiheit, der Sicherheit und des Rechts", befand der Europäische Rat, dass es entscheidend sei, bis 2015 einen soliden allgemeinen Rahmen für den Datenschutz in der EU zu verabschieden (Europäischer Rat 2014, 2 Nr. 4). Auf der Ministerratssitzung vom Oktober 2014 folgte zudem eine weitere, sehr wichtige Einigung der Minister im Hinblick auf Kapitel IV (Pflichten der für die Verantwortlichen und Auftragsverarbeiter). Dem risikobasierten Ansantz entsprechend wurde darin die weitgehende Reduzierung der administrativen Pflichten vorgesehen (EU-Ministerrat 2014b, 7).

Auf der Folgesitzung im Dezember 2014 einigte sich der Ministerrat auf die – lange umstrittenen – Regelungen zum öffentlichen Sektor (betreffend die Art. 1, Art. 6 Absätze 2 und 3, Art. 21 und Kapitel IX).[417] Die stark umstrittene Frage, wie mit dem Prinzip der zentralen Kontaktstelle umgegangen werden sollte, konnte allerdings auch auf dieser Sitzung nicht geklärt werden (EU-Ministerrat 2014c, 8). Auf der Ministerratssitzung vom 13. März 2015 wurde schließlich auch eine Einigung im Hinblick auf die Kapitel VI und VII (und damit auch in Bezug auf das Prinzip der zentralen Kontaktstelle) sowie Kapitel II (Grundsätze) erreicht (EU-Ministerrat 2015a, 7).

Voraussetzung festgelegt, „dass nichts vereinbart ist, solange nicht alles vereinbar ist" (EU-Ministerrat 2014a, 10), sodass die Möglichkeit späterer Änderungen zum Zwecke der Gesamtkohärenz des Textes vorbehalten bleibt.

417 Die vor allem von Deutschland befürwortete weitgehende Ausklammerung des öffentlichen Sektors aus der DSGVO konnte sich letzten Endes nicht durchsetzen. Es konnten jedoch zahlreiche im Hinblick auf die Sonderbehandlung des öffentlichen Sektors relevante Öffnungsklauseln ausgehandelt werden (Jančiūtė 2018, 142 ff.).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

In der Zeit, in der die Verhandlungen im Ministerrat erstmals Schwung aufgenommen hatten, entwickelte sich eine neue Debatte in den westlichen Industriestaaten, die den Verhandlungsprozess beeinflusste und weitere Verzögerungen zur Folge hatte. War das Jahr 2013 stark von den Snowden-Enthüllungen und der Suche nach einem Umgang mit der Massenüberwachung geprägt, wurde seit dem Jahr 2014 deutlich stärker das Thema Digitalisierung debattiert. Hervorstechendste Elemente dieser Debatte waren die Schlagworte *Internet der Dinge* und *Big Data* (und: Schirrmacher 2015; vgl. z. B.: Sprenger und Engemann 2015).[418] Der datenschutzrechtlich relevante Knackpunkt an der Debatte betraf die Frage, ob und inwiefern zu strenge Datenschutz- bzw. Zweckbindungsvorgaben gesellschaftlich nützliche Aspekte der Digitalisierung erschweren oder verhindern würden. Die Prämisse dabei war, dass die meisten Geräte in den kommenden Jahren miteinander vernetzt würden. In Folge der Vernetzung würden ungekannte Datenmengen entstehen, die vielfältige gesellschaftlich wünschenswerte Potentiale bieten würden. Zur Analyse der Daten wiederum würde es neuer Analyseverfahren bedürfen, die in der Lage wären, mit den großen Datenmengen umzugehen. Da die Daten meist unstrukturiert und nicht auf bestimmbare Kontexte beschränkt wären (von Verkehrsfluss-Aufzeichnungen über die Messung von Körperfunktionen bis hin zur Vernetzung aller Haushaltsgeräte (Karaboga u. a. 2015)), könne nicht vorhergesagt werden, welche Form der Datennutzung die vielversprechendste wäre. Mit anderen Worten müsste schon zur Identifikation potentiell relevanter Nutzungszwecke der entsprechenden Daten auf Big Data-Analyseverfahren zurückgegriffen werden. Dies wiederum würde dem Zweckbindungsprinzip, einem der zentralen Datenschutz-Grundsätze, diametral entgegenstehen, sofern – und hiervon wäre bei vernetzten Haushaltsgeräten usw. mit Sicherheit auszugehen – auch personenbezogene Daten analysiert würden (Richter 2016). Dementsprechend erhielt der Diskurs um die Datenschutz-Grundverordnung eine neue Wendung, bei dem die Flexibilitätsbefürworter nun nicht mehr nur für die Flexibilisierung der Datenschutz-Vorgaben eintraten, um ihre administrativen Compliance-Kosten zu senken und dadurch volkswirtschaftlich wünschenswerte Wachstumseffekte zu generieren, sondern

418 Zwar waren Big Data und Datenschutz bereits vorher thematisiert worden (Craig und Ludloff 2011), doch erst im Jahr 2013 und 2014 folgte eine Reihe wichtiger Debattenbeiträge (Butler 2013; Mayer-Schönberger und Cukier 2013; President's Council of Advisors on Science and Technology 2014), die im Rahmen einer breiteren öffentlichen Debatten diskutiert wurden (Schulz 2014; Zuboff 2014).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auch mit der Begründung, auf diese Weise gesellschaftlich wünschenswerte Dienste entwickeln zu können (Bitkom 2015; ZBI 2015).[419] Zudem trat Anfang 2015 eine neue formelle Akteurskoalition erstmals in Erscheinung: Die *European Data Coalition* (EDC), bestehend aus großen Europäischen Unternehmen und Unternehmensgruppen (darunter Ericsson, Nokia, SAP und Volvo), forderte die Politik insbesondere dazu auf, internationale Datentransfers zu erleichtern, ein verhältnismäßiges (d. h. weniger scharfes) Sanktionsregime einzuführen eine einfache und praktikable Lösung für das Prinzip der zentralen Kontaktstelle zu verabschieden (EDC 2015b).[420]

Nachdem sich der Ministerrat breits im Oktober 2014 auf die Einführung eines risikobasierten Ansatzes (d. h. die Reduktion der Verarbeiterpflichten) geeinigt hatte und damit den Positionen der Flexibilitätsbefürworter in einem wichtigen Punkt entgegenkommen war, kündigte sich Anfang 2015 an, dass der Ministerrat auch bei der Zweckbindung Zugeständnisse machen würde. Im März 2015 einigte sich der Ministerrat schließlich dahingehend, den Verantwortlichen mehr Flexibilität bei der Weiterverwendung personenbezogener Daten für Zwecken, die vom ursprünglichen Erhebungszweck abweichen und bei Zweckänderungen einzuräumen (vgl. 4.3.1.3.2).

Dies führte wiederum zu einem erneuten Widerstand auf Seiten der Datenschutzbefürworter, die ein Zurückfallen hinter das Schutzniveau der DS-RL befürchteten. Berichterstatter Albrecht, der sich zu der Einigung des Ministerrats im Hinblick auf die Verarbeiterpflichten, die den Forderungen des Parlaments inhaltlich diametral gegenüberstanden (Veil 2015), ungewöhnlich still verhalten hatte, klärte im Frühjahr 2015 schließlich darüber auf, dass Kommission und Parlament sich im Rahmen eines informellen Dialogs mit dem Ministerrat Ende 2014 bereit erklärt hatten, einer Flexibilisierung der Verarbeiterpflichten im Rahmen des Trilogs zuzustimmen, sofern im Gegenzug starke Betroffenenrechte und ein einheitlicher Sanktionsmechanismus Eingang in den finalen Text finden würden (Albrecht 2015, 3). Nachdem die Pläne des Ministerrats zur Flexibilisierung der Weiterverarbeitung sowie der Zweckbindung bekannt geworden waren, sah Albrecht

419 Auch Merkel sprach sich u. a. auf dem CDU-Parteikongress 2015 im Zusammenhang von Big Data und der EU-Digitalwirtschaft für eine bessere Balance von Datenschutz und Wirtschaftsinteressen aus (Tomas Rudl 2015).

420 Bemerkenswerterweise wurde zwar das Thema administrative Überlast angesprochen und auch für Erleichterungen in dieser Hinsicht geworben. Der Fokus des Lobby-Papiers lag allerdings nicht auf diesem Thema (EDC 2015b).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

jedoch die rote Linie in den Verhandlungen überschritten. Sowohl Albrecht (2015) als auch weitere Datenschutzbefürworter warfen dem Ministerrat in der Folge vor, hinter das Schutzniveau der DS-RL zurückzufallen, das von Reding (2013e), Albrecht und allen weiteren Datenschutzbefürwortern stets als nicht zur Disposition stehende rote Linie angesehen worden war.[421] Albrecht drohte dem Ministerrat daraufhin mit der Blockade der weiteren Verhandlungen, sollte der Ministerrat durch Zugeständnisse bei den Betroffenenrechten und Sanktionsregelungen dem Parlament nicht Kompromissbereitschaft signalisieren (ebd., 4). EDRi, Access, die Panoptykon Foundation und PI veröffentlichten im März 2015 zunächst ein gemeinsames Lobby-Papier, in dem sie die Ministerratsposition zu den Datenschutz-Grundsätzen, Betroffenenrechten, kollektiven Rechtsbehelfen und Sanktionen, zum risikobasierten Ansatz sowie zum Prinzip der zentralen Kontaktstelle entsprechend kritisierten (EDRi, accessnow, u. a. 2015). Anfang März 2015 veröffentlichte zudem auch LobbyPlag eine neue Auswertung der Positionen, die von den Mitgliedstaaten zu den Kapiteln I bis III vertreten worden waren. Die Teil-Auswertung der Regierungspositionen zeigte, dass die Bundesrepublik mehr Änderungsvorschläge zur Schwächung des Datenschutzes eingebracht hatte, als das Vereinigte Königreich oder Irland. Die Delegationen der beiden Länder folgten aber auf Platz 2 und 3, die tschechische Republik auf Platz 4, Schweden auf Platz 5 und Belgien auf Platz 6. Als die einzigen Delegationen, die unterm Strich für eine Stärkung des Datenschutzniveaus plädierten, identifizierte LobbyPlag Ungarn, Österreich, Griechenland sowie die Schweiz (Gutjahr 2015; LobbyPlag 2015).[422] Etwa zeitgleich erschien zudem ein Bericht im Spiegel, der die Kumpanei zwischen den für die Datenschutzreform zuständigen Beamten des Innenministeriums und Interessenvertretern aus der Wirtschaft offenbarte (S. Becker 2015).[423] Ende April 2015 initiierten EDRi, Access, PI, BoF, die Open

421 Tatsächlich stand aus Sicht der Kommission zu Beginn der Datenschutzreform nicht ansatzweise infrage, dass angesichts der Gefährdungen der Privatheit im Ergebnis der technologischen Entwicklung und Globalisierung eine Stärkung des Datenschutzniveaus nötig sein würde (vgl. 4.1.2 und 4.2.2). Und trotz ihrer grundsätzlich ablehnenden Haltung hatten selbst auf Seiten der Flexibilitätsbefürworter nur die wenigsten Akteure offen oder verdeckt für ein niedrigeres Datenschutzniveau als das der DS-RL plädiert (vgl. 4.1.1.3 und 4.2.1.3).

422 Die Medienresonanz auf die neuen Auswertungen fiel allerdings deutlich geringer aus (Beckedahl 2015; Beuth 2015a).

423 Netzpolitik.org veröffentlichte eine Informationsfreiheitsanfrage (Meister 2015) und einige Monate später die E-Mails, auf denen der Spiegel-Artikel basierte (Thomas Rudl 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Rights Group und Panoptykon Foundation schließlich mit einer formellen Koalition, bestehend aus insgesamt 66 Akteuren (vgl. 4.3.1.2.1 und vgl. Tabelle Anhang 12 für die vollständige Akteursliste), einen Brief an den neuen Kommissionspräsidenten Juncker, die Vize-Präsidenten Timmermans und Andrus Ansip sowie die neue Justizkommissarin Věra Jourová. In dem Brief erinnerten sie die neue Kommission an die Versprechen der ehemaligen Justizkommissarin Reding und forderten die Kommission dazu auf, nicht hinter das Datenschutzniveau der DS-RL und damit die versprochene rote Linie Redings zurückzufallen (EDRi und Access (International) 2015).[424] Derweil vertrat auch die neue Justiz-Kommissarin Věra Jourová die Linie ihrer Vorgängerin. Beispielsweise veröffentlichte sie, gemeinsam mit Andrus Ansip, Digitalkommissar und Vize-Kommissionspräsident, anlässlich des Europäischen Datenschutztages am 28. Januar 2015 eine Stellungnahme, in der die Ziele der Kommission bekräftigt und der Rat erneut zu einer raschen Verabschiedung seiner Position aufgefordert wurde (EC 2015a).

Kurz vor der Einigung im Ministerrat veröffentlichte die ICDP zwei Stellungnahmen, die sich zum einen an den Ministerrat und zum anderen an das Parlament und die Kommission richteten. Darin begrüßten die Verbände die Fortschritte im Ministerrat, drückten aber ihre anhaltende Besorgnis über die Einführung aufwendiger neuer Datenschutzregelungen aus. Stattdessen riefen sie die EU-Organe dazu auf, ein flexibles Datenschutz-Regime zu verabschieden, das auch in der Zukunft Innovationen ermöglichen und dem Wachstum der europäischen Digitalwirtschaft zuträglich sein würde (ICDP 2015a). Im Einzelnen forderte die ICDP: Die Anerkennung des Werts pseudonymer Daten, die Beibehaltung der Regelungen zu berechtigten Interessen, die Streichung des Erfordernisses einer ausdrücklichen Einwilligung unter allen Umständen, die Gewährleistung eines praktikablen Prinzips der zentralen Kontaktstelle, die Gewährleistung des freien Flusses personenbezogener Daten über Grenzen hinweg, die Implementierung eines klar definierten risikobasierten Ansatzes, die Notwendigkeit, sich von der pauschalen Mithaftung für Verantwortliche und Auftragsverarbeiter zu lösen sowie Profiling nur bei Verarbeitungen einzuschränken, die erhebliche negative Auswirkungen haben (ICDP 2015c).

424 Trotz der Bitte der Unterzeichner, noch vor der Verabschiedung der Ratsposition eine Antwort zu erhalten, kam diese erst fast drei Monate später und somit mehr als einen Monat nach der Festlegung der Ratsposition vom Kabinettschef Timmermans'. Darin bekannte sich die Kommission dazu, dem Versprechen Redings nachkommen zu wollen (European Commission 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nachdem partielle allgemeine Ausrichtungen im Hinblick auf mehrere wichtige Kapitel auf verschiedenen Ratssitzungen seit Mitte 2014 gebilligt worden waren, erfolgte die Verabschiedung der endgültigen allgemeinen Ausrichtung[425] des Rates auf der Ministerratssitzung vom 15./16. Juni 2015 (EU-Ministerrat 2015b, 3). Die Mitgliedstaaten kamen den Flexibilitätsbefürwortern in der Ratsposition sowohl horizontal, in Form der Abschwächung der Verordnungsbestimmungen entgegen als auch in Form der Einführung zahlreicher Öffnungsklauseln.[426]

Nur eine Woche nach Billigung der Ratsposition wurden die interinstitutionellen Verhandlungen im Rahmen des Trilogs aufgenommen. Die Verhandlungsführer des Parlaments und des Rates berieten unter Beteiligung der Kommission zwischen dem 24. Juni 2015 und dem 15. Dezember 2015 über einen Kompromiss.[427] Der Kompromisstext zur Datenschutz-Grundverordnung und der JI-Richtlinie wurde am 15. Dezember informell ver-

425 Diese allgemeine Ausrichtung des Rates bildete zwar informell die Position des Rates in erster Lesung ab, wurde formell aber nicht als solche verabschiedet. Erst der im Rahmen der informellen Trilog-Verhandlungen vereinbarte Kompromisstext wurde später als offizielle Ratsposition in erster Lesung verabschiedet. Das ordentliche Gesetzgebungsverfahren der EU sieht vor, dass zunächst das Parlament seine formelle Position in erster Lesung verabschiedet. Im Anschluss kann der Ministerrat die Parlamentsposition bestätigen oder einen abweichenden Standpunkt in erster Lesung verabschieden, worauf das Parlament in einer zweiten Lesung reagieren muss. In der Regel dient die Festlegung einer allgemeinen Ausrichtung des Ministerrats der Beschleunigung des Gesetzgebungsverfahrens, indem es in jenen Fällen Anwendung findet, in denen das Parlament noch keinen Standpunkt in erster Lesung festgelegt hat und dadurch die Möglichkeit erhält, auf die Ansichten des Ministerrats zu reagieren und das Verfahren innerhalb einer Lesung abzuschließen (EU-Ministerrat 2018a, 2019). Im Rahmen des Aushandlungsprozesses zur DSGVO wurde die allgemeine Ausrichtung des Ministerrats mehr als ein Jahr nach der in erster Lesung verabschiedeten Parlamentsposition angenommen. Eine Verkürzung des Verfahrens stellte dies dennoch dar, weil eine 2. formelle Lesung im Rat sowie die formelle Stellungnahme der Kommission entfielen. Wenn im Folgenden von der Ministerratsposition die Rede ist, ist desen im Sommer 2015 verabschiedete allgemeine Ausrichtung gemeint.

426 So sah Art. 21 (1) lit. c) DSGVO-RE vor, dass fortan auch eine Einschränkung der Datenschutz-Grundsätze in Art. 5 durch Rechtsvorschriften der Union oder der Mitgliedstaaten möglich sein sollte, sofern diese dem „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaates, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit und zum Schutz der Marktstabilität und Marktintegrität“ dient.

427 Siehe Tabelle Anhang 9 für den Sitzungskalender und die Tagesordnungen.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

abschiedet (EU-Kommission 2015), am 17. Dezember zunächst vom LIBE-Ausschuss mit 48 Stimmen (bei 4 Gegenstimmen und 4 Enthaltungen) (EU-Parlament 2015) und einen Tag später am 18. Dezember auch vom AStV bestätigt (EU-Ministerrat 2015c).

Nachdem die Texte durch Rechts- und Sprachsachverständige überarbeitet wurden, verabschiedete der Ministerrat die Kompromisstexte am 8. April 2016 als Standpunkt des Rates in erster Lesung (Council of the EU 2016). Diesem stimmte zunächst der LIBE-Ausschuss am 12. April 2016 fast einstimmig zu (Albrecht 2016b). Im Anschluss billigte das Parlament den Kompromisstext am 14. April 2016 in zweiter Lesung ohne weitere Abstimmung und beauftragte den Parlamentspräsidenten, den Vorschlag final zu unterzeichnen (EU-Parlament 2016, 2).

Am 27. April unterzeichnete dieser schließlich gemeinsam mit dem Präsidenten des Ministerrats die Datenschutz-Grundverordnung mit der finalen Bezeichnung *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)* (Europäische Union 2018).

4.3.2.7 Überblick der Inhalte des DSGVO-Kompromisses

Die finale DSGVO spiegelt inhaltlich einen Kompromiss zwischen den Vorschlägen des Ministerrats auf der einen und den Vorschlägen des Parlaments und der Kommission auf der anderen Seite wider (vgl. für eine Gegenüberstellung der unterschiedlichen Positionen Tabelle 4-40). Grundsätzlich kann konstatiert werden, dass der Ministerrat sich mit Erleichterungen für die Verantwortlichen und nationalen Freiräumen durchsetzen konnte, während das Parlament ein hohes Schutzniveau im Bereich der Betroffenenrechte und das hohe Sanktionsmaß erhalten konnte. Da die Inhalte der DSGVO und die Positionen aller Akteure bereits ausführlich vorgestellt wurden, soll an dieser Stelle benannt werden, den Positionen welches EU-Organs die einzelnen Elemente der finalen DSGVO am ehesten entsprechen.[428]

428 Ein Überblick darüber, wessen (Ministerrat, Kommission oder EP) Formulierungsvorschläge es in welcher Weise letztlich in die finale DSGVO schafften, findet sich in den einzelnen Abschnitten zu den Rechtselementen der DSGVO in Simitis et al. (2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Im einzelnen konnte sich der Ministerrat insbesondere bei den folgenden Elementen der DSGVO durchsetzen: den Bestimmungen über besondere Kategorien personenbezogener Daten, dem Recht auf Vergessenwerden, der Meldepflicht bei Datenschutzverletzungen, den Vorgaben zu automatisierten Entscheidungen bzw. Profiling und zu Privacy by Design und Default, der Zertifizierung, der verpflichtenden Bestellung eines bDSB, der Datenschutz-Folgenabschätzung und dem Verbandsklagerecht. Im Hinblick auf viele dieser als auch der vom Parlament durchgesetzten Bestimmungen konnte der Ministerrat zudem Öffnungsklauseln (in Form von Regelungsaufträgen und Regelungsoptionen) verankern, die zur weiteren Absenkung des Datenschutzniveaus verwendet werden können.[429]

Das Parlament scheiterte zwar in den meisten Fällen (bis auf die Durchsetzung des hohen Sanktionsniveaus) mit der Durchsetzung seiner eigenen Position, es war jedoch vor allem darin erfolgreich, das von der Kommission vorgeschlagene Schutzniveau vor allem im Bereich der Betroffenenrechte zu erhalten und eine Absenkung auf oder unter das Schutzniveau der DS-RL zu verhindern. Dazu zählen insbesondere die Bestimmungen zur Einwilligung, zu besonderen Kategorien personenbezogener Daten, zur Transparenz, zu den Modalitäten für die Wahrnehmung der Betroffenenrechte und zum Recht auf Datenportabilität. Zudem konnte sich das Parlament im Gegenzug zu den Lockerungen der Verarbeiterpflichten mit der Festschreibung strenger Dokumentationspflichten durchsetzen.

429 Siehe Albrecht und Jotzo (2016, 134 Rn. 4-10) für einen Überblick der wichtigsten Öffnungsklauseln und Roßnagel (2017) für eine aufführliche Kritik an der Vielzahl an Öffnungsklauseln.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Finale DSGVO	Parlamentsentwurf	Ratsentwurf	Kommissionsentwurf	DS-RL 95/46/EG
C1B Räumlicher Anwendungsbereich	4	5	4	4	3
C1C Definition personenbezogener Daten	4	5	3	4	3
C2C Grundsatz der Datenminimierung	4	4	3	4	3
C3C Verarbeitung zu anderen Zwecken	3	5	1	2	4
C3D Bedingungen für die Einwilligung	4	5	3	5	3
C 4 A Besondere Kategorien personenbezogener Daten	4	5	4	4	3
C 4 D Datenschutz bei Kindern	4	5	3	5	3
C5A Transparenz	3	4	2	4	3
C5C Modalitäten für die Wahrnehmung der Betroffenenrechte	4	5	3	4	3
C 5 E Recht auf Vergessenwerden	3	5	3	4	2
C 5 G Recht auf Datenportabilität	4	5	3	4	1
C 5 I Automat. Verarbeitung / Profiling	3	4	3	4	3
C5L Benachrichtigung bei Datenschutzverletzung	3	4	2	4	1
C 6 A Privacy by Default	3	4	2	4	2
C 6 B Privacy by Design	3	5	2	4	2
C 6 H Datensicherheit	4	5	3	3	3
C 7 Übermittlung in Drittstaaten	4	5	3	3	3
C 13 A Verhaltensregeln	3	4	2	4	3
C 13 B Zertifizierungen/Gütesiegel	4	5	2	3	1
C 13 C Bestellung eines bDSB	3	5	2	4	2
C 13 D Datenschutz-Folgenabschätzung	3	5	2	4	1
C 17 D Verbands- / Sammelklagerecht	3	5	3	4	1
C 17 E Sanktionen und Geldbußen	5	5	3	4	1

Tabelle 4-40: Positionen der Kommission, des Ministerrats und des EP im Vergleich zu zur finalen DSGVO sowie zur DS-RL (eigene Codierung der Positionen, grün für inhaltliche Überschneidung, hellgrün für inhaltliche Nähe zum finalen DSGVO-Text)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

4.3.2.8 Reaktionen auf die Einigung im Trilog und die Verabschiedung der DSGVO

Die Reaktionen der Flexibilitätsbefürworter auf die Bekanntgabe des finalen DSGVO-Kompromisses fielen harsch aus. Während Bitkom (2015) auf vergleichsweise versöhnliche Weise eine begrüßenswerte EU-weite Vereinheitlichung des Datenschutzes auf der einen und einen unzumutbaren Anstieg des bürokratischen Aufwands und eine zunehmende Rechtsunsicherheit auf der anderen Seite ausmachte, äußerten die beiden formellen Akteurskoalitionen EDC und ICDP vernichtende Kritik. Die EDC (2015a) kritisierte, dass die von ihr geäußerten Vorschläge kein Gehör gefunden hätten, sodass die neuen Datenschutzregelungen weder eine Harmonisierung, noch eine Vereinfachung oder Modernisierung mit sich brächten. Besonders hervorgehoben wurden die Sanktionen und die Rechtsunsicherheit, in deren Folge ein Aufschließen der Europäischen Digitalwirtschaft an die internationale Konkurrenz in weite Ferne gerückt sei. Die ICDP (2015b) ging noch härter ins Gericht und prophezeite, dass die Europäische Digitalwirtschaft in Folge der neuen Datenschutzregelungen Schaden nehmen und die Entwicklung innovativer Technologien fortan anderswo stattfinden werde. In anderen Weltregionen genutzte Dienste würden in der Folge verspätet oder gar nicht in die EU gelangen und somit das Bedürfnis von Nutzerinnen und Nutzern nach datengetriebenen Diensten missachtet. Die Verordnung werde zudem insbesondere für KMU eine größere Belastung darstellen als für größere, etablierte Konzerne. Sowohl EDC als auch ICDP kündigten ihre Bereitschaft an, bei der Sicherstellung einer wirtschaftsfreundlichen Implementierung mitzuwirken. Die ICDP ging noch einen Schritt weiter und brachte ihre Hoffnung zum Ausdruck, dass der im Trilog erreichte Kompromiss doch noch zurückgenommen werde und eine zweite Lesung erfolge.

Seitens der Datenschutzbefürworter wurde der finale DSGVO-Kompromiss mit Erleichterung aufgenommen. In einer gemeinsamen Stellungnahme von EDRi, BoF, Digital Rights Ireland, Privacy International und Digitale Gesellschaft e.V. (2015) hieß es etwa: „In den letzten vier Jahren wirkte es immer wieder so, als würden diese Vorschläge zerrieben. Insofern ist bereits das Zustandekommen der Datenschutzgrundverordnung ein Erfolg von Politikern aus verschiedensten Lagern ebenso wie der Zivilgesellschaft." Angesichts des Lobbyansturms der vorangegangenen Jahre wurde der finale Text als *absolutes Minimum* bewertet, das zumindest „um einiges besser [ist] als das, was der Rat und einige Parlamentsausschüsse vorgeschlagen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

hatten – er bleibt jedoch weit hinter den ursprünglichen Zielen zurück." Im einzelnen wurden die Themen Profilbildung, Einwilligung, darunter insb. die unzureichende Klarstellung berechtigter Interessen, und die Vielzahl der Öffnungsklauseln kritisiert. Auch der VZBV (2016) vertrat die Auffassung, dass der finale Text zwar in Teilen zu kritisieren sei, insgesamt aber besser ausfiel, als „man noch in den Jahren 2013 und 2014 befürchten musste." (ebd.) Die Bewertungen der BfDI (2016) und des EDSB (EDPS 2016) waren ebenfalls überwiegend positiv. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2016) bemängelten zwar zahlreiche Elemente, sahen aber auch positive Seiten am Kompromisstext.

Der Europäische Rat, der die DSGVO als Teil zur Vollendung des digitalen Binnenmarktes betrachtete, bezeichnete die Einigung über das Datenschutzreformpaket als einen wichtigen Fortschritt (Europäischer Rat 2015, 6).

Die folgenden zwei Unterabschnitte widmen sich nun der Beantwortung der Forschungsfragen.

4.4 Beantwortung der Forschungsfragen: Die Entstehung der DSGVO

Im Folgenden soll die übergeordnete Fragestellung der vorliegenden Arbeit beantwortet werden. Diese lautet:

Wie lässt sich die Entstehung der EU-Datenschutz-Grundverordnung (DSGVO) vor dem (datenschutz-)polit-historischen Kontext erklären?

Die DSGVO ist somit Ergebnis der jahrzehntewährenden politischen Auseinandersetzung zwischen den Befürwortern verbindlicher staatlicher Datenschutzregelungen auf der einen Seite und den Befürwortern wirtschaftsfreundlicher Datenschutzregelungen auf der anderen Seite. Nach einem Jahrzehnt der Versicherheitlichung in Folge der Terroranschläge in den Vereinigten Staaten und in Europäischen Staaten, konnte die Datenschutzreform, die zur Verabschiedung der DSGVO führte, im Jahr 2009 nur deshalb initiiert werden, weil mehrere wichtige Kontextfaktoren dies begünstigten: So insb. das Inkrafttreten des Lissabon-Vertrags und das Wirksamwerden der EU-GRCh. In den Worten des ACF handelt es sich dabei um *Veränderungen in der verfassungsmäßigen Struktur der EU* die eine Reform (insb. im Hinblick auf die sicherheitsrelevanten Datenschutzaspekte) und den Erlass umfassender sekundärrechtlicher Datenschutzregelungen formal erforderlich machten. Dass die Reform praktisch angestoßen werden konnte, ist auf das Wirken des datenschutzbefürwortenden Flügels der EU-Organe

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zurückzuführen. Zu diesen zählten die EU-Parlamentsfraktionen links der Mitte und Ende der 2000er-Jahre auch die liberale Fraktion, daneben aber auch Teile der Kommission, darunter insb. der damalige Kommissar für Justiz, Freiheit und Sicherheit, Franco Frattini. Nachdem die Positionen dieser Akteure in vergangenen Politik-Prozessen nicht berücksichtigt worden waren, gelang es ihnen, vor dem Hintergrund eines wachsenden öffentlichen Rufs nach einem verbesserten Schutz personenbezogener Daten, gemeinsam mit einigen Mitgliedstaaten den Datenschutz-Reform-Prozess in der EU-Agenda zu verankern. Aber auch die abnehmende Anzahl an Terroranschlägen, die wachsende Sorge in der Bevölkerung vor dem Missbrauch personenbezogener Daten seitens privatwirtschaftlicher als auch staatlicher Akteure sowie zunehmende Proteste gegen Überwachungsmaßnahmen gaben den Positionen der Datenschutzbefürworter Auftrieb.

Die von Frattini Mitte 2009 initiierte Reform wurde bald darauf von der überzeugungsgetriebenen, neuen Justizkommissarin Viviane Reding übernommen. Reding und ihr Team verfolgten mit der Reform die Absicht, das Datenschutzniveau in der EU angesichts der durch den technologischen Wandel und die Globalisierung bedingten Herausforderungen deutlich anzuheben. Im Rahmen der beiden Konsultationsphasen zwischen 2009 und 2011 zeigte sich, dass nicht nur einige Mitgliedstaaten diesem Wunsch skeptisch gegenüber standen, sondern insbesondere die europäische und außereuropäische Wirtschaft. Nachdem ein enormer Lobbyansturm dieser von mir als Flexibilitätsbefürworter bezeichneten Akteure vergeblich die Absenkung des Schutznvieaus des Verordnungsvorschlags der Kommission bezweckte, ging die Kommission dazu über, ihren grundrechtsorientierten Vorschlag unter Rückgriff auf das sog. Vertrauensargument gleichsam als Vorteil für die Wirtschaft zu präsentieren. Demnach würde ein erhöhtes Datenschutzniveau zwar zu Mehrkosten auf Seiten der Datenverarbeiter führen, diese würden in Folge des gesteigerten Vertrauens von Nutzerinnen und Nutzern in deren Dienste aber zu einer größeren Nutzungsbereitschaft und damit zu deutlich höheren Gewinnen führen. Die Akteure der Flexibilitätsbefürworter zeigten sich von dieser Argumentation unbeeindruckt und fokussierten ihr Lobbying nach der Eröffnung des ordentlichen Gesetzgebungsverfahrens Anfang 2012 auf das Europäische Parlament und den Ministerrat.

Einen wesentlichen Anteil beim Zustandekommen der DSGVO hatte die Vergabe des Berichterstatterpostens im federführenden LIBE-Ausschuss an den grünen MdEP Jan Philipp Albrecht. Dieser war in den folgenden Jahren gefordert, einen parlamentsinternen Kompromiss auszuhandeln, dem

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

auch die parlamentarischen Gegner eines höheren Datenschutzniveaus in Gestalt der konservativen Fraktionen zustimmen können mussten. Außerdem wurden die Berichterstatterposten der mitberatenden Parlamentsausschüsse von Parlamentier(-inne)n übernommen, die dem Lager der Flexibilitätsbefürworter zuzuordnen sind. Denn selbst mit den Stimmen der liberalen Fraktion erreichten die Datenschutzbefürworter im EP nicht die für eine Annahme erforderliche Mehrheit. Parallel zu den intensiven Diskussion im Parlament zeigte sich im Ministerrat bzw. auf Seiten vieler EU-Mitgliedstaaten eine Skepsis gegenüber dem Reformvorschlag der Kommission. Die Mitgliedstaaten vertraten Positionen, die dem Lager der Flexibilitätsbefürworter zuzuordnen sind und sahen in einem Großteil der Kommissionsvorschläge in erster Linie eine Mehrbelastung der datenverarbeitenden Wirtschaft, während das Vertrauensargument für sie praktisch keine Rolle spielte.

Albrecht und sein Team erwarteten, dass die im Rahmen des Gesetzgebungsverfahrens anstehenden interinstitutionellen Verhandlungen zwischen Parlament und Ministerrat beide Seiten zu Kompromissen drängen würden und dass der Ministerrat eine deutliche Abschwächung des Schutzniveaus anstreben würde. Deshalb gingen sie zu der Strategie über, ihrerseits in der Parlamentsposition eine weitere deutliche Stärkung des von der Kommission vorgeschlagenen Datenschutzniveaus festzuschreiben.[430] Auf diese Weise konnte Albrecht zwar die volle Unterstützung der zivilgesellschaftlichen Datenschützer erringen, verlor aber auf Ebene des Parlaments die Unterstützung der bis dahin wohlwollenden liberalen Fraktion, während die konservativen Fraktionen den Vorschlägen Albrechts ohnehin ablehnend gegenüberstanden. In der Folge kam es im Parlament zu einer Pattsituation, die den Aushandlungsprozess für mehrere Monate lahmlegte.

Die Kontextanalyse hat demonstriert, dass bei vergangenen Gesetzgebungsverfahren in derartigen Pattsituationen die Flexibilitätsbefürworter regelmäßig siegreich hervorgingen. Vor dem Hintergrund dieser Erkenntnis wäre zu erwarten gewesen, dass die konservativen Fraktionen und die liberale Fraktion, gegebenenfalls unter Hinzuziehung wirtschaftsfreundlicher Sozialdemokrat(-inn)en, die Änderungsvorschläge des Albrecht-Berichts entweder schon im LIBE-Ausschuss oder spätestens bei der Plenums-

430 Was nicht heißen soll, dass ich der Ansicht bin, dass Albrecht et al. nicht überzeugungsgetrieben handelten. Vielmehr bin ich der Ansicht, dass sie sich an diesem Zeitpunkt kompromissbereiter gezeigt hätten, wenn die Signale aus Wirtschaft und Ministerrat nicht in Richtung einer dermaßen starken Senkung des Schutzniveaus verwiesen hätten.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

abstimmung fallengelassen und wirtschaftsfreundliche Änderungsanträge angenommen hätten. Alternativ wäre denkbar gewesen, dass Albrecht in Antizipation dieses Szenarios und um einer noch stärkeren Senkung des Schutzniveaus vorzubeugen, freiwillig eine deutliche Abschwächung seines finalen Berichts vorgenommen hätte. Auf dem Höhepunkt der Pattsituation bewirkte schließlich ein *externer Shock* in Form der Snowden-Enthüllungen, dass keines dieser Szenarien eintrat. Das Bekanntwerden der weltweiten Massenüberwachung seitens der Five Eyes, das insbesondere durch den Zugriff auf personenbezogene Daten ermöglicht wurde, die bei privatwirtschaftlichen Datenverarbeitern anfielen, bewirkte, dass sich eine große Mehrheit des EU-Parlaments hinter Albrechts Vorschläge stellte. In dieser Phase agierten Reding und Albrecht als Policy Entrepreneure, um die europäische Politik zum Handeln zu bewegen. Angesichts der weitgehenden Machtlosigkeit des Europäischen Parlaments im Hinblick auf den politischen Umgang mit der Massenüberwachung, bezweckten die Parlamentarier(-innen) mit der Befürwortung starker Datenschutzregeln ein deutliches Zeichen gegen die aus ihrer Sicht ausufernden Überwachungspraktiken zu setzen. Die Bemühungen Redings und Albrechts wurden seit Anfang 2013 zudem seitens eines Bündnisses zivilgesellschaftlicher Organisationen und seitens zahlreicher Medien unterstützt. Auch wenn der konkrete Einfluss der Medienberichterstattung und des zivilgesellschaftlichen Engagements nur schwer messbar ist, kann davon ausgegangen werden, dass sie der öffentlichen Anerkennung der Positionen der Datenschutzbefürworter weiteren Auftrieb verliehen.

Während das Handeln Redings und Albrechts bei den MdEPs Erfolg hatte, scheiterte es jedoch bei der Mehrzahl der Mitgliedstaaten. Denn die Mehrheit der Mitgliedstaaten hatten kein Interesse an der Anhebung des Datenschutzniveaus. Nicht zuletzt deshalb, weil einige unter ihnen selbst in fragwürdige Überwachungspraktiken verstrickt waren, von denen sie nicht abzurücken gedachten. Dies betraf insbesondere konservative, aber auch sozialdemokratische Regierungen, die sich mit der Praxis weitgehender Überwachungsmaßnahmen entweder arrangiert oder diese selbst ins Leben gerufen hatten. Zudem fruchtete die Argumentation der datenverarbeitenden Wirtschaft, wonach ein höheres Datenschutzniveau zu wirtschaftlichen Nachteilen führen würde, insbesondere bei den konservativen mitgliedstaatlichen Regierungen. Folglich war der Ministerrat nicht bereit, ein höheres Datenschutzniveau zu unterstützen. Zugleich wurde vor dem Hintergrund der allgemeinen öffentlichen Empörung auf die Snowden-Enthüllungen befürchtet, dass die Verabschiedung einer Ministerratsposition,

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

in der die Absenkung des Datenschutzniveaus vorgeschlagen wird, zu einem ernstzunehmenden öffentlichen Aufschrei geführt hätte. Deshalb setzten der Ministerrat bzw. die tonangebenden Mitgliedstaaten auf den Faktor Zeit: Würde die Verabschiedung der Ministerratsposition nur ausreichend weit in die Zukunft verschoben, würde sich irgendwann wieder die Gelegenheit ergeben, für die Absenkung des Schutzniveaus einzutreten, ohne größere politische Konsequenzen befürchten zu müssen. Mit dem allmählichen Abklingen des Überwachungsskandals im Laufe des Jahres 2014 begann der Ministerrat damit, erste Einigungen im Hinblick auf einzelne Elemente und Teile des Verordnungsvorschlags zu treffen, sodass die Ministerratsposition Mitte 2015 verabschiedet werden konnte.

Doch weshalb kam es letztlich zur erfolgreichen Verabschiedung der DSGVO, die zudem trotz des Abwartens des Ministerrats datenschutzfreundlicher ausfiel, als unter *normalen* Bedingungen – also ohne die Snowden-Enthüllungen – zu erwarten gewesen wäre? Hätte der Ministerrat den Prozess nicht genauso gut länger blockieren oder gar von der Kommission die Vorlage eines neuen wirtschaftsfreundlicheren Vorschlags fordern können?

Ein Teil der Antwort auf diese Fragen findet sich in der Überzeugungsstruktur von Teilen der Flexibilitätsbefürworter. So waren nicht alle Flexibilitätsbefürworter der Überzeugung, dass überhaupt keine Reform der Datenschutzregeln erforderlich sei. Auf Seiten der Mitgliedstaaten war die schwierige Durchsetzbarkeit der nationalen Datenschutzregeln gegenüber transnationalen datenverarbeitenden Konzernen ein drängendes Problem. Elemente der DSGVO, wie der One-Stop-Shop oder die Ausweitung des Anwendungsbereichs der Verordnung auf außereuropäische Anbieter wurden in diesem Zusammenhang besonders stark begrüßt. Daneben hatte die Kommission ursprünglich bezweckt, eine einzelne sowohl auf den zivilen (öffentlichen und privatwirtschaftlichen) als auch den sicherheitsrelevanten Bereich anwendbare Verordnung vorzuschlagen. Im Laufe der Konsultationsphase war die Kommission von dieser Idee wieder abgerückt, doch hatte sie ihren DSGVO- und JI-Richtlinienvorschlag als Reform*paket* veröffentlicht, mit der sie die Umsetzung der Vorgaben der EU-Grundrechtecharta anstrebte. Dass sich Parlament und Ministerrat zu Beginn des Gesetzgebungsverfahrens zur gemeinsamen Behandlung beider Vorschläge verpflichteten, bedeutete, dass insbesondere ein Abbruch der Verhandlungen nicht infrage kam, weil damit primärrechtliche EU-Vorgaben verletzt worden wären. Insofern stellte die Einigung im Trilog im Sinne des ACF einen ausgehandelten Kompromiss dar, der angesichts einer unerwünsch-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ten politischen Pattsituation erreicht werden konnte. Doch warum wurden die Verhandlungen nicht zurückgesetzt oder weiter verzögert?

Darüber hinaus hatten nicht nur die Datenschutzbefürworter Interesse an der Verabschiedung des Datenschutzrahmens, sondern auch einige Mitgliedstaaten. Am offensichtlichsten zeigte sich dies in der für das Jahr 2015 vorgesehenen Vollendung des Binnenmarktes. Neben weiteren Maßnahmen, wie einer Cybersicherheitsrichtlinie, bildete die DSGVO einen Eckpfeiler der digitalen Binnenmarkt-Strategie. Interessanterweise – denn im Ministerrat fand das Argument ansonsten kaum Beachtung – wurde Datenschutz darin als vertrauensbildende Maßnahme beschrieben (KOM 2015b), und auch der Europäische Rat hatte bereits 2013 die Bedeutung von Datenschutzregelungen für das Vertrauen in die digitale Wirtschaft unterstrichen. Die späteren Äußerungen des Europäisches Rates zum Datenschutz-Rahmen wurden stets aus wirtschaftspolitischen Erwägungen heraus getroffen.

Wer sorgte nun dafür, dass diese unterschiedlichen Fäden im Ministerrat zusammenliefen und die Initiierung der Trilog-Verhandlungen ermöglichten?

Eine wichtige Rolle kam den bedingten Datenschutzbefürwortern im Ministerrat (darunter insb. Frankreich, Italien, Polen und Luxemburg) zu, die im Laufe der Verhandlungen für ein höheres Schutzniveau als die meisten anderen Mitgliedstaaten eingetreten waren. Laut Viviane Reding habe letztlich die luxemburgische Ratspräsidentschaft maßgeblichen Einfluss auf die Initiierung der Trilog-Verhandlungen gehabt.[431] Hier kam offenbar dem federführenden, grünen Justizminister Déi Gréng eine wichtige Rolle zu (Jančiūtė 2018, 170). Erwähnt sei auch, dass die Kommission in den Trilog-Verhandlungen im Gegensatz zu den Jahren davor kompromissbereiter agierte und auf diese Weise letztlich erfolgreicher darin war, das Schutzniveau zu erhalten (ebd., 168). Dass im Ergebnis der Trilog-Verhandlungen keine besonders starke Absenkung des Datenschutzniveaus erfolgte, ist schließlich darauf zurückzuführen, dass dem Ministerrat mit dem Parlament und der Kommission zwei EU-Organe gegenüberstanden, die beide gemeinsam für ein hohes Schutzniveau eintraten und, dass nicht alle Mitgliedstaaten an der vor allem von Deutschland und Großbritannien forcierten Abschwächung Interesse hatten.

Die DSGVO kann somit als relativer Sieg für die Datenschutzbefürworter bewertet werden. Dennoch sollte nicht unterschätzt werden, dass sich

431 Rede Viviane Redings auf der CPDP 2016.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

der Ministerrat in den meisten inhaltlichen Punkten gegenüber Parlament und Kommission durchsetzen konnte – jedoch eben nicht in der Intensität, wie sie es in der Datenschutzpolitik in den Jahrzehnten zuvor vermocht hatte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

5 Schluss

Diese Schrift hat sich mit der übergeordneten Frage auseinandergesetzt, *wie die Entstehung der DSGVO im Kontext der historischen EU-Datenschutzpolitik erklärt werden kann*.

Den Hintergrund für das Thema bildet die rasante Bedeutungszunahme der Datenschutzpolitik in den vergangenen Jahrzehnten. Vom Nischenthema unter Fachjuristen und Informatikern in den 1970er Jahren avancierte Datenschutz zuletzt zu einer zentralen Frage der zunehmend auf der Verarbeitung von Daten basierenden Gegenwartsgesellschaft.

Politikwissenschaftliche Analysen zur Datenschutzpolitik befassten sich über viele Jahre mit einzelnen Politiken, etwa der DS-RL, den Datenschutzbehörden oder mit überwachungspolitischen Maßnahmen wie dem transatlantischen Austausch von Banktransaktionsdaten. Andere Arbeiten blicken auf das Thema Datenschutz aus einer Perspektive, die Datenschutz trotz seiner jahrzehntelangen Vorgeschichte oftmals als Teil der modernen Netzpolitik einordnet. Sie bieten letztlich wenig Erklärungspotential dafür, warum die Datenschutzpolitik dazu geworden ist, was sie heute ist: Ein Querschnittspolitikfeld, das zwischen dem Schutz von Grundrechten und der Ermöglichung des Datenaustauschs hin- und hergerissen ist.

Zur Beantwortung der übergeordneten Fragestellung unterteilte ich die Fragestellung in zwei miteinander zusammenhängende Teile. Im Rahmen von FF1 stand die zentrale Forschungsfrage im Vordergrund, wie sich die Entstehung der DSGVO im engeren Sinne erklären lässt. Mit FF2 widmete ich mich dem historischen datenschutzpolitischen Kontext, indem ich untersuchte, welche politischen und historischen Faktoren als kausale, treibende Faktoren auf dem Weg zur DSGVO wirkten.

Im Folgenden fasse ich zunächst die Ergebnisse der Arbeit im Hinblick auf die Forschungsfragen zusammen (5.1), nehme eine kritische Reflexion der Ergebnisse vor und gehe dabei auf Forschungsdesiderate ein (5.2) und schließe mit einem kurzen Ausblick zur Zukunft der EU-Datenschutzpolitik (5.3).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

5.1 Zusammenfassung und Beantwortung der Forschungsfragen

Das Ziel der vorliegenden Schrift ist es, die Frage nach der Entstehung der DSGVO im Kontext der historischen EU-Datenschutzpolitik zu beantworten. Insbesondere sollten dabei die politischen und historischen Faktoren berücksichtigt werden, die als kausale, treibende Faktoren bei der Entstehung der DSGVO wirkten.

Im ersten Schritt (Unterabschnitt 2.1 und 2.2) stellte ich den dieser Arbeit zugrunde liegenden theoretischen Rahmen in Gestalt des Advocacy Coalitions Frameworks (ACF) vor. Unter Rückgriff auf den politikwissenschaftlichen Stand der Forschung zum Thema der EU-Datenschutzpolitik legte ich den Hauptfokus auf die ACF-Elemente der Überzeugungssysteme und Advocacy-Koalitionen. Das Forschungsdesign (2.3) unterteilte ich in Analyseeinheit, Fall und Beobachtung. Die Analyseeinheit bildet „die Politische Regulierung des Schutzes personenbezogener Daten in der Europäischen Union", kurz „die EU-Datenschutzpolitik". Als Fall legte ich das Zustandekommen der DSGVO fest. Als Forschungsstrategie wählte ich die Einzelfallstudie und als Untersuchungsmethode zur systematischen Erfassung von Beobachtungspunkten die Prozessanalyse.

Im Unterabschnitt (2.3.3) zum analytischen Rahmen spezifizierte ich zum Einen die unabhängigen Variablen und die abhängige Variable und führte zum Anderen aus, wie die unabhängigen Variablen die abhängige Variable erklären. Als abhängige Variable definierte ich die Verabschiedung der DSGVO. Die unabhängigen Variablen ergaben sich unmittelbar aus dem ACF: Die Überzeugungssysteme, Zusammensetzung und Ressourcen einer Adocacy-Koalition.

Den analytischen Rahmen des empirischen Teils untergliederte ich schließlich in eine *einführende Kontextanalyse* und eine *detaillierte Akteurs- und Prozessanalyse*. Als Ziel der Kontextanalyse (Abschnitt 3), die alle zentralen datenschutzpolitischen Auseinandersetzungen auf EU-Ebene bis zur Initiierung des Aushandlungsprozesses der DSGVO zum Gegenstand hatte, legte ich die Ermittlung der vom ACF vorgegebenen relevanten Kontextbedingungen fest, die als entscheidend im Hinblick auf das Zustandekommen eines Politik-Ergebnisses gelten. Zu diesen zählen:

- Relativ stabile Parameter, die in der Regel über zehn oder mehr Jahre unverändert bleiben, diese sind:
  - Grundlegende Merkmale des betrachteten Problems
  - Verteilung natürlicher Ressourcen

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

  - Grundlegende soziokulturelle Wertvorstellungen und Sozialstruktur
  - Grundlegende verfassungsmäßige Struktur
- Externe Systemereignisse im Vorfeld der DSGVO, die sich innerhalb von zehn Jahreszeiträumen eher verändern können, diese sind:
  - Wandel sozioökonomischer Bedingungen
  - Wandel in der öffentlichen Meinung
  - Wandel maßgeblicher (Regierungs-)Koalitionen
  - Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen
- Langfristig wichtige politische Gelegenheitsstrukturen
  - Grad der erforderlichen Zustimmung für wesentlichen Wandel
  - Die relative Offenheit des untersuchten politischen Systems
  - Mögliche, traditionelle Konfliktlinien

Zu den zentralen datenschutzpolitischen Auseinandersetzungen auf EU-Ebene, die im Rahmen der Kontextanalyse untersucht wurden, zählte ich:

- OECD-Datenschutz-Richtlinien
- Datenschutz-Konvention des Europarats
- Datenschutz-Richtlinie 95/46/EG
- Erster und zweiter Bericht über die Durchführung der DS-RL
- ISDN-Richtlinie 97/66/EG
- Datenschutz-Verordnung 45/2001
- ePrivacy-Richtlinie 2002/58/EG
- Richtlinie zur Vorratsdatenspeicherung 2006/24/EG
- Zugriff auf Fluggastdaten
- JI-Rahmenbeschluss 2008/977/JHA
- Cookie-Richtlinie 2009/136/EG

Zur Durchführung der Kontextanalyse (Abschnitt 3) griff ich überwiegend auf die Durchsicht der einschlägigen Sekundärliteratur zurück. Ergänzend wurden zur Ausfüllung von Leerstellen auch Primärdokumente und die Medienberichterstattung herangezogen. Im Ergebnis der Kontextanalyse wurden die entscheidenden polit-historischen Kontextbedingungen der EU-Datenschutzpolitik ermittelt, die entscheidend im Hinblick auf das Zustandekommen der DSGVO waren. So zeigte ich, dass der datenschutzpolitische Hauptkonflikt grundsätzlich zwischen zwei Akteursgruppen ausgetragen wurde. Einem Lager, das an einer möglichst ungehinderten Nutzung personenbezogener Daten interessiert ist und das sich in zwei (sich teilweise überlappende) Advocacy-Koalitionen aufteilt: Eine Advocacy-Ko-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

alition der sog. *Flexibilitätsbefürworter*, die sich weitestgehend aus privatwirtschaftlichen Akteuren, aber auch den konservativen und liberalen parlamentarischen Fraktionen im EU-Parlament sowie einigen Regierungen der Mitgliedstaaten zusammensetzt und für eine weitgehend ungehinderte Nutzung personenbezogener Daten für wirtschaftliche Zwecke eintritt, jedoch nur sehr eingeschränkt für eine Nutzung zu Sicherheitszwecken. Und eine Advocacy-Koalition der sog. Sicherheitsbefürworter, die sich überwiegend aus Sicherheitsbehörden, konservativen sowie sozialdemokratisch regierten EU-Mitgliedstaaten zusammensetzt und für eine ungehinderte Verwendung personenbezogener Daten für Sicherheitszwecke eintritt. Wenn es um Fragen des Ausgleichs zwischen Wirtschaftsinteressen und Datenschutz geht, rückten die konservativen Akteure eher in Richtung der Flexibilitätsbefürworter und die sozialdemokratischen Akteure in Richtung der Datenschutzbefürworter. Diesen beiden, auf möglichst große Freiräume bei der Verarbeitung personenbezogener Daten für die von ihnen favorisierten Bereiche (Wirtschaft und Sicherheit) fokussierten, Advocacy-Koalitionen stand eine Advocacy-Koalition der Datenschutzbefürworter entgegen, die sich zunächst hauptsächlich aus Datenschutzbehörden und dem linken Flügel des EU-Parlaments aber auch einigen sozialdemokratischen mitgliedstaatlichen Regierungen und später auch zivilgesellschaftlichen Akteuren zusammensetzte. Unabhängig davon, ob wirtschafts- oder sicherheitspolitische Fragen zur Debatte standen, vertraten die Datenschutzbefürworter ein grundrechtsschutzorientiertes Datenschutz-Verständnis, auf dessen Basis sie sich stets für Regulierungen zur Stärkung des Datenschutzniveaus eintraten.

Die Advocacy-Koalition der Datenschutzbefürworter konnte sich zunächst durchsetzen: Von den ersten überstaatlichen Regelungen zum Datenschutz bis zur Datenschutz-Richtlinie 95/46/EG (DS-RL). Dies vermochten sie jedoch nicht allein aufgrund der grundrechtlichen Bedeutung, die sie selbst personenbezogenen Daten beimaßen, sondern insbesondere, weil Akteure, die später den Flexibilitätsbefürwortern angehören würden, die Harmonisierung nationaler Datenschutzregelungen mittels überstaatlicher Datenschutzregelungen unterstützten, um eine reibungslose grenzüberschreitende Verarbeitung personenbezogener Daten zu gewährleisten. In der zweiten Hälfte der 1990er-Jahre geriet dieser Prozess zunächst angesichts der zunehmenden wirtschaftlichen Bedeutung ins Stocken. In Folge der Terroranschläge in New York (2001), Madrid (2004) und London (2005) wurde der Diskurs dann von der sicherheitspolitischen Bedeutung der Verarbeitung personenbezogener Daten überschattet. Die Spaltung der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

parlamentarischen Datenschutzbefürworter in Sicherheitsfragen führte dazu, dass sich die die Befürworter weitreichender Verarbeitungsmöglichkeiten zu Sicherheitszwecken in den Folgejahren in praktisch jeder politischen Auseinandersetzung mit Datenschutz-Bezug durchsetzen konnten.

Die EU-Kommission bzw. die zuständigen Kommissionsstellen, nahmen bei diesen Entwicklungen eine Rolle als Policy Broker ein. Zu Beginn der Verhandlungen der DS-RL bis in zur Mitte der 2000er-Jahre vermittelte die Kommission zwischen den unterschiedlichen Interessen vermittelte. In der schrittweisen institutionellen Verschiebung der Datenschutz-Zuständigkeit vom Binnenmarkt-Generaldirektorat in das Informationsgesellschaft-Generaldirektorat ab dem Jahr 2000 und in das Generaldirektorat für Justiz, Freiheit und Sicherheit ab dem Jahr 2005 spiegelten sich auch die neuen Prioritäten in Form der Förderung der Verarbeitung personenbezogener Daten im Sinne der Wirtschaft einerseits und im Sinne der Sicherheitsbehörden andererseits wider.

Die Kontextanalyse zeigte außerdem, dass die *grundlegende verfassungsmäßige Struktur* eine wichtige Rolle beim Zustandekommen von Datenschutzpolitiken spielte. So ermöglichte erst die für 1992 vorgesehene Vollendung des Binnenmarktes, dass gemeinschaftsweite Datenschutzregelungen erlassen werden konnten. Von der EMRK, auf die sich vor allem das Europäische Parlament bei seinem Eintreten für Datenschutzregelungen gestützt hatte, war hingegen keine vergleichbare Wirkung ausgegangen. Schließlich war im Hinblick auf die Initiierung der Datenschutzreform im Jahr 2009, die zur Verabschiedung der DSGVO führte, das Inkrafttreten des Lissabon Vertrags im selben Jahr entscheidend. Damit wurden die Bestimmungen der EU-Grundrechtecharta verbindlich und die in den Artikeln 7 und 8 vorgesehene Achtung des Privat- und Familienlebens bzw. der Schutz personenbezogener Daten zum EU-Grundrecht und damit zum Teil des EU-Primärrechts erhoben, den es fortan mittels sekundärrechtlicher Maßnahmen wirksam zu gewährleisten galt.

Die Analyse der institutionellen EU-Bestimmungen (*Grad der erforderlichen Zustimmung für wesentlichen Wandel*) zeigte, dass einzelne Akteure durchaus in der Lage waren, politische Veränderungen mitanzustoßen. So waren es die Datenschutzbehörden, die vor dem Hintegrund des geplanten Inkrafttretens des Binnenmarkt-Projekts unter Rückgriff auf ihre behördlichen Kompetenzen den Stein des Anstoßes zur Erarbeitung der Datenschutz-Richtlinie gaben, indem sie damit drohten, den Datentransfer in jene Mitgliedstaaten zu stoppen, die über keine Datenschutzgesetze verfügten. Grundsätzlich zeigte die Analyse, dass die entscheidenden Para-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

meter der untersuchten datenschutzpolitischen Maßnahmen jedoch nicht von den Datenschutzbehörden oder dem EU-Parlament festgelegt wurden, sondern von den EU-Mitgliedstaaten. Weder auf die Gestaltung der sicherheitspolitischen motivierten Verarbeitungsfreiräume noch auf den JI-Rahmenbeschluss konnten die Datenschutzbefürworter in nennenswerter Weise Einfluss nehmen. Doch änderte sich auch dieser institutionelle Umstand mit dem Inkrafttreten des Lissabon-Vertrags. Seit dem 1. Dezember 2009 ist das EU-Parlament dem Ministerrat formal in nahezu allen Politikbereichen der EU gleichgestellt. Trotz der hervorgehobenen Stellung des Ministerrats zeigte die Kontextanalyse (*relative Offenheit des politischen Systems*), dass eine zunehmende Zahl an Akteuren in die datenschutzpolitischen Aushandlungsprozesse involviert gewesen ist.

Die Kontextanalyse zeigte auch, dass der *Wandel der sozioökonomischen Bedingungen* einen wesentlichen Einfluss auf den datenschutzpolitischen Diskurs hatte. Je mehr die wirtschaftliche Bedeutung der Verarbeitung personenbezogener Daten zunahm, umso mehr rückte der Diskurs weg von der grundrechtlichen Bedeutung der Thematik und hin zu einem wirtschaftspolitischen Framing, wonach Datenschutzregelungen dazu dienten, das Vertrauen in die datenverarbeitende Wirtschaft zu stärken und damit Wirtschaftswachstum zu ermöglichen.

Einfluss auf die Initiierung der Datenschutz-Reform hatte auch ein *Wandel in der öffentlichen Meinung*, der sich im Laufe der 2000er-Jahre vollzog. Während die Unterstützung für Anti-Terror-Maßnahmen zwar konstant blieb, wuchsen die Datenschutz-Sorgen der EU-Bevölkerung im selben Zeitraum, sodass im Jahr 2008 erstmals eine Bevölkerungsmehrheit für den Erlass EU-weiter Datenschutzgesetze war. Diese Datenschutz-Sorgen wurden nicht allein vom möglichen Missbrauch der für sicherheitspolitische Zwecke erhobenen personenbezogenen Daten genährt, sondern auch von der zunehmenden und umstrittenen Verarbeitung personenbezogener Daten für wirtschaftliche Zwecke, z. B. im Zuge des Populärwerdens von sozialen Online-Netwerken und in Folge des Bekanntwerdens einer Reihe an öffentlichkeitswirksamen Datenschutz-Skandalen seit Mitte der 2000er-Jahre. Zeitgleich erstarkten europaweit zivilgesellschaftliche Bewegungen, die sich gegen die aus ihrer Sicht ausufernden Anti-Terror-Maßnahmen richteten und die angesichts der zunehmenden Ausweitung von sicherheitsstaatlichen Maßnahmen verhältnismäßig große Teile der Bevölkerung gegen die Maßnahmen mobilisieren konnten.

Die Vollendung des Binnenmarktes, die Terroranschläge zu Beginn der 2000er-Jahre und in eingeschränkter Weise auch die zunehmende wirt-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

schaftspolitische Bedeutung der Verarbeitung personenbezogener Daten fungierten zudem als externe Shocks. Dies verdeutlicht, dass Datenschutzpolitik als Querschnittsthema stets auch abhängig von *Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen* ist.

Die Initiierung der Datenschutz-Reform, die später in der Verabschiedung der DSGVO und der JI-Richtlinie mündete, war somit aufgrund einer Mischung aus verschiedenen Einflussfaktoren möglich: Veränderungen in der verfassungsmäßigen Struktur der EU in Gestalt des Inkrafttretens des Lissabon-Vertrags und des Verbindlichwerdens der EU-Grundrechtecharta machten den Erlass von umfassenden sekundärrechtlichen Datenschutzregelungen erforderlich. Die an stärkeren Datenschutzregelungen für den Sicherheitsbereich interessierten Akteure, insb. die EU-Parlamentsfraktionen links der Mitte sowie die liberale Fraktion, aber auch Teile der EU-Kommission (insb. das Kommissariat für Justiz, Freiheit und Sicherheit), deren Stimmen über Jahre trotz gegenüber dem Ministerrat erbrachter Zugeständisse und klarer Absprachen regelmäßig nicht erhört worden waren, übten schließlich gemeinsam mit den Regierungen einiger Mitgliedstaaten Druck aus, damit die Datenschutzreform initiiert werden konnte. Eine abnehmende Anzahl an Terroranschlägen, die wachsende Sorge vor dem Missbrauch personenbezogener Daten seitens privatwirtschaftlicher als auch staatlicher Akteure und zunehmende Proteste gegen Überwachungsmaßnahmen gaben den Forderungen der Datenschutzbefürworter zusätzlichen Auftrieb.

Nachdem die Entstehungsbedingungen der Datenschutz-Reform im Rahmen der Kontextanalyse untersucht wurden, widmete sich der letzte inhaltliche Abschnitt 4, die *Akteurs- und Prozessanalyse*, schließlich der Beantwortung der *zentralen, ersten Forschungsfrage*, indem die Fäden der Kontextanalyse mit den politischen Auseinandersetzungen um die DSGVO zusammengeführt wurden.

Für jede der drei Phasen, in die ich in den Aushandlungsprozess der DSGVO unterteilt hatte (*1. Orientierungsphase, 2. Entwurfsphase, 3. Konfliktphase*), untersuchte ich für jede der Advocacy-Koalitionen deren *Überzeugungssystem*, *Zusammensetzung* und *Ressourcen*. Die sich daran anschließende Prozessanalyse hatte zum Ziel, das Wirken der einzelnen Advocacy-Koalitionen im Hinblick auf das Zustandekommen der DSGVO zu analysieren, indem die kausalen Wirkungsmechanismen und Wechselbeziehungen zwischen den verschiedenen Akteuren, ihren Aktivitäten, den externen Systemereignissen und langfristig wichtigen politischen Gelegenheitsstrukturen herausgearbeitet wurden. Die Akteurs- und Prozessanalyse baute überwiegend auf der quantitativen und qualitativen Analyse von

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Primärdokumenten der am Aushandlungsprozess der DSGVO beteiligten Akteure. Ergänzend wurde auch auf Sekundärliteratur und die Medienberichterstattung zurückgegriffen.

Die Akteursanalyse zur *Orientierungsphase*, die von der Initiierung der Datenschutz-Reform im Mai 2009 bis zur Veröffentlichung der Konsultationsergebnisse im November 2010 andauerte, bestätigte auf Basis einer Cluster-Analyse der quantitativ erfassten Positionen aller Subsystem-Akteure die Existenz der zwei konkurrienden Lager in Form der Flexibilitätsbefürworter einerseits und der Datenschutzbefürworter andererseits. Aufgrund des Mangels an nicht-trivialen Kooperationsstrukturen zwischen den Akteuren handelte es sich dabei präziserweise um Advocacy-Communities. Da die Policy-Kernüberzeugung der Datenschutzbefürworter darin bestand, Datenschutz als Grundrecht anzusehen und weil die Akteure zugleich der Überzeugung waren, dass die Globalisierung und der technologische Wandel eine Bedrohung darstellten, wurden die bestehenden Datenschutzregelungen als unzureichend bewertet und eine Stärkung der datenschutzrechtlichen Vorgaben gefordert. Die Flexibilitätsbefürworter hingegen agierten auf Grundlage der Policy-Kernüberzeugung, dass staatliches Handeln möglichst gering ausfallen und der Privatwirtschaft ein möglichst großer Freiraum überlassen bleiben sollte. In der Globalisierung und im technologischen Wandel wurden eher Chancen statt Herausforderungen gesehen. Die Prinzipien bzw. Ziele der bestehenden Datenschuzregelungen wurden zwar unterstützt, doch wurden die bestehenden administrativen Bestimmungen zur Erreichung dieser Ziele als ineffektiv, schwerfällig und unflexibel kritisiert. Die Flexibilitätsbefürworter traten bei den Diskussionen um die Datenschutzreform deshalb für wirtschaftsfreundliche Erleichterungen ein und forderten insb. die Abschaffung der Meldepflicht, die Vereinfachung von Drittstaatentransfers und die Förderung von Selbstregulierungsmaßnahmen, die sie im Sinne einer wirtschaftsfreundlich verstandenen Rechenschaftspflicht zur Ersetzung konkreter gesetzlicher Bestimmungen vorschlugen.

Die Prozessanalyse zur Orientierungsphase machte deutlich, dass die nach der Ernennung Jacques Barrots zum neuen Kommissar für Justiz, Freiheit und Sicherheit 2008 begonnene eindeutige Positionierung zugunsten der Stärkung der Datenschutzregelungen weiteren Schwung erhielt. Zum einen wurde das Kommissariat für Justiz, Freiheit und Sicherheit auf Drängen der neuen Justizkommissarin aufgeteilt und das auf diese Weise neu entstandene Justizkommissariat erhielt die Federführung für die Datenschutz-Reform, sodass der Einfluss von sicherheits- bzw. innen-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

politisch motivierten Kommissionsmitgliedern wirksam zurückgedrängt wurde. Zum anderen übernahm mit Viviane Reding eine ausgesprochene Datenschutzbefürworterin den Posten der einflussreichen Justizkommissarin. Reding intensivierte die Bestrebungen ihres Amtsvorgängers und setzte sich klar für ein hohes Datenschutzniveau ein. Im Ergebnis sah das zum Ende der ersten Konsultationsphase veröffentlichte Konzeptpapier der Kommission durchweg die Stärkung der datenschutzrechtlichen Vorgaben vor. Gegenüber den datenverarbeitenden Akteuren aus der Privatwirtschaft wurde die weitere Harmonisierung der EU-weiten Regelungen, Erleichterungen bei Drittstaatentransfers, die Angleichung oder Abschaffung der Bestimmungen zur Meldepflicht und der europäischen Wirtschaft gegenüber zusätzlich die Angleichung der Wettbewerbsverhältnisse gegenüber ihren außereuropäischen Konkurrenten angekündigt. Im Hinblick auf die von den Flexibilitätsbefürwortern erwünschten verwaltungsrechtlichen Vereinfachungen und den Übergang zu einer wirtschaftsfreundlichen Rechenschaftspflicht stellte die Kommission klar, dass die Reform in jedem Fall nicht zu einer Reduktion der Verantwortung der Verarbeiter führen würde.

Ähnliche Ergebnisse zeigte auch die Analyse der *Entwurfsphase*, die von November 2010 bis zur Veröffentlichung des Legislativvorschlags der Kommission am 25. Januar 2012 dauerte. Im Rahmen der Akteursanalyse wurde zunächst deutlich, dass sich die Akteure weiterhin im Wesentlichen auf zwei konkurrierende Lager aufteilten. Neu war allerdings, dass eine kleine Gruppe von Akteuren, die ich als Kompromisswillige bezeichne, Positionen formulierte, die sich nicht klar den Datenschutz- oder Flexibilitätsbefürwortern zuordnen lassen. Eine praktische Relevanz hatte diese dritte Gruppe während des Aushandlungsprozesses jedoch nicht, da die politische Auseinandersetzung weiterhin zwischen den Datenschutz- und Flexibilitätsbefürwortern verlief. Zugleich intensivierten sich die Kooperationsstrukturen der Akteure beider Lager dahingehend, dass sich die Akteursstruktur sowohl der Datenschutz- als auch Flexibilitätsbefürworter von einer Advocacy-Community hin zu einer Advocacy-Koalition entwickelte. Als Kulminationspunkte der Datenschutzbefürworter wirkten die zivilgesellschaftliche Dachorganisation EDRi sowie die EU-Kommission bzw. das Justiz-GD und das Datenschutz-Referat. Auf Seiten der Flexibilitätsbefürworter schlossen sich mehrere wichtige Industrieverbände zum Ende der Entwurfsphase zur *Industry Coalition for Data Protection* (ICDP) zusammen. Das Überzeugungssystem der Datenschutzbefürworter blieb im Wesentlichen unverändert, wurde aber in entscheidenden Bereichen spezifiziert. So wurde nunmehr gefordert, dass eine wirksame Anhebung

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

des Datenschutzniveaus nur durch die Kombination aus der Intensivierung der Verarbeiterpflichten, der Stärkung der Betroffenenrechte und der Stärkung des Aufsichtsrahmens erreicht werden könne. Die Vorschläge aus dem Konzeptpapier der Kommission wurden durchgängig begrüßt bzw. deren weitere Stärkung gefordert. Das Überzeugungssystem der Flexibilitätsbefürworter blieb ebenfalls stabil. So wurde Datenschutz weiterhin weniger als Grundrecht, denn als vertrauensbildende Maßnahme aufgefasst. Aufgrund der Kommissionsäußerungen, die eine Anhebung des Datenschutzniveaus mit großer Sicherheit vermuten ließen, gingen die Flexibilitätsbefürworter dazu über, die wirtschaftliche und gesellschaftliche Bedeutung der Verarbeitung personenbezogener Daten hervorzuheben. Letztlich wurden alle verpflichtenden Bestandteile der Kommissionsankündigung abgelehnt. Stattdessen wurde entsprechend der Idee einer wirtschaftsfreundlichen Rechenschaftspflicht der Übergang zu Maßnahmen der Selbstregulierung in praktisch allen Bereichen des Datenschutzrechts gefordert. Mit diesen konträren Positionierungen kündigte sich also bereits im Jahr 2011, noch bevor das ordentliche Gesetzgebungsverfahren begonnen hatte, die spätere Verhärtung der Fronten zwischen Flexibilitäts- und Datenschutzbefürwortern an.

Die Prozessanalyse zur Entwurfsphase hat gezeigt, dass die Kommission im Vorfeld der Veröffentlichung des Datenschutz-Reformpakets Ziel massiven Lobbyings seitens privatwirtschaftlicher Akteure war. Abgesehen von der Verzögerung des Kommissionszeitplans hatte dieses Lobbying allerdings kaum Auswirkungen auf den Inhalt des DSGVO-Entwurfs der Kommission.[432] Stattdessen sah der Kommissionsvorschlag in nahezu allen Bereichen die Stärkung der datenschutzrechtlichen Vorgaben vor. Im Einzelnen betraf dies die Definition besonderer Kategorien personenbezogener Daten, den Grundsatz der Datenminimierung, die Einwilligung, den Datenschutz bei Kindern, Transparenzvorgaben und Informationspflichten des Verantwortlichen, die Modalitäten für die Wahrnehmung von Betroffenenrechten, das Recht auf Vergessenwerden, das Recht auf Datenübertragbarkeit, Automatisierte Entscheidungen und Profiling, Privacy by Design und by Default, die Dokumentationspflichten des Verantwortlichen, die Meldepflicht bei Datenschutzverletzungen, Datenschutzfolgenabschätzung, die Benennung eines betrieblichen Datenschutzbeauftragten, kollek-

432 Neben kleinren Änderungen im Bereich des Datenschutzes bei Kindern oder in den Profiling-Vorgaben war auf Druck der US-Regierung die später als Anti-Fisa-Klausel bezeichnete Passage aus dem Entwurf entfernt worden (vgl. auch Fn 333).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tive Rechtsbehelfe sowie Sanktionen und Geldbußen. Den Forderungen der Flexibilitätsbefürworter entsprachen dagegen lediglich die Abschaffung der Meldepflicht, die Vereinfachung von Drittstaatentransfers, die Beibehaltung der Definition personenbezogener Daten und Erleichterungen bei der Weiterverarbeitung für Zwecke, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind. Einige der Kommissionsvorschläge entsprachen zudem den Vorstellungen beider Seiten (Harmonisierung, Stärkung der Unabhängigkeit der Datenschutzaufsichtsbehörden, Einführung eines One-Stop-Shops zur Vereinfachung der Bürokratie, Ausweitung des räumlichen Anwendungsbereichs) und einige wenige entsprachen weder den Forderungen der Datenschutz- noch der Flexibilitätsbefürworter, beispielsweise die Vorgaben zum Europäischen Datenschutzausschuss (EDSA), der an die Stelle der Art. 29-Datenschutzgruppe treten sollte und die generelle Intention der Kommission, über einer Vielzahl an delegierten und Durchführungsrechtsakten mehr Macht bei sich zu bündeln sowie die Bestimmungen zu Verhaltensregeln und zu Zertifizierungen. Trotz des mit dem Kommissionsvorschlag auf inhaltlicher Ebene offensichtlich verfolgten Ziels der deutlichen Anhebung des Datenschutzniveaus ging die Kommission auf Abstand zu ihrer während der Konsultationsphasen verfolgten Strategie der Hervorhebung der Grundrechtsdimension des Datenschutzes. Stattdessen bemühte sie sich unter Rückgriff auf das Vertrauensargument darum, die Förderung von Wirtschaftswachstum und Wettbewerbsfähigkeit der EU durch die Stärkung und Harmonisierung der datenschutzrechtlichen Vorgaben als zwei Seiten einer Medaille zu präsentieren.

Das Handeln der Kommission lässt sich durch drei Faktoren erklären: *Erstens* demonstrierte die Akteurs- bzw. Cluster-Analyse, dass die Positionen von Kommission und Datenschutzbefürwortern größtenteils überlappend waren, sodass hier angesichts der relativ intensiven Kooperationsbemühungen zwischen Kommission und Zivilgesellschaft bzw. Datenschutzbehörden zumindest von einer gewissen Einflussnahme gesprochen werden kann. *Zweitens* zeigte sich, dass der ausschlaggebende Grund wohl in der Person von Justizkommissarin Reding gelegen hat. So war Reding bereits im Vorfeld der Datenschutzreform mit Äußerungen, die in Richtung des Vertrauensarguments gingen, aufgefallen. Zusammengenommen mit ihren Äußerungen zum Grundrechtscharakter des Datenschutzes kann davon ausgegangen werden, dass sie Grundrechtsschutz und Wirtschaftswachstum tatsächlich als zwei Seiten einer Medaille betrachtete und keinen wesentlichen Widerspruch darin sah. *Drittens* kann davon ausgegangen werden, dass das gegen die Kommission gerichtete Lobbying der datenver-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

arbeitenden Wirtschaft und die dabei zur Schau gestellte inhaltliche Generalablehnung und Verzerrung der Kommissionsposition trotz der dabei verwendeten vermeintlich kompromissorientierten Sprache, eher abschreckend auf die Kommission gewirkt haben müssen. Schließlich blieb Reding und ihrem Team nur ein eingeschränkter Handlungsspielraum: Entweder mussten sie entgegen der eigenen Überzeugungen eine Abschwächung des Datenschutzniveaus vornehmen, um den Forderung der datenverarbeitenden Wirtschaft zu entsprechen oder sie mussten einen Weg finden, den zur Stärkung des Datenschutzniveaus vorgesehenen Legislativvorschlag so zu rahmen, dass er mit möglichst wenig Widerstand und erfolgreich verabschiedet werden könnte. Angesichts der festen Überzeugung, das Datenschutzniveau stärken zu wollen, griff die Kommission unter Reding darauf zurück, Ihren Legislativvorschlag rhetorisch als eine Win-Win-Situation für Datenschützer als auch Datenverarbeiter zu bewerben.

Wie diese Strategie der Kommission zur Schaffung von Akzeptanz bei der datenverarbeitenden Wirtschaft scheiterte und wie es trotzdem zu einer erfolgreichen Verabschiedung der DSGVO kam, untersuchte ich im Rahmen der Konfliktphase, die sich von der Veröffentlichung des Kommissionsvorschlags Anfang 2012 bis zu dessen Verabschiedung am 27. April 2016 erstreckte. Hier zeigte sich, dass sowohl auf Seiten der Datenschutzbefürworter als auch bei den Flexibilitätsbefürwortern in Folge der Beteiligung weiterer Akteure jeweils zwei Flügel entstanden. Während die in der Entwurfsphase als Adovcacy Koalition identifizierten Datenschutzbefürworter weitgehend unverändert blieben und aufgrund ihrer starken Pro-Datenschutz-Forderungen als extreme Datenschutzbefürworter auftraten, bezog eine weitere Gruppe von Datenschutzbefürwortern, bestehend aus den Parlamenten einiger Mitgliedstaaten, dem Europäischen Wirtschafts- und Sozialausschuss und der Europäischen Grundrechteagentur, vergleichsweise gemäßigte datenschutzbefürwortende Positionen. Auf dieselbe Weise setzten sich auch die Flexibilitätsbefürworter aus einem extremen Lager, in dem überwiegend privatwirschaftliche Akteure versammelt waren und die mehrheitlich als Teile der Advocacy-Koalition fungierten sowie aus einem gemäßigten Lager zusammen. Dieses bestand vor allem aus Akteuren, die allenfalls teilweise als Mitglied einer Advocacy-Community bezeichnet werden können, darunter neben einigen privatwirtschaftlichen Akteuren insb. die Mehrzahl der EU-Mitgliedstaaten. Das Überzeugungssystem der Datenschutzbefürworter blieb gegenüber den vorangegangenen Phasen weitgehend unverändert. So wurde der Kommissionsvorschlag und dessen Inhalt als überfälliger Schritt in die richtige Richtung begrüßt. Kritik ern-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

tete die unzureichende Spezifizierung vieler der Kommissionsvorschläge und die Idee der Kommission, diese auf dem Wege von delegierten und Durchführungsrechtsakten zu konkretisieren. Daneben bedienten sich zunächst die Kommission und später auch der Parlamentsberichterstatter Jan Philipp Albrecht und zuletzt sogar einige der zivilgesellschaftlichen Akteure des Vertrauensarguments, um die vorgeschlagene Anhebung des Datenschutzniveaus gleichsam als Vorteil für die datenverarbeitende Wirtschaft darzustellen. Das Überzeugungssystem der Flexibilitätsbefürworter blieb ebenfalls weitgehend unverändert gegenüber den vorherigen Phasen. Neben der grundsätzlichen Begrüßung datenschutzrechtlicher Vorgaben und der Überarbeitung des bestehenden Rechtsrahmens gab es Kritik an nahezu allen verpflichtenden Kommissionsvorschlägen und die Forderung, diese durch Selbstregulierungsmaßnahmen zu ersetzen (siehe für eine abschließende, zusammenfassende Darstellung der Überzeugungssysteme der Datenschutz- und Flexibilitätsbefürworter Tabelle 5-1). Eine deutliche Veränderung erfuhr in diesem Zusammenhang der Tonfall der vorgebrachten Kritik. So trat die gegenüber dem Vertrauensargument zuvor entgegengebrachte Akzeptanz in den Hintergrund. Stattdessen malten große Teile der Flexibilitätsbefürworter im Laufe der Konfliktphase zunehmend Katastrophenszenarien aus, wonach die europäische Wirtschaft infolge der datenschutzrechtlichen Bestimmungen schweren Schaden nehmen würde. Auch in der Konfliktphase existierte eine dritte, überwiegend aus einigen mitgliedstaatlichen Regierungen bestehende Akteursgruppe. Da jeder der dieser Gruppe zurechenbaren Akteure größtenteils unabhängig voneinander agierte, fungierte sie zwar nicht als eigenständige Advocacy-Community oder -Koalition, dennoch wäre ihre Zuordnung zu den Datenschutz- oder Flexibilitätsbefürwortern unpassend. So hatten Mitgliedstaaten wie Frankreich, Polen, Ungarn und Österreich im Vergleich zu den übrigen Mitgliedstaaten datenschutzfreundlichere Positionen vertreten und mit Italien, Griechenland und Zypern waren unter ihnen auch drei Ratspräsidentschaften. Zudem spiegelte der final verabschiedete DSGVO-Kompromiss am ehesten die Position der zu dieser Gruppe zählenden Akteure. Insofern bezeichnete ich diese Akteursgruppe als *bedingte Datenschutzbefürworter*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Policy-Kern-überzeugungen	Datenschutzbefüworter	Flexibilitätsbefürworter
Problemwahr-nehmung	Technologischer Wandel und Globalisierung erschweren die Gewährleistung des Schutzes personenbezogener Daten. Gefährdung individueller Selbstbestimmung in Folge allgegenwärtiger und unsichtbarer Datenverarbeitung.	Technologischer Wandel und Globalisierung bergen wirtschaftliches und gesellschaftliches Potential. Gefährdung des Wirtschaftswachstums und der Entstehung innovativer und gesellschaftlich erwünschter Dienste in Folge zu strenger und zu spezifischer Vorschriften.
Grundlegende Wertepriorisierung	Datenschutz ist ein Grundrecht, das geschützt werden muss. Teils auch: Strengere Datenschutzstandards schaffen Vertrauen gegenüber Betreibenden datenverarbeitender Dienste und kommen damit sowohl der Wirtschaft als auch Grundrechten zugute.	Datenschutz als wichtiges Recht muss geschützt und in ein angemessenes Gleichgewicht mit konkurrierenden Rechten und (ökonomischen) Interessen gebracht werden. Teils auch: Datenschutz kann Vertrauen schaffen, aber die dadurch erzielten Profite kompensieren nicht die Kosten zur Einhaltung der strengeren Datenschutzvorschriften.
Grundlegende Zielvorstellungen	Das Recht auf Datenschutz muss durch verbindliche und strenge Vorschriften gestärkt werden.	Datenschutzvorschriften müssen den Datenverarbeitern Flexibilität für kontextsensitive Datenschutz-Maßnahmen einräumen.
Sekundärüberzeugungen	Für die verbindliche Festlegung der Stärkung von Betroffenenrechten, der Erhöhung der Verarbeiterpflichten, der Verbesserung der Datenschutzaufsicht und der Erhöhung des Sanktionsmaßes im Gesetzestext.	Für die Festlegung von Zielen im Gesetzestext während die Mittel zur Zielerreichung den Verarbeitern überlassen bleiben sollen.

Tabelle 5-1: Zusammenfassung der zentralen Elemente der Überzeugungssysteme der Datenschutz- und Flexibilitätsbefürworter (eigene Darstellung, inspiriert von Larsen et al. (2006, 217)).

Im Rahmen der Prozessanalyse zur Konfliktphase untersuchte ich schließlich das ordentliche Gesetzgebungsverfahren, in dessen Verlauf die DSGVO verabschiedet wurde. Die mit der Veröffentlichung des Legislativvorschlags der Kommission initiierte ordentliche Gesetzgebungsverfahren initiiert wurde, musste der Vorschlag fortan von Parlament und Ministerrat begutachtet und verhandelt werden, während der Kommission die Vermittlerrolle zukam. Dementsprechend verlagerte sich das Lobbying in Richtung des EP und des Ministerrats. Nachdem der federführende LIBE-Ausschuss des Parlaments unter der Führung des grünen Abgeordneten Jan Philipp Albrecht, der der Advocacy-Koalition der extremen Datenschutzbefürworter zuzuordnen ist, den Entwurf der Parlamentsposition Anfang Januar 2013 präsentierte, eskalierte der Konflikt im Parlament. Albrecht und der LIBE-Ausschuss vertraten in dem Dokument Positionen, die dem extremen Flügel der Datenschutzbefürworter zuzuordnen sind und eine weitere deutliche Anhebung des von der Kommission vorgestellten Datenschutzniveaus

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

vorsahen. Die Positionen der Flexbilisierungsbefürworter fanden hingegen praktisch keine Berücksichtigung. Der Hintergrund dieses Handelns war, dass Albrecht und sein Team erwarteten, dass der Ministerrat die deutliche Absenkung des Datenschutzniveaus vorschlagen würde. Die Verabschiedung einer besonders datenschutzfreundlichen Parlamentsposition sollte bei der finalen interinstitutionellen Kompromissbildung den Erhalt von aus Datenschutzperspektive akzeptablen Kompromissen gewährleisten und der Absenkung des Schutzniveaus des Kommissionsvorschlags vorbeugen. Die von Albrecht vorgesehene Stärkung des Schutzniveaus stieß nur auf Seiten der zivilgesellschaftlichen Datenschützer auf Unterstützung. Kritik entlud sich hingegen nicht nur seitens der privatwirtschaftlichen Akteure, sondern auch seitens der mitberatenden Parlamentsausschüsse und Fraktionen. Letztlich verspielte Albrecht auf diese Weise die Unterstützung der liberalen Fraktion, die im Hinblick auf die Abstimmung im Parlament das Zünglein an der Waage darstellte, weil der linke Block im Europaparlament alleine nicht auf ausreichend viele Stimmen kam. Im Ergebnis kam es für mehrere Monate zu einer Pattsituation im Europäischen Parlament, die den Aushandlungsprozess lahmlegte.

Obwohl angesichts der Ergebnisse der Kontextanalyse zu erwarten war, dass sich der konservative Block im EP mit der Unterstützung der liberalen Fraktion bei der Verabschiedung eines niedrigeren Datenschutzniveaus durchsetzen würde, kam es aufgrund der Snowden-Enthüllungen anders. Diese wirkten als externer Schock und führten zum Erstarken des Überzeugungssystems der Datenschutzbefürworter. Albrecht und Reding agierten in dieser Phase mit der Unterstützung der übrigen Datenschutzbefürworter und der Medienberichterstattung als Policy Entrepreneure und forcierten strenge Datenschutzregeln erfolgreich als europäische Antwort auf die weltweite Massenüberwachung der Five Eyes. Albrecht überarbeitete seinen Berichtsvorschlag zugleich, indem er den Positionen der Flexibilitätsbefürworter in einigen Bereichen leicht entgegenkam. Der Entwurf, der trotz dieser Anpassungen weiterhin ein höheres Schutzniveau als der Kommissionsvorschlag vorsah, wurde Ende 2013 zunächst im LIBE-Ausschuss und Anfang 2014 im Europäischen Parlament mit großer Mehrheit angenommen.

Die große Mehrheit der Mitgliedstaaten, allen voran Deutschland und Großbritannien, hatten derweil kein Interesse an der Anhebung des Datenschutzniveaus. Viele der mitgliedstaatlichen Regierungen standen den Positionen der Flexibilitätsbefürworter nahe und befürchteten wirtschaftliche Nachteile in Folge von als zu streng wahrgenommenen Datenschutzgeset-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

zen. Weil die Befürwortung eines niedrigeren Schutzniveaus zur Hochphase der Snowden-Enthüllungen aufgrund der befürchteten öffentlichen Empörung taktisch wenig sinnvoll gewesen wäre, zögerte der Ministerrat die Verabschiedung seiner Position erfolgreich hinaus. Die Ministerratsposition, die eine deutliche Absenkung des von der Kommission vorgeschlagenen Schutzniveaus vorsah, wurde Mitte 2015 verabschiedet. In den darauffolgenden Trilog-Verhandlungen konnte sich der Ministerrat zwar bei den meisten Forderungen durchsetzen, doch stellte der finale DSGVO-Kompromiss eine Erhöhung des Schutzniveaus im Vergleich zur DS-RL dar. Dies lag vor allem daran, dass sich Parlament und Kommission bei den Betroffenenrechten und dem Sanktionsniveau durchsetzten. Demgegenüber nahmen die Datenschutzbefürworter deutliche Abschwächungen im Bereich der Verarbeiterpflichten und im Hinblick auf nationale Freiräume in Kauf. Dass es in der Folge nicht zu einer weiteren Absenkung des Schutzniveaus kam, lag an einer Mischung aus verschiedenen Faktoren. *Erstens* hatte die Mehrheit der EU-Mitgliedstaaten trotz der anfänglichen Ablehnung der Reform und trotz der Befürwortung eines niedrigeren Schutzniveaus grundsätzlich Interesse an einem neuen Datenschutzrahmen, da der Status Quo der DS-RL als unzureichend gewertet wurde. *Zweitens* wurde die DSGVO zusammen mit der JI-Richtlinie als Reformpaket verhandelt und diente der sekundärrechtlichen Umsetzung der mit dem Inkrafttreten des Lissabon-Vertrags geänderten EU-Bestimmungen auf Ebene des Primärrechts, in deren Folge die EU-GRCh verbindlich und der Schutz personenbezogener Daten zum EU-Grundrecht geworden war. *Drittens* spielte die Einbettung der DSGVO in die digitale Binnenmarktstrategie der EU eine wichtige Rolle. Datenschutz konnte dabei als vertrauensbildende Maßnahme für wirtschaftliches Wachstum dargestellt werden. *Viertens* stellten sich der vor allem von Deutschland und Großbritannien forcierten deutlichen Senkung des Schutzniveaus andere Mitgliedstaaten wie Frankreich, Italien, Polen und Luxemburg erfolgreich entgegen. *Fünftens* zogen Parlament und Kommission, anders als in vorherigen datenschutzpolitischen Auseinandersetzungen, bis zuletzt am gleichen Strang und konnten gemeinsam mit den bedingten Datenschutzbefürwortern im Ministerrat weitere Absenkungen des Schutzniveaus verhindern. Insofern stellte die Einigung im Trilog im Sinne des ACF einen ausgehandelten Kompromiss dar, der angesichts einer unerwünschten politischen Pattsituation erreicht werden konnte.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

5.2 Kritische Reflexion der Ergebnisse und Forschungsdesiderate

Im Folgenden möchte ich die Ergebnisse der Arbeit kritisch reflektieren und dabei auch auf weiteren Forschungsbedarf hinweisen.

Aus mehreren Gründen stellt diese Arbeit einen Mehrwert für die politikwissenschaftliche Untersuchung der EU-Datenschutzpolitik dar. *Erstens* stellt die empirische Analyse der Positionen aller Datenschutz-Subsystem-Akteure auf Grundlage eines umfassenden Dokumentenkorpusses und einer intersubjektiv nachvollziehbaren Erhebungsweise[433] die erste Analyse dieser Art im Bereich der Datenschutzpolitik dar. Sie geht damit zum einen über andere politikwissenschaftliche Analysen (Hildén 2019; Jančiūtė 2018; Laurer und Seidl 2021), die eine geringe Dokumentenanzahl analysieren, hinaus. Zum anderen geht sie aber auch über die nicht aus der Wissenschaftscommunity stammenden Analysen, wie die von LobbyPlag, hinaus und kann künftigen Forschenden als umfassende empirische Grundlage dienen.

Zweitens werden die Ergebnisse bestehender politikwissenschaftlicher Analysen durch diese Arbeit mittels einer umfassenden empirischen Untersuchung zum Teil bestätigt und zum Teil entkräftet. Bestätigt wird beispielsweise die Rolle von Akteurskoalitionen bei der Gestaltung der EU-Datenschutzpolitik, die schon in Newman (2008b) angeführt wurde oder die von Jančiūtė (2018) benannten Gründe für die Verabschiedung der DSGVO. Doch während das Wirken der Akteurskoalition der Datenschutzbefürworter bei Newman quasi-alleinige Erklärungskraft für das Zustandekommen der DS-RL beansprucht, zeigen meine Ergebnisse, dass auch institutionelle und vertragsrechtliche Faktoren eine wichtige Rolle spielten. Die Analyse der Entwicklung der datenschutzpolitischen Konfliktlinien im Laufe der Geschichte der Datenschutzpolitik und dessen, wie diese letztlich in den politischen Ergebnissen der DSGVO kulminierten, geht schließlich über die Erklärung von Jančiūtė Fokus hinaus, in der auf vier ausgewählte Problembereiche fokussiert wird. Anders als Laurer und Seidl (2021) zeigt die vorliegende Arbeit zudem auf, dass nicht allein die Datenschutzgruppe, sondern die Koalition der Datenschutzbefürworter bestehend aus Teilen der EU-Kommission, des EU-Parlamens und bedeutsame Figuren wie Roman Herzog es gemeinsam mit der Datenschutzgruppe vermochten, den

433 Die entsprechenden Excel-Daten, der Codierbogen, die SPSS-Auswertungen und sonstige relevante Dokumente lassen sich unter dem folgenden Link erreichen: https://owncloud.fraunhofer.de/index.php/s/XveVMq9FU4vuZZE

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Schutz personenbezogener Daten als Grundrecht in die GRCh einzuführen. Ebenfalls abweichend von Laurer und Seidl zeigte ich auf, dass die Mehrzahl der im Ministerrat vertretenen Regierungen und auch die Bundesregierung in Folge der Snowden-Enthüllungen taktierten und abwarteten, um letztlich eine Absenkung des Datenschutzniveaus zu bewirken. Davon, dass die deutsche Bundesregierung ihre ablehnende Haltung gegenüber der DSGVO nach den Snowden-Enthüllungen aufgegeben hätte, kann also keine Rede sein.

Drittens wird durch die Analyse der Entstehung der DSGVO mittels des Advocacy Coalition Frameworks (ACF) die Erklärungskraft dieses Ansatzes am Fall eines zentralen EU-Gesetzgebungsverfahrens getestet. Die Ergebnisse bestätigen die Erklärungskraft mehrerer Elemente des ACF: Advocacy Koalitionen bzw. Communities spielten im Laufe der Geschichte der Datenschutzpolitik und bei der Entstehung der DSGVO eine entscheidende Rolle; relativ stabile Parameter, langfristig wichtige politische Gelegenheitsstrukturen und externe Systemereignisse bildeten den Rahmen, innerhalb dessen das Akteurshandeln stattfand; Policy-Wandel in Gestalt der Verabschiedung der DSGVO konnte vor dem Hintergrund einer unerwünschten politischen Pattsituation in Folge eines externen Schocks und eines ausgehandelten Kompromisses stattfinden. Allerdings sind auch einige Fragen offengeblieben. Konzeptionell schwierig zu greifen war beispielsweise das Agieren der als bedingte Datenschutzbefürworter bezeichneten Akteursgruppe. Ganz offensichtlich handelte es sich dabei nicht um eine Advocacy Koalition, doch selbst die Bezeichnung als Advocacy Community hielt ich für unpassend. Für einige der Akteure wäre eventuell der Begriff des Policy Brokers zutreffend gewesen, doch stieß ich bei dem Versuch, hier mehr in die Tiefe zu gehen an die Grenzen der dokumentenanalytischen Vorgehensweise. Agierte etwa die luxemburgische Regierung während ihrer Ratspräsidentschaft tatsächlich als neutraler Policy Broker oder schlugen sie sich vielleicht doch auf die Seite der Datenschutzbefürworter? Aufgrund der gewählten dokumentenanalytischen Vorgehensweise muss auch offenbleiben, ob und inwiefern der externe Schock durch die Snowden-Enthüllungen bei den konservativen und liberalen Parlamentarierinnen zu einem nachhaltigen internen Schock geführt haben könnte, bei dem die eigenen Überzeugungssysteme hinterfragt wurden. Wollten die MdEPs tatsächlich nur einmalig als EP ein möglichst geschlossenes politisches Zeichen setzen oder wurden die eigenen Überzeugungen hinsichtlich Massenüberwachung und der Kontrolle dieser womöglich auch nachhaltig verändert? Die Ergebnisse deuten m. E. in diese Richtung – eine verlässliche Antwort bedarf

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

allerdings weiterer Forschung. Kritisch könnte auch der kaum vorhandene, sehr kursorische Einblick in die Trilog-Verhandlungen gewertet werden. Allerdings steht das System der informellen Trilog-Verhandlungen ohnehin seit geraumer Zeit in der Kritik, intransparent zu sein. Bemängelt wird etwa, dass keine der auf den Trilog-Sitzungen diskutierten Dokumente öffentlich zugänglich sind (Proust 2015) und die Berichterstattung gegenüber den Parlamentsausschüssen unzureichend sei (Brandsma 2019). Auch im Hinblick auf die Einigung zur DSGVO im Trilog herrschte weitgehende Intransparenz. Während Berichterstatter Albrecht den LIBE-Ausschuss mehrfach mündlich knapp über den Stand der Verhandlungen informierte (LIBE-Ausschuss 2015c, 2015a, 2015b), war auf Seiten des Ministerrats nahezu keine Transparenz gegeben (so etwa, lediglich: Council of the EU 2015). Angesichts meiner Untersuchungsmethode werte ich diese Intransparenz jedoch nicht als weiter problematisch, da sich die wichtigsten Positionierungen bereits ausreichend klar aus dem Politik-Prozess ergeben hatten. Alle relevanten Argumente für und gegen jede der Bestimmungen der DSGVO wurden im Vorfeld, aber auch im Nachgang der Verabschiedung in aller Ausführlichkeit genannt und in der vorliegenden Arbeit diskutiert.

Viertens hat sich die Kombination aus ACF und Prozessanalyse als sinnvoll erwiesen. Die Ausführungen zur Beantwortung der übergeordneten Forschungsfrage bauen durch die Kombination aus dokumentenanalytisch fundierter Überprüfung von Präferenzerzielung (hoop test) sowohl auf großer Gewissheit als auch weisen sie durch die umfassende Analyse und historische Einbettung des Akteurshandelns eine hohe Trennschärfe auf, sodass sie die Bedingungen des doubly decisive-Tests erfüllen. Sicherlich hätte der Rückgriff auf Interviews im Rahmen der Prozessanalyse die Aussagekraft der Ergebnisse weiter steigern können – dadurch, dass bestehende interviewbasierte Analysen zur Entstehung der DSGVO meine dokumentenanalytischen Schlüsse stützten, relativiert sich diese Schwäche allerdings etwas.

Schließlich besitzt die vorliegende Untersuchung, *fünftens*, auch vielfache Anknüpfungspunkte an die laufende politikwissenschaftliche EU-(Integrations-)Forschung. Beispielsweise liefert die Analyse des erfolgreichen Agierens der Datenschutzbefürworter während der Snowden-Enthüllungen Belege dafür, dass Outside-Lobbying, also die Hinwendung an die Öffentlichkeit zum Zwecke der Ausübung politischen Drucks, dann sinnvoll ist, wenn das Anliegen auf öffentliche Unterstützung bauen kann (De Bruycker und Beyers 2019). Ein weiterer Anknüpfungspunkt könnte die Erkenntnis sein, dass trotz der besonderen Bedingungen, die die Verabschiedung der

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

DSGVO ermöglichten, die Mitgliedstaaten weitgehende nationale Freiräume durchsetzen konnten. Für künftige Forschung dürfte dies verdeutlichen, dass selbst in einer EU mit einem seit dem Lissabon-Vertrag gestärkten Europäischen Parlament, weiterhin und selbst angesichts bedeutsamer externer Schocks keine Politik ohne die Mitgliedstaaten zu machen ist.

Auch für den Datenschutzdiskurs bietet die Arbeit mehrere Erkenntnisse. *Erstens* verdeutlichen meine Ergebnisse, dass dem Wirken von Akteurskoalitionen eine große Bedeutung in der Gestaltung der EU-Datenschutzpolitik zugekommen ist. Die DSGVO wäre nicht entstanden, wenn Akteure aus Kommission, Parlament, Datenschutzbehörden und Zivilgesellschaft nicht gemeinsam und auf unterschiedlichen Ebenen unter Rückgriff auf ihre jeweiligen Ressourcen für deren Initiierung und Verabschiedung eingetreten wären. In diesem Zusammenhang sei auch das Einwirken auf verschiedene Venues hervorgehoben: So war das Agieren der Datenschutzbefürworter während der Entstehung der Grundrechtecharta, die zum damaligen Zeitpunkt noch keine Verbindlichkeit innehatte, später entscheidend bei Initiierung, inhaltlicher Gestaltung sowie Verabschiedung der DSGVO.

Zweitens zeigt meine Analyse, dass das Vertrauensargument als eine Art letzte Bastion der Datenschutzbefürworter eine ambivalente Entwicklung durchgemacht hat. Einerseits scheint das Vertrauensargument der einzige gemeinsame Nenner zwischen einigen Datenschutz- und Flexibilitätsbefürwortern zu sein: So konnte sich letztlich nicht nur die Verabschiedung der DS-RL, sondern auch der DSGVO auf dieses Argument stützen. Andererseits scheint es, als würde es sich dabei eher um ein Verlegenheitsargument beider Seiten handeln. Dabei gehe ich durchaus davon aus, dass Akteure wie Bangemann, Reding oder einige mitgliedstaatliche Regierungen überzeugt von dem Argument sind. Ich stelle vielmehr infrage, ob Vertrauen bei der Nutzung datenverarbeitender Dienste tatsächlich eine so große Rolle zukommt, wie seitens der Vertreter dieses Arguments angenommen wird, oder ob nicht andere Gründe wie der Preis oder die Zugänglichkeit eines Dienstes, sozialer Druck bzw. Netzwerkeffekte usw. wichtiger als Vertrauen sind. Dies stellt m. E. die zentrale Forschungslücke aus Datenschutzperspektive dar, die es zu erforschen gilt. Sollte sich meine Vermutung als zutreffend herausstellen, müsste die Argumentationsstrategie für künftige politische Auseinandersetzungen überdacht und angepasst werden.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

5.3 Ausblick oder: Quo Vadis Datenschutz?

Die Ergebnisse machen deutlich, dass die EU-Datenschutzpolitik spätestens seit den 1990er-Jahren von einer unversöhnlich wirkenden Konfliktlinie durchzogen ist: Auf der einen Seite eine Koalition, die ein grundrechtsorientiertes Datenschutzverständnis hat und für hohe regulatorische Datenschutzstandards plädiert. Auf der anderen Seite eine Koalition, die zwar den Wert von Datenschutzregelungen nicht vollkommen abspricht, aber vor allem aus einer wirtschaftspolitischen, gewinnorientierten Perspektive auf das Thema blickt und für Selbstregulierung und damit gegen staatliche Regulierung eintritt. Dass Datenschutzregelungen auf EU-Ebene verabschiedet werden konnten, ist sowohl dem Agieren der Datenschutzbefürworter als auch den institutionellen Rahmenbedingungen und verfassungsrechtlichen Gegebenheiten der EU und damit letztlich der politischen Agenda der EU geschuldet. Dies bedeutet, dass ohne die notwendigen Rahmenbedingungen keine relevanten datenschutzrechtlichen Veränderungen in der EU herbeizuführen sind. Dies zeigt sich insbesondere daran, dass die Inhalte der DSGVO trotz der Kritik vonseiten beider Koalitionen und trotz intensiver datenpolitischer Regulierungsbemühungen mit Data Act, Data Governance Act, usw. unangetastet bleiben. Gleichzeitig liegt das einzige politische Vorhaben, das eine Weiterentwicklung datenschutzrechtlicher Bestimmungen zum Gegenstand hatte, die ePrivacy-Verordnung, seit Jahren auf Eis. In anderen Worten: Die DSGVO bildet den gegenwärtigen EU-Datenschutzstandard an dem derzeit weder vonseiten der Datenschutz- noch der Flexibilitätsbefürworter gerüttelt werden kann. Es liegt also gewissermaßen erneut eine Pattsituation vor.

Damit verknüpft ist auch die Frage der Europäisierung bzw. EU-weiten Harmonisierung des Datenschutzrechts: In einer Situation der Dauerkrise, in der sich die Europäische Union befindet, können sich die Befürworter von weitgehenden EU-Regelungen gegenüber den Befürwortern nationaler Eigenwege, die oftmals zugleich Befürworter von Selbstregulierung sind, nicht durchsetzen. Selbst im historisch (für den Bereich Datenschutz) einzigartigen Fall der Verabschiedung der DSGVO, bei dem mehrere Faktoren die Verabschiedung eines vergleichsweise hohen Datenschutzniveaus begünstigten, setzten die Mitgliedstaaten drastische nationale Freiräume durch, die eine Bedrohung für die mit der DSGVO verfolgte Harmonisierung darstellen.

Zugleich scheinen sich viele Mitgliedstaaten und die Europäische Union insgesamt zunehmend darin einig zu sein, dass Datenschutzrechte als

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

ein Kernbestandteil des Europäischen Selbstverständnisses anzusehen sind. Gegenüber der noch vor rund drei Jahrzehnten praktizierten Ablehnung EU-weiter Regelungen zum Datenschutz durch die EU-Kommission unter Verweis auf ihre mangelnde Kompetenz in solchen Fragen, stellt dies eine enorme Veränderung der EU-Politik dar. Diese Etablierung von Datenschutzrechten als EU-Grundrecht spiegelt somit auch den langsamen Wandel der EU von einer Wirtschafts- hin zu einer politischen und damit auch Grundrechtsunion wider.

Und dennoch handelt es sich bei der EU-Datenschutzpolitik auch immer um eine politische Zwittererscheinung: In dem Maße, wie sie durch grundrechtsorientierte Datenschutzbefürworter geprägt wurde, ist sie Ausdruck eines Verständnisses, das den Schutz persönlicher Grundrechte anstrebt. Zugleich ist sie ebenso Ausdruck des wirtschaftspolitischen Verständnisses von Akteuren, die allenfalls möglichst flexible staatliche Regelungen befürworten, Daten als ein Wirtschaftsgut betrachten und Datenschutz als Mittel sehen, um den möglichst ungehinderten Fluss von (personenbezogenen) Daten zu gewährleisten. Wie die Setzung dieser Prioritäten die Datenschutzpolitik beeinflusst lässt sich seit 2022 an der geplanten Aufweichung der Einwilligung im Bereich des Europäischen Gesundheitsdatenraums beobachten. Dabei soll künftig auf die Einholung der individuellen Einwilligung verzichtet werden, was den historischen Datenschutzgrundsätzen zwar zuwiderläuft, aufgrund des öffentlichen Interesses an Gesundheit jedoch in Kauf genommen wird.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Literaturverzeichnis

Abbate, Janet. 1999. *Inventing the Internet*. Cambridge, Mass: MIT Press.

ACCIS IVZW. 2009. „Position Paper on the Consultation on the legal framework for the fundamental right to protection of personal data". 18.

———. 2011. „Consultation on the Commission's comprehensive approach on personal data protection in the European Union". 66.

———. 2012a. „ACCIS position paper on the EC's proposed data protection Regulation (COM (2012) 11 final) ("the draft Regulation")". 208.

———. 2012b. „Proposal for amendments to the proposed review of the EU's Data Protection Legal Framework". 157.

Ackeret, Markus. 2019. „Seit der Krim-Annexion geht ein Riss durch den Europarat. Nun soll Russland sein Stimmrecht zurückerhalten | NZZ". *Neue Zürcher Zeitung*. https://www.nzz.ch/international/seit-der-krim-annexion-geht-ein-riss-durch-den-europarat-nun-soll-russland-sein-stimmrecht-zurueckerhalten-ld.1482712 (4. Januar 2020).

ACT u. a. 2009. „Joint Response by ACT, AER, AIG, EACA, EGTA, EPC, FEDMA, IAB Europe and the WFA to the European Commission Consultation on the Data Protection Directive". 19.

———. 2011. „A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION RESPONSE from the ASSOCIATION of COMMERCIAL TELEVISION in EUROPE (ACT)". 67.

ADR. 2012. *Stellungnahme des Ausschusses der Regionen: „Datenschutzpaket"*. Brüssel: Ausschuss der Regionen (ADR).

AK Vorrat. 2006. „Demonstration in Berlin am 17. Juni 2006 - Freiheit statt Angst!" *www.wiki.vorratsdatenspeicherung.de*. http://wiki.vorratsdatenspeicherung.de/Demonstration_in_Berlin_am_17._Juni_2006 (8. Juli 2019).

———. 2008a. „Stoppt die Vorratsdatenspeicherung! - Demo ‚Freiheit statt Angst 2008'". *www.vorratsdatenspeicherung.de*. http://www.vorratsdatenspeicherung.de/content/view/242/144/lang,de (8. Juli 2019).

———. 2008b. „Stoppt die Vorratsdatenspeicherung! - ‚Freedom not Fear': Worldwide protests against surveillance (12-10-2008)". *www.vorratsdatenspeicherung.de*. http://www.vorratsdatenspeicherung.de/content/view/267/79/lang,en/ (8. Juli 2019).

———. 2008c. „Stoppt die Vorratsdatenspeicherung! - Historische Sammel-Verfassungsbeschwerde gegen Vorratsdatenspeicherung eingereicht (29.02.2008)". *www.vorratsdatenspeicherung.de*. http://www.vorratsdatenspeicherung.de/content/view/202/55/ (9. Juli 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Albrecht, Jan Philipp. 2013a. *Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)(COM(2012)0011 - C7-0025/2012 - 2012/0011(COD))*. Europäisches Parlament.

———. 2013b. *EP draftsperson Jan Philipp Albrecht presents his legislative report*. European Parliament. https://web.archive.org/web/20130122083220/http://www.greenmediabox.eu/archive/2013/01/09/data-protection/ (2. März 2020).

———. 2013c. „EU-Datenschutz: Ministerrat muss beim Datenschutz liefern". *GrünDigital. Das grüne Blog zur Netzpolitik*. https://www.gruen-digital.de/2013/03/eu-datenschutz-ministerrat-muss-beim-datenschutz-liefern/ (10. Mai 2018).

———. 2013d. ****I Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))*.

———. 2013e. *Jan auf Veranstaltungen zum Thema Datenschutz*.

———. 2013f. *Jans Treffen mit Interessenvertretern: Aktualisierte Transparenzliste*.

———. 2013g. „Lobbyism and the EU data protection reform". https://www.janalbrecht.eu/themen/datenschutz-digitalisierung-netzpolitik/lobbyism-and-the-eu-data-protection-reform.html (2. September 2014).

———. 2013h. „Lobbyismus zur EU-Datenschutzreform". *Jan Philipp Albrecht MdEP*. https://www.janalbrecht.eu/themen/datenschutz-digitalisierung-netzpolitik/artikel/2013-05-23-lobbyismus-zur-eu-datenschutzreform.html (1. Juli 2017).

———. 2015. „No EU Data Protection Standard Below the Level of 1995". *European Data Protection Law Review* 1(1): 3–4.

———. 2016a. „Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung". *Computer und Recht* 32(2): 88–98.

———. 2016b. *Empfehlung für die zweite Lesung zu dem Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (05419/1/2016 – C8–0140/2016 – 2012/0011(COD))*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

Albrecht, Jan Philipp, und Florian Jotzo. 2016. *Das neue Datenschutzrecht der EU: Grundlagen | Gesetzgebungsverfahren | Synopse*. 1. Aufl. Baden-Baden: Nomos.

Albrecht, Jan Philipp, Katarzyna Szymielewicz, und Kirsten Fiedler. 2012. *The Grand EU Data Protection Reform: A Latest Battle Report by Some Key Actors from Brussels*. 29c3. /v/29c3-5274-en-grand_eu_data_protection_reform_h264 (29. Februar 2020).

Albright, Elizabeth A. 2011. „Policy change and learning in response to extreme flood events in Hungary: an advocacy coalition approach". *Policy studies journal* 39(3): 485–511.

Alvaro, Alexander. 2013. „ALVARO: Grüne Datenschutzvorschläge: #fail". *portal liberal*. https://www.liberale.de/content/alvaro-gruene-datenschutzvorschlaege-fail (23. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Alvaro, Alexander Nuno. 2005. *Bericht über die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss des Rates über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus (8958/2004 – C6-0198/2004 – 2004/0813(CNS))*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

———. 2015. *Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005)0438 – C6-0293/2005 – 2005/0182(COD))*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

Aly, Götz, und Karl Heinz Roth. 2000. *Die restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsoziaismus.* 3. Auflage, Überarbeitete Neuausgabe. Frankfurt am Main: FISCHER Taschenbuch.

AmCham EU. 2010. „AmCham EU response to the Commission consultation on protection of personal data". 21.

———. 2011. „AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union". 68.

———. 2012. „AmCham EU - Position Paper on Data Protection". 170.

———. 2013. „AmCham EU Proposed Amendments on the General Data Protection Regulation". 225.

———. 2019. „One Year after the GDPR: A Milestone in a Long Journey". *AmCham EU*. https://www.amchameu.eu/news/one-year-after-gdpr-milestone-long-journey (11. April 2021).

Appelbaum, Jacob, und Laura Poitras. 2013. „Als Zielobjekt markiert. Der Enthüller Edward Snowden über die geheime Macht der NSA". *DER SPIEGEL* (28/2013): 22–24.

Art. 29 DS-Gruppe. 1999. *Empfehlung 4/99 Über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog*. Brüssel: Artikel 29-Datenschutzgruppe.

Article 29 WP. 2001. „Letter to Mr. Göran Persson, Acting President of the Council of the European Union". http://www.statewatch.org/news/2001/jun/07Rodota.pdf (15. Juni 2019).

———. 2009. *The Article 29 Working Party held its 72nd plenary session in Brussels on October 12 and 13, 2009*. Brussels: Article 29 Data Protection Working Party. Press Release.

———. 2012. *Opinion 01/2012 on the Data Protection Reform Proposals*. Article 29 Data Protection Working Party. 162.

———. 2013. *Press Release*. Brussels: Article 29 Data Protection Working Party.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Article 29 WP und WPPJ. 2009. *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. Brussels: Article 29 Data Protection Working Party and Working Party on Police and Justice. Press Release.

Artikel 29-Datenschutzgruppe. 2000. *Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 KOM(2000)385*. Artikel 29-Datenschutzgruppe. Stellungnahme.

———. 2002. *Fünfter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Europäischen Union und in Drittländern - Berichtsjahr 2000 - Teil 1.*

———. 2006. *Stellungnahme 8/2006 zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation*. Brüssel: Artikel 29-Datenschutzgruppe.

———. 2007. *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten"*. Brüssel: Artikel 29-Datenschutzgruppe.

———. 2008. *Stellungnahme 2/2008 zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)*. Brüssel: Artikel 29-Datenschutzgruppe.

———. 2011. *Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung*. Brüssel: Artikel 29-Datenschutzgruppe.

———. 2014. *Erklärung zu den Ergebnissen der letzten Tagung des Rates „Justiz und Inneres" (JI)*. Brüssel: Artikel 29-Datenschutzgruppe.

Bahrke, Jeannine. 2011. Nr. 17 *Über den öffentlichen Umgang mit privaten Daten am Beispiel Facebook*. Berlin: Universitätsverlag der TU Berlin.

Bainbridge, David u. a. 1994. *An evaluation of the financial impact of the proposed European Data Protection Directive - Final Report*. Aston Business School, Tilburg University, Leiden University. Report to the European Commission.

———. 1996. *EC Data Protection Directive*. London, Dublin, Edinburgh: Butterworths.

Balzli, Beat, Jürgen Dahlkamp, Frank Dohmen, und Klaus-Peter Kerbusk. 2008. „Affären: Projekt ‚Clipper'". *Der Spiegel* 22. http://www.spiegel.de/spiegel/print/d-57119353.html (16. Februar 2019).

Bandelow, Nils C. 1999. *Lernende Politik: Advocacy-Koalitionen und politischer Wandel am Beispiel der Gentechnologiepolitik*. Berlin: Ed. Sigma.

———. 2009. „Politisches Lernen: Begriff und Ansätze". In *Lehrbuch der Politikfeldanalyse 2.0*, hrsg. Klaus Schubert und Nils C. Bandelow. München: De Gruyter Oldenbourg.

———. 2015. „Advocacy Coalition Framework". In *Handbuch Policy-Forschung*, hrsg. Georg Wenzelburger und Reimut Zohlnhöfer. Wiesbaden: Springer Fachmedien Wiesbaden, 305–24.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bandelow, Nils C., Stefan Kundolf, und Kirstin Lindloff. 2014. *Agenda Setting für eine nachhaltige EU-Verkehrspolitik: Akteurskonstellationen, Machtverhältnisse und Erfolgsstrategien*. Berlin: ed. sigma.

Bangemann, Martin. 1994. *Europe and the global information society: Recommendations of the high-level group on the information society to the Corfu European Council (Bangemann group)*. Brussels, Luxembourg: Office for Official Publications of the European Communities.

Barlow, John Perry. 1996. „A Declaration of the Independence of Cyberspace". https://projects.eff.org/~barlow/Declaration-Final.html.

Barrot, Jacques. 2008. *Rede vor dem Europäischen Parlament*. Strasburg: Europäisches Parlament.

Battcock, Rupert. 1995. „Data Protection: Where Next?" *International Journal of Law and Information Technology* 3(2): 156–78.

Baumann, Max Otto. 2013. „Datenschutz im Web 2.0". In *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter*, hrsg. Ulrike Ackermann. Frankfurt: Humanities Online, 15–52.

Bayerl, Alfons. 1979. *Report drawn up on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of technical developments in data processing*. European Parliament - Committee on Legal Affairs (JURI).

BBC News. 2008. „Up to 1.7m People's Data Missing". http://news.bbc.co.uk/2/hi/uk_news/politics/7667507.stm (9. Juli 2019).

BDIU. 2012. „Stellungnahme des Bundesverbandes Deutscher Inkasso-Unternehmen e.V. (BDIU) zum Vorschlag der Europäischen Kommission zu einer EU-Datenschutz-Grundverordnung (KOM(2012) 11/4 vom 25. Januar 2012)". 160.

BDZV, und VDZ. 2011. „Mitteilung der Europäischen Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen KOM(2010) 609 endgültig v. 4.11.2010". 127.

Beach, Derek, und Rasmus Brun Pedersen. 2013. *Process-tracing methods: Foundations and guidelines*. University of Michigan Press. http://books.google.com/books?hl=en&lr=&id=5iulb1MInPcC&oi=fnd&pg=PR5&dq=%225.+Causal+Inference+and%22+%22methods+or+traditional+case+study+methodology%3F%E2%80%9D+We+were%22+%22and+workshops%3B+in+particular,+we+thank+the+participants+on+panels%22+%22Beach+and+Rasmus+Brun%22+&ots=Q4DNJ_69_K&sig=o0I8xzaTa59h_OoDKoXZMU7qbrI (27. Januar 2017).

Beckedahl, Markus. 2015. „EU-Datenschutzreform: Datenschlussverkauf in Brüssel". *netzpolitik.org*. https://netzpolitik.org/2015/eu-datenschutzreform-datenschlussverkauf-in-bruessel/ (30. Oktober 2019).

Becker, Peter, und Olaf Leisse. 2005. *Die Zukunft Europas: der Konvent zur Zukunft der Europäischen Union*. 1. Aufl. Wiesbaden: Verlag für Sozialwissenschaften.

Becker, Sven. 2015. „Lobbyismus: ‚Danke für Deine Zeit'". *Spiegel Online* 11. https://www.spiegel.de/spiegel/print/d-132212233.html (30. Oktober 2019).

Behrens, Maria. 2003. „Quantitative und qualitative Methoden der Politikfeldanalyse". In *Lehrbuch der Politikfeldanalyse*, hrsg. Klaus Schubert und Nils C. Bandelow. München, Wien: De Gruyter Oldenbourg, 203–34.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Belfiore, Rosanna. 2013. „The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters". In *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, hrsg. Stefano Ruggeri. Berlin, Heidelberg: Springer Berlin Heidelberg, 355–70. http://link.springer.com/10.1007/978-3-642-32012-5_24 (5. April 2017).

Bendrath, Ralf. 2007a. *Privacy Self-Regulation and the Changing Role of the State: From Public Law to Social and Technical Mechanisms of Governance*. Bremen: University of Bremen, Jacobs University Bremen. Working Papers. http://edoc.vifapol.de/opus/volltexte/2013/4100/ (20. Juli 2016).

———. 2007b. „The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection". In *Myriam Dunn / Sai Felicia Krishna-Hensel / Victor Mauer, eds. (2007): The Resurgence of the State: Trends and Processes in Cyberspace Governance, Aldershot: Ashgate*, http://edoc.vifapol.de/opus/volltexte/2008/617/pdf/sfbgov_wp14_en.pdf (9. Mai 2014).

———. 2009. „Stockholm-Programm: Debatte über innere Sicherheit in der EU spitzt sich zu | netzpolitik.org". *Netzpolitik.org*. https://netzpolitik.org/2009/stockholm-programm-debatte-ueber-innere-sicherheit-in-der-eu-spitzt-sich-zu/ (11. November 2016).

Bennett, Andrew, und Jeffrey T. Checkel. 2014. *Process tracing: From metaphor to analytic tool*.

———. 2015a. *Process tracing: From metaphor to analytic tool*. Cambridge: Cambridge University Press.

———. 2015b. „Process tracing: from philosophical roots to best practices". In *Process tracing: From metaphor to analytic tool*, hrsg. Andrew Bennett und Jeffrey T. Checkel. Cambridge: Cambridge University Press, 3–38.

Bennett, Colin J. 2008. *The privacy advocates: resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, Colin J., und Charles D. Raab. 1997. „The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response". *The Information Society* 13(3): 245–64.

———. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd and updated ed. Aufl. Cambridge Mass.: MIT Press.

Benz, Arthur, Susanne Lütz, Uwe Schimank, und Georg Simonis, hrsg. 2007. *Handbuch Governance: theoretische Grundlagen und empirische Anwendungsfelder*. 1. Auflage. Wiesbaden: VS, Verlag für Sozialwissenschaften.

Bergemann, Benjamin. 2013a. „De Maizière: "Reform des Datenschutzrechts notwendig"". *netzpolitik.org*. https://netzpolitik.org/2013/de-maiziere-reform-des-datenschutzrechts-notwendig/ (28. Oktober 2019).

———. 2013b. „EU-Ministerrat reitet auf Trojanischen Pferden Richtung Datenschutzreform". *Netzpolitik.org*. https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/ (10. September 2014).

———. 2013c. „EU-Parlament: Erster Ausschuss pfuscht bei Datenschutzreform – weitere Fails verhindern!" *netzpolitik.org*. https://netzpolitik.org/2013/erster-ausschuss-pfuscht-bei-datenschutzreform-weitere-fails-verhindern/ (5. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2013d. „Realitätscheck: Merkels janusköpfige Datenschutzrhetorik vs. Verhandlungsstand im EU-Ministerrat". *netzpolitik.org*. https://netzpolitik.org/2013/realitatscheck-merkels-januskopfige-datenschutzrhetorik-vs-verhandlungsstand-im-eu-ministerrat/ (28. Oktober 2019).

———. 2014. „Die Reform des europäischen Datenschutzes – ...und der Einfluss der Snowden-Enthüllungen –". Bachelorarbeit. Freie Universität Berlin: Fachbereich Politik- und Sozialwissenschaften - Otto-Suhr-Institut für Politikwissenschaft.

Bergius, Michael. 2011. „Viviane Reding: EU fordert deutsche Vorratsdatenspeicherung | Datenschutz - Frankfurter Rundschau". *Frankfurter Rundschau*. https://web.archive.org/web/20120127014650/http://www.fr-online.de/datenschutz/viviane-reding-eu-fordert-deutsche-vorratsdatenspeicherung,1472644,8604588.html (5. Oktober 2019).

Berliner DSB. 2012. „The Reform of the EU Data Protection framework – Building trust in a digital and global world". 182.

Berlinghoff, Marcel. 2013a. „Computerisierung und Privatheit – Historische Perspektiven". *Aus Politik und Zeitgeschichte, Beilage zur Wochenzeitung 'Das Parlament'* 63. Jahrgang(15-16/2013): 14–19.

———. 2013b. „‚Totalerfassung' im ‚Computerstaat'. Computer und Privatheit in den 1970er und 1980er Jahren". In *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter*, hrsg. Ulrike Ackermann. Frankfurt: Humanities Online, 93–110.

Berlinguer, Luigi, Juan Fernando López Aguilar, und Carlo Casini. 2009. *Entschliessungsantrag eingereicht im Anschluss an Erklärungen des Rates und der Kommission gemäß Artikel 110 Absatz 2 der Geschäftsordnung zu der Mitteilung der Kommission an das Europäische Parlament und den Rat – Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger – das Programm von Stockholm*. Brüssel: Rechtsausschuss, Ausschuss für konstitutionelle Fragen, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

Bernet, David. 2015. *Democracy - Im Rausch der Daten*. Deutschland: INDI Film GmbHm, Atmosfilm.

BEUC. 2008. *Europäische Gruppenlkage: Zehn Goldene Regeln*. Brussels: The European Consumers' Organisation.

———. 2009. „EU General Data Protection Framework - BEUC answer to the consultation". 24.

———. 2011. „A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION". 71.

———. 2012. „Data Protection Proposal for a Regulation BEUC Position Paper". 172.

———. 2013. „Our Members". *www.beuc.eu*. https://www.beuc.eu/beuc-network/our-members (7. Februar 2020).

Beuth, Patrick. 2011. „Facebook: Innenminister Friedrich bringt Datenschützer auf die Palme". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2011-09/friedrich-facebook-datenschutz/komplettansicht (25. August 2019).

———. 2012. „Privacy by default: Wie Facebook gegen Datenschutz lobbyiert". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2012-11/facebook-lobby-datenschutzverordnung/komplettansicht (25. August 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2013a. „EU-Datenschutz: ‚Lobbyplag suggeriert, Abgeordnete seien Spielball der Industrie'". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2013-02/interview-alexander-alvaro-datenschutzverordnung/komplettansicht (25. August 2019).

———. 2013b. „Europäischer Datenschutztag: Mit Dollars gegen mehr Datenschutz". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2013-01/datenschutztag-datenschutzverordnung-lobbyismus/komplettansicht (25. August 2019).

———. 2013c. „EU-Verordnung: Datenschutzreform sollte auch IP-Adressen schützen". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2013-01/datenschutz-eu-parlament (25. August 2019).

———. 2015a. „EU-Datenschutzverordnung: Bundesregierung hofiert Lobbyisten". *Die Zeit*. http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag (13. März 2015).

———. 2015b. „Metadaten: Die geheime Vorratsdatenspeicherung der USA". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2015-04/metadaten-geheime-vorratsdatenspeicherung-usa-dea (12. Januar 2020).

Beyer, Daniela, Graeme Boushey, und Christian Breunig. 2015. „Die Punctuated-Equilibrium-Theorie". In *Handbuch Policy-Forschung*, hrsg. Georg Wenzelburger und Reimut Zohlnhöfer. Wiesbaden: Springer Fachmedien Wiesbaden, 355–78.

Beyers, Jan, und Bart Kerremans. 2012. „Domestic Embeddedness and the Dynamics of Multilevel Venue Shopping in Four EU Member States". *Governance* 25(2): 263–90.

BfDI. 2011. „Konsultation zur Mitteilung der Europäischen Kommission ‚Gesamtkonzept für den Datenschutz in der EU'". 87.

———. 2015. *Andrea Voßhoff: Die EU Kommission muss jetzt Klartext reden!* http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/01_AndreaVosshoffDieEUKommissionMussJetztKlartextReden.html (12. Februar 2015).

———. 2016. „Rote Linien eingehalten? Zur Verabschiedung der Datenschutz-Grundverordnung". *DANA - Datenschutz Nachrichten* (2): 68–69.

Bieber, Christoph. 2012. „Datenschutz als politisches Thema". In *Datenschutz: Grundlagen, Entwicklungen und Kontroversen*, Bundeszentrale für politische Bildung, Schriftenreihe, hrsg. Jan-Hinrik Schmidt und Thilo Weichert. Bonn, 34–44.

Biermann, Kai. 2013a. „Datenschutzreform: Mehr Datenschutz in der EU dank Snowden". *Die Zeit*. http://www.zeit.de/digital/datenschutz/2013-10/eu-datenschutzreform-abstimmung-libe/komplettansicht (30. November 2016).

———. 2013b. „Lobbyismus: Gegen die Copy-Paste-Politik". *Die Zeit*. http://www.zeit.de/digital/datenschutz/2013-02/lobbyplag-datenschutz/komplettansicht (18. April 2017).

Bignami, Francesca. 2005. „Transgovernmental networks vs. democracy: The case of the European information privacy network". *Michigan Journal of International Law* 26: 807.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bigo, Didier u. a. 2011. *Towards a New EU Legal Framework for Data Protection and Privacy*. Brussels: European Parliament - Directorate-General for Internal Policies (DG IPOL): Policy Department C - Citizens' Rights and Constitutional Affairs. Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) - Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits (C&C).

Birnbaum, Robert, und Frank Jansen. 2012. „Friedrich: ‚Ein Verbot der NPD wird nicht leicht werden'". *Der Tagesspiegel*. https://www.tagesspiegel.de/politik/bundesinnenminister-friedrich-ein-verbot-der-npd-wird-nicht-leicht-werden/6067864.html (22. Oktober 2019).

BITKOM. 2009. „Stellungnahme: Online-Konsultation der EU-Kommission zum Review der Richtlinie 95/46/EG". 25.

———. 2011. „Response on the consultation for the purpose of reforming of Directive 95/46/EC". 72.

———. 2012a. „Amendments to the General Data Protection Regulation". 189.

———. 2012b. *Stellungnahme zum Vorschlag der EU-Kommission für eine EU-DatenschutzGrundverordnung vom 25.01.2012*.

Bitkom. 2015. *Big Data und europäisches Datenschutzrecht*.

———. 2020. *GDPR Review – Recommendations for the EU's Data Protection Framework*. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM). https://www.bitkom.org/Recommendations-EU-Data-Protection-Framework (20. November 2020).

BITKOM e. V. 2015. „Bitkom zur EU-Datenschutzverordnung". *Bitkom e.V.* https://www.bitkom.org/Presse/Presseinformation/Bitkom-zur-EU-Datenschutzverordnung.html (12. April 2019).

Blatter, Joachim, und Markus Haverland. 2012. *Designing Case Studies: Explanatory Approaches in Small-N Research*. London: Palgrave Macmillan UK. http://link.springer.com/10.1057/9781137016669 (13. Januar 2017).

Blatter, Joachim, Phil C. Langer, und Claudius Wagemann. 2018. *Qualitative Methoden in der Politikwissenschaft*. Wiesbaden: Springer Fachmedien Wiesbaden. http://link.springer.com/10.1007/978-3-658-14955-0 (13. November 2019).

Blum, Sonja, und Klaus Schubert. 2011. *Politikfeldanalyse*. 2. Wiesbaden: VS-Verl.

BMI. 2013. „EU-Justizkommissarin trifft Friedrich". *Bundesministerium des Innern, für Bau und Heimat*. http://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2013/03/jirat_datenschutz.html?nn=9390260 (25. Oktober 2019).

BMWi und BMF. 2019. *Blockchain-Strategie der Bundesregierung: Wir stellen die Weichen für die Token-Ökonomie*. Bundesministerium für Wirtschaft und Energie (BMWi), Bundesministerium der Finanzen (BMF). https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjLjuTYgvbvAhXqgf0HHZx5D4MQFjAAegQIBxAD&url=https%3A%2F%2Fwww.bmwi.de%2FRedaktion%2FDE%2FPublikationen%2FDigitale-Welt%2Fblockchain-strategie.pdf%3F__blob%3DpublicationFile%26v%3D8&usg=AOvVaw2xd3eSJsXFM0659ATsrI-Q (20. November 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bock, Tim. 2017. „5 Ways to Deal with Missing Data in Cluster Analysis". *Displayr*. https://www.displayr.com/5-ways-deal-missing-data-cluster-analysis/ (19. August 2019).

Boehm, Franziska. 2012. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/978-3-642-22392-1 (29. Mai 2019).

BoF, EDRi, und PI. 2013. „The Brussels Privacy Declaration". https://web.archive.org/web/20130127015852/http://www.brusselsdeclaration.net/ (13. Februar 2018).

Borowsky, Martin. 2010. „Die Grundrechtecharta als normatives Fundament der Europäischen Union". In *Die Europäische Union nach dem Vertrag von Lissabon*, hrsg. Olaf Leisse. Wiesbaden: VS, Verlag für Sozialwissenschaften, 147–59.

Bortz, Jürgen, und Christof Schuster. 2010. *Statistik für Human- und Sozialwissenschaftler*. 7. Aufl. Berlin Heidelberg: Springer.

Bradwell, Peter. 2013. „The Independent View: The Battle for Privacy in the EU and How the Liberal Democrats Can Help". *Liberal Democrat Voice*. https://www.libdemvoice.org/the-independent-view-the-battle-for-privacy-in-the-eu-and-how-the-liberal-democrats-can-help-33882.html (22. Oktober 2019).

Brandsma, Gijs Jan. 2019. „Transparency of EU Informal Trilogues through Public Feedback in the European Parliament: Promise Unfulfilled". *Journal of European Public Policy* 26(10): 1464–83.

Breuer, Theresa, und Ole Reißmann. 2013. „10.000 Menschen protestieren gegen NSA-Überwachung". *Spiegel Online*. http://www.spiegel.de/politik/deutschland/10-000-menschen-protestieren-gegen-nsa-ueberwachung-a-913513.html (25. Februar 2015).

Brewster, Thomas. 2012. „Facebook Lobbying Brussels In Earnest On EU Data Privacy Proposals". *Silicon UK*. https://www.silicon.co.uk/workspace/facebook-lobbying-eu-data-privacy-98645 (4. März 2020).

Brewster, Tom. 2012. „Justice Committee Tells EU To Rethink Data Protection Proposals | TechWeekEurope UK". *Techweek Europe*. https://web.archive.org/web/20130120210404/http://www.techweekeurope.co.uk/news/justice-committee-eu-data-protection-98022 (23. Oktober 2019).

Breyer, Patrick. 2011. „Stellungnahme". 121.

Briegleb, Volker. 2013. „Selbstregulierung von Social Networks gescheitert". *Heise Online*. https://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html (12. Februar 2018).

Brooks, Eleanor. 2018. „Using the Advocacy Coalition Framework to Understand EU Pharmaceutical Policy". *European Journal of Public Health* 28(suppl_3): 11–14.

Brummer, Klaus. 2008. *Der Europarat: eine Einführung*. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss.

BSA. 2009. „BSA Response to the Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data". 26.

———. 2011. „Views of the Business Software Alliance on the Commission's Data Protection Strategy". 74.

———. 2012. *BSA Position on the European Commission's Draft General Data Protection Regulation*. Business Software Association (BSA).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Bundesnetzagentur. 2009. *Unterrichtung durch die Bundesregierung: Tätigkeitsbericht 2008/2009 der Bundesnetzagentur – Telekommunikation mit Sondergutachten der Monopolkommission – Telekommunikation 2009: Klaren Wettbewerbskurs halten*. Deutscher Bundestag - 17. Wahlperiode.

Bunyan, Tony. 2002. „Was wird aus den Verkehrsdaten? Konflikte um EU-Regelungen | CILIP Institut und Zeitschrift". *CILIP - Bürgerrechte & Polizei* (071). https://www.cilip.de/2002/02/25/was-wird-aus-den-verkehrsdaten-konflikte-um-eu-regelungen/ (1. Juni 2019).

———. 2003. *The story of Tampere: an undemocratic process excluding civil society*. Statewatch. Statewatch briefing.

———. 2006. *EU data protection in police and judicial cooperation matters: Rights of suspects and defendants under attack by law enforcement demands*. Statewatch. http://www.statewatch.org/news/2006/oct/eu-dp.pdf (17. Juni 2019).

———. 2008. *The Shape of Things to Come - EU Future report - Analysis*. London: Statewatch.

Burkert, Herbert. 1988. „Die Konvention des Europarates zum Datenschutz". *Computer und Recht (CR)* 4: 751–58.

Burn-Murdoch, John. 2013. „Europe Deadlocked over Data Protection Reform". *The Guardian*. http://www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu (24. November 2015).

Burri, Mira, und Rahel Schär. 2016. „The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy". *Journal of Information Policy* 6: 479–511.

Busch, Andreas. 2012a. „Die Regulierung transatlantischer Datenströme". In *Politik und die Regulierung von Information*, Politische Vierteljahresschrift Sonderheft 46, hrsg. Andreas Busch und Jeanette Hofmann. Baden-Baden: Nomos, 408–40.

———. 2012b. „Freiheits- und Bürgerrechte nach 9/11". In *Die Welt nach 9/11. Auswirkungen des Terrorismus auf Staatenwelt und Gesellschaft*, Sonderheft der Zeitschrift für Außen- und Sicherheitspolitik, Sonderheft 2/2011, hrsg. Thomas Jäger. Wiesbaden: VS Verlag für Sozialwissenschaften/Springer Fachmedien, 861–81.

Busch, Heiner. 1996. „EUROPOL – Eigenständiger Organismus mit Zukunft". *CILIP* (053). https://www.cilip.de/1996/02/24/europol-eigenstaendiger-organismus-mit-zukunft/ (1. Mai 2019).

———. 2002. „Überwachung auf industriellem Niveau – Echelon und das Versagen des Europäischen Parlaments". *CILIP - Bürgerrechte & Polizei* (071). https://www.cilip.de/2002/02/25/ueberwachung-auf-industriellem-niveau-echelon-und-das-versagen-des-europaeischen-parlaments/ (12. Juni 2019).

Butler, Declan. 2013. „When Google got flu wrong". *Nature* 494(7436): 155–56.

Buzan, Barry, Ole Waever, und Jaap de Wilde. 1998. *Security: a new framework for analysis*. Boulder, Colo: Lynne Rienner Pub.

BVerfG. 1983. (BVerfGE 65, 1 - Volkszählung) *Urteil vom 15.12.1983*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2008. „Eilantrag in Sachen ‚Vorratsdatenspeicherung' teilweise erfolgreich: Pressemitteilung Nr. 37/2008 vom 19. März 2008". *www.bundesverfassungsgericht.de*. https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-037.html (9. Juli 2019).

Cáceres, Javier. 2013. „Internetkonzerne schreiben bei Datenschutzregeln mit". *Süddeutsche.de*. http://www.sueddeutsche.de/digital/lobby-einfluss-auf-neue-eu-verordnung-internetkonzerne-schreiben-bei-datenschutzregeln-mit-1.1596560 (2. September 2014).

Caiani, Manuela, und Paolo Graziano. 2018. „Europeanisation and Social Movements: The Case of the Stop TTIP Campaign". *European Journal of Political Research* 57(4): 1031–55.

Cairney, Paul, und Nikolaos Zahariadis. 2016. „Multiple Streams Approach: A Flexible Metaphor Presents an Opportunity to Operationalize Agenda Setting Processes". In *Handbook of Public Policy Agenda Setting*, hrsg. Nikolaos Zahariadis. Edward Elgar Publishing, 87–105. http://www.elgaronline.com/view/9781784715915.xml (22. Mai 2018).

Campbell, Duncan. 2001. „Echelon Chronology". *Telepolis*. http://www.heise.de/tp/artikel/7/7795/ (27. Januar 2015).

Cappato, Marco. 2001. *Zweiter Bericht betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM(2000) 385 – C5-0439/2000 – 2000/0189(COD))*. Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten - Europäisches Parlament.

———. 2002. *Empfehlung für die zweite Lesung betreffend den Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (15396/2/2001 - C5-0035/2002 - 2000/0189(COD))*. Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten - Europäisches Parlament.

———. 2004. *Bericht über den Ersten Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG) (KOM(2003) 265 – C5-0375/2003 – 2003/2153(INI))*. Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten - Europäisches Parlament.

Cappato, Marco, und Ilka Schröder. 2001. *Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM(2000) 385 – C5-0439/2000 – 2000/0189(COD))*. Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten; Ausschuss für Industrie Außenhandel, Forschung und Energie - Europäisches Parlament.

CAST e.V. 2017. „CAST-Workshop: Recht und IT-Sicherheit". *www.cast-forum.de*. https://cast-forum.de/workshops/programm/235 (20. November 2019).

Christ, Sebastian, und Axel Hildebrand. 2009. „Bahn-Spitzelaffäre: Alle gegen Mehdorn". *Stern.de*. https://www.stern.de/wirtschaft/news/bahn-spitzelaffaere-alle-gegen-mehdorn-3425232.html (16. Februar 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Civil Rights Organisations. 2014. *Civil Rights Organisations Letter to the Greek Presidency of the Council of the European Union*.

Clark, Liat. 2013a. „MEP's strict amendments to EU data protection worry tech industry (Wired UK)". *Wired*. https://web.archive.org/web/20160507225044/http://www.wired.co.uk/news/archive/2013-01/09/eu-data-protection-debate/viewall (8. Oktober 2019).

———. 2013b. „US data privacy advocates head to Brussels in show of support (Wired UK)". *Wired*. https://web.archive.org/web/20130208062146/http://www.wired.co.uk/news/archive/2013-01/22/us-eu-data-protection-advocates (23. Oktober 2019).

Coen, David, und J. J. Richardson, hrsg. 2009. *Lobbying the European Union: institutions, actors, and issues*. Oxford ; New York: Oxford University Press.

Collier, David. 2011. „Understanding Process Tracing". *PS: Political Science & Politics* 44(04): 823–30.

COM. 1990. *Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. Draft Resolution of the Representatives of the Governments of the Member States of the European Communities meeting within the Council. Commission Declaration on the application to the institutions and other bodies of the European Communities of the principles contained in the Council Directive concerning the protection of individuals in relation to the processing of personal data. Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks. Recommendation of a Council Decision on the opening of negotiations with a view to the sccession of the European Communities to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data. Proposal for a Council Decision in the field of information security*. http://aei.pitt.edu/3768/ (2. Juni 2019).

———. 1992. *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Brussels: Commission of the European Communities.

———. 1995. *Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 189 B (2) of the EC Treaty: Council common position of 20 February 1995 on the proposal for a Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels: Commission of the European Communities. http://aei.pitt.edu/13838/1/sec_%2895%29_303_final.pdf (22. Mai 2019).

———. 2020a. *On the European democracy action plan*. Brussels: European Commission. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions.

———. 2020b. *White Paper: On Artificial Intelligence - A European approach to excellence and trust*. Brussels: European Commission.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Comi, Lara. 2013. *Opinion of the Committee on the Internal Market and Consumer Protection (IMCO) on the GDPR*. European Parliament - Committee on the Internal Market and Consumer Protection (IMCO).

Comité des Sages. 1996. *For a Europe of Civic and Social Rights: Brussels, October 1995 - February 1996*. Luxemburg: Office for Official Publications of the European Communities.

Commission of the European Communities. 1972. *The European Community and Data Processing - Government Development Aids Permitted*. Brussels: Commission of the European Communities. Information.

———. 1973. *Community Policy on Data Processing (Communication of the Commission to the Counci)*. Brussels. http://aei.pitt.edu/6337/1/6337.pdf.

———. 1976. *A Four-Year Programme for the Development of Informatics in the Community (Submitted to the Council by the Commission)*. Brussels: Commission of the European Communities. Communication of the Commission to the Council.

———. 1981. *Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individual rights with regard to the automatic processing of personal data*. Brussels. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31981H0679&from=EN.

———. 1982. *Community Data-Processing Policy: Report on the Status of Community Programmes at 31 May 1982*. Brussels: Commission of the European Communities. Communication of the Commission to the Council.

———. 1990. *Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security*. Brussels: Commission of the European Communities. http://aei.pitt.edu/3768/1/3768.pdf.

———. 2003. *Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)*. Brussels: Commission of the European Communities.

Computerwoche. 1990. „Datenschutz zwischen BDSG-Novelle und EG-Richtlinie: Wirtschaft fürchtet Nachteile durch verschärften Datenschutz". http://www.computerwoche.de/a/wirtschaft-fuerchtet-nachteile-durch-verschaerften-datenschutz,1149120 (19. Juli 2016).

Conference of European Data Protection Authorities. 2006. *Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. Brussels.

Corporate Europe Observatory. 2005. „Bulldozing REACH - the industry offensive to crush EU chemicals regulation". *corporateeurope.org*. http://archive.corporateeurope.org/lobbycracy/BulldozingREACH.html (10. September 2019).

Council. 2008. *Press Release 2877th Council Meeting - Transport, Telecommunications and Energy*. Luxembourg: Council of the European Union.

———. 2009. *Review of the Regulatory Framework for Electronic Communications Networks and Services*. Brussels: Council of the European Union.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Council of Europe. 1973. *Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Private Sector*. Council of Europe - Committee of Ministers. Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

———. 1974. *Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector*. Council of Europe - Committee of Ministers. Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

———. 1981. *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 (1. August 2016).

———. 1987. *Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector*. Council of Europe - Committee of Ministers.

———. 2019. „Chart of Signatures and Ratifications of Treaty 108 - Status as of 23/04/2019". *Council of Europe: Treaty Office*. https://www.coe.int/en/web/conventions/full-list (23. April 2019).

Council of Ministers. 2007. *Press Release 2835th Council Meeting Transport, Telecommunications and Energy Brussels, 29-30 November/3 December 2007*. Brussels: Council of the European Union.

———. 2014. *Press Release: 3298th Council Meeting (Justice and Home Affairs) Brussels, 3 and 4 March 2014*. Brussels: Council of the European Union.

Council of the EU. 2013a. *Press Release: 3260th Council Meeting (Justice and Home Affairs) in Luxembourg, 7/8 October 2013*. Luxembourg: Council of the European Union.

———. 2013b. *Press Release: 3279th Council Meeting (Justice and Home Affairs), Brussels, 5 and 6 December 2013*. Brussels: Council of the European Union.

———. 2015. *Preparation for trilogue*. Brussels: Council of the European Union.

———. 2016. *Position of the Council at First Reading with a View to the Adoption of ARegulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) - Statement of the Council's Reasons – Adopted by the Council on 8 April 2016*. Brussels: Council of the European Union.

Council of the European Communities. 1991. *Working Party on Economic Questions (Data Protection) Meeting on 25 February 1991*. Brussels: Council of the European Communities. Outcome of Proceedings.

Council of the European Union. 2013. *The Council of the European Union, 1952-2012 60 Years of Law and Decision-Making*. Brussels: European Council.

Council Presidency. 2009. *Review of the Regulatory Framework for Electronic Communications Networks and Services - Analyses of the Compromise Text with a View to Agreement*. Brussels: Council of the European Union.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2012. *Note from the Presidency to DAPIX - Revised GDPR Art 10-27*. Brussels: Council of the European Union.

———. 2013. *Note from the Presidency to DAPIX - Revised Version of the GDPR*. Brussels: Council of the European Union.

Cousté, Pierre Bernard. 1974. *Mündliche Anfrage Nr. 193/73 mit Aussprache: Schutz der Privatsphäre der Bürger der Gemeinschaft*. Brüssel.

Cox, James. 2012. *Canada and the Five Eyes Intelligence Community*. Canada Defence and Foreign Affairs Institute and Canadian International Council. http://opencanada.org/wp-content/uploads/2012/12/SSWG-Paper-James-Cox-December-2012.pdf.pdf (19. Januar 2015).

CPDP. 2014. *CPDP 2014: EU Data Protection Reform: State Of Play*. Brüssel. https://www.youtube.com/watch?v=kl8an9Myrek (28. Oktober 2019).

———. 2015. *CPDP 2015: EU data protection reform: Have we found the right balance ...* Brussels. https://www.youtube.com/watch?v=wPHsz9Y6SZM (26. Oktober 2019).

———. 2019. „CPDP2020 Computers, Privacy & Data Protection • Organisation". *https://www.cpdpconferences.org/*. https://www.cpdpconferences.org/organisation (20. November 2019).

Craig, Terence, und Mary E. Ludloff. 2011. *Privacy and Big Data*. Beijing: O'Reilly Media, Inc.

Culnan, Mary J. 1997. „Self-Regulation on the Electronic Frontier: Implications for Public Policy". In *Privacy and self-regulation in the information age*, Washington, D.C: U.S. Dept. of Commerce, National Telecommunications and Information Administration. https://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age (11. Februar 2019).

Culnan, Mary J., und Robert J. Bies. 2003. „Consumer Privacy: Balancing Economic and Justice Considerations". *Journal of Social Issues* 59(2): 323–42.

Daimer, Stephanie. 2008. „Grosser Dissens, grosser Konsens: Die EU-Dienstleistungsrichtlinie-Ein typischer Fall der EU-Gesetzgebung?" Universität Mannheim.

DAPIX. 2012. *Summary of Discussions of the DAPIX Meeting on 23-24 February 2012*. Brussels: Council of the European Union.

Das Erste. 2013. *Bericht aus Berlin - Sommerinterview mit Angela Merkel | Video | ARD Mediathek*. /daserste/player/Y3JpZDovL2Rhc2Vyc3RlLmRlL2JlcmljaHQgYXVzIGJlcmxpbi9lYWY5ZDQ5YS1kODY3LTQ4ZjktYTMwMi1lYTBjZjBjZjBiNzQ/bericht-aus-berlin-sommerinterview-mit-angela-merkel (27. Oktober 2019).

Das Europäische Parlament und der Rat der Europäischen Union. 1997. Nr. L 24 ABl. EG vom 30.01.1998 *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation*.

———. 2001. L 8 *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2002. Nr. L 201 ABl. EG vom 31.07.2002 *Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:de:HTML (29. Juli 2015).

Datenschutzkommission. 2010. „Mitteilung der Kommission an das Europäische Parlament und den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Gesamtkonzept für den Datenschutz in der Europäischen Union". 84.

Datenspeicherung.de. 2007. „Forsa-Meinungsumfrage zur Sicherheitspolitik [3. Update]". *Daten-Speicherung.de - minimum data, maximum privacy*. https://www.daten-speicherung.de/index.php/forsa-meinungsumfrage-zur-sicherheitspolitik/ (9. Juli 2019).

Dawidowicz, Ricardo. 2014. „Class Action Lawsuits in Europe: A Comparative and Economic Analysis". In *Law and Economics in Europe: Foundations and Applications*, Economic Analysis of Law in European Legal Scholarship, hrsg. Klaus Mathis. Dordrecht: Springer Netherlands, 231–52. https://doi.org/10.1007/978-94-007-7110-9_10 (9. Januar 2019).

DDV. 2012. „Stellungnahme zum Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung (KOM (2012) 11 endgültig)". 161.

De Bruycker, Iskander, und Jan Beyers. 2019. „Lobbying Strategies and Success: Inside and Outside Lobbying in European Union Legislative Politics". *European Political Science Review* 11(1): 57–74.

De Hert, Paul, und Vagelis Papakonstantinou. 2012. „The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals". *Computer Law & Security Review* 28(2): 130–42.

Debusseré, Frederic. 2005. „The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?" *International Journal of Law and Information Technology* 13(1): 70–97.

Denninger, Erhard. 2002. „Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz". *Aus Politik und Zeitgeschichte (APuZ)* (10–11): 22–30.

Der Spiegel. 1983a. „‚Ohne Drohgebärde, ohne Angst'". *Der Spiegel* 16/1983. https://www.spiegel.de/spiegel/print/d-14019545.html (8. Juli 2019).

———. 1983b. „Volkszählung: Laßt 1000 Fragebogen glühen". *Der Spiegel* (13/1983): 28–32.

———. 1993. „Datenschutz: In Brüssel verwässert". *Der Spiegel* 48: 15.

Deutscher Bundestag. 1991. *13. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)*. Bonn: Deutscher Bundestag - 12. Wahlperiode. Unterrichtung durch den Bundesbeauftragten für den Datenschutz.

———. 1993. *14. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes - Berichtszeitraum Anfang 1991 bis Anfang 1993* -. Bonn: Deutscher Bundestag - 12. Wahlperiode. Unterrichtung durch den Bundesbeauftragten für den Datenschutz.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Dialer, Doris, und Margarethe Richter, hrsg. 2019. *Lobbying in the European Union: Strategies, Dynamics and Trends*. Cham: Springer International Publishing. http://link.springer.com/10.1007/978-3-319-98800-9 (27. März 2019).

Diedrich, Oliver. 2013. „Bericht: Deutschland bremst beim europäischen Datenschutz". *Heise Online*. https://www.heise.de/newsticker/meldung/Bericht-Deutschland-bremst-beim-europaeischen-Datenschutz-2058375.html (13. Januar 2018).

Diez, Thomas. 2010. „Postmoderne Ansätze". In *Theorien der Internationalen Beziehungen*, UTB, hrsg. Siegfried Schieder und Manuela Spindler. Opladen: Budrich, 491–520.

DIGITALEUROPE. 2011. „Position Paper on the European Commission's Communication on "A comprehensive approach on personal data protection in the European Union"". 83.

———. 2012a. „DIGITALEUROPE Amendments to Data Protection Regulatioin". 197.

———. 2012b. „DIGITALEUROPE COMMENTS ON PROPOSED EUROPEAN COMMISSION'S REGULATION ON DATA PROTECTION". 149.

Digitaleurope. 2020. *Two years of GDPR: A report from the digital industry*. https://www.digitaleurope.org/resources/two-years-of-gdpr-a-report-from-the-digital-industry/ (20. November 2020).

Dix, Alexander. 1996. „Case Study: North America and the European Union Directive". Gehalten auf der 18th International Privacy and Data Protection Conference: Privacy Beyond Borders, Ottawa, Canada. https://web.archive.org/web/20070204164343/www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm (10. Juni 2019).

———. 2000. „ECHELON auf dem parlamentarischen Prüfstand". *DuD* 24(9): 659–62.

———. 2013. „EU Data Protection Reform: Opportunities and Concerns". *Intereconomics* 48(5): 268–85.

Dobusch, Leonhard. 2014. *Digitale Zivilgesellschaft in Deutschland: Stand und Perspektiven 2014*. Discussion Paper, School of Business & Economics: Management. http://www.econstor.eu/handle/10419/95863 (12. Dezember 2014).

DPA. 2008. „Zehntausende demonstrieren für den Datenschutz". *www.aerztezeitung.de*. https://www.aerztezeitung.de/politik_gesellschaft/article/516006/zehntausende-demonstrieren-datenschutz.html (8. Juli 2019).

Dudley, Geoffrey, und Jeremy Richardson. 1999. „Competing Advocacy Coalitions and the Process of ‚Frame Reflection': A Longitudinal Analysis of EU Steel Policy". *Journal of European Public Policy* 6(2): 225–48.

Dür, Andreas. 2008. „Measuring Interest Group Influence in the EU: A Note on Methodology". *European Union Politics* 9(4): 559–76.

Dür, Andreas, Patrick Bernhagen, und David Marshall. 2013. *Interest group success in the European Union: When (and why) does business lose?* http://www.intereuro.eu/file.php/13/IGInfluence_paper1_031213.pdf.

Dye, Thomas R. 1972. *Understanding Public Policy*. Englewood Cliffs.

eBay. 2011. „eBay's submission to the European Commission's Consultation on the Communication 'A comprehensive approach on personal data protection in the European Union'". 93.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

EBF. 2012. „EUROPEAN BANKING FEDERATION PROPOSED AMENDMENTS TO THE EUROPEAN COMMISSION PROPOSAL FOR A REGULATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND THE FREE MOVEMENT OF SUCH DATA". 192.

EC. 2005. *Call for Input on the Forthcoming Review of the EU Regulatory Framework for Electronic Communications and Services Including Review of the Recommendation on Relevant Markets*. Brussels: European Commission - Information Society and Media Directorate-General.

———. 2006a. *Communication on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services {COM(2006) 334 Final} Proposed Changes*. Brussels: Commission of the European Communities. Commission Staff Working Document.

———. 2006b. *Public Consultation on a Draft Commission Recommendation On Relevant Product and Service Markets within the Electronic Communications Sector Susceptible to Ex Ante Regulation in Accordance with Directive 2002/21/EC of the European Parliament and of the Council on a Common Regulatory Framework for Electronic Communication Networks and Services (Second Edition)*. Brussels: Commission of the European Communities. Commission Staff Working Document.

———. 2006c. *Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste*. Brüssel: Europäische Kommission. Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2007a. *Bericht über das Ergebnis der Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste gemäß der Richtlinie 2002/21/EG und Zusammenfassung der Reformvorschläge 2007*. Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2007b. „Responses to the Consultation on the Review, October 2006". *www.ec.europa.eu*. https://web.archive.org/web/20070411231930/http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/public_consult/review_2/index_en.htm (17. Juli 2019).

———. 2007c. KOM(2007) 698 endgültig *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (von der Kommission vorgelegt) {SEK(2007) 1472} {SEK(2007) 1473}*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2008. *Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz*. Brüssel: Kommission der Europäischen Gemeinschaften.

———. 2009a. *Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger*. Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung der Kommission an das Europäische Parlament und den Rat.

———. 2009b. *Mitteilung der Kommission an das Europäische Parlament gemäß Artikel 251 Absatz 2 Unterabsatz 2 EG-Vertrag zu den Gemeinsamen Standpunkten des Rates im Hinblick auf den Erlass der Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, der Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden und der Verordnung des Europäischen Parlaments und des Rates zur Einrichtung der Gruppe Europäischer Regulierungsstellen für Telekommunikation*. Brüssel: Kommission der Europäischen Gemeinschaften.

———. 2010. *Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas: Aktionsplan zur Umsetzung des Stockholmer Programms*. Brüssel: Europäische Kommission. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2015a. *Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market - Joint Statement by Vice-President Andrus Ansip and Commissioner Věra Jourová*. Brussels: European Commission. Fact Sheet.

———. 2015b. *Standard Eurobarometer 84 - Autumn 2015 Annex*.

ECJ. 2001. (European Court of Justice) *Judgement of the Court (First Chamber) in Case C-450/00, Commission of the European Communities, represented by X. Lewis, acting as Agent, with an address for service in Luxembourg, applicant, v Grand Duchy of Luxembourg, represented by N. Mackel, acting as Agent, defendant*.

ECLN. 2009. *Widerstand gegen das "Stockholm-Programm" Erklärung [1] des Europäischen Bürgerrechtsnetzwerks*[2] zum neuen Fünfjahresplan der EU zur Justiz- und Innenpolitik*. European Civil Liberties Network (ECLN).

ECTA. 2011. „Public consultation on a comprehensive approach on personal data protection in the EU". 95.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

EDC. 2015a. *Coalitions statement on the outcome of the trilogue negotiations: After more than 4 years of hard work it's disappointing that EU policy makers have stumbled at the finishing line*. European Data Coalition (EDC).

———. 2015b. *Keep Europe Growing*. European Data Coalition (EDC).

Eder, Florian. 2013. „Brüssel: Der EU-Gipfel der viel zu vielen Wünsche". *DIE WELT*. https://www.welt.de/politik/ausland/article121165406/Der-EU-Gipfel-der-viel-zu-vielen-Wuensche.html (27. Oktober 2019).

Edith. 2022. „Google Tracks 39 Types of Private Data, the Highest Among Big Tech Companies - StockApps". *Stockapps.com*. https://stockapps.com/blog/google-tracks-39-types-of-private-data-the-highest-among-big-tech-companies/ (6. Dezember 2022).

EDPS. 2008. *EDPS Sees Adoption of Data Protection Framework for Police and Judicial Cooperation Only as a First Step*. Brussels: European Data Protection Supervisor (EDPS). Press Release.

———. 2011. *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - „A Comprehensive Approach on Personal Data Protection in the European Union"*. Brussels. 135.

———. 2013. *Meeting of the Committee on Civil Liberties: Justice and Home Affairs Presentation of the Reports on the Draft General Data Protection Regulation and on the Draft Directive on the Processing of Data for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences*. Brussels: European Data Protection Supervisor (EDPS).

———. 2016. „The EU GDPR as a Clarion Call for a New Global Digital Gold Standard". *European Data Protection Supervisor*. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_en (5. Juni 2020).

EDRi. 2004. „EDRI response to EU copyright consultation". *EDRi*. https://edri.org/edrigramnumber2-21copyright/ (20. August 2019).

———. 2005a. „Data retention: Council barks but cannot bite". *EDRi*. https://edri.org/edrigramnumber3-21retention/ (30. Mai 2019).

———. 2005b. „EDRI-gram - Number 3.17, 24 August 2005 - EDRi". *www.edri.org*. https://web.archive.org/web/20180621221836/https://edri.org/edrigramnumber3-17/ (16. Januar 2020).

———. 2005c. „Secret minutes EU data retention meeting". *EDRi*. https://edri.org/edrigramnumber3-7retention/ (30. Mai 2019).

———. 2007. „EDRI's contributions to the RFID Expert Group". *EDRi*. https://edri.org/edrigramnumber5-15rfid-edri-papers/ (4. März 2016).

———. 2011a. „Brief overview of the leaked EU Data Protection Regulation". *EDRi*. https://edri.org/edrigramnumber9-24overview-data-protection-regulation/ (17. Februar 2020).

———. 2011b. „EDRi response to EC consultation on the review of the Data Protection Directive". 97.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2011c. „US lobbying against draft Data Protection Regulation". *EDRi*. https://edri.org/us-dpr/ (30. Juni 2017).

———. 2012a. „Committees and Timetable". *EDRi*. https://web.archive.org/web/20121120173616/https://protectmydata.eu/committees/ (10. Mai 2018).

———. 2012b. „EDRi Initial Comments on the Proposal for a Data Protection Regulation". *EDRi*. https://edri.org/commentsdpr/ (30. Juni 2017).

———. 2013a. „European Parliament Data protection draft – compromise or compromised?" *EDRi*. https://edri.org/ep-eudatap/ (23. Oktober 2019).

———. 2013b. „The ACTA Archive". *www.edri.org*. https://edri.org/acta-archive/ (23. Januar 2020).

EDRi, BoF, u. a. 2015. „Vorentscheidung zur Europäischen Datenschutzgrundverordnung: Am Ende reichte es nur zur Sicherung von Mindeststandards › Digitale Gesellschaft". https://digitalegesellschaft.de/2015/12/vorentscheidung-dsgvo-mindeststandard/ (31. Oktober 2019).

EDRi. 2019. „why we do it". *EDRi*. https://edri.org/why-we-do-it/ (23. August 2019).

EDRi und Access (International). 2015. *Letter to Commission President Juncker*.

EDRi, accessnow, Panoptykon Foundation, und Privacy International. 2015. *Data Protection - Broken Badly*.

EDRi und BoF. 2009. „Response to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data". 37.

EDSB. 2005. *Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (KOM(2005) 475 endgültig)*. Brüssel: Der Europäische Datenschutzbeauftragte. Stellungnahme.

———. 2006. *Zweite Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Brüssel: Der Europäische Datenschutzbeauftragte. Stellungnahme.

———. 2007a. *Dritte Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Brüssel: Europäischer Datenschutzbeauftragter (EDSB).

———. 2007b. *Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie"*. Brüssel: Europäischer Datenschutzbeauftragter (EDSB). Stellungnahme.

———. 2008. *Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation)*. Brüssel: Europäischer Datenschutzbeauftragter (EDSB). Stellungnahme.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2009. *Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger" (2009/C 276/02)*. Brüssel: Europäischer Datenschutzbeauftragter (EDSB). Amtsblatt der Europäischen Union vom 17.11.2009.

———. 2012a. *EDSB begrüßt „riesigen Schritt vorwärts für den Datenschutz in Europa", bedauert aber ungenügende Regelungen für den Bereich Polizei und Justiz*. Brüssel: Der Europäische Datenschutzbeauftragte (EDSB). Pressemitteilung.

———. 2012b. *Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket*. Brüssel: Der Europäische Datenschutzbeauftragte.

———. 2013. *Ein wichtiger und begrüßenswerter Schritt hin zu einem stärkeren und effektiveren Datenschutz in Europa*. Brüssel: Der Europäische Datenschutzbeauftragte (EDSB).

EG. 1977. *Gemeinsame Erklärung des Europäischen Parlaments, des Rates und der Kommission betreffend die Achtung der Grundrechte sowie der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten*. Luxemburg.

EK. 2009. *Soziale Netzwerke: Kommission handelt Vereinbarung der wichtigsten Website-Anbieter aus*. Brüssel: Europäische Kommission.

———. 2010. *Gesamtkonzept für den Datenschutz in der Europäischen Union*. Brüssel: Europäische Kommission. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2011. *Digitale Agenda: Nur zwei soziale Netze schützen standardmäßig die Profile Minderjähriger*. Brüssel: Europäische Kommission. Pressemitteilung.

Ellger, Reinhard. 1990. *Der Datenschutz im grenzüberschreitenden Datenverkehr: eine rechtsvergleichende und kollisionesrechtliche Untersuchung*. Nomos Verlagsgesellschaft.

EMOTA. 2011. „EMOTA's response to the public Consultation on the Commission's Communication on a comprehensive approach on personal data protection in the European Union COM(2010) 609 final". 98.

ENPA, und EMMA. 2012. „ENPA and EMMA Position paper on PROPOSAL FOR A DATA PROTECTION REGULATION, 25 JANUARY 2012 (COM(2012) 11)". 175.

ENPA, und FAEP. 2011. „ENPA and FAEP joint response to the consultation on the Commission Communication "A comprehensive approach on personal data protection in the European Union" [COM (2010) 609]". 99.

EP. 1979. *Proceedings of the Round Table on „Special rights and a charter of the rights of the citizens of the European Community" and related documents (Florence, 26 to 28 October 1978)*. Luxembourg: European Parliament - Directorate-General for Research.

———. 1992a. *25. Datenschutz (Abstimmung) ** 1 (Bericht Hoon - A3-10/92)*. Strassburg. Europäisches Parlament Sitzungsperiode 1991/1992 - Tagung vom 10. bis 14. Februar 1992 - Protokoll der Sitzung vom Mittwoch, 12. Februar 1992.

———. 1992b. *Sitzungsperiode 1991-1992: Ausführliche Sitzungsberichte vom 10. bis 14. Februar - 5. Informationssysteme*. Straßburg.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 1993. *Änderung der Rechtsgrundlage und/oder des Annahmeverfahrens - Recht und Bürgerrechte: Abstimmung vom 11. März 1992 (5) über eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (KOM(90)0314.1)*. . Europäisches Parlament Sitzungsperiode 1993-1994 - Protokoll der Sitzung vom Donnerstag 2. Dezember 1993.

———. 1995. *Beschluss betreffend den gemeinsamen Standpunkt des Rates im Hinblick auf die Annahme einer Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (C4-0051/95 - 00/0287(COD))*. . Europäisches Parlament Sitzungsperiode 1995-1996 - Protokoll der Sitzung vom Donnerstag, 15. Juni 1995.

———. 1999. *Entschließung zur Ausarbeitung der Charta der Grundrechte*.

———. 2000. „Angenommene Texte - Dienstag, 14. November 2000 - Charta der Grundrechte der Europäischen Union ***". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2000-0497+0+DOC+XML+V0//DE#ref_1_3 (2. Juli 2019).

———. 2008a. *Ergebnisse der namentlichen Abstimmungen - Anlage*. Europäisches Parlament.

———. 2008b. *Plenardebatten - Dienstag, 2. September 2008*. Brüssel.

———. 2008c. „Plenardebatten - Dienstag, 23. September 2008 - Terrorismusbekämpfung - Schutz personenbezogener Daten (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20080923+ITEM-004+DOC+XML+V0//DE (21. Juni 2019).

———. 2008d. „Plenardebatten - Mittwoch, 24. September 2008 - Schriftliche Stimmerklärungen". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20080924&secondRef=ITEM-011&language=DE&ring=A6-2008-0318#3-207 (19. Juli 2019).

———. 2009a. *Anlage: Ergebnisse der Abstimmungen - Mehrjahresprogramm 2010-2014 für den Raum der Freiheit, der Sicherheit und des Rechts (Stockholm-Programm)*. Straßburg: Europäisches Parlament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+PV+20091125+RES-VOT+DOC+PDF+V0//DE&language=DE (12. Juli 2019).

———. 2009b. *Ergebnis der namentlichen Abstimmungen - Anlage: B7-0155/2009 – Mehrjahresprogramm 2010–2014 –*. Straßburg: Europäisches Parlament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+PV+20091125+RES-RCV+DOC+PDF+V0//DE&language=DE (12. Juli 2019).

———. 2009c. *Ergebnisse der Abstimmungen - Anlage*. Straßburg: Europäisches Parlament.

———. 2009d. *Mehrjahresprogramm 2010-2014 für den Raum der Freiheit, der Sicherheit und des Rechts (Stockholm-Programm)*. Europäisches Parlament. Entschließung des Europäischen Parlaments vom 25. November 2009 zu der Mitteilung der Kommission an das Europäische Parlament und den Rat – Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger – Stockholm-Programm.

———. 2009e. *Plenardebatten - Dienstag, 5. Mai 2009*. Straßburg.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

———. 2009f. „Plenardebatten - Dienstag, 24. November 2009 - Mehrjahresprogramm 2010-2014 für den Raum der Freiheit, der Sicherheit und des Rechts (Stockholm-Programm) (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20091124&secondRef=ITEM-009&language=DE&ring=B7-2009-0155 (12. Juli 2019).

———. 2009g. „Plenardebatten - Mittwoch, 25. November 2009 - Stimmerklärungen: - Entschließungsantrag (B7-0155/2009) - Mehrjahresprogramm 2010-2014 für den Raum der Freiheit, der Sicherheit und des Rechts (Stockholm-Programm)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20091125&secondRef=ITEM-008&language=DE&ring=B7-2009-0155#3-132 (13. Juli 2019).

———. 2020a. „5. Wahlperiode | Ilka SCHRÖDER | Abgeordnete | Europäisches Parlament". *www.europaparl.europa.eu*. https://www.europarl.europa.eu/meps/de/4296/ILKA_SCHRODER/history/5 (7. Juni 2020).

———. 2020b. „6. Wahlperiode | Marco CAPPATO | Abgeordnete | Europäisches Parlament". *www.europaparl.europa.eu*. https://www.europarl.europa.eu/meps/de/4740/MARCO_CAPPATO/history/6 (7. Juni 2020).

———. 2020c. „7. Wahlperiode | Juan Fernando LÓPEZ AGUILAR | Abgeordnete | Europäisches Parlament". *www.europaparl.europa.eu*. https://www.europarl.europa.eu/meps/de/96812/Doktor+Professor_JUAN+FERNANDO_LOPEZ+AGUILAR/history/7 (17. Januar 2020).

———. 2020d. „7th Parliamentary Term | Malcolm HARBOUR | MEPs | European Parliament". *www.europaparl.europa.eu*. https://www.europarl.europa.eu/meps/en/4538/MALCOLM_HARBOUR/history/7 (17. Januar 2020).

EPC. 2009. „EU Institutions Pose Threat to Internet Economy of Europe | EPC". http://epceurope.eu/eu-institutions-pose-threat-to-internet-economy-of-europe-2/ (11. März 2018).

———. 2011. „RESPONSE FROM THE EUROPEAN PUBLISHERS COUNCIL TO THE COMMUNICATION BY THE EUROPEAN COMMISSION ON "A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION"". 2011. 101.

epic.org. 2009. *Ergebnisse der namentlichen Abstimmungen - Anlage*. Straßburg: Europäisches Parlament.

EPP. 2015. „Data protection reform timetable | Actualités | EPP Group in the European Parliament". *www.eppgroup.eu*. https://web.archive.org/web/20160322012158/https://www.eppgroup.eu/fr/news/Data-protection-reform-timetable (4. März 2020).

Ermert, Monika. 2012. „Oberster EU-Datenschützer greift Redings Reformpaket an". *Heise Online*. https://www.heise.de/newsticker/meldung/Oberster-EU-Datenschuetzer-greift-Redings-Reformpaket-an-1465832.html (12. Februar 2018).

———. 2014. „European ministers largely agree on international aspects of future data protection regulation, other issues unsolved". *Internet Policy Review*. https://policyreview.info/articles/news/european-ministers-largely-agree-international-aspects-future-data-protection (28. Oktober 2019).

ETNO. 2005. *ETNO Expert Contribution on Data retention in ecommunications - Council's Draft Framework Decision, Commission's Proposal for a Directive*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2009. „ETNO Reflection Document on the EC Public Consultation on the Framework Data Protection Directive". 42.

———. 2011. „ETNO Reflection Document on the EC Public Consultation on the Communication on a comprehensive approach on personal data protection in the European Union". 102.

ETNO, EuroISPA, und ECTA. 2002. *Joint Industry Memo in view of the 2nd Reading of the Cappato Report: The Implications of "Data Retention" in Article 15.1 of the Common Position on the Electronic Communications Data Protection Directive*.

EU. 1995. Nr. L 281 ABl. EG vom 23.11.1995 *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. http://wiki.piratepartei.lu/images/d/d0/01_Datenschutzrichtlinie.pdf (22. August 2014).

———. 2007. „Schengener Informationssystem der zweiten Generation (SIS II)". https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Al14544 (16. Januar 2020).

———. 2009. Nr. L 337 ABl. EU vom 18.12.2009 *Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:de:PDF (29. Juli 2015).

———. 2010. C 83 ABl. EU vom 30.03.2010 *Charta der Grundrechte der Europäischen Union*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:DE:PDF (29. Juli 2015).

———. 2018. „Richtlinien der Europäischen Union, EUR-Lex - l14527". *eur-lex.europa.eu*. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Al14527 (7. Februar 2020).

EU Commission. 2004. *Annex to the: European Electronic Communications Regulation and Markets 2004 (10th Report) {COM(2004)759 final}*. Brussels: Commission of the European Communities. Commission Staff Working Paper.

———. 2005. *Annex to the: Proposal for a Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-Operation in Criminal Matters - Impact Assessment {COM(2005) 475 Final}*. Brussels: Commission of the European Communities. Commission Staff Working Document.

———. 2010. *Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data*. Brussels: European Commission Directorate-General Justice: Directorate C: Fundamental rights and Union citizenship - Unit C.3: Data protection.

———. 2011. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf (17. April 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2012. *Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*. Brussels: European Commission. Commission Staff Working Paper.

———. 2013a. *Informal Justice Council in Vilnius*. Brussels: European Commission. Memo.

———. 2013b. *Letter from Reding to Holder*. Brussels: European Commission.

———. 2013c. *PRISM Scandal: The Data Protection Rights of EU Citizens Are Non-Negotiable - Press Conference, EU-U.S. Justice and Home Affairs Ministerial /Dublin*. Dublin: European Commission. Speech.

———. 2013d. *Vice-President Reding's Intervention at the Justice Council on the Data Protection Reform and the One-Stop Shop Principle*. Luxembourg: European Commission. Speech.

———. 2014. *Data Protection Day 2014: Full Speed on EU Data Protection Reform*. Brussels: European Commission. Memo.

EU Parliament. 2013a. *Forum: Who's Watching You? Who's Protecting You?* https://multimedia.europarl.europa.eu/en/forum-whos-watching-you-whos-protecting-you_D001-0038_ev (25. Oktober 2019).

———. 2013b. „Prism: A wake-up call for data protection". *News | European Parliament*. http://www.europarl.europa.eu/news/en/news-room/20130617STO12378/prism-a-wake-up-call-for-data-protection (14. März 2017).

———. 2014. „Hearings: LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/parlArchives/comArch/com7/hearingsSheet.do?language=EN&body=LIBE (26. Oktober 2019).

EuGH. 2001. *Urteil des Gerichtshofs (Vierte Kammer): Kommission der Europäischen Gemeinschaften, vertreten durch B. Mongin als Bevollmächtigten, Klägerin, gegen Französische Republik, vertreten durch K. Rispal-Bellanger und A. Lercher als Bevollmächtigte, Zustellungsanschrift in Luxemburg, Beklagte*.

———. 2015. „Urteil des Gerichtshofs (Große Kammer): In der Rechtssache C-362/14 betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland) mit Entscheidung vom 17. Juli 2014, beim Gerichtshof eingegangen am 25. Juli 2014, in dem Verfahren Maximillian Schrems gegen Data Protection Commissioner, Beteiligte: Digital Rights Ireland Ltd",. *curia.europa.eu*. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=7395584 (10. Januar 2020).

EU-Kommission. 2000a. *Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA*.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2000b. *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2000/C 365 E/17)*.

———. 2001a. *Antwort von Herrn Liikanen im Namen der Kommission*. Brüssel. Amtsblatt der Europäischen Gemeinschaften.

———. 2001b. *Europäisches Regieren - Ein Weissbuch*.

———. 2001c. *Europäisches Regieren - Ein Weissbuch [KOM(2001) 428 endgültig]*.

———. 2002. *Mitteilung der Kommission an das Europäische Parlament gemäß Artikel 251 Absatz 2 Unterabsatz 2 EG-Vertrag betreffend den vom Rat angenommenen gemeinsamen Standpunkt im Hinblick auf den Erlaß einer Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation*. Brüssel: Europäische Kommission. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52002SC0124&from=DE (12. Juni 2019).

———. 2003. „Stellungnahmen interessierter Kreise". *Europa - Die Europäische Kommission - Der Binnenmarkt - Datenschutz*. https://web.archive.org/web/20031206215047/http://europa.eu.int/comm/internal_market/privacy/lawreport/paper_de.htm (14. August 2019).

———. 2004. *Europäische Vorschriften zur elektronischen Kommunikation und Märkte 2004 [SEC(2004)1535]*. Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2005. *Achter Jahresbericht der Art. 29 Datenschutzgruppe: Berichtsjahr 2004*. Europäische Gemeinschaften.

———. 2006. *Neunter Jahresbericht der Art. 29 Datenschutzgruppe: Berichtsjahr 2005*. Europäische Gemeinschaften.

———. 2009. *Präsident Barroso stellt seine neue Mannschaft vor*. Brüssel: Europäische Kommission.

———. 2010. *Europa 2020: Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum*. Brüssel: Europäische Kommission. Mitteilung der Kommission.

———. 2011. *Bekämpfung von schwerer Kriminalität und Terrorismus: EU-Vorschlag zur Verwendung von Fluggastdaten*. Brüssel: Europäische Kommission. Press Release. http://europa.eu/rapid/press-release_IP-11-120_de.htm?locale=en (26. November 2014).

———. 2012a. *Der Schutz der Privatsphäre in einer vernetzten Welt: Ein europäischer Datenschutzrahmen für das 21. Jahrhundert (Text von Bedeutung für den EWR)*. Brüssel: Europäische Kommission. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2012b. *Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern*. Brüssel: Europäische Kommission. Pressemitteilung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2012c. *Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.*

———. 2012d. *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

———. 2012e. *Zusammenfassung der Folgenabschätzung Begleitunterlage zu der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr*. Brüssel: Europäische Kommission. Arbeitsdokument der Kommissionsdienststellen.

———. 2013. *Viviane Reding auf der zweiten Cloud computing-Konferenz - Reform des EU-Datenschutzrechts: Es ist an der Zeit, Nägel mit Köpfen zu machen!* Brüssel: Europäische Kommission. Pressemitteilung.

———. 2015. *Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen*. Brüssel: Europäische Kommission. Pressemitteilung. http://link.springer.com/10.1007/s11623-016-0548-3 (5. März 2019).

EU-Ministerrat. 2001. *Schlussfolgerungen des Rates (Justiz und Inneres) vom 20. September 2001*. Brüssel: Rat der Europäischen Union.

———. 2002. *Gemeinsamer Standpunkt (EG) Nr. 26/2002 vom Rat festgelegt am 28. Januar 2002 im Hinblick auf den Erlass der Richtlinie 2002/. . ./EG des Europäischen Parlaments und des Rates vom . . . über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/C 113 E/03)*. Brüssel: Rat der Europäischen Union.

———. 2004a. *Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus*. Brüssel: Rat der Europäischen Union. Übermittlungsvermerk.

———. 2004b. *Erläuternder Vermerk zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus*. Brüssel: Rat der Europäischen Union. Vermerk.

———. 2005a. *Außerordentliche Tagung des Rates Justiz und Inneres*. Brüssel: Rat der Europäischen Union.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2005b. *Strategie der Europäischen Union zur Terrorismusbekämpfung*. Brüssel: Rat der Europäischen Union.

———. 2007. *Beratungsergebnisse der JI-Referenten vom 30. November 2007 betreffend den Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Brüssel: Rat der Europäischen Union.

———. 2008a. *Beschluss 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität*. Luxemburg: Rat der Europäischen Union.

———. 2008b. *Mitteilung an die Presse: 2907. Tagung des Rates - Verkehr, Telekommunikation und Energie*. Brüssel: Rat der Europäischen Union.

———. 2008c. *Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*.

———. 2009a. *Begründung des Rates - Gemeinsamer Standpunkt des Rates vom 16. Februar 2009 im Hinblick auf die Annahme einer Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz*. Brüssel: Rat der Europäischen Union.

———. 2009b. *Gemeinsamer Standpunkt des Rates im Hinblick auf die Annahme einer Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz*. Brüssel: Rat der Europäischen Union.

———. 2012. *Datenschutzpaket – Bericht über die unter zyprischem Vorsitz erzielten Fortschritte*. Brüssel: Rat der Europäischen Union.

———. 2013a. *Entwurf eines Protokolls: 3244. Tagung des Rates der Europäischen Union (Justiz und Inneres) in Luxemburg, den 6./7. Juni 2013*. Brüssel: Rat der Europäischen Union.

———. 2013b. *Mitteilung an die Presse: 3228. Tagung des Rates*. Brüssel: Rat der Europäischen Union.

———. 2014a. *3319. Tagung des Rats (JHA) vom 5. und 6. Juni 2014 in Luxemburg*. Luxemburg: Rat der Europäischen Union. Entwurf eines Protokolls.

———. 2014b. *3336. Tagung des Rats (JHA) vo 9. und 10. Oktober 2014 in Luxemburg*. Brüssel: Rat der Europäischen Union. Entwurf eines Protokolls.

———. 2014c. *Mitteilung an die Presse: 3354 Tagung des Rates (Justiz und Inneres) Brüssel, 4. und 5. Dezember 2014*. Brüssel: Rat der Europäischen Union.

———. 2015a. *3376. Tagung des Rats (JHA) vom 12./13. März 2015 in Brüssel*. Brüssel: Rat der Europäischen Union. Entwurf eines Protokolls.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2015b. *3396. Tagung des Rates der Europäischen Union (Justiz und Inneres) vom 15./16. Juni 2015 in Luxemburg*. Brüssel.

———. 2015c. *EU-Datenschutzreform: Rat bestätigt Einigung mit dem Europäischen Parlament*. Brüssel: Rat der Europäischen Union. Pressemitteilung.

———. 2015d. *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Date nund zum freien Datenverkehr (Datenschutz-Grundverordnung) - Vorbereitung einer allgemeinen Ausrichtung*. Brüssel: Rat der Europäischen Union.

———. 2017. „Schlussfolgerungen und Entschließungen des Rates". http://www.consiliu m.europa.eu/de/council-eu/conclusions-resolutions/ (5. Januar 2020).

———. 2018a. „Die Beschlussfassung im Rat - Consilium". *www.consilium.europe.eu*. https://www.consilium.europa.eu/de/council-eu/decision-making/ (20. Oktober 2019).

———. 2018b. „Die Ratsformationen". *www.consilium.europa.eu*. http://www.consilium. europa.eu/de/council-eu/configurations/ (6. Januar 2020).

———. 2019. „Das ordentliche Gesetzgebungsverfahren - Consilium". *www.consili- um.europe.eu*. https://www.consilium.europa.eu/de/council-eu/decision-making /ordinary-legislative-procedure/ (20. Oktober 2019).

———. 2020. „Der Vorsitz im Rat der EU". *www.consilium.europa.eu*. http://www.consi lium.europa.eu/de/council-eu/presidency-council-eu/ (7. Januar 2020).

EU-Parlament. 2012a. *Konferenz der Ausschussvorsitze - Protokoll 2012-04-18*. Straßburg: Europäisches Parlament.

———. 2012b. *Konferenz der Ausschussvorsitze - Protokoll 2012-05-22*. Straßburg: Europäisches Parlament.

———. 2012c. *Plenarsitzungsprotokoll - Donnerstag, 14. Juni 2012*. Europäisches Parlament.

———. 2012d. *Plenarsitzungsprotokoll - Donnerstag, 16. Februar 2012: 4. Vorlage von Dokumenten*. Straßburg: Europäisches Parlament. http://www.europarl.europa.eu/si des/getDoc.do?pubRef=-//EP//TEXT+PV+20120216+ITEMS+DOC+XML+V0//DE &language=DE (4. Oktober 2019).

———. 2012e. *Plenarsitzungsprotokoll - Donnerstag, 24. Mai 2012*. Straßburg: Europäisches Parlament.

———. 2012f. *Protokoll - Ergebnis der namentlichen Abstimmungen - Anlage*. Europäisches Parlament.

———. 2013a. „Dimitris Droutsas: Wir dürfen hohe Datenschutz-Standards nicht verwässern | Aktuelles | European Parliament". *Europäisches Parlament - Aktuell*. http:// www.europarl.europa.eu/news/de/headlines/society/20130708STO16804/dimitris -droutsas-wir-durfen-hohe-datenschutz-standards-nicht-verwassern (12. September 2017).

———. 2013b. *Entschließung des Europäischen Parlaments vom 4. Juli 2013 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Privatsphäre der EU-Bürger (2013/2682(RSP))*. Strasbourg: Europäisches Parlament.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2013c. „Plenardebatten - Dienstag, 10. September 2013 - Internetsicherheitsstrategie der EU – ein offener, sicherer und geschützter Cyberraum - Digitale Agenda für Wachstum, Mobilität und Beschäftigung (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20130910+ITEM-021+DOC+XML+V0//DE (24. Oktober 2019).

———. 2013d. „Plenardebatten - Dienstag, 11. Juni 2013 - Überwachung von EU-Bürgern im Internet durch die USA (NSA-PRISM-Programm) (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20130611+ITEM-004+DOC+XML+V0//DE (24. Oktober 2019).

———. 2013e. „Plenardebatten - Mittwoch, 3. Juli 2013 - Überwachungsprogramm der US-amerikanischen NSA sowie Überwachungsbehörden in verschiedenen Mitgliedstaaten; ihr Einfluss auf die Privatsphäre der EU-Bürger (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20130703+ITEM-014+DOC+XML+V0//DE (24. Oktober 2019).

———. 2013f. „Plenardebatten - Mittwoch, 9. Oktober 2013 - Aussetzung des SWIFT-Abkommens infolge der Überwachung durch die NSA (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20131009+ITEM-019+DOC+XML+V0//DE (24. Oktober 2019).

———. 2013g. *Protokoll: Ergebnis Der Namentlichen Abstimmungen - Anlage*. Strasbourg: Europäisches Parlament.

———. 2014a. *Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI))*.

———. 2014b. *Protokoll - Ergebnis der namentlichen Abstimmungen - Anlage*.

———. 2015. *EU-Datenschutzreform: Mehr Rechte für Europas Internetnutzer*. Europäisches Parlament. Pressemitteilung.

———. 2016. *Ergebnisse der Abstimmungen - Anlage*. Straßburg.

Euractiv. 2009. „Brussels to Tighten Data Protection Rules". *euractiv.com*. https://www.euractiv.com/section/digital/news/brussels-to-tighten-data-protection-rules/ (10. September 2019).

———. 2011. „Reding: ‚Companies Don't Take Protection of Personal Data Seriously Enough'". *www.euractiv.com*. https://www.euractiv.com/section/justice-home-affairs/interview/reding-companies-don-t-take-protection-of-personal-data-seriously-enough/ (20. Oktober 2019).

———. 2012a. „Commission Strife Risks Delaying Data Protection Overhaul". *www.euractiv.com*. https://www.euractiv.com/section/justice-home-affairs/news/commission-strife-risks-delaying-data-protection-overhaul/ (20. Oktober 2019).

———. 2012b. „Companies 'Left in Limbo' by New Data Protection Regime". *www.euractiv.com*. https://www.euractiv.com/section/digital/news/companies-left-in-limbo-by-new-data-protection-regime/ (21. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2012c. „IT Giants Still Wary of EU on Data Protection“. *www.euractiv.com*. https://www.euractiv.com/section/digital/news/it-giants-still-wary-of-eu-on-data-protection/ (20. Oktober 2019).

———. 2013. „Reding: Doubts over EU Institutions' Data Protection Are a 'Red Herring'“. *www.euractiv.com*. https://www.euractiv.com/section/justice-home-affairs/interview/reding-doubts-over-eu-institutions-data-protection-are-a-red-herring/ (25. Oktober 2019).

eurofinas. 2009. „Eurofinas consultation response on the legal framework for the fundamental right to protection of personal data“. 43.

EUROFINAS. 2011. „Response to the consultation on the Commission's comprehensive approach on personal data protection in the European Union“. 104.

Eurofinas. 2012a. *Eurofinas observations on the Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final)*. 147,5.

———. 2012b. „Eurofinas proposals for amendments on the Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final)“. 195.

EuroISPA. 2011. „CONSULTATION ON THE COMMISSION'S COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION“. 105.

Euronews. 2013. „New Platform Tracks Lobbyists Copy-Pasting Their Way into EU Legislation“. *Euronews*. https://www.euronews.com/2013/02/14/xyz-new-platform-tracks-lobbyists-copy-pasting-their-way-into-eu-legislation (24. Oktober 2019).

Europäische Datenschutzbeauftragte. 2012. „Resolution on the European data protection reform“. 159.

Europäische Gemeinschaften. 1957. *Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft*. Rom.

———. 1987. *Einheitliche Europäische Akte*. . Amtsblatt der Europäischen Gemeinschaften.

———. 1992. *Vertrag über die Europäische Union, unterzeichnet zu Maastricht am 7. Februar 1992*. Maastricht. Mitteilungen und Bekanntmachungen.

Europäische Kommission. 1981. *Empfehlung der Kommission vom 29. Juli 1981 betreffend ein Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*. Brüssel. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31981H0679&from=EN.

———. 1985. *Mitteilung der Kommission auf dem Gebiet der Datenverarbeitung: Aufforderung zur Einreichung von Vorschlägen für Vorhaben auf den Gebieten Datensicherheit und Datenschutz, Schutz von Computerprogrammen, Verletzlichkeit der informatisierten Gesellschaft*. Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 1990. (90/C 277/04) *Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen.*

———. 1994a. 94/C 200/04 *Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen.*

———. 1994b. *Wachstum, Wettbewerbsfähigkeit, Beschäftigung: Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert - Weißbuch.* Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften.

———. 1997. *Stellungnahme der Kommission zu den Abänderungen des Europäischen Parlaments des gemeinsamen Standpunkts des Rates betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen.* Brüssel: Kommission der Europäischen Gemeinschaften.

———. 1999a. *Entwicklung neuer Rahmenbedingungen für elektronische Kommunikationsinfrastrukturen und zugehörige Dienste: Kommunikationsbericht 1999.* Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 1999b. 1999/0153(COD) *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.*

———. 2000a. *Datenschutz: Kommission verklagt fünf Mitgliedstaaten.* Brüssel: Europäische Kommission. Pressemitteilung.

———. 2000b. *Die Ergebnisse der öffentlichen Anhörung zum Kommunikationsbericht 1999 und Leitlinien für den neuen Rechtsrahmen.* Brüssel: Kommission der Europäischen Gemeinschaften. Mitteilung der Kommission.

———. 2002. *Eurobarometer 57 - Bericht.*

———. 2005a. *Das Haager Programm: Zehn Schwerpunkte für die nächsten fünf Jahre.* Straßburg: Europäische Kommission. Memo.

———. 2005b. *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.* Brüssel: Kommission der Europäischen Gemeinschaften.

———. 2005c. KOM(2005) 475 endgültig, {SEC(2005) 1241} *Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2008a. *11. Jahresbericht der Art. 29 Datenschutzgruppe über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Europäischen Union und in Drittländern - Berichtsjahr 2007*.

———. 2008b. *Standard-Eurobarometer 69: Die öffentliche Meinung in der Europäischen Union - Erste Ergebnisse*.

———. 2010. *Eine Digitale Agenda für Europa*. Brüssel: Europäische Kommission. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

———. 2011. *EU-Justizkommissarin Viviane Reding und Bundesverbraucherministerin Ilse Aigner setzen sich gemeinsam für einen stärkeren Datenschutz auf EU-Ebene ein*. Brüssel: Europäische Kommission.

Europäische Union, hrsg. 1997. *Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte*. Luxemburg: Amt für Amtl. Veröff. der Europ. Gemeinschaften.

———. 2001. *Klage der Kommission der Europäischen Gemeinschaften gegen die Bundesrepublik Deutschland, eingereicht am 1. Dezember 2000*. Europäische Union. Amtsblatt der Europäischen Gemeinschaften.

———. 2002. *Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft.* . Amtsblatt der Europäischen Gemeinschaften.

———. 2006. Amtsblatt der Europäischen Union, L 105/54, 13.04.2006 *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF (3. Dezember 2014).

———. 2010. *Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union.* . Amtsblatt der Europäischen Union. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:C:2010:083:FULL&from=de.

———. 2018. *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*.

Europäische Wissenschaftlerinnen und Wissenschaftler. 2013. „Datenschutz in Europa – Über 100 Wissenschaftler melden sich zu Wort". *www.dataprotection.eu*. https://web.archive.org/web/20130606193040/http://dataprotectioneu.eu/index_de.html (1. Oktober 2019).

Europäischer Rat. 1989. *Schlussfolgerungen des Vorsitzes (Strassburg, 8./9. Dezember 1989)*. Strassburg: Europäischer Rat.

———. 1994a. *Tagung am 9.-10. Dezember 1994 in Essen: Schlussfolgerungen des Vorsitzes*. Essen: Europäischer Rat.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 1994b. *Tagung am 24.-25. Juni 1994 in Korfu: Schlussfolgerungen des Vorsitzes*. Korfu: Europäischer Rat.

———. 1999a. *Schlussfolgerungen des Vorsitzes - Köln 3. und 4. Juni 1999*. Köln.

———. 1999b. *Tampere Europäischer Rat 15. und 16. Oktober 1999 - Schlussfolgerungen des Vorsitzes*. Tampere: Europäischer Rat. http://www.europarl.europa.eu/summits/tam_de.htm.

———. 2000a. *Schlussfolgerungen des Vorsitzes - Nizza, 7.-9. Dezember 2000*. Europäischer Rat.

———. 2000b. *Schlussfolgerungen des Vorsitzes: Europäischer Rat (Lissabon) 23. und 24. März 2000*. Lissabon: Europäischer Rat.

———. 2001. *Schlussfolgerungen des Vorsitzes - Europäischer Rat (Laeken) 14. und 15. Dezember 2001*. Laeken: Europäischer Rat.

———. 2003. *Europäische Sicherheitsstrategie: Ein sicheres Europa in einer besseren Wel*. Brüssel: Europäischer Rat.

———. 2004. *Erklärung zum Kampf gegen Terrorismus*. Brüssel: Europäischer Rat.

———. 2005a. *Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union*. . Amtsblatt der Europäischen Union. https://www.easo.europa.eu/sites/default/files/public/Haager-Programm.pdf.

———. 2005b. *Tagung des Europäischen Rates (Brüssel, 22./23. März 2005) Schlussfolgerungen des Vorsitzes*. Brüssel: Rat der Europäischen Union.

———. 2009. *Schlussfolgerungen des Europäischen Rates (10./11. Dezember 2009)*. Brüssel: Europäischer Rat. Übermittlungsvermerk.

———. 2010. *Das Stockholmer Programm - Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger*. . Amtsblatt der Europäischen Union.

———. 2013. *Schlussfolgerungen des Europäischen Rates (Tagung vom 24./25. Oktober 2013)*. Brüssel: Europäischer Rat. Schlussfolgerungen.

———. 2014. *Schlussfolgerungen des Europäischen Rates (26. und 27. Juni 2014)*. Brüssel: Europäischer Rat.

———. 2015. *Tagung des Europäischen Rates (17. und 18. Dezember 2015) - Schlussfolgerungen*. Brüssel: Europäischer Rat. Übermittlungsvermerk.

Europäisches Parlament. 1975. *Entschliessung über den Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung*. . Mitteilungen und Bekanntmachungen.

———. 1976. *Entschliessung zum Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung*. Europäische Union.

———. 1979. *Entschliessung zum Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung*. Europäische Union.

———. 1982. *Entschliessung zum Schutz der Rechte des einzelnen angeischts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung*. Brussels. Amtsblatt der Europäischen Gemeinschaften.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 1992. A3-10/92 C 94/202 *Legislative Entschliessung (Verfahren der Zusammenarbeit: Erste Lesung) mit der Stellungnahme des Europäischen Parlaments zu dem Vorschlag der Kommission an den Rat für eine Richtlinie betreffend den Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen.*

———. 1997a. A4-0415/96 *Beschluß betreffend den Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlaß der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen.*

———. 1997b. *Beschluß betreffend den vom Vermittlungsausschuß gebilligten gemeinsamen Entwurf für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (C4-0571/97 — 00/0288(COD)).* Europäisches Parlament. Amtsblatt der Europäischen Union - Mitteilungen und Bekanntmachungen.

———. 1997c. *Sitzungsperiode 1997/1998 - Ausführlicher Sitzungsbericht vom 17. bis 21. November 1997*. Europagebäude, Straßburg: Europäisches Parlament. Amtsblatt der Europäischen Gemeinschaften - Verhandlungen des Europäischen Parlaments.

———. 2001a. *Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)).*

———. 2001b. „Plenardebatten - Mittwoch, 5. September 2001 - Datenschutz in der elektronischen Kommunikation". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20010905+ITEM-007+DOC+XML+V0//DE (12. Juni 2019).

———. 2001c. „Plenardebatten - Mittwoch, 5. September 2001 - Datenschutz in der elektronischen Kommunikation (Fortsetzung)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20010905+ITEM-011+DOC+XML+V0//DE&language=DE (12. Juni 2019).

———. 2001d. „Plenardebatten - Montag, 12. November 2001 - Elektronische Kommunikation und Schutz der Privatsphäre". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20011112+ITEM-009+DOC+XML+V0//DE&language=DE (13. Juni 2019).

———. 2002a. *Ergebnisse der namentlichen Abstimmungen vom 6. September 2001: Datenschutz in der elektronischen Kommunikation - Bericht Cappato A5-0270/2001.* . Mitteilungen und Bekanntmachungen.

———. 2002b. *Ergebnisse der namentlichen Abstimmungen vom 13. November 2001: Datenschutz in der elektronischen Kommunikation - Bericht Cappato A5-0374/2001.* . Mitteilungen und Bekanntmachungen.

———. 2002c. „Plenardebatten - Mittwoch, 29. Mai 2002 - Elektronische Kommunikation und Schutz der Privatsphäre". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20020529+ITEM-010+DOC+XML+V0//DE&language=DE (14. Juni 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2003. *Ergebnisse der namentlichen Abstimmung vom 30. Mai 2002 Elektronische Kommunikation und Schutz der Privatsphäre Empfehlung Cappato A5-0130/2002.* . Mitteilungen und Bekanntmachungen.

———. 2004. *Ergebnisse der namentlichen Abstimmung vom Dienstag, 9. März 2004: Bericht Cappato A5-0104/2004 Entschließung.* Europäisches Parlament. Mitteilungen und Bekanntmachungen.

———. 2005. *Terroristische Straftaten: Austausch von Informationen und nachrichtendienstlichen Erkenntnissen: Empfehlung des Europäischen Parlaments an den Europäischen Rat und den Rat zum Austausch von Informationen und zur Zusammenarbeit betreffend terroristische Straftaten.* Europäisches Parlament. Empfehlung.

———. 2006a. *Empfehlung des Europäischen Parlaments an den Rat zu den Entwicklungen in den Verhandlungen über den Rahmenbeschluss des Rates über den Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (2006/2286(INI)).*

———. 2006b. *Legislative Entschließung des Europäischen Parlaments zu dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (KOM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))*. Strasbourg.

———. 2006c. „Plenardebatten - Dienstag, 13. Juni 2006 - Schutz personenbezogener Daten (polizeiliche und justizielle Zusammenarbeit) (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20060613+ITEM-017+DOC+XML+V0//DE (19. Juni 2019).

———. 2006d. „Plenardebatten - Mittwoch, 13. Dezember 2006 - Datenschutz (Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20061213+ITEM-013+DOC+XML+V0//DE&language=DE (20. Juni 2019).

———. 2006e. „Plenardebatten - Mittwoch, 14. Juni 2006 - Schutz personenbezogener Daten (polizeiliche und justizielle Zusammenarbeit) (Abstimmung)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20060614+ITEM-004-03+DOC+XML+V0//DE (19. Juni 2019).

———. 2006f. „Plenardebatten - Mittwoch, 27. September 2006 - Raum der Freiheit, der Sicherheit und des Rechts — Gemeinsame Einwanderungspolitik (Aussprache)(Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20060927+ITEM-003+DOC+XML+V0//DE&language=DE (19. Juni 2019).

———. 2007. „Plenardebatten - Mittwoch, 6. Juni 2007 - Vertrag von Prüm: Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität – Visa-Informationssystem (VIS) – Zugang zum Visa-Informationssystem (VIS) für Datenabfragen – Schutz personenbezogener Daten (Fortsetzung der Aussprache)". *www.europaparl.europa.eu*. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070606+ITEM-018+DOC+XML+V0//DE&language=DE (21. Juni 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2017. „Abschaffung der Roaming-Gebühren wird Wirklichkeit | Aktuelles | Europäisches Parlament“. *www.europaparl.europa.eu*. http://www.europarl.europa.eu/news/de/headlines/economy/20170612STO77250/abschaffung-der-roaming-gebuhren-wird-wirklichkeit (18. Juli 2019).

———. 2020. „Das Parlament: Die Legislativbefugnis“. *Legislativbefugnis*. https://www.europarl.europa.eu/about-parliament/de/powers-and-procedures/legislative-powers (5. Januar 2020).

Europarat. 1981. *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*. Straßburg: Europarat. Sammlung Europäischer Verträge. https://www.coe.int/de/web/conventions/full-list (15. April 2019).

———. 2010. *Die Europäische Menschenrechtskonvention in der Fassung der Protokolle Nr. 11 und 14 samt Zusatzprotokoll und Protokolle Nr. 4, 6, 7, 12, 13 und 16*. Strasburg: Europarat.

European Academics. 2013. „Data Protection in Europe – Academics Are Taking a Position“. *Computer Law & Security Review* 29(2): 180–84.

European Commission. 1997. *Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation: Towards an Information Society Approach*. Brussels: European Commission.

———. 1998. *Summary of the Results of the Public Consultation on the Green Paper on the Convergence of the Telecommunications, MEdia and Information Technology Sectors; Areas for further reflection*. Brussels: Commission of the European Communities. Commission Working Document.

———. 1999. *The Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation: Results of the Public Consultation on the Green Paper [COM(97)623]*. Brussels: Commission of the European Communities. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions.

———. 2002. *Conference on the Implementation of Directive 95/46/EC (Data Protection), Brussels, 30 September - 1 October 2002 Final Programme*. European Commission.

———. 2005. „Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data“. *www.europa.eu.int*. https://web.archive.org/web/20050308163751/europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm (8. Juni 2019).

———. 2008. *Flash Eurobarometer 225: Data Protection in the European Union - Citizens' perceptions - Analytical Report*.

———. 2009a. „Consultation on the legal framework for the fundamental right to protection of personal data“. *Justice and Home Affairs - Newsroom - Consulting the public*. https://web.archive.org/web/20090715022458/http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm (18. August 2019).

———. 2009b. *Press Release: Data Protection Conference „Personal Data - More Use, More Protection?“*

———. 2009c. *Programme: Data Protection Conference „Personal data - more use, more protection?“* Brussels.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2010a. *Consultation with Private Stakeholders - Annex 3: List of Participants*. Brussels.

———. 2010b. *Draft Minutes of the Targeted Private Stakeholders' Consultation Future of Personal Data Protection - Annex 4*. Brussels: European Commission - DG Justice, Freedom and Security, Directorate D: Fundamental Rights and Citizenship, Unit D5: Data Protection. Draft Minutes.

———. 2010c. „Justice - News - Public Consultations: Consultation on the Commission's comprehensive approach on personal data protection in the European Union". *www.ec.europa.eu*. https://web.archive.org/web/20110317055139/http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm (16. Juli 2019).

———. 2010d. *Stakeholder's Consultations „Future of Data Protection"*. European Commission. Background Paper.

———. 2011a. „01 July 2010 Stakeholder Consultation Meeting on the Review of the Data Protection Regulatory Framework". *Justice - Newsroom - Events*. https://web.archive.org/web/20110314124908/http://ec.europa.eu/justice/news/events/events_en.htm#event_2010_07_01 (18. August 2019).

———. 2011b. *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union - Report*.

———. 2013. *Commission Welcomes European Parliament Rapporteurs' Support for Strong EU Data Protection Rules*. Brussels: European Commission. Memo.

———. 2015. *Juncker's Reply to EDri's letter*. Brussels.

———. 2017. „Studies - European Commission". *European Commission: Justice - Building a European Area of Justice*. https://web.archive.org/web/20170810200353/http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (25. August 2019).

European Commission DG InfSo. 2006. „Responses to the ‚CALL FOR INPUT on the forthcoming review of the EU regulatory framework for electronic communications and services including review of the Recommendation on relevant markets'". *www.ec.europa.eu*. https://web.archive.org/web/20070411224450/http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/public_consult/review/index_en.htm (17. Juli 2019).

European Commission: Directorate-General for Justice, Freedom and Security - Directorate C: Civil Justice, Fundamental Rights and Citizenship - The Director. 2008. *Open Invitation to tender JLS/2008/C4/011*. Brussels: European Commission.

European Communities. 1974. *Oral Question No. 193/73, with Debate, on Protecting the Privacy of the Community's Citizens*. Strasbourg, Europe House.

European Convention Presidency. 2000a. *Draft Charter of Fundamental Rights of the European Union*. Brussels.

———. 2000b. *Draft Charter of Fundamental Rights of the European Union – Proposed Articles (Articles 10 to 19)*. Brussels.

———. 2000c. *Draft List of Fundamental Rights*. Brussels.

European Data Protection Authorities. 2006a. *Budapest Declaration*. Budapest: Conference of European Data Protection Authorities.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2006b. *London Declaration Adopted by the European Data Protection Authorities*. London.

———. 2007. *Cyprus Declaration Adopted by the European Data Protection Authorities*. Cyprus.

———. 2013. *Lisbon Resolution on the Future of Data Protection in Europe*. Lisbon: Spring Conference 2013 of the European Data Protection Authorities.

European Parliament. 1999. „New Technical group formed". *The Week: 20-07-99(s)*. https://www.europarl.europa.eu/press/sdp/pointses/en/1999/p990720s.htm (7. Januar 2020).

European Union. 2005. *Results of vote in Parliament*.

EWSA. 2012. *Stellungnahme zur DSGVO*. Brüssel: Europäischer Wirtschafts- und Sozialausschuss (EWSA).

Expertengruppe „Grundrechte". 1999. *Die Grundrechte in der Europäischen Union verbürgen: Zeit zum Handeln ; Bericht der Expertengruppe „Grundrechte"*. Ms. abgeschlossen im Februar 1999. Luxemburg: Amt für Amtliche Veröff. der Europ. Gemeinschaften.

Facebook. 2012. „Comments from Facebook on the European Commission's proposal for a Regulation "On the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"". 156.

Farrell, Henry. 2003. „Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement". *International Organization* 57(2): 277–306.

———. 2004. „New Issue Areas in the Trans-Atlantic Relationship: E-Commerce and the Safe Harbor Arrangement". *University of Toronto*: 22.

FBF. 2011. „FBF RESPONSE: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS". 107.

———. 2012. „PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION)". 173.

FEDMA. 2011. „FEDMA submission on the Comprehensive Strategy on Data Protection in the European Union". 108.

Feld, Christian. 2013. „Reform des EU-Datenschutzes in weite Ferne gerückt". *tagesschau.de*. https://www.tagesschau.de/ausland/eu-datenschutz108.html (28. Oktober 2019).

Fenger, Menno, und Pieter-Jan Klok. 2001. „Interdependency, beliefs, and coalition behavior: A contribution to the advocacy coalition framework". *Policy sciences* 34(2): 157–70.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Fey, Marco. 2012. „Trauma 9/11 und die normative Ordnung der amerikanischen Sicherheitspolitik". In *Die Welt nach 9/11. Auswirkungen des Terrorismus auf Staatenwelt und Gesellschaft*, Sonderheft der Zeitschrift für Außen- und Sicherheitspolitik, Sonderheft 2/2011, hrsg. Thomas Jäger. Wiesbaden: VS Verlag für Sozialwissenschaften/Springer Fachmedien, 32–52.

Fiedler, Kirsten. 2013a. „Brüssel entscheidet über Eure Daten!" *netzpolitik.org*. https://netzpolitik.org/2013/brussel-entscheidet-uber-eure-daten/ (5. Oktober 2019).

———. 2013b. „Bye bye Datenschutz: EU-Parlament kopiert von Amazon, ebay & Co." *netzpolitik.org*. https://netzpolitik.org/2013/bye-bye-datenschutz-eu-parlament-kopiert-von-amazon-ebay-co/ (17. Februar 2020).

Filippi, Primavera De, und Danièle Bourcier. 2016. „"Three-Strikes" Response to Copyright Infringement: The Case of HADOPI". In *The Turn to Infrastructure in Internet Governance*, hrsg. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, und Nanette S. Levinson. New York: Palgrave Macmillan US, 125–52. http://link.springer.com/10.1057/9781137483591 (29. Januar 2018).

Finck, Michèle, European Parliament, European Parliamentary Research Service, und Scientific Foresight Unit. 2019. *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? : Study*. https://data.europa.eu/doi/10.2861/535 (9. Januar 2020).

Fleischer, Peter. 2011. „Peter Fleischer: Privacy...?: Foggy thinking about the Right to Oblivion". *Peterfleischer.blogspot.com*. http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (23. September 2019).

———. 2014. „Turning our Backs on 2013". *Peter Fleischer: Privacy...?* http://peterfleischer.blogspot.com/2014/01/turning-our-backs-on-2013.html (28. Oktober 2019).

Fleming, Jeremy. 2013. „New Data Protection Rules at Risk, EU Watchdog Warns". *www.euractiv.com*. https://www.euractiv.com/section/digital/news/new-data-protection-rules-at-risk-eu-watchdog-warns/ (24. Oktober 2019).

Focus Online. 2008. „Erneut gigantische Datenpanne". *www.focus.de*. https://www.focus.de/politik/ausland/grossbritannien-erneut-gigantische-datenpanne_aid_339766.html (9. Juli 2019).

Fontanella-Khan, James. 2013a. „Brussels: Astroturfing Takes Root". *Financial Times*. https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de#axzz2XLjof7HR (24. Oktober 2019).

———. 2013b. „Washington Pushed EU to Dilute Data Protection". *Financial Times*. http://www.ft.com/intl/cms/s/0/42d8613a-d378-11e2-95d4-00144feab7de.html (17. Oktober 2014).

Fontanella-Khan, James, und Bede McCarthy. 2013. „Brussels to Soften Data Protection Rules". *Financial Times*. https://www.ft.com/content/dbf20262-8685-11e2-b907-00144feabdc0 (10. Mai 2018).

Forgó, Nikolaus. 2014. „Und täglich grüßt die Datenschutzgrundverordnung ..." *Zeitschrift Datenschutz (ZD)* (53). https://www.beck.de/cms/main?docid=354464 (28. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Forschungsgruppe Wahlen. 2013. „Politbarometer November I 2013". *Forschungsgruppe Wahlen e.V.* https://www.forschungsgruppe.de/Umfragen/Politbarometer/Archiv/Politbarometer_2013/November_I_2013/ (4. März 2020).

———. 2014. „Politbarometer 2014 > Januar I 2014". *Forschungsgruppe Wahlen e.V.* http://www.forschungsgruppe.de/Umfragen/Politbarometer/Archiv/Politbarometer_2014/Januar_I_2014/ (4. März 2020).

Fouilleux, Eves, Jacques de Maillard, und Andy Smith. 2005. „Technical or Political? The Working Groups of the EU Council of Ministers". *Journal of European Public Policy* 12(4): 609–23.

FRA. 2012. *Jahresbericht 211 - Grundrechte: Herausforderungen und Erfolge im Jahr 2011*. Luxemburg: FRA - Agentur der Europäischen Union für Menschenrechte.

Frattini, Franco. 2007. „Closing speech on Public Security, Privacy and Technology". Gehalten auf der Conference on Public Security, Privacy and Technology, Brussels, Charlemagne building. https://web.archive.org/web/20080320181300/https://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/728&format=HTML&aged=0&language=EN&guiLanguage=en (10. Juli 2019).

Fritz, Johannes. 2013. *Netzpolitische Entscheidungsprozesse. Datenschutz, Urheberrecht und Internetsperren in Deutschland und Großbritannien*. Baden-Baden: Nomos.

Frühjahrskonferenz der Europäischen Datenschutzbeauftragten. 2005. *Erklärung von Krakau*. Krakau, Polen.

Gallagher, Ryan. 2013. „European Commissioner Squares Up to Eric Holder Over ‚Completely Illegal' Surveillance". *Slate Magazine*. https://slate.com/technology/2013/06/viviane-reding-european-commission-vice-president-on-meeting-with-eric-holder-over-surveillance.html (25. Oktober 2019).

Gallo, Marielle. 2013. *Opinion of the Committee on Legal Affairs (JURI) on the GDPR*. European Parliament - Committee on Legal Affairs (JURI). 234.

Garritzmann, Julian L. 2016. *The Political Economy of Higher Education Finance - The Politics of Tuition Fees and Subsidies in OECD Countries,1945–2015*. Berlin: Springer. https://www.palgrave.com/gp/book/9783319299129 (19. August 2019).

Gassmann, Hans Peter. 2010. „Session 1: The Development of the Privacy Guidelines". Gehalten auf der 30 Years after: The Impact of the OECD Privacy Guidelines, Paris. http://www.oecd.org/sti/ieconomy/44945922.doc (16. April 2019).

GDV. 2009. „Positionspapier zur Konsultation zur Überarbeitung der Richtlinie 95/46/EG vom 24. Oktober 1995: Beitrag des Gesamtverbandes der Deutschen Versicherungswirtschaft ID-Nummer 643780268-55". 49.

———. 2011. „Comments on the Communication from the European Commission of 4 November 2010 "A comprehensive approach on personal data protection in the European Union"". 112.

———. 2012a. „GDV Stellungnahme Artikel 11-21". 158.

———. 2012b. „GDV Stellungnahme Artikel 22-37". 158.

———. 2012c. „GDV Stellungnahme Artikel 73-78". 158.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Gellman, Robert, und Pam Dixon. 2016. „Failures of Privacy Self-Regulation in the United States". In *Enforcing Privacy*, hrsg. David Wright und Paul De Hert. Cham: Springer International Publishing, 53–77. http://link.springer.com/10.1007/978-3-319-25047-2_3 (4. September 2019).

General Secretariat of the Council of the European Union. 2002. *Structure and Number of JHA Working Parties and JHA Activities Other than Legislative Work (Reports, Evaluations, Etc.)*. Brussels: Council of the European Union. „I" Item Note.

George, Alexander Lawrence, und Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge; Mass: MIT. http://www.worldcat.org/oclc/465175071.

Gerber, Tim. 2012. „Innenminister Friedrich widerspricht EU-Plänen zur Datenschutzmodernisierung". *Heise Online*. https://www.heise.de/newsticker/meldung/Innenminister-Friedrich-widerspricht-EU-Plaenen-zur-Datenschutzmodernisierung-1413367.html (17. Februar 2018).

GILC. 2002. „Brief an Mr. Pat Cox zu Vorratsdatenspeicherung, 22. Mai 2002". *www.gilc.org*. http://gilc.org/cox_de.html (15. Juni 2019).

Golem. 2018. „Eine kurze Geschichte des CCC - die 1980er - Video.Golem.de". *Golem.de*. https://video.golem.de/internet/22281/eine-kurze-geschichte-des-ccc-die-1980er.html (8. Juli 2019).

González Fuster, Gloria. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham, Switzerland: Springer International Publishing.

Google. 2012. „Preliminary Views on the Proposed Data Protection and Privacy Regulation in the European Union". 145.

Goyal, Nihit, Michael Howlett, und Araz Taeihagh. 2021. „Why and How Does the Regulation of Emerging Technologies Occur? Explaining the Adoption of the EU General Data Protection Regulation Using the Multiple Streams Framework". *Regulation & Governance* 15(4): 1020–34.

Greenleaf, Graham. 2012. „The influence of European data privacy standards outside Europe: implications for globalization of Convention 108". *International data privacy law*: ips006.

Greenwood, Justin. 2011. *Interest representation in the European Union*. 3rd ed. Houndmills, Basingstoke, Hampshire ; New York: Palgrave Macmillan.

Greis, Friedhelm. 2015. „Fluggastdatenspeicherung: EU-Parlament macht Weg für PNR-Datenbank frei". *Golem.de*. http://www.golem.de/news/fluggastdatenspeicherung-eu-parlament-macht-weg-fuer-pnr-datenbank-frei-1502-112303.html (13. Februar 2015).

Greis, Friedhelm, Nico Ernst, und Jörg Thoma. 2013. „NSA: Chronologie der Enthüllungen von Edward Snowden". *Golem.de*. https://www.golem.de/news/nsa-chronologie-der-enthuellungen-von-edward-snowden-1307-100411.html (25. Oktober 2019).

Grupp, Dr Hariolf, Dr Harald Legler, und Barbara Breitschopf. 2003. *Zur technologischen Leistungsfähigkeit Deutschlands 2002*. Karlsruhe, Hannover: Fraunhofer Institut für System- und Innovationsforschung ISI, Niedersächsisches Institut für Wirtschaftsforschung, Institut für Wirtschaftspolitik und Wirtschaftsforschung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Gruppe „Telekommunikation und Informationsgesellschaft". 2008. *Vorbereitung der Tagung des Rates (Verkehr/Telekommunikation und Energie) am 27. November 2008*. Brussels: Rat der Europäischen Union. Bericht.

Gschwend, Thomas, und Frank Schimmelfennig. 2007. „Forschungsdesign in der Politikwissenschaft:Ein Dialog zwischen Theorie und Daten". In *Forschungsdesign in der Politikwissenschaft: Probleme - Strategien - Anwendungen*, hrsg. Thomas Gschwend und Frank Schimmelfennig. Frankfurt: Campus Verlag, 13–29.

GSMA. 2011. „GSMA Europe response to the European Commission consultation on "A comprehensive approach to personal data protection in the EU"". 113.

GSMA, ETNO, ECTA, und Cable Europe. 2012. „GSMA Europe – ETNO – ECTA – Cable Europe briefing papers on the Data Protection Regulation". 178.

GSMA Europe. 2009. „GSMA Europe response to the European Commission consultation on the framework for the fundamental right to the protection of personal data". 50.

Guarascio, Francesco. 2012. „US lobbying waters down EU data protection reform". *EURACTIV.com*. http://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/ (30. Juni 2017).

Günther, Oliver u. a. 2013. „Datenschutz-Verordnung: Auch anonyme Daten brauchen Schutz". *Die Zeit*. https://www.zeit.de/digital/datenschutz/2013-02/stellungnahme-datenschutz-professoren/komplettansicht (1. Oktober 2019).

Gusy, Christoph. 2014. „Architektur und Rolle der Nachrichtendienste in Deutschland". *Aus Politik und Zeitgeschichte, Beilage zur Wochenzeitung 'Das Parlament'* 64. Jahrgang(18-19/2014): 9–14.

Gutjahr, Richard. 2013. „LobbyPlag: Die Copy & Paste-Gesetzgeber aus Brüssel | G! gutjahrs blog". http://gutjahr.biz/2013/02/lobbyplag/? (10. September 2014).

———. 2015. „» Datenschlussverkauf in Brüssel | G! gutjahrs blog". *gutjahr.biz*. https://www.gutjahr.biz/2015/03/lobbyplag-dataleaks-2/ (30. Oktober 2019).

Hajer, Maarten, und David Laws. 2008. „Ordering through Discourse". In *Goodin, Robert E./Moran, Michael/Rein, Martin (Hrsg.): The Oxford Handbook of Public Policy*, Oxford/New York: Oxford University Press, 251–68.

Hall, Peter A. 2008. „Systematic Process Analysis When and How to Use It!". *European Political Science* 7(3): 304–17.

Harbour, Malcolm, und Alexander Alvaro. 2008. *Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz*. Europäisches Parlament.

Harmsen, Robert, und Menno Spiering, hrsg. 2004. *Euroscepticism: Party Politics, National Identity and European Integration*. Amsterdam: Rodopi.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Härting, Niko. 2013. „Datenschutzreform in Europa: Einigung im EU-Parlament Kritische Anmerkungen". In *Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation*, Otto Schmidt, 715–21. http://www.computerundrecht.de/media/CR_2013_S._715_Haerting_Datenschutzreform_in_Europa_Einigung_im_EU-Parlament.pdf (1. August 2014).

Härting, Niko, und Jörn Lübben. 2013. „Vom Verbotsprinzip zur Risikoorientierung". *Härting Rechtsanwälte*. https://www.haerting.de/neuigkeit/vom-verbotsprinzip-zur-risikoorientierung (10. Mai 2018).

Hayes, Ben, und Chris Jones. 2013. *Catalogue of EU Counter-Terrorism Measures Adopted since 11 September 2001*. http://www.statewatch.org/news/2013/dec/secile-catalogue-of-EU-counter-terrorism-measures.pdf (25. Februar 2015).

Hayes, Ben, Steve Peers, und Tony Bunyan. 2004. *"Scoreboard" on post-Madrid counter-terrorism plans*. Statewatch.

Hayes-Renshaw, Fiona. 2017. „The Council of Ministers: Conflict, Consensus, and Continuity". In *The institutions of the European Union*, New european union series (neu), hrsg. Dermot Hodson und John Peterson. New York, NY: Oxford University Press, 80–107.

Heath, Nick. 2013. „EU Privacy Laws to Spell an End to Facebook for Free?" *ZDNet*. https://www.zdnet.com/article/eu-privacy-laws-to-spell-an-end-to-facebook-for-free/ (8. Oktober 2019).

Hecking, Claus. 2013. „Deutsche Beamte bremsen Europas Datenschutz aus". *Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html (4. September 2014).

Heclo, Hugh. 1974. *Modern Social Politics in Britain and Sweden: From Relief to Income Maintenance*. New Haven and London: Yale University Press.

Heikkila, Tanya, und Paul Cairney. 2017. „Comparison of Theories of the Policy Process". In *Theories of the Policy Process*, hrsg. Christopher M. Weible und Paul A. Sabatier. New York, NY: Routledge, 301–28.

Hellmann, Vanessa. 2009. *Der Vertrag von Lissabon: vom Verfassungsvertrag zur Änderung der bestehenden Verträge: Einführung mit Synopse und Übersichten*. Berlin Heidelberg: Springer.

Henry, Adam Douglas. 2011. „Ideology, power, and the structure of policy networks". *Policy Studies Journal* 39(3): 361–83.

Hering, Linda, und Robert J. Schmidt. 2014. „Einzelfallanalyse". In *Handbuch Methoden der empirischen Sozialforschung*, hrsg. Nina Baur und Jörg Blasius. Wiesbaden: Springer Fachmedien Wiesbaden, 529–41. http://link.springer.com/10.1007/978-3-531-18939-0_37 (13. November 2019).

Hermida, Alfred. 2006. „UK Rapped on Data Retention Law". *BBC News*. http://news.bbc.co.uk/2/hi/technology/4744304.stm (26. August 2019).

de Hert, Paul, und Vagelis Papakonstantinou. 2009. „The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – A Modest Achievement However Not the Improvement Some Have Hoped For". *Computer Law & Security Review* 25(5): 403–14.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2014. „The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on Its Global Ambition". *Computer Law & Security Review* 30(6): 633–42.

———. 2016. „The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" *Computer Law & Security Review* 32(2): 179–94.

Hert, Paul De, Vagelis Papakonstantinou, und Cornelia Riehle. 2008. „Chapter 6 – Data Protection in the Third Pillar: Cautious Pessimism". In *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, hrsg. Martin Maik. London, UK: Justice, 75.

Herweg, Nicole. 2013. „Der Multiple-Streams-Ansatz – ein Ansatz, dessen Zeit gekommen ist?" *Zeitschrift für Vergleichende Politikwissenschaft* 7(4): 321–45.

———. 2015. „Multiple Streams Ansatz". In *Handbuch Policy-Forschung*, hrsg. Georg Wenzelburger und Reimut Zohlnhöfer. Wiesbaden: Springer Fachmedien Wiesbaden, 325–54.

Hijmans, Hielke. 2006. „The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority". *Common Market Law Review* (43): 1313–42.

Hijmans, Hielke, und Alfonso Scirocco. 2009. „Shortcomings in EU Data Protection in the third and the second pillars. Can the Lisbon Treaty be expected to help? " *Common Market Law Review* (46): 1485–1525.

Hildén, Jockum. 2019. „The Politics of Datafication : The Influence of Lobbyists on the EU's Data Protection Reform and Its Consequences for the Legitimacy of the General Data Protection Regulation". https://helda.helsinki.fi/handle/10138/305981 (6. Dezember 2022).

Hirsch, Nadja. 2013. *Opinion of the Committee on Employment and Social Affairs (EMPL) on the GDPR*. European Parliament - Committee on Employment and Social Affairs (EMPL). 231.

Hochrangige Beratende Gruppe zur Zukunft der Europäischen Justizpolitik. 2008. *Lösungsvorschläge für das zukünftige Programm der EU im Justizbereich*. Brüssel: Rat der Europäischen Union.

Hofferbert, Richard I. 1974. *Study of Public Policy*. Imprint unknown.

Hohage, Christoph. 2013. *Moschee-Konflikte*. Wiesbaden: Springer Fachmedien. http://link.springer.com/10.1007/978-3-658-03624-9 (28. Mai 2014).

Holznagel, Bernd, und Raymund Werle. 2004. „Sectors and strategies of global communications regulation". *Knowledge, Technology & Policy* 17(2): 19–37.

Hondius, Frits W. 1975. *Emerging Data Protection in Europe*. Amsterdam : New York: American Elsevier Pub. Co.

Hoon, Geoffrey. 1992. *Legislative Entschließung (Verfahren der Zusammenarbeit: Erste Lesung) mit der Stellungnahme des Europäischen Parlaments zu dem Vorschlag der Kommission an den Rat für eine Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (Hoon-Bericht)*. Ausschuss für Recht und Bürgerrechte - Europäisches Parlament. Europäisches Parlament Sitzungsperiode 1991-1992 - Sitzung vom 9. bis 13. März 1992.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Horchert, Judith. 2014. „‚Freiheit statt Angst': Tausende demonstrieren in Berlin gegen Überwachung". *Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-demonstration-gegen-ueberwachung-in-berlin-a-989016.html (28. Januar 2015).

Hornung, Gerrit. 2012. „Eine Datenschutz-Grundverordnung für Europa: Licht und Schatten im Kommissionsentwurf vom". *Zeitschrift Datenschutz* 25(2012): 99–106.

———. 2019. „Artikel 3 Räumlicher Anwendungsbereich". In *Datenschutzrecht: DSGVO mit BDSG*, NomosKommentar, hrsg. Spiros Simitis, Gerrit Hornung, und Indra Spiecker Döhmann. Baden-Baden: Nomos, 265–82.

Hornung, Gerrit, und Korbinian Hartl. 2014. „Datenschutz durch Marktanreize–auch in Europa?" *Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD* 219.

Horten, Monica. 2012. „Reding handbags DeGucht over ECJ referral". *iptegrity.com*. http://www.iptegrity.com/index.php/acta/746-reding-handbags-degucht-over-ecj-referral (2. Oktober 2019).

Horvath, John. 1996. „Die Unabhängigkeit des Internet und der Massengeist". *Telepolis*. http://www.heise.de/tp/artikel/1/1019/ (25. Februar 2015).

Hülsmann, Werner. 2012. „Bundesinnenministerium immer wieder für eine Überraschung gut – Ein Grundprinzip des Datenschutzes wird offen in Frage gestellt". *Blog eines Datenschutzsachverständigen*. https://extdsb.wordpress.com/2012/06/29/bundesinnenministerium-immer-wieder-fur-eine-uberraschung-gut-grundprinzip-des-datenschutzes-wird-offen-in-frage-gestellt/ (12. Februar 2018).

Hummer, Waldemar. 2011. „Die SWIFT-Affäre. US-Terrorismusbekämpfung versus Datenschutz". *Archiv des Völkerrechts* 49(3): 203–45.

Hustinx, Peter. 2014. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. European Data Protection Supervisor (EDPS).

IAB Europe. 2010. „IAB Europe Response to European Commission Consultation on the DP Framework". 51.

———. 2011. „IAB Europe Response to European Commission Consultation on the DP Framework". 114.

ICC. 2011. „International Chamber of Commerce (ICC) Comments on EU Directive: 95/46/EC". 115.

———. 2013. „ICC comments on EU General Data Protection Regulation Issues". 219.

ICDP. 2011. „Industry Coalition for Data Protection Paper on proposals for a "New EU legal framework on data protection"". 140.

———. 2012. *Reforming Europe's Privacy Framework - How to find the right balance*.

———. 2013a. *Industry Concerned Over Negative Impact of Albrecht Draft Report*. Brussels: Industry Coalition for Data Protection (ICDP).

———. 2013b. „Industry Groups Call on Council, European Parliament to Achieve Workable Data Protection Regulation". *Europe internet services providers association*. http://www.euroispa.org/industry-groups-call-council-european-parliament-achieve-workable-data-protection-regulation/ (20. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2015a. *EU Data Protection Reform: Industry Cautious on Council General Approach*. Industry Coalition for Data Protection (ICDP). Press Release.

———. 2015b. *Europe's New Data Rules Take a Wrong Turn*. Brussels: Industry Coalition for Data Protection (ICDP). Press Release.

———. 2015c. *Open Letter to the EU Institutions on the General Data Protection Regulation „The Opportunity for Trialogues"*. Brussels: Industry Coalition for Data Protection (ICDP).

ICDPPC. 1989. *Berlin Resolution of the international Conference of Data Protection Commissioners of 30 August 1989*. Berlin: International Conference of Data Protection and Privacy Commissioners.

———. 2017. „History of the Conference – International Conference of Data Protection & Privacy Commissioners". *icdppc.org*. https://icdppc.org/the-conference-and-executive-committee/history-of-the-conference/ (2. Juni 2019).

ICO. 2011. „The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union". 88.

Ingold, Karin. 2011. „Network structures within policy processes: Coalitions, power, and brokerage in Swiss climate policy". *Policy Studies Journal* 39(3): 435–59.

Intel. 2009. „Intel corporation responste to European Commission public consultation on the legal framework for the fundamental right to protection of personal data". 53.

Irische Ratspräsidentschaft. 2013. *Programm des irischen Vorsitzes im Rat der Europäischen Union 1. Januar - 30. Juni 2013*.

Irmisch, Anna. 2011. *Astroturf: eine neue Lobbyingstrategie in Deutschland?* 1. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften.

ITRE-Ausschuss. 2012. *Protokoll der Mini-Anhörung zum Thema „Perspektiven der Datenschutz-Grundverordnung für die Bereiche Industrie und Forschung"*. Brüssel: Europäisches Parlament - Ausschuss für Industrie, Forschung und Energie (ITRE). Protokoll.

Jackson, Caroline. 1993. „The First British MEPs: Styles and Strategies". *Contemporary European History* 2(2): 169–95.

Jacobs, Alan M. 2014. „Process Tracing the Effects of Ideas". In *Process Tracing*, hrsg. Andrew Bennett und Jeffrey T. Checkel. Cambridge: Cambridge University Press, 41–73. https://www.cambridge.org/core/product/identifier/CBO9781139858472A011/type/book_part (8. März 2019).

James Losey. 2014. „The Anti-Counterfeiting Trade Agreement and European Civil Society: A Case Study on Networked Advocacy". *Journal of Information Policy* 4: 205.

Jančiūtė, Laima. 2018. „EU Politics and the Making of the General Data Protection Regulation: Consociationalism, Policy Networks and Institutionalism in the Process of Balancing Actor Interests". University of Westminster.

Jaspers, Andreas. 2012. „Die EU-Datenschutz-Grundverordnung". *Datenschutz und Datensicherheit-DuD* 36(8): 571–75.

Jenkins-Smith, Hank C., Daniel Nohrstedt, Christopher M. Weible, und Karin Ingold. 2017. „The Advocacy Coalition Framework: An Overview of the Research Program". In *Theories of the Policy Process*, hrsg. Christopher M. Weible und Paul A. Sabatier. New York, NY: Routledge, 135–71.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Jenkins-Smith, Hank C., Daniel Nohrstedt, Christopher M. Weible, und Paul A. Sabatier. 2014. „The Advocacy Coalition Framework: Foundations, Evolution, and Ongoing Research". In *Theories of the Policy Process*, hrsg. Paul A. Sabatier und Christopher M. Weible. Boulder, CO: Westview Press, 183–223.

Jenkins-Smith, Hank C., und Paul A. Sabatier. 1993a. „Methodological Appendix: Measuring Longitudinal Change in Elite Beliefs Using Content Analysis of Public Documents". In *Policy Change and Learning: An Advocacy Coalition Approach*, Theoretical Lenses on Public Policy, hrsg. Paul A. Sabatier und Hank C. Jenkins-Smith. Boulder, Colo.: Westview Press, 237–56.

———. 1993b. „The Study of Public Policy Processes". In *Policy Change and Learning: An Advocacy Coalition Approach*, Theoretical Lenses on Public Policy, hrsg. Paul A. Sabatier und Hank C. Jenkins-Smith. Boulder, Colo.: Westview Press, 1–9.

Jenkins-Smith, Hank C., und Gilbert St. Clair. 1993. „The Politics of Offshore Energy: Empirically Testing the Advocacy Coalition Framework". In *Policy Change and Learning: An Advocacy Coalition Approach*, Theoretical Lenses on Public Policy, hrsg. Paul A. Sabatier und Hank C. Jenkins-Smith. Boulder, Colo.: Westview Press, 149–75.

Jur. Dienst d. Rats. 2013. *Wirksamer Schutz der Grundrechte betroffener Personen im Kontext des geplanten Prinzips der zentralen Kontaktstelle*. Brüssel: Rat der Europäischen Union - Juristischer Dienst.

Kalyanpur, Nikhil, und Abraham L. Newman. 2019. „The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation". *JCMS: Journal of Common Market Studies* 57(3): 448–67.

Karaboga, Murat u. a. 2015. *White Paper Das versteckte Internet: Zu Hause - Im Auto - Am Körper*. 1. Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung. https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (25. Februar 2015).

———. 2018. „Die Datenschutzpolitik der EU auf dem Weg zur Konsolidierung? Zuständigkeitsstrukturen für Datenschutzpolitiken in Kommission, Ministerrat und Parlament zwischen 1990 und 2017". In *Privatheit und selbstbestimmtes Leben in der digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen*, hrsg. Michael Friedewald. Wiesbaden: Springer Fachmedien Wiesbaden, 127–75. http://link.springer.com/10.1007/978-3-658-21384-8_5 (8. April 2018).

Kayali, Laura. 2015. „Snowden's biggest European fan stays loyal". *Politico.eu*. http://www.politico.eu/article/snowdens-biggest-european-fan-stays-loyal/ (19. Januar 2016).

Kazim, Hasnain. 2014. „BND-Spionage in der Türkei: Ankara verärgert über Deutschland". *Spiegel Online*. http://www.spiegel.de/politik/ausland/bnd-spionage-in-der-tuerkei-ankara-veraergert-ueber-deutschland-a-986528.html (18. August 2014).

Kelly, Sean. 2013. *Opinion of the Committee on Industry, Research and Energy (ITRE) on the GDPR*. European Parliament - Committee on Industry, Research and Energy (ITRE). 230.

King, Gary, Robert O. Keohane, und Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, N.J: Princeton University Press.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Kirby, Michael. 1980. „An Introduction to the Basic Rules of Data Protection and Data Security". Gehalten auf der Australien & New Zealand Association for the Advancement of Science Jubilee Congress, Adelaide.

———. 2011. „The History, Achievement and Future of the 1980 OECD Guidelines on Privacy". Gehalten auf der 30 Years after: The Impact of the OECD Privacy Guidelines, Paris. https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipq002 (16. April 2019).

Klingst, Martin. 2001. „Persönliche Daten: ‚Datenschutz = Terroristenschutz? Unsinn!' Ein Gespräch mit Spiros Simitis, dem Vater des deutschen Datenschutzrechts". *Die Zeit*. https://www.zeit.de/2001/41/200141_datenschutz.xml/komplettansicht (28. Mai 2019).

Kluger Dionigi, Maja. 2017. *Lobbying in the European Parliament*. Cham: Springer International Publishing. http://link.springer.com/10.1007/978-3-319-42688-4 (14. August 2017).

Klüver, Heike. 2013. *Lobbying in the European Union: Interest Groups, Lobbying Coalitions, and Policy Change*. Oxford: Oxford University Press.

Knyrim, Rainer. 2013. „Entwurf der neuen EU-Datenschutz-Grundverordnung". In *Scholz, Matthias / Funk, Axel (Hrsg.): DGRI Jahrbuch 2012, Informationstechnik und Recht*, Tagungsband, Köln: Verlag Dr. Otto Schmidt, 25–38.

Koch, Dieter L. 2013. *Maximalforderungen verteuern Dienstleistungen Datenschutz gibt es nicht zum Nulltarif.* . Infobrief.

Kohnstamm, Jacob. 2010. „New European Rules on Data Protection?" Gehalten auf der Joint High Level Meeting on Data Protection Day. 132.

KOM. 1990. Amtsblatt der Europäischen Gemeinschaften 90/C 277/03 *Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten*.

———. 1992. *Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.* . Amtsblatt der Europäischen Gemeinschaften 35. Jahrgang.

———. 1995. *Stellungnahme der Kommission gemäß Artikel 189b, Absatz 2, Buchstabe d) des EG-Vertrags zu den Abänderungen des Europäischen Parlaments des gemeinsamen Standpunkts des Rates betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. Brüssel: Kommission der Europäischen Gemeinschaften.

———. 2003. *Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46)*. Brüssel: Kommission der Europäischen Gemeinschaften. Bericht der Kommission.

———. 2007. *Mitteilung der Kommission an das Europäische Parlament und an den Rat: Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie*. Brüssel: Kommission der Europäischen Gemeinschaften.

———. 2010a. *Kommission schafft zwei neue Generaldirektionen und baut höhere Führungsebene um*. Brüssel: Europäische Kommission. Pressemitteilung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2010b. *Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union*. Brüssel: Europäische Kommission. Mitteilung der Kommission.

———. 2015a. *Special Eurobarometer 431: Datenschutz*. Europäische Kommission. Report.

———. 2015b. *Strategie für einen digitalen Binnenmarkt für Europa*. Brüssel: Europäische Kommission. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen.

Komitee der Weisen. 1996. *Für ein Europa der politischen und sozialen Grundrechte: Brüssel, Oktober 1995 - Februar 1996*. Luxemburg: Amt für Amtliche Veröff. der Europ. Gemeinschaften.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder u. a. 2016. „2016_Konferenz der Datenschutzbeuaftragten_Bewertung DSGVO.pdf". *DANA - Datenschutz Nachrichten* (2): 75–77.

Koops, Bert-Jaap. 2014. „The trouble with European data protection law". *International Data Privacy Law* 4(4): 250–61.

Korff, Douwe. 2002. *EC Study on Implementation of Data Protection Directive - Comparative Summary of National Laws*. Cambridge, UK: Human Rights Centre (University of Essex), Colchester UK.

Korff, Douwe, und Ian Brown. 2010. *Vergleichende Studie über verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen - Schlussbericht*. Cambridge/London/Oxford: LRDP Kantor Ltd (Leader) in Zusammenarbeit mit Centre for Public Reform (CPR). Studie für die Europäische Kommission - Generaldirektion Justiz, Freiheit und Sicherheit.

Krempl, Stefan. 1997. „Die Informationsgesellschaft in Europa und ihre Macher: People first?!" *heise online*. https://www.heise.de/tp/features/Die-Informationsgesellschaft-in-Europa-und-ihre-Macher-People-first-3411347.html (7. Januar 2020).

———. 2002. „Der lange Weg zur europäischen Cyber-Rights-Union". *Telepolis*. https://www.heise.de/tp/features/Der-lange-Weg-zur-europaeischen-Cyber-Rights-Union-3423213.html (15. Juni 2019).

———. 2008a. „EU-Rat verabschiedet laxe Regeln zum Datenschutz im Bereich innere Sicherheit". *Heise Online*. https://www.heise.de/newsticker/meldung/EU-Rat-verabschiedet-laxe-Regeln-zum-Datenschutz-im-Bereich-innere-Sicherheit-218725.html (12. Februar 2018).

———. 2008b. „Illegaler Handel mit Kundendaten: Der ‚GAU' wird immer noch größer". *Heise Online*. https://www.heise.de/newsticker/meldung/Illegaler-Handel-mit-Kundendaten-Der-GAU-wird-immer-noch-groesser-197174.html (24. Februar 2018).

———. 2009a. „EU-Datenschützer fordert unabhängige Agentur für zentralisierte Fahndungsdatenbank [Update]". *Heise Online*. https://www.heise.de/newsticker/meldung/EU-Datenschuetzer-fordert-unabhaengige-Agentur-fuer-zentralisierte-Fahndungsdatenbank-Update-879500.html (15. Juli 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2009b. „Fünfjahresplan zur Sicherheitspolitik der EU verabschiedet". *Heise Online*. http://www.heise.de/newsticker/meldung/Fuenfjahresplan-zur-Sicherheitspolitik-der-EU-verabschiedet-884130.html (11. November 2016).

———. 2012a. „29C3: Bürgerrechtler warnen vor Scheitern der EU-Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/29C3-Buergerrechtler-warnen-vor-Scheitern-der-EU-Datenschutzreform-1774878.html (13. Februar 2018).

———. 2012b. „Datenschutz: Friedrich für mehr Selbstkontrolle der Wirtschaft". *Heise Online*. https://www.heise.de/newsticker/meldung/Datenschutz-Friedrich-fuer-mehr-Selbstkontrolle-der-Wirtschaft-1731717.html (12. Februar 2018).

———. 2012c. „EU-Parlament segnet Fluggastdaten-Transfer in die USA ab". *heise online*. http://www.heise.de/newsticker/meldung/EU-Parlament-segnet-Fluggastdaten-Transfer-in-die-USA-ab-1542874.html (24. Februar 2015).

———. 2012d. „Konzerne sehen geplante EU-Datenschutzreform skeptisch". *Heise Online*. https://www.heise.de/newsticker/meldung/Konzerne-sehen-geplante-EU-Datenschutzreform-skeptisch-1569494.html (12. Februar 2018).

———. 2012e. „Marketing-Experten kritisieren geplante EU-Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/Marketing-Experten-kritisieren-geplante-EU-Datenschutzreform-1586145.html (13. Februar 2018).

———. 2013a. „Brüsseler Erklärung für starke EU-Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/Bruesseler-Erklaerung-fuer-starke-EU-Datenschutzreform-1792169.html (13. Februar 2018).

———. 2013b. „EU-Rat will Datenschutzreform verwässern". *Heise Online*. https://www.heise.de/newsticker/meldung/EU-Rat-will-Datenschutzreform-verwaessern-1861432.html (12. Februar 2018).

———. 2013c. „Keine Einigung auf EU-Datenschutzreform im EU-Rat". *Heise Online*. http://www.heise.de/newsticker/meldung/Keine-Einigung-auf-EU-Datenschutzreform-im-EU-Rat-2062360.html (26. Januar 2014).

———. 2013d. „US-Diplomat warnt vor Handelskrieg wegen EU-Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/US-Diplomat-warnt-vor-Handelskrieg-wegen-EU-Datenschutzreform-1792765.html (13. Februar 2018).

———. 2017. „Privacy Shield: EU-Datenschützer distanzieren sich von der Kommission". *Heise Online*. https://www.heise.de/newsticker/meldung/Privacy-Shield-EU-Datenschuetzer-distanzieren-sich-von-der-Kommission-3871043.html (12. Februar 2018).

Krosnick, Jon A. 1999. „Survey Research". *Annual Review of Psychology* 50(1): 537–67.

Lahmann, Henning. 2015. *Gesellschaftliche Konfliktlinien im Kontext von Big Data am Beispiel von Smart Health und Smart Mobility*. . Diskussionspapier.

Landes, David. 2013. „Sweden enters fray in EU data privacy fight - The Local". *The Local - Sweden's News in English*. http://www.thelocal.se/20130121/45734#.UP_3f2d1_JQ (23. Juni 2014).

Larsen, Jakob Bjerg, Karsten Vrangbæk, und Janine M. Traulsen. 2006. „Advocacy Coalitions and Pharmacy Policy in Denmark—Solid Cores with Fuzzy Edges". *Social Science & Medicine* 63(1): 212–24.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Laurer, Moritz, und Timo Seidl. 2021. „Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation". *Policy & Internet* 13(2): 257–77.

Legal Affairs Committee of the EP und Lord Mansfield. 1975. *Interim Report Drawn on Behalf of the Legal Affairs Committee on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*. Luxembourg: European Communities.

Legislative Observatory European Parliament. 2019. „Procedure File: 2012/0011(COD) | Legislative Observatory | European Parliament". *www.oeil.secure.europarl.europa.eu*. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011(OLP) (4. Oktober 2019).

Leisegang, Daniel. 2013b. „Schöne neue Überwachungswelt". *Blätter für deutsche und internationale Politik* (8/2013): 5–8.

Leisse, Olaf, hrsg. 2010. *Die Europäische Union nach dem Vertrag von Lissabon*. 1. Aufl. Wiesbaden: VS, Verlag für Sozialwissenschaften.

Lelieveldt, Herman, und Sebastiaan Princen. 2015. *The politics of the European Union*. Cambridge University Press. http://books.google.com/books?hl=en&lr=&id=hetBCgAAQBAJ&oi=fnd&pg=PR20&dq=%22to+the+provisions+of+relevant+collective+licensing%22+%22catalogue+record+for+this+publication+is+available+from+the+British%22+%22of+cambridge+University%22+%22cm.+%E2%80%93+(cambridge+textbooks+in+comparative%22+&ots=vmc2pUN7EO&sig=x_sUR6dTP8LtmpSvcuxmRzh7aTQ (21. Dezember 2016).

Lewinski, Kai von. 2009. „Geschichte des Datenschutzrechts von 1600 bis 1977". In *Freiheit - Sicherheit - Öffentlichkeit: 48. Assistententagung Öffentliches Recht, Heidelberg 2008*, hrsg. Felix Arndt u. a. Baden-Baden: Nomos, 196–220.

LIBE Committee. 2012. *Draft Agenda: Workshop on the Proposed Data Protection Regulation*. Brussels, Room Hemicycle: European Parliament - Committee on Civil Liberties, Justice and Home Affairs (LIBE).

LIBE-Ausschuss. 2012a. *Arbeitsdokument 2 zur DSGVO*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

———. 2012b. *Arbeitsdokument 3 zur DSGVO*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

———. 2012c. *Arbeitsdokument zur DSGVO*. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament.

———. 2012d. *Sitzung vom 12. April 2012*. https://www.europarl.europa.eu/ep-live/de/committees/video?event=20120412-0900-COMMITTEE-LIBE (4. Oktober 2019).

———. 2015a. *Berichterstatter erläutert den Stand der laufenden Trilogverhandlungen*. Brüssel: Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament. Protokoll.

———. 2015b. *Berichterstattung gegenüber dem Ausschuss über den Stand der Trilogverhandlungen*. Brüssel: Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament. Protokoll.

———. 2015c. *Stand der laufenden Trilog-Verhandlungen*. Brüssel: Ausschuss für bürgerliche Freiheiten, Justiz und Inneres - Europäisches Parlament. Protokoll.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Liberty Global. 2009. „Liberty Global response to the European Commission's public consultation on the legal framework for the fundamental right to protection of personal data". 54.

———. 2011. „Liberty Global response to the European Commission's public consultation on a comprehensive approach on data protection in the European Union". 117.

Lijphart, Arend. 1971. „Comparative Politics and the Comparative Method". *American Political Science Review* 65(03): 682–93.

Little, Roderick J. A., und Donald B. Rubin. 2019. *Statistical Analysis with Missing Data*. Third edition. Hoboken, NJ: Wiley.

LobbyPlag. 2013. „Amendments/Overview". *LobbyPlag.eu*. http://lobbyplag.eu/map (11. Mai 2014).

———. 2015. „LobbyPlag: Governments Rating". *LobbyPlag.eu*. http://lobbyplag.eu/governments (30. Oktober 2019).

Long, William J., und Marc Pang Quek. 2002. „Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise". *Journal of European Public Policy* 9(3): 325–44.

Lord Avebury. 2006. *Speech at the Joint Parliamentary Meeting on EU developments in the area of freedom, security and justice at the European Parliament*. Heiligendamm. http://www.statewatch.org/news/2006/oct/eric-avebury-heiligendamm1.pdf (19. Juni 2019).

Lovink, Geert, und Pit Schultz. 1996. „Der Anti-Barlow". *Telepolis*. http://www.heise.de/tp/artikel/1/1030/ (25. Februar 2015).

Ludford, Sarah. 2013a. „EU Data Protection, dialogue on draft Regulation | Sarah Ludford MEP". *Sarah Ludford Homepage*. https://web.archive.org/web/20140101004704/http://www.sarahludfordmep.org.uk/node/2238 (30. Juni 2017).

———. 2013b. „‚Privacy need not be compromised': letter in Financial Times | Sarah Ludford MEP". *Sarah Ludford Homepage*. https://web.archive.org/web/20140101005503/http://www.sarahludfordmep.org.uk/node/2188 (30. Juni 2017).

———. 2013c. „Sarah Ludford writes …Creating EU Data Protection rules that safeguard both privacy and jobs". *Liberal Democrat Voice*. http://www.libdemvoice.org/sarah-ludford-writes-creating-eu-data-protection-rules-that-safeguard-both-privacy-and-jobs-34758.html (30. Juni 2017).

Lüke, Falk. 2006. „Big Brother Awards: Ein Preis, den keiner will". *Die Zeit*. https://www.zeit.de/online/2006/43/big-brother-awards-2006/komplettansicht (8. Juli 2019).

———. 2012. „USA beanspruchen Mitspracherecht bei EU-Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/USA-beanspruchen-Mitspracherecht-bei-EU-Datenschutzreform-1445922.html (23. Oktober 2019).

MacAskill, Ewen u. a. 2013. „GCHQ taps fibre-optic cables for secret access to world's communications". *The Guardian*. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (25. Juni 2014).

MacDonald, Raegan. 2013. „European Parliament Vote on Privacy Regulation: Major Losses Obscure Other Gains". *Access Now*. https://www.accessnow.org/european-parliament-vote-on-privacy-regulation-major-losses-obscure-other-g/ (4. März 2020).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

MacKenzie, Alex, Christian Kaunert, und Sarah Léonard. 2015. „Counter-Terrorism: Supranational EU Institutions Seizing Windows of Opportunity". In *Policy Change in the Area of Freedom, Security and Justice: How EU Institutions Matter*, Routledge studies on government and the European Union, hrsg. Florian Trauner. London: Routledge, 93–113.

Mahoney, James. 2007. „Qualitative Methodology and Comparative Politics". *Comparative Political Studies* 40(2): 122–44.

———. 2010. „After KKV: The New Methodology of Qualitative Research". *World Politics* 62(01): 120–47.

Mahony, Honor. 2009a. „Barroso to Publish Policy Programme for next Commission". *EUobserver*. https://euobserver.com/news/28610 (2. September 2019).

———. 2009b. „Next Commission Set for Human Rights Post". *EUobserver*. https://euobserver.com/news/28643 (2. September 2019).

Mantelero, Alessandro. 2013. „The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'". *Computer Law & Security Review* 29(3): 229–35.

Maras, Marie-Helen. 2011. „While the European Union was Sleeping, the Data Retention Directive Was Passed: The Political Consequences of Mandatory Data Retention." *Hamburg Review of Social Sciences* 6(2). http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=18623921&AN=73466897&h=pjpyaul5DX8ePwui2YANV61BlKRrB6gBZnMi9xNNrzcNfv%2BFppMa8NaIsgxwP5VkyJvHLNtB79YKL58DnwPlpg%3D%3D&crl=c (19. April 2014).

Marshall, David. 2012. „Do Rapporteurs Receive Independent Expert Policy Advice? Indirect Lobbying via the European Parliament's Committee Secretariat". *Journal of European Public Policy* 19(9): 1377–95.

Marshall, David John. 2012. „Organised interest representation and the European Parliament". London School of Economics and Political Science. http://core.ac.uk/download/pdf/5890877.pdf (21. Dezember 2016).

Matheou, Demetrios. 2015. „A Good American Review: Fascinating Revelations about the NSA's Role in 9/11". *The Guardian*. https://www.theguardian.com/film/2015/nov/09/a-good-american-review-nsa-whistleblower-william-binney-911-world-trade-centre (12. Januar 2020).

Matti, Simon, und Annica Sandström. 2011. „The rationale determining advocacy coalitions: examining coordination networks and corresponding beliefs". *Policy studies journal* 39(3): 385–410.

Mauersberger, Christof. 2016. *Advocacy Coalitions and Democratizing Media Reforms in Latin America*. Cham: Springer International Publishing. http://link.springer.com/10.1007/978-3-319-21278-4 (18. August 2015).

Mayer-Schönberger, Viktor, und Kenneth Cukier. 2013. *Big Data: Die Revolution, die unser Leben verändern wird*. München: Redline Verlag.

McCarthy, Caroline. 2009. „Facebook Beacon Has Poked Its Last". *CNET*. https://www.cnet.com/news/facebook-beacon-has-poked-its-last/ (30. August 2018).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

McNamee, Joe. 2009. „Annahme des Stockholmprogramms steht kurz bevor". *www.unwatched.org*. https://web.archive.org/web/20110415134158/http://www.unwatched.org/node/1510 (11. Juli 2019).

Meister, Andre. 2015. „IFG-WTF des Tages: Das Innenministerium schickt uns eine CD mit einer EXE-Datei, die wir ausführen sollen". *netzpolitik.org*. https://netzpolitik.org/2015/ifg-wtf-des-tages-das-innenministerium-schickt-uns-eine-cd-mit-einer-exe-datei-die-wir-ausfuehren-sollen/ (30. Oktober 2019).

Meyer, Berthold. 2002. *Im Spannungsfeld von Sicherheit und Freiheit - Staatliche Reaktionen auf den Terrorismus*. Hessische Stiftung Friedens- und Konfliktforschung.

Meyer, Jürgen, und Markus Engels, hrsg. 2001. *Die Charta der Grundrechte der Europäischen Union: Berichte und Dokumentation*. Lizenzausg. des Deutschen Bundestages. Opladen: Leske + Budrich.

Microsoft. 2009. „Microsoft Response to the Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data". 55.

———. 2012. „The EU's Proposed Data Protection Regulation: Microsoft's Position". 146.

———. „Microsoft positions and suggestions for the draft General Data Protection Regulation". 171.

Microsoft Corporation. 2011. „Microsoft Corporation response to the Consultation on the Commission's comprehensive approach on personal data protection in the European Union". 119.

Ministerrat. 1974. *Entschließung des Rates vom 15. Juli 1974 über eine gemeinschaftliche Politik auf dem Gebiet der Datenverarbeitung*. Brüssel: Rat der Europäischen Gemeinschaften. Entschließung des Rates.

———. 1977. *Beschluss des Rates vom 27. September 1977 betreffend eine Reihe von Studien auf dem Gebiet der Förderung des Einsatzes der Datenverarbeitung (77/616/EWG)*. Brüssel: Rat der Europäischen Gemeinschaften.

———. 1984a. *Beschluss des Rates vom 10. April 1984 zur Änderung des Beschlusses 79/8´783/EWG zur Festlegung eines Mehrjahresprogramms (1979-1983) auf dem Gebiet der Datenverarbeitung*. Luxemburg: Rat der Europäischen Gemeinschaften. Beschluss.

———. 1984b. *Beschluss des Rates vom 22. November 1984 zur Änderung des Beschlusses 79/783/EWG hinsichtlich der allgemeinen Aktionen auf dem Gebiet der Datenverarbeitung*. Brüssel: Rat der Europäischen Gemeinschaften. Beschluss.

———. 1996. (96/C 315/06) C 315/30 *Gemeinsamer Standpunkt (EG) Nr. 57/96 des Ministerrats im Hinblick auf den Erlaß der Richtlinie 96/.../EG des Europäischen Parlaments und des Rates vom ... über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im Diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen*.

———. 2001. *Entwurf einer Entschließung über die Regeln für den Schutz personenbezogener Daten in den Rechtsakten der dritten Säule der Europäischen Union*. Brüssel: Rat der Europäischen Union.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2003. *2514. Tagung des Rats „Justiz und Inneres" am 5.-6. Juni 2003 in Luxemburg*. Luxemburg: Rat der Europäischen Union.

Möchel, Erich. 2013a. „Irland torpediert EU-Datenschutz - fm4.ORF.at". *FM4.ORF.at*. http://fm4v3.orf.at/stories/1710981/index.html (13. Februar 2018).

———. 2013b. „Transatlantischer Zwist um EU-Datenschutz". *FM4.ORF.at*. http://fm4.orf.at/stories/1711385/.

Monroy, Matthias. 2009a. „Kritik am ‚Stockholm Programm'". *Telepolis*. https://www.heise.de/tp/features/Kritik-am-Stockholm-Programm-3380857.html (11. November 2016).

———. 2009b. „Warum hast du nichts gemacht, um das aufzuhalten?" *Telepolis*. https://www.heise.de/tp/features/Warum-hast-du-nichts-gemacht-um-das-aufzuhalten-3382644.html (11. November 2016).

Moraes, Claude. 2014. *Bericht über das Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI))*. Europäisches Parlament.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: PublicAffairs.

Motejl, Christina. 2012. „German Government Expresses Issues with the Commission's Data Protection Reform Proposals". *datonomy, the data protection blog*. http://datonomy.eu/2012/07/04/german-government-expresses-issues-with-the-commissions-data-protection-reform-proposals/ (12. Februar 2018).

Moyson, S. 2016. „Policy Learning over a Decade or More and the Role of Interests Therein: The European Liberalization Policy Process of Belgian Network Industries". *Public Policy and Administration*. http://ppa.sagepub.com/cgi/doi/10.1177/0952076716681206 (27. Januar 2017).

Murphy, Martin und dpa-AFX. 2008. „Nach neuer Telekom-Datenpanne: Kritik an Konzernführung wächst". *Heise Online*. https://www.heise.de/newsticker/meldung/Nach-neuer-Telekom-Datenpanne-Kritik-an-Konzernfuehrung-waechst-210873.html (24. Februar 2018).

National Business Coalition. 2000. „Letter to Ambassador David L. Aaron Re: Safe Harbor agreement under EU privacy directive signed by Susan D. Pinder." https://web.archive.org/web/20010621181427/http://www.export.gov/safeharbor/Comments400/NatBusCoalonEcomComments.htm (10. Januar 2020).

Naurin, Daniel. 2014. „Representation in the Councils of the EU". In *Political Representation in the European Union: Still Democratic in Times and Crisis?*, Routledge advances in European politics, hrsg. Sandra Kröger. London New York: Routledge, Taylor & Francis Group, 69–85.

Newman, Abraham. 2007a. „Protecting privacy in Europe: administrative feedbacks and regional politics". *Making History: European Integration and Institutional Change at Fifty* 8: 123.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2007b. „Recursive Governance in Data Privacy: institutional layering, unintended consequences, and policy feedbacks". In *article presented in EU Governance: Towards a New Architecture Workshop, Madison, Wisconsin, April 19-21.*, http://eucenter.wisc.edu/Conferences/GovNYDec06/Docs/AbrahamNewman.pdf (29. April 2014).

Newman, Abraham L. 2008a. „Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive". *International Organization* 62: 103–30.

———. 2008b. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca, N.Y.: Cornell University Press.

Nickerson, Raymond S. 1998. „Confirmation Bias: A Ubiquitous Phenomenon in Many Guises". *Review of General Psychology* 2(2): 46.

Nielsen, Nikolaj. 2013. „New EU data law could end up weaker than old one". *EUObserver*. https://euobserver.com/justice/120301 (30. Juni 2017).

Nohrstedt, D. 2010. „Do Advocacy Coalitions Matter? Crisis and Change in Swedish Nuclear Energy Policy". *Journal of Public Administration Research and Theory* 20(2): 309–33.

Nohrstedt, Daniel. 2011. „Shifting resources and venues producing policy change in contested subsystems: A case study of Swedish Signals Intelligence Policy". *Policy studies journal* 39(3): 461–84.

Nohrstedt, Daniel, und Christopher M. Weible. 2010. „The Logic of Policy Change after Crisis: Proximity and Subsystem Interaction". *Risk, Hazards & Crisis in Public Policy* 1(2): 1–32.

NOKIA. 2011. „POSITION ON THE EUROPEAN COMMISSION'S CONSULTATION ON PROPOSED REFORMS TO THE EUROPEAN DATA PROTECTION FRAMEWORK". 120.

———. 2012a. „Implementing the Accountability Concept in the Data Protection Regulation". 179.

———. 2012b. „Set of Amendments implementing the Accountability Principle into Law". 199.

O'Brien, Kevin J. 2013. „Silicon Valley Companies Lobbying Against Europe's Privacy Proposals". *The New York Times*. https://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html (18. Februar 2018).

O'Connor, John. 2013. „EU data protection vote delayed | Lexology". *Lexology*. http://www.lexology.com/library/detail.aspx?g=781c955a-3fbf-40ba-967a-14cbaf7dfb35 (30. Juni 2017).

OECD. 1980a. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: Organisation for Economic Co-operation and Development. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (27. Juli 2015).

———. 1980b. *OECD Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten*. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2017. *OECD Legal Instruments*. https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=2ahUKEwjTptj76dbhAhVikosKHRRRAAwQFjAGegQIARAC&url=http%3A%2F%2Fwww.oecd.org%2Fpcd%2FLEG_PCD.pdf&usg=AOvVaw0S4f2cy1luowtS-pE83WT7 (17. April 2019).

———. 2018. „OECD Legal Instruments". *legalinstruments.oecd.org*. https://legalinstruments.oecd.org/en/ (17. April 2019).

Paciotti, Elena Ornella. 2000. *Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles*. European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. Report.

Parliamentary Assembly of the CoE. 1968. *Human Rights and Modern Scientific and Technological Developments: Recommendation 509*. Strasbourg: Council of Europe. Recommendation.

———. 1980. *Data processing and the protection of human rights*. Strasbourg: Council of Europe - Parliamentary Assembly. Resolution.

Patalong, Frank. 2009. „Cookie-Richtlinie: Wie die EU Internet-Nutzer nerven will". *Spiegel Online*. http://www.spiegel.de/netzwelt/web/cookie-richtlinie-wie-die-eu-internet-nutzer-nerven-will-a-622121.html (8. Januar 2019).

Pearce, Graham, und Nicholas Platten. 1998. „Achieving personal data protection in the European Union". *JCMS: Journal of Common Market Studies* 36(4): 529–47.

Peers, Steve. 2007. *Statewatch analysis: The Revised Data Protection Framework Decision.pdf*. Statewatch.

Persson, Christian. 1999. „Studie: Mittelstand verschläft ECommerce". *Heise Online*. https://www.heise.de/newsticker/meldung/Studie-Mittelstand-verschlaeft-ECommerce-12337.html (10. Juni 2019).

Pew Research Center. 2014. „Global Opinions of U.S. Surveillance". *Pew Research Center's Global Attitudes Project*. https://www.pewresearch.org/global/interactives/global-opinions-of-u-s-surveillance/ (4. März 2020).

PI. 2009. „PRIVACY INTERNATIONAL'S RESPONSE TO THE EUROPEAN COMMISSION CONSULTATION: Consultation on the legal framework for the fundamental right to protection of personal data". 58.

———. 2011. „RESPONSE TO THE EUROPEAN COMMISSION'S COMMUNICATION ON THE 'COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION'". 122.

———. 2012. „Summary analysis of European Commission proposal for a general Data Protection Regulation". 176.

Pierce, Jonathan J. 2011. „Coalition stability and belief change: Advocacy coalitions in US foreign policy and the creation of Israel, 1922–44". *Policy Studies Journal* 39(3): 411–34.

Pierce, Jonathan J., Holly L. Peterson, und Katherine C. Hicks. 2016. *Policy Change: An Advocacy Coalition Framework Perspective*. Prague, Czech Republic: Charles University,. Paper presented at the European Consortium for Political Research General Conference.

Pinder, John. 2007. „Altiero Spinelli's European Federal Odyssey". : 15.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Piquer, Jose. 2014. „In Europe we mistrust | European Council on Foreign Relations". *www.ecfr.eu*. https://www.ecfr.eu/blog/entry/in_europe_we_mistrust (15. Juli 2019).

Pittella, Gianni, Alejo Vidal-Quadras, und Georgios Papastamkos. 2014. *Tätigkeitsbericht über Verfahren der Mitentscheidung und Vermittlungsverfahren 14. Juli 2009 - 30. Juni 2014 (7. Wahlperiode)*. Europäisches Parlament.

Präsidium des Europäischen Konvents. 2000. *Entwurf der Charta der Grundrechte der Europäischen Union – vom Präsidium vorgeschlagener vollständiger Text der Charta*. Brüssel.

Presidency of the Council of Ministers. 2013. *Implementation of Risk-Based Approach in the General Data Protection Regulation*. Brussels: Council of the European Union. Note.

Presidency of the Council of the European Union. 2006. *Future Role of the Working Party on Data Protection*. Brussels: Council of the European Union. Note.

———. 2009. *Implications of the Treaty of Lisbon Provisions for the JHA Working Structures*. Brussels: Council of the European Union. „I" Item Note.

President's Council of Advisors on Science and Technology. 2014. *Report to the President. Big Data and Privacy: A Technological Perspective*. Washington, DC.

Princen, Sebastiaan, und Mark Rhinard. 2006a. „Crashing and creeping: agenda-setting dynamics in the European Union". *Journal of European Public Policy* 13(7): 1119–32.

———. 2006b. „Crashing and Creeping: Agenda-Setting Dynamics in the European Union". *Journal of European Public Policy* 13(7): 1119–32.

Privacycampaign.eu. 2013. „Privacy Campaign | European Campaign Portal for the Data Protection Reform". *http://www.privacycampaign.eu/*. https://web.archive.org/web/20130209155408/http://www.privacycampaign.eu/ (23. Oktober 2019).

Proust, Olivier. 2015. „Unravelling the mysteries of the GDPR trilogues - Privacy, Security and Information Law Fieldfisher". *fieldfisher Privacy, Security and Information Law Blog*. https://privacylawblog.fieldfisher.com/2015/unravelling-the-mysteries-of-the-gdpr-trilogues (8. April 2019).

Prümer Vertrag. 2005. Prüm, Deutschland.

Przyborski, Aglaja, und Monika Wohlrab-Sahr. 2014. „Forschungsdesign für die qualitative Sozialforschung". In *Handbuch Methoden der empirischen Sozialforschung*, Handbuch, hrsg. Nina Baur und Jörg Blasius. Wiesbaden: Springer VS, 117–34.

Pütter, Norbert. 2006. „Wachstumsringe Innerer Sicherheit: Tampere und Den Haag in der Umsetzung". *Bürgerrechte & Polizei/CILIP* 84(2).

Quaglia, Lucia. 2010. „Completing the Single Market in Financial Services: The Politics of Competing Advocacy Coalitions". *Journal of European Public Policy* 17(7): 1007–23.

Raab, Charles D., und Colin J. Bennett. 2003. „The Governance of Global Issues: Protecting Privacy in Personal Information". *European Consortium for Political Research*: 6.

Radaelli, Claudio M. 1999. „Harmful tax competition in the EU: policy narratives and advocacy coalitions". *JCMS: Journal of Common Market Studies* 37(4): 661–82.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Rat. 1995. *Gemeinsamer Standpunkt (EG) Nr. 1/95 vom Rat festgelegt am 20. Februar 1995 im Hinblick auf den Erlaß der Richtlinie 95/../EG des Europäischen Parlaments und des Rates vom ... zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.* . Mitteilungen und Bekanntmachungen.

Rat der Europäischen Union. 1998. *Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts*. Brüssel: Rat der Europäischen Union.

———. 1999. *Sitzung der horizontalen Gruppe „Informatik" vom 11. Februar 1999*. Brüssel: Rat der Europäischen Union. Beratungsergebnisse.

Ratsvorsitz. 2009a. *Das Stockholmer Programm - Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger*. Brüssel: Rat der Europäischen Union.

———. 2009b. *Entwurf eines Mehrjahresprogramms für einen Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger (Stockholmer Programm)*. Brüssel: Rat der Europäischen Union.

Reding, Viviane. 2006a. „The Review 2006 of EU Telecom rules: Strengthening Competition and Completing the Internal Market". Gehalten auf der Annual Meeting of BITKOM, Brussels, Bibliothèque Solvay.

———. 2006b. „Towards a true internal market for electronic communications". Gehalten auf der European Regulators Group, Paris.

———. 2009. *Securing personal data and fighting data breaches - Speech at EDPS-ENISA Seminar „Responding to Data Breaches"*. Brussels: European Commission.

———. 2010. *Opening remarks at the European Parliament Hearing in the Committee on Civil Liberties, Justice and Home Affairs (LIBE)*. Brussels: European Commission.

———. 2011a. *Building trust in the Digital Single Market: Reforming the EU's data protection rules*. Brussels: Conference organised by the Industry Coalition for Data Protection and American Chamber of Commerce to the European Union.

———. 2011b. „Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive". *Zeitschrift für Datenschutz* 1(1/2011): 1–2.

———. 2011c. „The upcoming data protection reform for the European Union". *International Data Privacy Law* 1(1): 3–5.

———. 2012. „The European data protection framework for the twenty-first century". *International Data Privacy Law* 2(3): 119–29.

———. 2013a. *Data Protection: Vice-President Reding's Intervention in the Justice Council*. Brussels: European Commission.

———. 2013b. „‚Europas Antwort: strenger Datenschutz'". *DGAP e.V.* https://zeitschrift-ip.dgap.org/de/ip-die-zeitschrift/archiv/jahrgang-2013/september-oktober/europas-antwort-strenger-datenschutz (14. September 2013).

———. 2013c. *Justice Council: We Need a Simple Solution for Citizens and Business on Data Protection*. Brussels: European Commission.

———. 2013d. *Reform des EU-Datenschutzrechts: Es ist an der Zeit, Nägel mit Köpfen zu machen!* Brüssel: Europäische Kommission.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

———. 2013e. *Vice-President Reding's Intervention during Justice Council Press Conference, 6 June 2013*. Luxembourg: European Commission. Speech.

———. 2014a. *The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights*. Brussels: European Commission. Speech.

———. 2014b. *Today's Justice Council – A Council of Progress*. Luxembourg: European Commission.

Regan, Priscilla M. 1999. „American Business and the European Data Protection Directive: Lobbying Strategies and Tactics". In *Visions of Privacy. Policy Choices for the Digital Age*, hrsg. Colin J. Bennett und Rebecca Grant. Toronto, Ontario, Canada: University of Toronto Press.

———. 2003. „Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows". *Journal of Social Issues* 59(2): 263–82.

———. 2015. „Privacy and the common good: revisited". In *Social Dimensions of Privacy*, hrsg. Beate Roessler und Dorota Mokrosinska. Cambridge: Cambridge University Press, 50–70. https://www.cambridge.org/core/product/identifier/9781107280557%23CN-bp-12/type/book_part (27. August 2018).

Regan, Prisclla M. 1993. „The Globalization of Privacy". *American Journal of Economics and Sociology* 52(3): 257–74.

Regnery, Christian. 2011. „Datenleck beim Zoll: Forderung nach Security Breach Notice für Behörden". *Zeitschrift für Datenschutz* (1/2011): VII–XIII.

Reiberg, Abel. 2018. *Netzpolitik: Genese eines Politikfeldes*. Baden-Baden: Nomos Verlagsgesellschaft. https://buchfindr.de/buecher/netzpolitik-3/ (4. November 2019).

Reißmann, Ole. 2013. „Freiheit statt Angst 2013: Demonstration gegen NSA-Überwachung". *Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html (25. Februar 2015).

Reutter, Werner, hrsg. 2012. *Verbände und Interessengruppen in den Ländern der Europäischen Union*. Wiesbaden: VS Verlag für Sozialwissenschaften. http://link.springer.com/10.1007/978-3-531-19183-6 (12. September 2014).

Richter, Philipp. 2016. „Big Data, Statistik und die Datenschutz-Grundverordnung". *Datenschutz und Datensicherheit-DuD* 40(9): 581–86.

Ripoll Servent, Ariadna. 2013. „Holding the European Parliament Responsible: Policy Shift in the Data Retention Directive from Consultation to Codecision". *Journal of European Public Policy* 20(7): 972–87.

———. 2015. *Institutional and Policy Change in the European Parliament*. Basingstoke (England); New York: Palgrave Macmillan.

Robinson, Francis. 2013. „Lobby, Copy, Paste, Legislate: How EU Law on Inetrnet Privacy Is Made? - Real Time Brussels". *The Wall Street Journal*. https://web.archive.org/web/20130215062432/https://blogs.wsj.com/brussels/2013/02/11/copy-paste-legislate/ (24. Oktober 2019).

Robinson, Neil u. a. 2009. *Review of the European Data Protection Directive*. RAND Europe. Technical Report - sponsored by the Information Commissioner's Office.

Rossi, Agustín. 2018. „How the Snowden Revelations Saved the EU General Data Protection Regulation". *The International Spectator* 53(4): 95–111.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Rössler, Beate. 2001. *Der Wert des Privaten*. 1. Aufl., Orig.-Ausg. Frankfurt am Main: Suhrkamp.

Roßnagel, Alexander. 2017. *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*. 1. Auflage. Baden-Baden: Nomos.

Rötzer, Florian. 2007. „EU und USA erzielen Vereinbarungen über Flugpassagier- und Finanzdaten". *heise online*. http://www.heise.de/newsticker/meldung/EU-und-USA-erzielen-Vereinbarungen-ueber-Flugpassagier-und-Finanzdaten-144928.html (11. März 2015).

Roure, Martine. 2006. *Bericht über den Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Europäisches Parlament.

———. 2007. *Bericht über den Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (erneute Konsultation)*. Europäisches Parlament.

———. 2008. *Bericht über den Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Europäisches Parlament.

Rozbicka, Patrycja. 2013. „Advocacy coalitions: influencing the policy process in the EU". *Journal of European Public Policy* 20(6): 838–53.

Rudl, Thomas. 2015. „Wie Einflussnahme funktioniert: Lobby-Mails zum Durchklicken". *netzpolitik.org*. https://netzpolitik.org/2015/wie-einflussnahme-funktioniert-lobby-mails-zum-durchklicken/ (10. Juli 2015).

Rudl, Tomas. 2015. „Merkel stellt sich gegen Datenschutz und Netzneutralität". *netzpolitik.org*. https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/ (30. Oktober 2019).

Rupp, André A. 2013. „Clustering and Classification". In *The Oxford Handbook of Quantitative Methods*, Oxford library of psychology, hrsg. Todd D. Little. New York: Oxford University Press, 517–50.

Sabatier, Paul A. 1987. „Knowledge, Policy-Oriented Learning, and Policy Change: An Advocacy Coalition Framework". *Knowledge* 8(4): 649–92.

———. 1991. „Toward Better Theories of the Policy Process". *PS: Political Science and Politics* 24(2): 147–56.

———. 1993. „Advocacy-Koalitionen, Policy-Wandel und Policy-Lernen: Eine alternative zur Phasenheuristik". In *Adrienne Héritier (Hg.): Policy-Analyse: Kritik und Neuorientierung*, Politische Vierteljahresschrift, Opladen: Westdeutscher Verlag, 116–48.

———. 1998. „The Advocacy Coalition Framework: Revisions and Relevance for Europe". *Journal of European Public Policy* 5(1): 98–130.

———. 2007. „The Need for Better Theories". In *Theories of the Policy Process*, hrsg. Paul A. Sabatier. Boulder, Colo.: Westview Press, 3–20. http://site.ebrary.com/id/10510160 (29. April 2014).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Sabatier, Paul A., und Hank Jenkins-Smith. 1999. „The Advocacy Coalition Framework: An Assessment". In *Paul A. Sabatier (Hg.): Theories of the Policy Process*, Boulder, CO: Westview Press, 117–66.

Sabatier, Paul A., und Hank C. Jenkins-Smith, hrsg. 1993. *Policy Change and Learning: An Advocacy Coalition Approach*. Boulder, Colo.: Westview Press.

Sabatier, Paul A., und Christopher M. Weible. 2005. *Innovations in the advocacy coalition framework*. Milwaukee, WI. Paper presented at the National Conference of the American Society of Public Administration.

Sanders, Claudia. 2001. „Der Rechtsstaat und der Terrorismus: Die Pläne von Bundesinnenminister Schily". *Deutschlandfunk*. https://www.deutschlandfunk.de/der-rechtsstaat-und-der-terrorismus.724.de.html?dram:article_id=97299 (28. Mai 2019).

Schäfer, Ulrich. 2010. „Geheimaktion ‚Clipper' - Obermanns Prüfung". *Sueddeutsche.de*. https://www.sueddeutsche.de/wirtschaft/telekom-spitzelaffaere-geheimaktion-clipper-obermanns-pruefung-1.213711 (16. Februar 2019).

Scheffel, Folke. 2016. *Netzpolitik als Policy Subsystem?* Baden-Baden: Nomos. http://www.nomos-elibrary.de/index.php?doi=10.5771/9783845274492 (30. Juni 2016).

Schiedermair, Stephanie. 2012. *Der Schutz des Privaten als internationales Grundrecht*. 1. Aufl. Tübingen: Mohr Siebeck.

Schildberger, Lukas. 2016. „Lobbying and Its Influence on the Draft of a General Data Protection Regulation of the European Union Unveiled in 2012". Diplomarbeit. Fakultät für Informatik der Technischen Universität Wien.

Schimmelfennig, Frank. 2015. „Efficient process tracing: European integration". In *Process tracing: From metaphor to analytic tool*, hrsg. Andrew Bennett und Jeffrey T. Checkel. Cambridge: Cambridge University Press, 98–125.

Schirrmacher, Frank. 2015. *Technologischer Totalitarismus: Eine Debatte*. 1. Aufl. Suhrkamp Verlag.

Schlager, Edella. 1995. „Policy making and collective action: Defining coalitions within the advocacy coalition framework". *Policy sciences* 28(3): 243–70.

Schmahl, Stefanie, und Marten Breuer, hrsg. 2017. *The Council of Europe: Its Law and Policies*. First edition. Oxford, United Kingdom: Oxford University Press.

Schmitz, Gregor Peter. 2013. „Trotz Abhöraffäre: Merkel bremst beim Datenschutz in Europa". *Spiegel Online*. https://www.spiegel.de/netzwelt/netzpolitik/abhoeraffaere-merkel-bremst-immer-noch-beim-datenschutz-a-930321.html (27. Oktober 2019).

Schneider, Adrian. 2014. „EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt". *Telemedicus*. http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html (12. Februar 2019).

Schneider, Volker, und Frank Janning. 2006. *Politikfeldanalyse Akteure, Diskurse und Netzwerke in der öffentlichen Politik*. Wiesbaden: VS Verlag für Sozialwissenschaften. http://dx.doi.org/10.1007/978-3-531-90267-8 (12. September 2014).

Schneider, Volker, und Raymund Werle. 2007. „Telecommunications Policy". In *Europeanization: new research agendas*, hrsg. Paolo Graziano und Maarten Peter Vink. Houndmills, Basingstoke, Hampshire [England] ; New York: Palgrave Macmillan, 266–80.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Schönberger, Christoph. 2007. „Der Rahmenbeschluss Unionssekundärrecht zwischen Völkerrecht und Gemeinschaftsrecht". *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 67: 1107–39.

Schröder, Ilka. 2001. „ilka.org: Denkpause 13 Militär/Krieg Presserecht Parteiordnungsverfahren Widerruf Parteiausschluss Grüne MdEP Heide Rühle Frankfurter Rundschau". *ilka.org*. http://www.ilka.org/material/denkpause/denkpause13f.html (7. Juni 2020).

Schubert, Klaus, und Nils C. Bandelow. 2009. *Lehrbuch der Politikfeldanalyse 2.0*. vollständig überarbeitete und erweiterte. München: De Gruyter Oldenbourg.

Schulz, Stefan. 2014. „Europas Datenschutzreform: Die Informationsfreiheit und das Prinzip Big Data". *FAZ.NET*. http://www.faz.net/1.2955004 (13. Januar 2018).

Schünemann, Wolf Jürgen, und Jana Windwehr. 2020. „Towards a 'Gold Standard for the World'? The European General Data Protection Regulation between Supranational and National Norm Entrepreneurship". *Journal of European Integration*: 1–16.

Schütz, Philip, und Murat Karaboga. 2015. *Akteure, Interessenlagen und Regulierungspraxis im Datenschutz: Eine politikwissenschaftliche Perspektive*. Karlsruhe: Fraunhofer ISI.

Schwartz, Paul M. 1994. „European data protection law and restrictions on international data flows". *Iowa L. Rev.* 80: 471.

Shanahan, Elizabeth A., Michael D. Jones, Mark K. McBeth, und Claudio M. Radaelli. 2017. „The Narrative Policy-Framework". In *Theories of the Policy Process*, hrsg. Christopher M. Weible und Paul A. Sabatier. New York, NY: Routledge, 173–214.

Siering, Peter. 1999. „Microsoft hat Kunden heimlich numeriert". *Heise Online*. https://www.heise.de/newsticker/meldung/Microsoft-hat-Kunden-heimlich-numeriert-11405.html (12. Februar 2019).

Simitis, Spiros. 1987. „Reviewing privacy in an information society". *University of Pennsylvania Law Review*: 707–46.

———. 1995. „From the market to the polis: The EU Directive on the protection of personal data". *Iowa L. Rev.* 80: 445–69.

———. 1997. „Die EU-Datenschutzrichtlinie - Stillstand oder Anreiz?" *Neue Juristische Wochenschrift* (5): 281–88.

———. 2000. „Die ungewisse Zukunft des Datenschutzes — Vorbemerkungen zu einer Prognose". In *E-Privacy*, hrsg. Helmut Bäumler. Wiesbaden: Vieweg+Teubner Verlag, 305–15. http://link.springer.com/10.1007/978-3-322-89183-9_27 (4. Juni 2019).

———. 2001. „Data Protection in the European Union - The Quest for Common Rules". In *Collected Courses of the Academy of European Law: 1997 European Community Law*, Academy of European Law, Florence, The Hague: Kluver Law International, 95–142.

Simitis, Spiros, Gerrit Hornung, und Indra Spiecker Döhmann, hrsg. 2019. *Datenschutzrecht: DSGVO mit BDSG*. 1. Auflage. Baden-Baden: Nomos.

Simitis, Spiros, Gerrit Hornung, Indra Spiecker Döhmann, und Jan Philipp Albrecht. 2019. „Einleitung". In *Datenschutzrecht: DSGVO mit BDSG*, NomosKommentar, Baden-Baden: Nomos, 158–240.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Singer, Natasha. 2013. „Consumer Data Protection Laws, an Ocean Apart - NYTimes.com". *New York Times*. https://web.archive.org/web/20130206000610/https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html (23. Oktober 2019).

Sloot, Bart van der. 2014. „Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation". *International Data Privacy Law* 4(4): 307.

Slynchuck, Andriy. 2022. „Big Brother Brands Report: Which Companies Access Our Personal Data the Most?" https://clario.co/blog/which-company-uses-most-data (6. Dezember 2022).

Sokolov, Daniel AJ. 2006. „Datenschutz-Organisation Bits of Freedom sperrt zu". *Heise Online*. https://www.heise.de/newsticker/meldung/Datenschutz-Organisation-Bits-of-Freedom-sperrt-zu-144325.html (26. August 2019).

Souhrada-Kirchmayer, Eva. 2010. „Zur Geschichte des europäischen Datenschutzrechts". In *Grundlagen der österreichischen Rechtskultur Festschrift für Werner Ogris zum 75. Geburtstag.*, hrsg. Alina Lengauer, Christian Neschwara, und Thomas Olechowski. s.l.: Böhlau Wien, 499–518.

Spiekermann, Sarah. 2012. „Datenschutzgesetz: Die Verwässerer". *Zeit Online*. http://www.zeit.de/2012/46/Deutsches-Datenschutzgesetz-Spiekermann (12. Januar 2015).

Sprenger, Florian, und Christoph Engemann, hrsg. 2015. *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und technische Durchdringung der Welt*. Bielefeld: transcript Verlag.

Stanley, Jay. 2013. „US Government Busy in Europe Defending Interests of Advertisers, Security Agencies, But Not Americans' Privacy". *ACLU*. https://web.archive.org/web/20130206041734/http://www.aclu.org/blog/technology-and-liberty-national-security/us-government-busy-europe-defending-interests (23. Oktober 2019).

Starke, Peter. 2015. „Prozessanalyse". In *Handbuch Policy-Forschung*, hrsg. Georg Wenzelburger und Reimut Zohlnhöfer. Wiesbaden: Springer Fachmedien Wiesbaden, 453–82. http://link.springer.com/10.1007/978-3-658-01968-6_18 (5. März 2019).

Statewatch. 2001. *Data Protection or Data Retention in the EU?* www.statewatch.org/news/2001/sep/dataprot.pdf (12. Juni 2019).

———. 2002a. „Coalition asks European Parliament to vote against data retention". *www.statewatch.org*. http://www.statewatch.org/news/2002/may/09coalition.htm (12. Juni 2019).

———. 2002b. „Statewatch News online: European Parliament caves in on data retention". *www.statewatch.org*. http://www.statewatch.org/news/2002/may/10epcavein.htm (15. Juni 2019).

———. 2002c. „Statewatch News online: Narrow vote in European Parliament on data retention". *www.statewatch.org*. http://www.statewatch.org/news/2002/apr/10dataret.htm (15. Juni 2019).

———. 2002d. „Telecommunications surveillance - a deal being done? European Parliament committee chair tries to reach a ‚deal' with the Council on the surveillance of communications". *www.statewatch.org*. http://www.statewatch.org/news/2002/may/08survep.htm (12. Juni 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2002e. „The vote in the European Parliament on the surveillance of communications". *www.statewatch.org*. http://www.statewatch.org/news/2002/may/15epvote.htm (12. Juni 2019).

———. 2005. *Statewatch News Online: EU policy "putsch": Data protection handed to the DG for "law, order and security"*. http://www.statewatch.org/news/2005/jul/06eu-data-prot.htm (17. Juni 2019).

———. 2006. *Statewatch News Online: EU: Data Protection Proposal in a Muddle - Member States Divided*. Statewatch. http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm (17. Juni 2019).

Statista. 2015. „Einschätzung der wichtigsten Probleme für Deutschland 2014 | Umfrage". *Statista*. http://de.statista.com/statistik/daten/studie/2739/umfrage/ansicht-zu-den-wichtigsten-problemen-deutschlands/ (25. Februar 2015).

Stein, Petra. 2014. „Forschungsdesign für die quantitative Sozialforschung". In *Handbuch Methoden der empirischen Sozialforschung*, Handbuch, hrsg. Nina Baur und Jörg Blasius. Wiesbaden: Springer VS, 135–52.

Steiner, Falk. 2013a. „EU-Datenschutzreform nimmt weiter Form an". *Heise Online*. https://www.heise.de/newsticker/meldung/EU-Datenschutzreform-nimmt-weiter-Form-an-1779603.html (13. Februar 2018).

———. 2013b. „Europaparlament: Lob und Kritik für Vorschläge zur Datenschutzreform". *Heise Online*. https://www.heise.de/newsticker/meldung/Europaparlament-Lob-und-Kritik-fuer-Vorschlaege-zur-Datenschutzreform-1780734.html (13. Februar 2018).

Stöcker, Christian. 2011. *Nerd Attack!: Eine Geschichte der digitalen Welt vom C64 bis zu Twitter und Facebook - Ein SPIEGEL-Buch*. 4. Aufl. München: Deutsche Verlags-Anstalt.

Stritch, Andrew. 2015. „The Advocacy Coalition Framework and Nascent Subsystems: Trade Union Disclosure Policy in Canada". *Policy Studies Journal* 43(4): 437–55.

Süddeutsche Zeitung. 2013. „NSA-Affäre - ‚Abhören von Freunden, das geht gar nicht'". *Süddeutsche.de*. https://www.sueddeutsche.de/politik/nsa-abhoerskandal-abhoeren-von-freunden-das-geht-gar-nicht-1.1709525 (27. Oktober 2019).

Susser, Daniel, Beate Roessler, und Helen Nissenbaum. 2018. *Online Manipulation: Hidden Influences in a Digital World*. Rochester, NY: Social Science Research Network. SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3306006 (6. Dezember 2022).

Swedish Delegation. 2002. *Alternative structure of the Working Parties in the JHA area*. Brussels: Council of the European Union. Note.

TACD. 2000. *Submission of theTransAtlantic Consumer Dialogue (TACD) concerning the U.S. Department of Commerce draft international Safe Harbor privacy principles and FAQs*. https://tacd.org/wp-content/uploads/2013/09/TACD-ECOM-20-00-US-Dept-of-Commerce-Draft-International-Safe-Harbor-Privacy-Principles-and-FAQs.pdf (10. Januar 2020).

———. 2011. *Letter to Mr. Mary Bono Mack and G.K. Butterfield, chair and ranking Subcommittee on Commerce, Manufacturing and Trade.*

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tangens, Rena, und padeluun. 2011. „Aktivitäten | Rena Tangens & padeluun". *ameublement.de*. https://ameublement.de/page_id=69/ (8. Juli 2019).

Taylor, Simon. 2010. „Reding gets her way as justice department splits in two". *Politico.eu*. https://www.politico.eu/article/reding-gets-her-way-as-justice-department-splits-in-two/ (1. September 2019).

TechAmerica Europe. 2009. „TechAmerica Europe's response to EU Commission Consultation on the legal framework for the fundamental right to protection of personal data". 59.

———. 2011. „TechAmerica Europe's Response to EU Commission Communication: "A comprehensive approach on personal data protection in the European Union"". 123.

Telefónica. 2011. „TELEFÓNICA'S REPLY TO THE EC PUBLIC CONSULTATION ON THE COMMUNICATION ON A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION". 124.

Telefonica. 2012a. „Telefonica Cloud Amendments". 206.

———. 2012b. „Telefónica's proposed amendments to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Directive)". 215.

Tene, Omer, und J Trevor Hughes. 2014. „The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study". *Maine Law Review* 66(2): 30.

The Economist. 2004. „E-commerce takes off". *The Economist*. https://www.economist.com/leaders/2004/05/13/e-commerce-takes-off (10. Juni 2019).

The Future Group. 2007. *First Meeting of the Future Group: Eltville (Germany), 20 and 21 May 2007 - Report*.

———. 2008. *Freedom, Security, Privacy - European Home Affairs in an open world.* . Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy („The Future Group").

The Washington Post. 2013. „NSA slides explain the PRISM data-collection program". http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (29. August 2014).

The White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (28. August 2015).

Thierbach, Cornelia, und Grit Petschick. 2014. „Beobachtung". In *Handbuch Methoden der empirischen Sozialforschung*, Handbuch, hrsg. Nina Baur und Jörg Blasius. Wiesbaden: Springer VS, 855–66.

Thoma, Jörg. 2013. „Geheimdienste: Auch Frankreich sammelt Metadaten - Golem.de". *Golem.de*. https://www.golem.de/news/geheimdienste-auch-frankreich-sammelt-metadaten-1307-100222.html (27. Oktober 2019).

Tinnefeld, Marie-Theres. 2009. „Reformvertrag von Lissabon, Charta der Grundrechte und Rechtspraxis im Datenschutz". *Datenschutz und Datensicherheit-DuD* 33(8): 504–504.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:09
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Tömmel, Ingeborg, hrsg. 2008. *Die Europäische Union governance und policy-making*. Wiesbaden: VS, Verl. für Sozialwiss. http://dx.doi.org/10.1007/978-3-531-90795-6 (18. Juli 2013).

Travis, Alan. 2013. „European Commission Backs Merkel's Call for Tougher Data Protection Laws". *The Guardian*. https://www.theguardian.com/world/2013/jul/15/european-commission-angela-merkel-data-protection (25. Oktober 2019).

Tréguer, Félix. 2017. „Intelligence Reform and the Snowden Paradox: The Case of France". *Media and Communication* 5(1): 17.

Trubow, George B. 1992. „European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow". *Northwestern Journal of International Law & Business* 13(1 Spring): 159.

Tzschentke, Karin. 2013. „Massives Lobbying gegen EU- Datenschutzverordnung". *Der Standard*. https://www.derstandard.at/story/1360161300194/massives-lobbying-gegen-datenschutzverordnung (25. August 2019).

UEAPME. 2009. „UEAPME1 position paper on the European Commission's consultation on the legal framework for fundamental rights to protection of personal data". 60.

———. 2011. „UEAPME1 position on a comprehensive approach on personal data protection in the European Union". 125.

———. 2012. *UEAPME position on the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (COM(2012) 11 final)*. 157,5.

UEAPME und HOTREC. 2013. *Joint position UEAPME and HOTREC General Data Protection Regulation (specifically the obligation for SMEs to designate a Data Protection Officer)*.

UK Ministry of Justice. 2010. „UK response to the European Commission consultation on the legal framework for the fundamental right to protection of personal data". 47.

———. 2011. „UK response to the Commission's consultation on 'a comprehensive approach on personal data protection in the European Union'". 110.

———. 2012. „Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework". 167.

UNCTAD. 2004. *E-Commerce and Development Report 2004*. Ney York and Geneva: United Nations Conference on Trade and Development.

US Administration. 2011. *Informal Note on Draft EU General Data Protection Regulation*.

———. 2013. „Protection privacy while maintaining global trade security and security requires flexible solutions".

US Congress. 2001. Public Law 107-71 *Aviation and Transportation Security Act*. https://www.tsa.gov/sites/default/files/publications/pdf/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf (10. Januar 2015).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

US DoC. 2012. „Remarks to the European Parliament Interparliamentary Committee Meeting on The Reform of the EU Data Protection Framework: Building Trust in a Digital and Global World Session VII: Data Protection in the global context - The transatlantic dimension". 187.

US FTC. 2006. *U.S. Federal Trade Commission Staff Comments to the European Commission on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services*.

U.S. Government Working Group on Electronic Commerce. 1998. *First Annual Report*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjHxYPShtndAhUMCewKHc75ChIQFjACegQIBxAC&url=http%3A%2F%2Fwww.kentlaw.edu%2Ffaculty%2Frstaudt%2Fclasses%2Foldclasses%2Finternetlaw%2Fcasebook%2FU.S.%2520Government%2520Working%2520Group%2520on%2520Electronic%2520Commerce.pdf&usg=AOvVaw3GfYL3xJaOjKPVaHfHYCef (26. September 2018).

US Mission to the EU. 2001. „US letter from Bush to Romano Prodi with demands for EU cooperation". *www.statewatch.org*. http://www.statewatch.org/news/2001/nov/06Ausalet.htm (14. Juni 2019).

US-Consumer Organizations. 2012. *Letter to Albrecht und Comi regarding GDPR*.

Vanchieri, c. 1993. „New EC Privacy Directive Worries European Epidemiologists". *JNCI Journal of the National Cancer Institute* 85(13): 1022–23.

VDZ. 2012. „Vorschläge für Änderungsanträge zum Entwurf Datenschutz-Grundverordnung". 164.

Veil, Winfried. 2015. „DS-GVO: Risikobasierter Ansatz statt ridriges Verbotsprinzip. Eine erste Bestandsaufnahme". *Zeitschrift für Datenschutz* (8): 347–53.

Vorsitz - EU-Ministerrat. 2006. *Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*. Brüssel: Rat der Europäischen Union. Vermerk.

Vorsitz - Rat der Europäischen Union. 1999. *Arbeitspapier zum Schutz personenbezogener Daten in der Dritten Säule der EU*. Brüssel: Rat der Europäischen Union.

VoteWatch Europe. 2012. „EU-USA agreement on the use and transfer of PNR to the US Department of Homeland Security". *VoteWatch Europe*. http://term7.votewatch.eu/en/eu-usa-agreement-on-the-use-and-transfer-of-pnr-to-the-us-department-of-homel and-security-draft-legi.html (12. November 2014).

VZBV. 2009. „Answers to the Consultation on the EU General Data Protection Framework: New challenges, current legal framework and future action to address identified challenges". 62.

———. 2011. „Stellungnahme des Verbraucherzentrale Bundesverbandes Im Rahmen der Konsultation der EU zur Mitteilung KOM(2010) 609". 128.

———. 2012. „Modernisierung des europäischen Datenschutzrechts Stellungnahme des Verbraucherzentrale Bundesverbandes". 147.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2013. „Modernisierung des europäischen Datenschutzrechts Änderungsvorschläge des Verbraucherzentrale Bundesverbandes zum Entwurf der EU-Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)". 216.

VZBV, und Florian Glatzner. 2016. „Datenschutz in Europa: Die roten Linien des vzbv zur europäischen Datenschutz-Grundverordnung – revisited". *DANA - Datenschutz Nachrichten* (2): 82–83.

Walker, Kent. 2001. „The Costs of Privacy". *Harvard Journal of Law & Public Policy* 25(1): 87.

Walters, Chris. 2009. „Facebook's New Terms Of Service: ‚We Can Do Anything We Want With Your Content. Forever.'" *www.consumerist.com*. https://web.archive.org/web/20091103175020/http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever (7. Juli 2019).

Ware, Willis H. 1973. *Records, Computers and the Rights of Citizens*. Santa Monica, California: The Rand Corporation.

Warman, Matt. 2012a. „EU 'Asking Google to Censor Web'". https://www.telegraph.co.uk/technology/internet/9081619/EU-asking-Google-to-censor-web.html (21. Oktober 2019).

———. 2012b. „EU Fights ‚fierce Lobbying' to Devise Data Privacy Law". https://www.telegraph.co.uk/technology/internet/9069933/EU-fights-fierce-lobbying-to-devise-data-privacy-law.html (21. Oktober 2019).

———. 2012c. „EU Privacy regulations subject to ‚unprecedented lobbying'". *The Telegraph*. http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html (1. September 2014).

———. 2012d. „Vint Cerf Attacks European Internet Policy". https://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html (22. Oktober 2019).

Warnke, Martin. 2011. *Theorien des Internet zur Einführung*. 1. Hamburg: Junius Hamburg.

Watt, Nicholas. 2013. „Prism Scandal: European Commission to Seek Privacy Guarantees from US". *The Guardian*. https://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees (25. Oktober 2019).

Weible, Christopher M. u. a. 2011. „A quarter century of the advocacy coalition framework: an introduction to the special issue". *Policy Studies Journal* 39(3): 349–60.

———. 2014. „Advancing Policy Process Research". In *Theories of the Policy Process*, hrsg. Paul A. Sabatier und Christopher M. Weible. Boulder, CO: Westview Press, 391–407.

Weible, Christopher M., und Paul A. Sabatier. 2007a. „A Guide to the Advocacy Coalition Framework". In *Handbook of public policy analysis: Theory, politics and methods*, hrsg. Frank Fischer, Gerald J. Miller, und Mara S. Sidney. New York: CRC Press, 123–36.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

———. 2007b. „The Advocacy Coalition Framework. Innovations and Clarifications". In *Theories of the Policy Process*, hrsg. Paul A. Sabatier. Boulder, Colo.: Westview Press, 189–220. http://site.ebrary.com/id/10510160 (29. April 2014).

Weible, Christopher M., Paul A. Sabatier, und Kelly McQueen. 2009. „Themes and variations: Taking stock of the advocacy coalition framework". *Policy Studies Journal* 37(1): 121–40.

Weichert, Thilo. 2007. „Deutsche Vereinigung für Datenschutz – DVD – 30 Jahre sind nicht genug –". *DANA - Datenschutz Nachrichten* (2/2007): 6.

Weishaar, Heide, Jeff Collin, und Amanda Amos. 2016. „Tobacco Control and Health Advocacy in the European Union: Understanding Effective Coalition-Building". *Nicotine & Tobacco Research* 18(2): 122–29.

Weitkamp, Jana, Simone Kimpeler, und Michael Friedewald. 2014. *Deliverable 6.2. Content and discourse analysis of security and privacy reporting in the European media*. Brussels: European Commission.

Wendelin, Manuel, und Maria Löblich. 2013. „Netzpolitik-Aktivismus in Deutschland. Deutungen, Erwartungen und Konstellationen zivilgesellschaftlicher Akteure in der Internetpolitik". *M&K*: 58–75.

Werle, Raymund. 2005. „Internetpolitik in Deutschland". *Technikfolgenabschätzung – Theorie und Praxis* 14(1): 26–32.

Wessels, Wolfgang. 2008. *Das Politische System Der Europäischen Union*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Westin, Alan F. 1967. *Privacy and Freedom*. 6. Aufl. New York: Atheneum.

Westlake, E.J. 2008. „Friend Me If You Facebook: Generation Y and Performative Surveillance". *TDR/The Drama Review* 52(4): 21–40.

Wetzel, Jens. 2012. „Stolperstein Terrorismusbekämpfung. Der Raum der Freiheit, der Sicherheit und des rechts vor einem unlösbaren Zielkonflikt?" In *Die Welt nach 9/11. Auswirkungen des Terrorismus auf Staatenwelt und Gesellschaft*, Sonderheft der Zeitschrift für Außen- und Sicherheitspolitik, Sonderheft 2/2011, hrsg. Thomas Jäger. Wiesbaden: VS Verlag für Sozialwissenschaften/Springer Fachmedien, 548–66.

Wiedenbeck, Michael, und Cornelia Züll. 2010. „Clusteranalyse". In *Handbuch der sozialwissenschaftlichen Datenanalyse*, hrsg. Christof Wolf und Henning Best. Wiesbaden: VS Verlag für Sozialwissenschaften, 525–52. http://link.springer.com/10.1007/978-3-531-92038-2_21 (19. August 2019).

Wikipedia. 2019a. „Ana de Palacio". *Wikipedia*. https://de.wikipedia.org/w/index.php?title=Ana_de_Palacio&oldid=192567800 (13. Januar 2020).

———. 2019b. „List of data breaches". *www.en.wikipedia.org*. https://en.wikipedia.org/wiki/List_of_data_breaches (9. Juli 2019).

———. 2019c. „re:publica". *Wikipedia*. https://de.wikipedia.org/w/index.php?title=Re:publica&oldid=192986250 (20. November 2019).

Woodward, Richard. 2004. „The Organisation for Economic Cooperation and Development: Global Monitor". *New Political Economy* 9(1): 113–27.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Working Party on Economic Questions (Data Protection). 1995. *Draft Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Brussels: Council of the European Union. Report.

WPISP. 2011. *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines*. OECD Directorate for Science, Technology and Industry: Committee for Information, Computer and Communications Policy: Working Party on Information Security and Privacy.

WSA. 1991. *Stellungnahme zu dem Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten, dem Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen, und dem Vorschlag für einen Beschluß des Rates auf dem Gebiet der Informationssicherheit*. Wirtschafts- und Sozialausschuss. Amtsblatt der Europäischen Gemeinschaften 34. Jahrgang.

———. 2001. *Stellungnahme des Wirtschafts- und Sozialausschusses zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation*". Brüssel: Wirtschafts- und Sozialausschuss.

Yahoo. 2012. „YAHOO! RATIONALE FOR AMENDMENTS TO DRAFT DATA PROTECTION REGULATION AS RELATE TO PSEUDONYMOUS DATA". 212.

Yahoo! Europe. 2009. „Yahoo! Europe response to the European Commission consultation on the legal framework for the fundamental right to protection of personal data". 63.

Zafonte, Matthew, und Paul Sabatier. 2004. „Short-Term Versus Long-Term Coalitions in the Policy Process: Automotive Pollution Control, 1963-1989". *Policy Studies Journal* 32(1): 75–107.

Zafonte, Matthew, und Paul A. Sabatier. 1998. „Shared Beliefs and Imposed Interdependencies as Determinants of Ally Networks in Overlapping Systems". *Journal of Theoretical Politics* 10(4): 473–505.

ZAW. 2012. „Main points of the ZAW position paper on the amendment of European data protection law: Proposal of the EU Commission for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – COM (2012) 11 final". 177.

ZAW E.V. 2011. „Stellungnahme des Zentralverbands der deutschen Werbewirtschaft ZAW e. V. zur Konsultation der EU-Kommission zu dem Gesamtkonzept für den Datenschutz in der Europäischen Union KOM (2010) 609 endgültig". 131.

ZBI. 2015. „Big Data – ein Wachstumsmarkt von morgen". *zbi-berlin.de*. https://www.zbi-berlin.de/index.php/93-big-data-ein-wachstumsmarkt-von-morgen (30. Oktober 2019).

ZDF. 2013. „ZDF-Politbarometer August II 2013 / CDU/CSU legt zu - SPD verliert / Fast zwei Drittel halten Ausgang der Bundestagswahl für offen (BILD)". *presseportal.de*. https://www.presseportal.de/pm/7840/2536521 (4. März 2020).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Zeit Online. 2019. „Abhöraffäre: Angela Merkel soll NSA-Überwachung als PR-Problem gesehen haben". *Die Zeit*. https://www.zeit.de/politik/deutschland/2019-02/abhoeraffaere-angela-merkel-nsa-us-geheimdienst (27. Oktober 2019).

Zerdick, Thomas. 1995. „European Aspects of Data Protection: What Rights for the Citizen?" *Legal Issues of Economic Integration* 22(2): 59–86.

———. 2008. „Folgerungen aus der Vergemeinschaftung der Justiz- und Innenpolitik für den Datenschutz". Gehalten auf der Fachtagung „Datenschutz in Deutschland nach dem Vertrag von Lissabon", Frankfurt. aus der Vergemeinschaftung der Justiz- und Innenpolitik für den Datenschutz (24. März 2017).

Ziedler, Christopher. 2014. „Neue EU-Datenschutzregeln kommen erst nach Europawahl". https://www.tagesspiegel.de/politik/aufgeschobene-reform-neue-eu-datenschutzregeln-kommen-erst-nach-europawahl/9377498.html (28. Oktober 2019).

Ziegler, Peter-Michael. 2002. „Europäische Digital-Rights-Initiative gegründet". *Heise Online*. https://www.heise.de/newsticker/meldung/Europaeische-Digital-Rights-Initiative-gegruendet-64411.html (15. Juni 2019).

———. 2008. „Datenschutzverletzungen: Lidl fällt als Wiederholungstäter auf". *Heise Online*. https://www.heise.de/newsticker/meldung/Datenschutzverletzungen-Lidl-faellt-als-Wiederholungstaeter-auf-192822.html (24. Februar 2018).

Zuboff, Shoshana. 2014. „Unsere Zukunft mit ‚Big Data' Lasst euch nicht enteignen!" *Frankfurter Allgemeine Zeitung*. http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/unsere-zukunft-mit-big-data-lasst-euch-nicht-enteignen-13152809.html?printPagedArticle=true#pageIndex_2 (29. September 2014).

———. 2018. *Das Zeitalter des Überwachungskapitalismus*. 1. Aufl. Frankfurt am Main New York: Campus Verlag.

Zyprische Ratspräsidentschaft. 2012. „Pressemitteilung – Positiver Start der zyprischen Ratspräsidentschaft in Sachen Datenschutz". *www.cy2012.eu*. http://www.cy2012.eu/index.php/de/news-categories/areas/justice-and-home-affairs/press-release---cyprus-presidency-off-to-a-positive-start-on-data-protection (4. Oktober 2019).

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Anhang

1.1 Fraktionen im Europäischen Parlament in den Wahlperioden seit 1979

1.2 Partizipation von Akteuren am Subsystem der EU-Datenschutzpolitik bis zur DSGVO

	Akteur	**DS-RL**	**2000 ePrivacy-RL**	**2002 DS-RL-Bericht**	**2006 Coo-kie-RL**	**2006 RFID**	**Häufig-keit der Partizip.**
1	Art. 29-Datenschutzgruppe		x	x	x	x	4
2	EICTA		x	x	x	x	4
3	EPC		x	x	x	x	4
4	UNICE	x	x	x	x		4
5	Beuc		x		x	x	3
6	BITKOM			x	x	x	3
7	C&W		x	x	x		3
8	ENPA		x	x	x		3
9	ETNO		x	x	x		3
10	FEDMA	x	x	x			3
11	ICC	x	x	x			3
12	MPA		x	x	x		3
13	Telecom Italia		x		x	x	3
14	Telefonica		x	x	x		3
15	ACT		x		x		2
16	AER		x		x		2
17	Alcatel		x		x		2
18	AMCHAM		x		x		2
19	ANEC		x		x		2
20	ARD/ZDF		x		x		2
21	Astel		x		x		2
22	BAKOM		x		x		2
23	BDI/BDA			x	x		2
24	Belgacom		x		x		2

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
25	BT plc		x		x		2
26	Bundesregierung Deutschland		x		x		2
27	Canal+		x		x		2
28	CEEP		x		x		2
29	COLT Telecom Group plc		x		x		2
30	Debitel		x		x		2
31	Deutsche Telekom AG		x		x		2
32	EADP			x	x		2
33	ECTA			x	x		2
34	EDF - European Disability Forum		x		x		2
35	EPOF			x	x		2
36	ERICSSON		x		x		2
37	ETP		x		x		2
38	EuroCommerce			x		x	2
39	EuroISPA		x		x		2
40	Europäischer Ausschuß gegen un-erwünschte elektronische Post zu Werbezwecken		x	x			2
41	European Broadcasting Union		x		x		2
42	France Telecom		x		x		2
43	Gouvernement de la Communaute francaise de Belgique		x		x		2
44	GSM Europe		x		x		2
45	IAB			x	x		2
46	ICRT		x	x			2
47	Intel Corp.		x		x		2
48	ISPA			x	x		2
49	Microsoft		x		x		2
50	NOKIA		x		x		2
51	Nortel Networks		x		x		2
52	ONITELCOM		x		x		2
53	OTE		x		x		2
54	Phoneability		x		x		2
55	Portugal Telecom		x		x		2
56	Regierung Japan		x			x	2

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
57	SES Global		x		x		2
58	ST Microelectronics		x	x			2
59	TAG		x		x		2
60	TDF		x		x		2
61	Tele2		x		x		2
62	Telekom Austria		x		x		2
63	Telenet		x		x		2
64	Teracom AB		x		x		2
65	USCIB		x	x			2
66	VATM		x		x		2
67	VPRT		x		x		2
68	WFA		x		x		2
69	Wind Telecommunicazioni		x		x		2
70	3 Group				x		1
71	Aberdeen Group					x	1
72	Abertis Telecom				x		1
73	ACCIS			x			1
74	ACUTEL		x				1
75	ADM			x			1
76	AeA Europe				x		1
77	AESC			x			1
78	AFCO		x				1
79	AFEC				x		1
80	AFOM				x		1
81	AFOPT		x				1
82	AFORS Telecom				x		1
83	AIIP				x		1
84	AIM Global					x	1
85	AIT				x		1
86	Allen & Overy			x			1
87	Alliance TICS				x		1
88	ALMA Media Corporation		x				1
89	AMARC		x				1
90	AMENA Retevision Movil		x				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	**DS-RL**	**2000 ePrivacy-RL**	**2002 DS-RL-Bericht**	**2006 Coo-kie-RL**	**2006 RFID**	**Häufig-keit der Partizip.**
91	Amt für Kommunikation Liech-tenstein		x				1
92	ANIA			x			1
93	ANIEL		x				1
94	Anya Moss					x	1
95	AOL Europe		x				1
96	APRITEL		x				1
97	APVTS				x		1
98	Arbeitskreis Rundfunkempfangs-anlagen		x				1
99	Arcor				x		1
100	ASNEF			x			1
101	Association des Televisions Com-merciales		x				1
102	Association of Pensioneer Trustees			x			1
103	AT Kearney					x	1
104	AT&T				x		1
105	AUTEL		x				1
106	Auto ID Service Providers Ldt.					x	1
107	Auto-ID Labs UK					x	1
108	Autorita per le Garanzie nelle Co-municazioni		x				1
109	Autorite de regulation des telecom-munications		x				1
110	Autorites francaises				x		1
111	AVICCA				x		1
112	BBA			x			1
113	BBC		x				1
114	Belgacom Moblie		x				1
115	Belgisches Institut für Postdienste und Telekommunikation		x				1
116	Bertelsmann				x		1
117	Bertelsmann Mediasystems		x				1
118	BIBA-IPS at University of Bremen - Intelligent Production and Logis-tic Systems					x	1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Cookie-RL	2006 RFID	Häufigkeit der Partizip.
119	BIICL				x		1
120	BIPAR			x			1
121	BLU S.p.A.		x				1
122	BMR			x			1
123	Bouygues Telecom		x				1
124	BREKO				x		1
125	BSA				x		1
126	BT, Cisco, Dell, Intel, Pipex				x		1
127	Bundesamt für Sicherheit und Informationstechnick					x	1
128	Bundeskammer für Arbeiter und Angestellte		x				1
129	Bundeskartellamt				x		1
130	Bundesministerium für Verkehr und Forschung Österreich		x				1
131	Bundesverband Deutscher Banken			x			1
132	Cable Europe				x		1
133	Cap Gemini					x	1
134	CASTEL		x				1
135	CBI			x			1
136	CDMA				x		1
137	CEA			x			1
138	CECUA		x				1
139	China					x	1
140	Cisco				x		1
141	Citigroup Europe			x			1
142	Clifford Chance LLP			x			1
143	CMA - Communications Management Association				x		1
144	CMBA				x		1
145	CODACONS			x			1
146	CODENET		x				1
147	Comptel				x		1
148	Concejal de Comunicacion		x				1
149	CONCERT		x				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	**DS-RL**	**2000 ePrivacy-RL**	**2002 DS-RL-Bericht**	**2006 Coo-kie-RL**	**2006 RFID**	**Häufig-keit der Partizip.**
150	Confindustria			x			1
151	Conseil Superieur de l´Audiovisuel de Wallonie		x				1
152	Consumer Agency and Ombuds-man				x		1
153	Consumers Association		x				1
154	Corning				x		1
155	COSMOTE		x				1
156	COST219ter				x		1
157	Covad Communications		x				1
158	Covington & Burling Brussles			x			1
159	CPRM Companhia Portuguesa Radio Marconi		x				1
160	CRID/FUNDP		x				1
161	CSI			x			1
162	CSIA				x		1
163	CTI & DATSA		x				1
164	CTU				x		1
165	Czech Ministry of Informatics				x		1
166	Danish Government				x		1
167	Datsa Belgium		x				1
168	De Streel				x		1
169	Deaf Broadcasting Council		x				1
170	Department of Public Enterprise		x				1
171	Deutsche Post World Net					x	1
172	Deutscher Kabelverband				x		1
173	DIEL		x				1
174	DIF				x		1
175	Digita Oy				x		1
176	DIHK				x		1
177	Direktorenkonferenz der Landes-medienanstalten in der Bundesre-publik Deutschland DLM		x				1
178	Discovery Networks Europe				x		1
179	DLM				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
180	DMA			x			1
181	DNA Networks				x		1
182	DUG			x			1
183	Dutch Government				x		1
184	DVB		x				1
185	EACEM		x				1
186	ECATRA			x			1
187	ECCA		x				1
188	ECP.NL/ Efficienta Offsetdrunk-kerijBV					x	1
189	EEAC			x			1
190	Eemvalley Systems&Technology				x		1
191	EFJ			x			1
192	EFTA				x		1
193	EIRCOM		x				1
194	EMOTA			x			1
195	Empresarios Cable, S.A		x				1
196	EMRA			x			1
197	ENCIP		x				1
198	Energis Carmelite		x				1
199	Enterprise Privacy Group					x	1
200	E-Plus Mobilfunk GmbH		x				1
201	EQUANT		x				1
202	Esat Digifone		x				1
203	Esat Telecon		x				1
204	ESOA				x		1
205	ETSI				x		1
206	EU Committee of American Chamber of Commerce			x			1
207	EU-Ausschuß der amerikanischen-Handelskammer in Belgien		x				1
208	EUD - European Union of Deaf				x		1
209	EURIM		x				1
210	Eurocities				x		1
211	Eurofinas			x			1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	**DS-RL**	**2000 ePrivacy-RL**	**2002 DS-RL-Bericht**	**2006 Coo-kie-RL**	**2006 RFID**	**Häufig-keit der Partizip.**
212	euroITcounsel			x			1
213	Europäische Konferenz für Post- und Fernmeldewesen			x			1
214	European Blind Union				x		1
215	European Consumers´ Organisati-on			x			1
216	European Publishers Council				x		1
217	European Union - Quality of Life and Management of Living Re-sources					x	1
218	Eversheds			x			1
219	FACT				x		1
220	FAEP		x				1
221	Fastweb				x		1
222	FCS - Federation of Communica-tion Services				x		1
223	FEB		x				1
224	Federal Office for Information Se-curity					x	1
225	Federal Trade Commission					x	1
226	FEI		x				1
227	Ficom				x		1
228	Ficora				x		1
229	Finnet Association				x		1
230	Finnet Group		x				1
231	Finnischer Zeitungsverband		x				1
232	Finnish Competition Authority				x		1
233	Finnish Ministry of Transport and Communications				x		1
234	First Telecom plc		x				1
235	FLA			x			1
236	FNV			x			1
237	France Televisions				x		1
238	französische Behörden		x				1
239	FRK		x				1
240	FTTH Council Europe				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
241	GDD			x			1
242	GE Capital Europe		x				1
243	Genossenschaft der Werkstätten für Behinderte eG		x				1
244	GITEP		x				1
245	Global Crossing		x				1
246	Global Telesystems Inc.		x				1
247	Gobierno de Canarias		x				1
248	Google				x		1
249	Government of Japan				x		1
250	GPA			x			1
251	GSA				x		1
252	GVF				x		1
253	Hearing Concert				x		1
254	Hrvatske Telekom				x		1
255	Hughes Network Systems/Space-way		x				1
256	Hungarian Ministry of Economic Affairs and Transport				x		1
257	IAC				x		1
258	IBM Deutschland/ METRO Group					x	1
259	ICAEW				x		1
260	ICSTIS		x				1
261	IEN				x		1
262	IMS			x			1
263	Independent Regulators Group		x				1
264	Industriellen Vereinigung				x		1
265	INFONXX				x		1
266	InformationsforumRFID					x	1
267	INFOSTRADA		x				1
268	Instituto das Comunicacoes de Portugal		x				1
269	Intellect				x		1
270	International Policy Consumer Bu-reau				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
271	INTUG - General the Interna-tional Telecommunications User Group		x				1
272	INTUG Europe & EVUA - Mobile the International Telecommunica-tions User Group		x				1
273	Ireland - Department of Commu-nications				x		1
274	IRG/ERG				x		1
275	Irish Competition Authority		x				1
276	Irish Multichannel		x				1
277	ISF			x			1
278	ISI				x		1
279	IS-Production		x				1
280	ITV		x				1
281	IUF				x		1
282	Japan Buisness Council in Europe			x			1
283	Jim Sandhu				x		1
284	JISC Technologie & Standarts Watch					x	1
285	Kabel BW				x		1
286	Kabel Deutschland				x		1
287	Kingston Communications				x		1
288	KPN				x		1
289	KPNRoyal KPN N.V.		x				1
290	LDMI Telecommunications		x				1
291	LEGAL-IST					x	1
292	Level 3		x				1
293	LFMI - Lithunian Free Market In-stitute				x		1
294	LIBA			x			1
295	Liberty Globel Europe				x		1
296	Logica CMG					x	1
297	Loyalty Partner			x			1
298	Lucent Technologies		x				1
299	Lyngby		x				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
300	Lyonnaise Cable		x				1
301	Magyar Telekom				x		1
302	Maltacom				x		1
303	Mannesmann		x				1
304	Mannesmann Arcor		x				1
305	Mannesmann Mobilfunk		x				1
306	Maxitel		x				1
307	MCI Worldcom International		x				1
308	Mediaset				x		1
309	Medienfachverlag Rommerskir-chen					x	1
310	Mencap		x				1
311	Mercantil Empresarios Cable		x				1
312	Meteor				x		1
313	Metro Group					x	1
314	Michelin					x	1
315	Ministere des telecommunications		x				1
316	Ministerio das Communicacoes do Portugal				x		1
317	Ministerio de Formento		x				1
318	Ministerium für Verkehr, Kommu-nikation und Bewirtschaftung Un-garn		x				1
319	Ministero delle comunicazioni		x				1
320	Ministry for Competitiveness and Communications of Malta				x		1
321	Ministry of Economic Affairs and Transport of Hungary				x		1
322	Ministry of Economic Affais - The Netherlands - Annex				x		1
323	Ministry of the Economy of Slove-nia				x		1
324	Ministry of Transport of Poland				x		1
325	Mobilix		x				1
326	Mobilkom				x		1
327	Mobistar		x				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
328	Motorola		x				1
329	MRS			x			1
330	MTV		x				1
331	National Consumer Council UK		x				1
332	National Deaf Children Society				x		1
333	NCR					x	1
334	NICC				x		1
335	Nordic Public Service Broadcasters				x		1
336	NTL		x				1
337	Ocean Communications Ltd		x				1
338	ODETTE					x	1
339	Office of Telecommunications		x				1
340	Office of Telecommunications / Consumer Communications for England		x				1
341	Office of the Director of telecom-munications Regulation		x				1
342	OLON				x		1
343	Omnitel Pronto Italia		x				1
344	ONCE				x		1
345	Ondas Media				x		1
346	One-2-One		x				1
347	ONO				x		1
348	Open Source Innovation Ltd.					x	1
349	Open TV		x				1
350	OPTA		x				1
351	OPTIMUS Telecomunicacoes SA		x				1
352	Orange Personal Communications Services Ltd		x				1
353	ORF				x		1
354	Pacific Gateway Exchange Inc.		x				1
355	Patrick Van Eecke - Georgia Sk-ouma					x	1
356	Philips		x				1
357	Prof. Kai Rannenberg				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
358	Public Utilities Access Forum		x				1
359	QSC Qualcomm				x		1
360	Radio Nazionali Associate		x				1
361	Radio Teilifis Eireann		x				1
362	RCO			x			1
363	Regierung Dänemark		x				1
364	Regierung Luxemburg		x				1
365	Regierung Niederlande		x				1
366	Regierung Schweden		x				1
367	Regierung Vereinigte Staaten		x				1
368	Regierung Vereinigtes Königreich		x				1
369	Republik Österreich				x		1
370	Reseaux Services Publiques		x				1
371	RETEVISION, Mobil Amena		x				1
372	Reuters Ltd.		x				1
373	RFID Asia					x	1
374	RNIB		x				1
375	RNID				x		1
376	RTE				x		1
377	RTL Group				x		1
378	RTS Wireless		x				1
379	SACD				x		1
380	SACOT		x				1
381	Sanoma-WSOY Oyj		x				1
382	Satellite Action Plan Regulatory Working Group		x				1
383	SBC Communications Inc.		x				1
384	SEC		x				1
385	SEMA Group		x				1
386	Sense Communications Internatio-nal AS		x				1
387	SFR				x		1
388	SIA			x			1
389	Siemens				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
390	SIIA				x		1
391	Skype				x		1
392	Sonaecom				x		1
393	Sonera		x				1
394	SONOFON		x				1
395	SPIG		x				1
396	STAKES				x		1
397	Stedenlink				x		1
398	Swedish government				x		1
399	Swisscom		x				1
400	Symantec				x		1
401	TDC				x		1
402	Tele Denmark		x				1
403	Telecel		x				1
404	Telecom e.V.				x		1
405	Telecoms Industry Association in DK				x		1
406	Teledesic		x				1
407	Telekom Slovenije				x		1
408	Telekom-Control		x				1
409	Telenor				x		1
410	Telenor AS		x				1
411	Telenordia		x				1
412	Telewest		x				1
413	Telfort		x				1
414	Telia AB		x				1
415	TeliaSonera AB				x		1
416	TerreStar Networks				x		1
417	The Center for Tele-Information		x				1
418	The Independent Television Com-mission		x				1
419	The Law Society of England			x			1
420	THUS				x		1
421	TIM Hellas				x		1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
422	Tiscali				x		1
423	Tite & Lewis			x			1
424	Toshiba					x	1
425	TRA		x				1
426	Ubisense					x	1
427	UK Information Commissioner´s Office				x		1
428	UK Operators Group		x				1
429	UK RFID Council					x	1
430	UKCTA				x		1
431	UKE				x		1
432	UMTS Forum				x		1
433	UNI-Europa				x		1
434	Unisys					x	1
435	United Kingdom				x		1
436	United Pan-European Communi-cations (UPC)		x				1
437	Uni-Telecom Europe		x				1
438	University of Luxembourg - Fac-ulty of Sciences, Technology and Communication					x	1
439	USG			x			1
440	Valerie Sedallian			x			1
441	VAT				x		1
442	VDAV				x		1
443	VECAI		x				1
444	Verbraucher-Ombudsmann Finn-land		x				1
445	Verkehrs- und Kommunikations-ministerium Finnland		x				1
446	Verkehrs- und Kommunikations-ministerium Norwegen		x				1
447	Versatel Telecom		x				1
448	VIAG Interkom GmbH&Co		x				1
449	VIATEL, Inc.		x				1
450	Vlaamse Gemeenschap		x				1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

	Akteur	DS-RL	2000 ePrivacy-RL	2002 DS-RL-Bericht	2006 Coo-kie-RL	2006 RFID	Häufig-keit der Partizip.
451	VNO-NCW		x				1
452	VODAFONE				x		1
453	Vodafone AirTouch Group		x				1
454	Voice of the Listener & Viewer		x				1
455	Vonage				x		1
456	WCA				x		1
457	Wipro Technologies					x	1
458	Wirtschaftkammer Österreich				x		1
459	WKO		x				1
460	World DAB		x				1
461	YPSO				x		1
462	ZAW			x			1

Tabelle Anhang 1: Häufigkeit und Zeitpunkt der Partizipation aller Akteure am Subystem der EU-Datenschutzpolitik bis zum Beginn des DSGVO-Aushandlungsprozesses

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

1.3 Detaillierte Tabellen für Abschnitt 5

Orientierungsphase:

Item	N	Mean	Std. Deviation	Missing	
				Count	Percent
B1 Einschätzung des techn. Wandels	44	2,98	1,303	15	25,4
B2 Grad an erwünschter staatlicher oder privater Aktivität	59	2,85	1,387	0	0
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	59	2,66	1,372	0	0
B6 Einstellung zu Harmonisierung	38	4,45	0,504	21	35,6
B8 Einschätzung der Globalisierung	29	2,86	1,356	30	50,8
B12 Haltung zur Überarbeitung des Datenschutzrahmens	45	2,96	1,429	14	23,7
C1B Räumlicher Anwendungsbereich	20	3,65	1,137	39	66,1
C1C Definition personenbezogener Daten	27	2,89	1,281	32	54,2
C2C Grundsatz der Datenminimierung	17	4,35	0,702	42	71,2
C3D Bedingungen für die Einwilligung	25	3,24	1,234	34	57,6
C5A Transparenz	27	3,59	1,248	32	54,2
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	21	3,52	1,03	38	64,4
C5L Benachrichtigung bei Datenschutzverletzung	23	3,57	1,08	36	61
C6A Privacy by Default	15	4,07	1,033	44	74,6
C6B Privacy by Design	22	3,86	1,207	37	62,7
C6C Meldepflicht/Verzeichnis von Verarbeitungstätigkeiten	28	2,71	1,049	31	52,5
C6H Verpflichtung des Verantwortlichen zu Datensicherheitsmaßnahmen	18	4,22	0,878	41	69,5
C6N Rechenschaftspflicht	45	2,64	1,246	14	23,7
C7 Übermittlung in Drittstaaten	36	2,36	1,125	23	39
C10D Bedeutung von Technologieneutralität	35	2,06	1,282	24	40,7
C13A Verhaltensregeln	20	2,8	1,152	39	66,1
C13B Zertifizierungen/Gütesiegel	18	3,17	1,465	41	69,5
C13C Bestellung eines organi 0sationsinternen Datenschutzbeauftragten	19	3,26	1,147	40	67,8
C13D DSFA bzw. vorherige Konsultation der zuständigen Datenschutzaufsichtsbehörde	18	4,11	1,132	41	69,5
C15B Zuständigkeit, Aufgaben und Befugnisse von Datenschutzaufsichtsbehörden	21	4,1	1,044	38	64,4
C17D Verbands-/Sammelklagerecht	17	3,65	1,412	42	71,2
C17E Sanktionen und Geldbußen	18	3,89	1,231	41	69,5
Durchschnitt der fehlenden Werte					52,03

Tabelle Anhang 2: Missing Value Analysis für alle 27 infrage kommenden Items in der Orientierungsphase (berechnet mit SPSS)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	DSGVO-E 2011	DSGVO-E 2012	AUT-Regierung	BRAK	CDT	Ministerratsposition	DEU-Regierung	DSAB-NOR	DSAB-PRT	DSAB-SWE	EPA	UK Justizmin.	GDD	LVA-Regierung	FTC	Häufigkeit d. Nennung
B1 Technologischer Wandel		4	5			4	4	4	3		4			4	4	8
B2 Staatl./Private Aktivität	5	5	3	1	4	4	2	4	4	4	3	3	4	5	3	13
B3 Policy-Orientierung im Falle staatlichen Handelns	6	5	3	2	3	2	2	4	4	3	2	2	3	3	2	13
B6 Harmonisierung		5	4	5	5	4	4	2			5			3		8
B8 Globalisierung		4	5											4	4	3
B12 Reformwunsch			5	4				5								3
C 1 B Räuml. Anwendungsbereich	5	4				4	4									2
C 1 C Definition personenb. Daten	5	4									1					1
C 2 C Grundsatz der Datenminimierung	4	4	5				4								4	3
C 3 D Einwilligung	5	5	5	4			2				5	2		2	3	7
C 4 A Besondere Kategorien personenbezogener Daten	4	4	2			4	4	4		2		2		3		7
C 4 D Datenschutz bei Kindern	5	5			2	5	4							4		4
C 5 A Transparenz	4	4	4		5	4	3	4	5					3	3	8
C 5 C Modalitäten für die Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung	4	4				4	3		3		4				2	5
C 5 E Recht auf Vergessenwerden	5	4	3		2		3					3		5		5
C 5 G Recht auf Datenportabilität	5	4	2		4		4									3
C 5 I Automat. Verarbeitung / Profiling	5	4					3									1

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

Item	DSGVO-E 2011	DSGVO-E 2012	AUT-Regierung	BRAK	CDT	Ministerratsposition	DEU-Regierung	DSAB-NOR	DSAB-PRT	DSAB-SWE	EPA	UK Justizmin.	GDD	LVA-Regierung	FTC	Häufigkeit d. Nennung
C 5 L Benachrichtigung bei Datenschutzverletzungen	5	4	4		5	3	4	5	4			3	4		4	9
C 6 A Privacy by Default	4	4				4									3	2
C 6 B Privacy by Design	4	4	4		5	4	3	5			5	4	4		4	9
C 6 C Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten	4	4	4	3	3	2	2			4		3	2			8
C 6 N Rechenschaftspflicht	5	4			4	5	2									3
C 7 Übermittlung in Drittstaaten	3	3	4		2	3	3				2	2	2		3	7
C 10 D Technologieneutralität	3	3	2				1		1			2	2	1		5
C 13 A Verhaltensregeln	4	4	3	2	3	2					3					5
C 13 B Zertifizierungen/Gütesiegel	3	3	3	3		3					4					4
C 13 C Bestellung eines bDSB	4	4	2		4	2	4	2	2			3	4	2		9
C 13 D Datenschutz-Folgenabschätzung	4	4	2		5		4	4		4		2				6
C 15 B Datenschutzbehörden	4	4	5	4	4	4	3		5	4		2			4	9
C 16 C Art. 29-Datenschutzgruppe	3	3	5		4	4	3					2				5
C 17 D Verbands- / Sammelklagerecht	4	4	3	2						4						3
C 17 E Sanktionen und Geldbußen	5	4	3				3					2				3

Tabelle Anhang 3: Positionierung der Community der Kompromisswilligen zu allen relevanten Themen in der Entwurfsphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb

Item	Ver 2016/679	Gesamtkonzept für DS in EU	Parlamentsposition	Ratsposition	DSGVO-Entwurf 2011	Vorschlag 2012/001 COD	DS-RL 95/46/EG	ICO 12-02	SWE-Parlament	SWE-Regierung	CPME	BRAK 12-11	ICO 13-02	EMPL-Bericht	EL/GR - Ratsvorsitz 2014-1	FR	IT - Ratsvorsitz 2014-2	CY - Ratsvorsitz 2012-2	HU	AT	PL	PT	RO	SK	Li - Liechtenstein	Häufigkeit d. Nennung
B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	3	4	5	2	5	4	3	2	4	3	2	3	3	3	4	4	3	3	4	4	5	2	2	3	3	25
C1B Räumliche Anwendungsbereich	4	5	5	4	5	4	3	3					3			2	4				5	5		2		15
C1C Definition personenbezogener Daten	4	4	5	3	5	4	3	4					4			3	3			4	3			3		14
C 2 C Grundsatz der Datenminimierung	4		4	3	4	4	3	4					4		3	3	3	3	3	3	3	3	3	3		18
C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	3	4	2	4	3	3	3	2					2	2		4	2	1	2			2				15
C3C Verarbeitung zu anderen Zwecken	3		5	1	2	2	4				4		3			3	4	3	3		4	4				15
C3D Bedingungen für die Einwilligung	4	4	5	3	5	5	3	4			3		4	4	4	4	4	4	4	2	4	2	4	2	4	22
C 4 A Besondere Kategorien personenbezogener Daten	4	4	5	3	4	4	3	3			4		3			2	3	2		2	4		4	4	2	18
C 4 D Datenschutz bei Kindern	4		5	3	5	5	3	3					3			5			5		3				4	12
C5A Transparenz	3	4	4	2	4	4	3	2				4	2			3	3	2	4		3	2	3		4	18
C5C Recht auf Auskunft bzw. Informationspflicht der Verarbeiter	3	4	5	3	4	4	3	3				3	3			4	2	2	4	3	3	2		2	4	19
C 5 E Recht auf Vergessenwerden	3	4	5	3	5	4	2	3					3			4	4	3	4	3	3	2	3			17
C 5 G Recht auf Datenportabilität	4	5	5	3	5	5	1						3			3	3		4		2			2		13
C5I Profiling / Automatisierte Entscheidungen bzw. Maßnahmen	3		4	3	5	4	3	4					3			3	5			3	2		3	4		14

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

C 5 L Benachrichtigung bei Datenschutzverletzungen	3	4	4	2	5	4	1	3					3		3	2	2	3	4	2	3	2		3		18
C6A Privacy by Default	3	4	4	2	4	4	2	3								5	4	3								11
C 6 B Privacy by Design	3	4	5	2	4	4	2	3					2			5	4	3						2		13
C 6 C Dokumentation	3	4	3	2	4	4	5						3			4	3				3	3	2	4		14
C 7 Übermittlung in Drittstaaten	4	3	5	2	4	4	3	2					3		3	3	3			4	4	4	3	3		17
C 13 A Verhaltensregeln	3	3	4	2	4	4	3						5			2					2	1		2		12
C 13 B Zertifizierungen/Gütesiegel	4	4	5	2	3	3	1						4			5					2	3		4		12
C 13 C Bestellung eines betrieblichen Datenschutzbeauftragten	3	4	5	2	4	4	2	3			2		3	4		2	2		3	4	3	4	4	3		19
C 13 D Datenschutz-Folgenabschätzung	3	4	5	2	4	4	1	3			2		3			2	2	3			3	2	2	2		17
C 15 C Datenschutzbehörden	4	4	5		4	4	3	4	3				3		3	2			4	5		3		2		15
C 17 D Verbands- /Sammelklagerecht	3	4	5	2	4	4	1						4				4				1	3		3		12
C 17 E Sanktionen und Geldbußen	5	4	5	3	5	4	1	3	3				3			4	2	3	4		4	4	4	3		18

Tabelle Anhang 4: Positionierung der Gruppe der bedingten Datenschutzbefürworter zu allen relevanten Themen in der Konfliktphase (eigene Erhebung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA – https://www.nomos-elibrary.de/agb

1.4 Überblick der formellen LIBE-Ausschusssitzungen zum DSGVO-E

Sitzung-Nr.	Datum	Inhalt
1	2012-02-27u28	Erläuterung des DSGVO-Entwurfs durch Françoise Le Bail, Generaldirektorin der GD Justiz
2	2012-05-30u31	Aussprache
3	2012-07-09u10	Aussprache und Erläuterung des ersten Arbeitsdokuments
4	2012-09-19u20	Zweite Aussprache über das erste Arbeitsdokument
5	2012-11-05u06	Prüfung der Arbeitsdokumente
6	2013-01-10	Vorstellung und Diskussion des Berichtsentwurfs
7	2013-01-21u22	Zweite Aussprache zum Berichtsentwurf
8	2013-03-20u21	Prüfung von Änderungsanträgen
9	2013-05-06u07	Prüfung von Änderungsanträgen
10	2013-10-21u24	Abstimmung und Annahme des Berichtsentwurfs und des Beschlusses, Verhandlungen mit dem Rat aufzunehmen

Tabelle Anhang 5: Liste aller mit der DSGVO befassten formellen LIBE-Ausschusssitzungen (eigene Zusammenstellung)

1.5 Überblick der formellen Rats-, AStV-, Ratsarbeitsgruppen- und Trilog-Sitzungen zur DSGVO

Nr.	Datum	Akteur	Thema	Beschluss
1	24.07.2012	Treffen der JI-Minister	Reduktion des Verwaltungsaufwands, Gleichbehandlung öff. und privater Sektor, Delegierte Rechtsakte bzw. Durchführungsrechtsakte	
2	26.10.2012	Treffen der JI-Minister	Wahl des Regulierungsinstruments (VO vs. RL)	
3	07.12.2012	Treffen der JI-Minister	Reduktion des Verwaltungsaufwands, Gleichbehandlung öff. und privater Sektor, Delegierte Rechtsakte bzw. Durchführungsrechtsakte	Erforderlichkeit eines risikoorientierten Ansatzes identifiziert Streichung vieler Akte
4	08.03.2013	Treffen der JI-Minister	Reduktion des Verwaltungsaufwands, Gleichbehandlung öff. und privater Sektor	
5	07.06.2013	Treffen der JI-Minister	Schutzniveau der Verordnung	Beibehaltung des Schutzniveaus der DS-RL (möglw. auch Stärkung)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema	Beschluss
6	08.10.2013	Treffen der JI-Minister	One-Stop-Shop / Kohärenzverfahren	
7	06.12.2013	Treffen der JI-Minister	One-Stop-Shop / Kohärenzverfahren	
8	04.03.2014	Treffen der JI-Minister	Räumlicher Anwendungsbereich, Kapitel V Grenzüberschreitende Datentransfers, Kapitel I-IV (Pseudonymisierung, Übertragbarkeit PB-Daten, Pflichten der Verantwortlichen), Profiling	Weitgehende Untersützung des Kommissionsentwurfs, Unterstützung des Kommissionsentwurfs im Grundsatz, jedoch für mehr Flexibilität
9	06.06.2014	Treffen der JI-Minister	Räuml. Anwendungsbereich Artikel 3 Abs. 2, Kapitel V, One-Stop-Shop / Kohärenzverfahren	Partielle allgemeine Ausrichtung zum Räuml. Anwendungsbereich und zu Kapitel V
10	09.07.2014	Treffen der JI-Minister	Wahl des Regulierungsinstruments (VO vs. RL)	VO mehrheitlich befürwortet, allerdings mehr Flexibilisität für MS gewünscht
11	10.10.2014	Treffen der JI-Minister	Kapitel IV, Recht auf Vergessenwerden	Partielle allgemeine Ausrichtung zu Kapitel IV
12	05.12.2014	Treffen der JI-Minister	Artikel 1, Artikel 6 Absätze 2 und 3, Artikel 21 und Kapitel IX, One-Stop-Shop / Kohärenzverfahren	Partielle allgemeine Ausrichtung zu Artikel 1, Artikel 6 Absätze 2 und 3, Artikel 21 und Kapitel IX, Erste Einigung zum One-Stop-Shop / Kohärenzverfahren
13	13.03.2015	Treffen der JI-Minister	One-Stop-Shop: Kapitel II, VI, VII	Partielle allgemeine Ausrichtung
14	16.06.2015	Treffen der JI-Minister		Verabschiedung der allgemeinen Ausrichtung des Rats

Tabelle Anhang 6: Lister aller mit der DSGVO befassten Treffen des Rats in der JI-Konfiguration (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
1	15.02.2012	AStV - 2396. Tagung	Application of the COMIX-procedure to the debates regarding the proposed JHA Data Protection Directive and General Data Protection Regulation
2	06.03.2012	AStV - 2399. Tagung - Coreper Part 2	Withdrawn: Optional consultation of the European Data Protection Supervisor 6911/12
3	09.10.2012	AStV - 2424. Tagung - Coreper Part 2	Preparation of the Council meeting (Justice and Home Affairs) on 25/26 October 2012 - (poss.) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free flow of such data (General Data Protection Regulation) : The Presidency will give an oral state of play and ask Ministers to instruct their collaborators to seek viable solutions to problems identified so far.
4	24.10.2012	AStV - 2426. Tagung - Coreper Part 2	The Chair informed the Committee that the Council would be invited to approve the implementation report on the Council conclusions on the protection of individuals with regard to the processing of personal data and on the free flow of such data
5	14.11.2012	AStV - 2429. Tagung - Coreper Part 2	Withdrawn: (poss.) GDPR Questionnaire on delegated/implementing acts 14946/1/12
6	27.11.2012	AStV - 2431. Tagung - Coreper Part 2	Report on progress achieved under the Cyprus Presidency 16525/12: The Committee discussed the Presidency's progress report, which was well received by many delegations. Regarding the issue of the risk-based approach, the Chair agreed to remove a possible ambiguity in the wording of the third indent of paragraph 25. Concerning the question of the flexibility for the public sector, several delegations wanted to highlight the issue of the choice of legal instrument more, whereas others, including the Commission, thought this issue should no longer be mentioned. The Chair decided not to change the fourth indent of paragraph 25, but to remove a possible contradiction by changing the last sentence of paragraph 24. The thus amended Progress report would be submitted to the JHA Council of 6-7 December 2012.
7	26.02.2013	AStV - 2442. Tagung - Coreper Part 2	Implementation of risk-based approach - Flexibility for the Public Sector - Orientation debate 6607/13 The Committee briefly discussed the Presidency note, which was broadly welcomed by delegations. The risk-based approach as outlined by the Presidency was widely supported. The Chair clarified at the outset of the debate that the Council was not going to discuss the question whether the draft Regulation could provide sufficient flexibility for the public sector. This was welcomed by several delegations and at their request the Chair indicated that the revised document for the Council would contain further clarification in this regard.
8	02.05.2013	AStV - 2450. Tagung - Coreper Part 2	Specific issues 8825/13 The Committee engaged in a detailed discussion of questions on 1-3 set out in the Presidency note. As the opinions of Member States on how to deal with these questions were divided, the Chair announced that the Presidency would reflect on how to deal with these questions in view of the June JHA Council meeting.
9	07.05.2013	AStV - 2451. Tagung - Coreper Part 2	Specific issues 8825/13 The Committee discussed questions 4 to 7 set out in the Presidency note. On question 4 there was a majority in favour of replacing the word "explicit" with "unambiguous" in Article 4 and in favour of deletion of paragraph 4 of Article 7. On question 5, many delegations indicated further scrutiny was

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
			required, especially in view of the links between this article and other parts of the draft Regulation. On question 6, while many delegations could agree to the text, others needed further scrutiny of the proposed text of Article 80. On question 7, most delegations could support the alternative proposal for Article 80a by the Swedish delegation, set out in DS 1376/13. The Chair concluded that the Presidency would further reflect on how to present this file to the JHA Council in June, in preparation of which the Committee would revert to the file.
10	23.05.2013	AStV - 2453. Tagung - Coreper Part 2	Agreement on key issues 9398/13 The Committee discussed the conclusions proposed by the Presidency in document 9398/13, as amended in DS 1452/13. The Committee also engaged in a brief discussion on the possible inclusion of EU institutions and bodies in the scope of the draft Regulation. The Chair indicated the item would be reverted to at the next meeting of the Committee.
11	28.05.2013	AStV - 2454. Tagung - Coreper Part 3	Key issues 9398/1/13 The Committee engaged in a discussion on the Presidency note, which was focused on the type of support Member States were willing to lend to key principles underlying the revised text of Chapters I-IV of the draft General Data Protection Regulation. A few other issues were raised as well. The Chair acknowledged that there were still a number of outstanding issues and indicated that the Presidency would further reflect as to the exact wording of the Presidency note that would be submitted to the Council.
12	25.09.2013	AStV - 2467. Tagung - Coreper Part 4	The one-stop-shop mechanism 13643/13 Following a presentation by the Presidency of its discussion note, the Committee engaged in a lengthy discussions of the issues raised in the paper. The vast majority of delegations intervening indicated that the need of 'proximity' of the supervisory authority was crucial element to be taken into account. Whilst many could lend support to the philosophy underlying the so-called one-stop-shop mechanism, only few Member states could accept the full implications referred to in question 1 of the Presidency note. Delegations gave varying answers regarding the alternatives in question 2.
13	02.10.2013	AStV - 2468. Tagung - Coreper Part 5	The one-stop-shop mechanism 14074/1/13 The Presidency presented its revised note. Following a lengthy debate, the Presidency indicated that it endeavour to further simplify the questions submitted to the Council, while at the same time ensuring that the Ministers were invited to make clear choices regarding the one-stop-shop mechanism.
14	27.11.2013	AStV - 2476. Tagung - Coreper Part 6	The one-stop-shop mechanism: partial general approach on essential elements 16626/1/13 The Chair announced that the Presidency would not be seeking a partial general approach on a legal text on this issue at the Council. This was welcomed by a large number of delegations, which stated that, notwithstanding the progress achieved on this topic, they were not in a position to agree to a partial general approach. Regarding the question whether the supervisory authority responsible for the main establishment of a controller could in some cases be entrusted with corrective powers, delegations were divided and some delegations were still undecided. The CLS intervened to make a number of points regarding the relationship between the one stop shop mechanism and judicial redress and judicial review for individuals affected by data protection violations. The Chair asked the CLS for written opinion on this.

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
15	03.12.2013	AStV - 2477. Tagung - Coreper Part 7	Essential elements of the one-stop-shop mechanism 16626/3/13 The Chair outlined the Presidency note, with which the Commission disagreed. A few delegations intervened, expressing regret that it had not been possible to achieve further progress on the important question of the one-stop shop mechanism. The Chair concluded that the Presidency note would be submitted to the Council.
16	26.02.2014	AStV - 2487. Tagung - Coreper Part 8	Orientation debate on certain issues 6762/14 Following a lengthy debate during which many delegations pleaded for a rewording of the questions and indicated that they were not willing to ask the Council for a partial general approach on any part of the legal text, the Presidency emphasised that it was seeking a political orientation debate at the Council. It also announced that it would endeavour to address the concerns expressed by delegations and that technical work would have to continue after the Council meeting. The Chair also indicated that the Presidency would provide, as soon as possible after the Council, information on how it intends to proceed further in relation to this file.
17	20.05.2014	AStV - 2498. Tagung - Coreper Part 9	Partial general approach 1 on Chapter V - Orientation debate on one-stop-shop mechanism 9865/14 An important number of delegations indicated that they would be able to support a partial general approach on Chapter V on the understanding that the caveats referred to in the Presidency note applied. Regarding the three questions set out in the Presidency note, it was concluded that JHA Counsellors would try to further fine-tune the proposed solutions and that the Committee would revert to the issue at its session of 28 May 2014.
18	28.05.2014	AStV - 2499. Tagung - Coreper Part 10	Partial general approach 1 on Chapter V – Orientation debate on one-stop-shop mechanism 9865/2/14 10139/14 The Committee discussed the Presidency proposal for a partial general approach on Chapter V, which received wide support from delegations. Austria and Slovenia made the following statement: "Austria and Slovenia are prepared to support the partial general approach under the conditions stated in paragraph 10 points i-iii of the document 9865/2/14 REV 2. The support is granted for the basic concept of Chapter V under the understanding that important issues were not sufficiently resolved and thus Member States are not precluded from discussing and making further proposals for improvement of Chapter V and articles linked with the rules stipulated therein. In this regard Austria underlines the importance of improvements and clarifications in particular regarding Art. 42 with a view to undoubtedly ensure that only legally binding and enforceable instruments may be considered as appropriate safeguards under this Article. Furthermore, Austria and Slovenia recall their conviction that the current wording of Art. 44 para 1 subpara h poses a high risk of circumvention of the overall concept of legal barriers and guarantees as set out in Chapter V and which would therefore undermine the objective of the latter. Finally, Austria and Slovenia underline the importance of the proposal for Art. 42a 'Disclosures not authorised by Union law' by the German Delegation (doc. 12884/13) and the corresponding amendments voted by the European Parliament to Art. 43a which should be discussed in detail at the technical level." Four delegations indicated their intention to submit statements at the Council meeting. The Presidency presented its discussion paper on the one-stop-shop mechanism. The Council Legal Service repeated its concerns regarding this mechanism, which had not been allayed by the amendments proposed by the Presidency. Some delegations took the same view, whereas others and the Commission disagreed.
19	24.09.2014	AStV - 2511. Tagung - Coreper Part 11	Partial general approach1 on Chapter IV 12312/2/14 The Committee discussed the questions in the Presidency note. A large num-

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
			ber of delegations indicated that they would be able to support a partial general approach on Chapter IV on the understanding that the caveats referred to in the Presidency note applied. Regarding the four questions set out in the Presidency note, it was concluded that JHA Counsellors would try to further fine-tune the proposed solutions and that the Committee would revert to the issue at its session of 1 October 2014.
20	30.09.2014	AStV - 2512. Tagung - Coreper Part 12	The right to be forgotten and the Google judgment - Orientation debate 13619/14 Partial general approach on Chapter IV 12312/4/14 The Chair briefly presented the Presidency note to the Council regarding 'the right to be forgotten'. The Committee discussed extensively the revised Presidency note on Chapter IV, which was widely welcomed. Some delegations nevertheless referred to a few outstanding issues. Following this discussion, the Chair indicated that the only issue on which further discussions would be held prior to the Council was the scope of the obligation for non-EU controllers to appoint representatives (Article 25). Germany made the below statement: "Statement by Germany on Chapter IV of the proposal for a General Data Protection Regulation as set out in Council document 12312/4/14 REV 4: Germany supports the partial general approach under the conditions listed in paragraph 8(i) to (iii) of the document. Germany reserves the right to return to the requirement for the mandatory appointment of a data protection officer for specific processing situations, due to its central importance in concluding discussions on the text."
21	19.11.2014	AStV - 2519. Tagung - Coreper Part 13	Public sector = Partial general approach (1) 15389/14 The Committee discussed extensively the Presidency note. Following this debate the Chair concluded that the document would be revised by JHA Counsellors and that a new document on the public sector, together with Chapter IX would be submitted to the next Committee meeting.
22	26.11.2014	AStV - 2520. Tagung - Coreper Part 14	Public sector and Chapter IX = Partial general approach - The one-stop-shop mechanism = Orientation debate 15655/14 15656/14 The Committee discussed extensively the Presidency note on the public sector and Chapter IX. Following this debate the Chair concluded that on the question of the inclusion of the public sector the right compromise had been found, but that on some other issues the document would be revised by JHA Counsellors with a view to submitting a revised document for a partial general approach to the Council. The Committee also discussed the Presidency note on the one-stop-shop mechanism. It was agreed that this question was not ripe for a partial general approach. The Chair concluded that the Presidency would endeavour to revise the document for the Council in order to take account of some of the most important comments made.
23	25.02.2015	AStV - 2531. Tagung - Coreper Part 15	Partial general approach1: One-stop-shop mechanism 6286/15 The Committee discussed the three questions set out in the Presidency's note. Following a lengthy debate, the Chair concluded that the draft text of the General Data Protection Regulation would be amended according to the following points: 1) no quantitative threshold would be set for submitting cases to the European Data Protection Board; 2) a system of judicial review of legally binding EDPB decisions would be designed in such a way that the time period for launching an action for the annulment of EDPB decisions will be triggered by the publication of that decision; and 3) the autonomy

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
			of staff from the European Data Protection Board working for the European Data Protection Board would be increased.
24	04.03.2015	AStV - 2532. Tagung - Coreper Part 16	Partial General approach1 – Chapter II – One-stop-shop mechanism (Chapter VI and VII) 6286/2/15 The Presidency presented the draft texts of Chapters II, VI and VII to the Committee with the request whether they could be supported with a view to reaching a partial general approach at the Council meeting on 12-13 March 2015. Following the discussion, the Chair concluded that the JHA Counsellors would be convened to attempt some further fine-tuning of the text of Chapter II. The current version of Chapters VI and VII would be submitted to the Council, subject to a possible modification of one provision.
25	29.04.2015	AStV - 2539. Tagung - Coreper Part 17	Preparation for a general approach: Chapter III 1 7978/1/15 On the basis of the Presidency compromise text annexed to document 7978/1/15 REV 1, the Committee identified the main issues regarding Chapter III of the Regulation that will need further work with a view to reaching a General Approach in the Council on 15/16 June 2015.
26	20.05.2015	AStV - 2542. Tagung - Coreper Part 18	Chapter VIII – Preparation of a general approach 8383/15 On the basis of the Presidency compromise text annexed to document 8383/15 the Committee discussed two questions on liability (Article 77) and confirmed the figures of administrative fines set out in the text (Article 79a). It was agreed that the JHA Counsellors would further elaborate the text of Article 77 with a view to reaching a General approach in the Council on 15/16 June 2015, as well as Article 76 on representation of the data subject.
27	27.05.2015	AStV - 2543. Tagung - Coreper Part 19	Article 6 and recital 40 in Chapter II and Chapter III = Preparation for a general approach 1 9082/15 On the basis of the Presidency compromise text annexed to document 9082/15, the Committee identified the main issues that will need further work with a view to reaching a General approach in the Council on 15/16 June 2015.
28	03.06.2015	AStV - 2544. Tagung - Coreper Part 20	Preparation for a general approach 9281/15 The Committee examined the Presidency compromise text for the General Data Protection Regulation in its entirety (doc. 9281/15) and the compromise text for the draft Data Protection Directive on scope (doc. 8745/2/15 REV 2). As a result of this examination, the Presidency instructed the Justice and Home Affairs Counsellors to prepare new compromise texts on the scope of the draft Regulation and Directive, the right to liability and compensation and other issues with a view to further discussion in the Committee on 9 June 2015.
29	09.06.2015	AStV - 2545. Tagung - Coreper Part 21	Preparation for a general approach 9657/15 On the basis of the Presidency compromise text annexed to document 9657/15, the Committee referred two issues to the JHA Counsellors in order to attempt to accommodate concerns voiced by some delegations. The outcome of the discussion is set out in documents 9788/15 and 8745/3/15 REV 3.
30	19.11.2015	AStV - 2564. Tagung - Coreper Part 22	Préparation du trilogue - Chapitres II, III, IV et V 13914/15 14076/15 With a view to preparing the next trilogue, the Committee examined Presidency compromise suggestions on the Chapters II, III, IV and V of the General Data Protection Regulation. The Presidency presented its suggestions on

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
			the main issues in document 13914/15. In addition, the Presidency submitted document 14076/15 which contains a comparative table reflecting in its fourth column the provisions on which either tentative agreements have been reached in the trilogues or on which the Presidency makes new compromise suggestions.
31	25.11.2015	AStV - 2565. Tagung - Coreper Part 23	Mündliche Informationen des Vorsitzes über die Ergebnisse des Trilogs = Vorbereitung des Trilogs – Kapitel I, VI, VII, VIII, IX, X und XI 14318/15 14319/15
32	02.12.2015	AStV - 2566. Tagung - Coreper Part 24	Vorbereitung des Trilogs 14481/15 14605/15 14824/15
33	09.12.2015	AStV - 2567. Tagung - Coreper Part 25	Vorbereitung des Trilogs 14901/15 14902/15 14936/15
34	16.12.2015	AStV - 2568. Tagung - Coreper Part 26	Analyse des endgültigen Kompromisstextes im Hinblick auf eine Einigung 15039/15
35	03.02.2016	AStV - 2572. Tagung - Coreper Part 27	Politische Einigung 5455/16 Statement by Austria

Tabelle Anhang 7: Liste aller mit der DSGVO befassten AStV-Sitzungen (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
1	23.02.2012	DAPIX Meeting	Discussion of Art. 1-4
2	14.03.2012	DAPIX Meeting	Discussions of Art. 5-21_mit Hustinx und Kohnstamm
3	23.05.2012	DAPIX Meeting	Articles 9 and following
4	27.06.2012	DAPIX Meeting	Brief Presentation of Presidency revision regarding Articles 1-9, Letter from the Chair of Working Party on Statistics, Article-by- article discussion of Articles 9 and following
5	11.07.2012	DAPIX Meeting	Articles 14(2) and following
6	03.09.2012	DAPIX Meeting	Articles 19 and following
7	25.09.2012	DAPIX Meeting	Discussion of Art. 28 and following
8	22.10.2012	DAPIX Meeting	Discussion of Replies to questionnaire on delegated/implementing Acts + Article-by-article discussion Art 34 and following
9	14.11.2012	DAPIX Meeting	Discussion of Replies to questionnaire on administrative burdens + Article-by-article discussion Art 39 and following
10	08.01.2013	DAPIX Meeting	Article-by-article discussion: Chapter VI and Section 3 of Chapter VII, followed by Sections 1 and 2 of Chapter VII
11	21.01.2013	DAPIX Meeting	Article-by-article discussion: Sections 2 of Chapter VII (Articles 61-63) and Chapter V (Articles 41-45)
12	29.01.2013	DAPIX Meeting	Article-by-article discussion: Chapters VIII, IX, X and XI
13	31.01.2013	DAPIX Meeting	Delegations were informed that DAPIX completed the first reading of the proposal on a GDPR and were briefed about the informal JHA ministers' meeting in Dublin on 17/18 January
14	12.02.2013	DAPIX Meeting	Implementation of risk-based approach in the GDPR
15	13.03.2013	DAPIX Mixed Committee Meeting	The right to be forgotten, the right to data portability and profiling + second examination of Chapters I and II
16	27.03.2013	DAPIX Mixed Committee Meeting	Main Establishment rule and consistency mechanism 7565/13
17	09.04.2013	DAPIX Mixed Committee Meeting	2. Lesung Kapitel I bis IV 8004/13
18	13.05.2013	DAPIX Mixed Committee Meeting	3. Lesung Kapitel I-V und Anwendbarkeit DSGVO auf Archive
19	14.06.2013	DAPIX Mixed Committee Meeting	2. Lesung von Kapitel 5 (Datentransfers)
20	03.07.2013	DAPIX Mixed Committee Meeting	Kapitel V ab Art 44, VI and Sektion 2 von Kap. VII - data transfers, supervisory authorities, co-operation and consistency
21	22.07.2013	DAPIX Mixed Committee Meeting	2. Lesung von Kapitel VI und VII (Supervisory Authorities, co-operation and consistency)
22	09.09.2013	DAPIX Mixed Committee Meeting	3. Lesung von Kapitel VI und VII (Supervisory Authorities, co-operation and consistency)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
23	23.09.2013	DAPIX Mixed Committee Meeting	3. Lesung von Kapitel VII und VIII (co-operation and consistency, remedies, liablility and sanctions)
24	28.10.2013	DAPIX Mixed Committee Meeting	4. Lesung von Kaitel VIII (Remedies, Liability and Sanctions)
25	20.11.2013	DAPIX Mixed Committee Meeting	One-Stop-Shop Mechanism
26	08.01.2014	DAPIX Mixed Committee Meeting	Kapitel IX und Profiling und Pseudonymisierung
27	20.01.2014	DAPIX Mixed Committee Meeting	Kapitel IX Art. 83a-83c, Pseudonymisierung, Profiling, Controller and Processor
28	05.02.2014	DAPIX Mixed Committee Meeting	Datenportabilität (Revision von Art. 18), Data Protection Impact Assessment and prior Checks, Controller and Processor (Revision of Art. 26), One-stop-shop-mechanism)
29	18.02.2014	DAPIX Mixed Committee Meeting	Provisions concerning Profiling, Provisions concerning processing for archiving, historical and research purposes, one-stop-shop mechanism
30	12.03.2014	DAPIX Mixed Committee Meeting	One-Stop-Shop Mechanism
31	31.03.2014	DAPIX Mixed Committee Meeting	Kapitel V Internationale Datentransfers, Datenportabilität
32	10.04.2014	DAPIX Mixed Committee Meeting	Provisions concerning Profiling, Data Protection Impact Assessment and prior Checks, Controller and Processor - Revision of Article 26
33	07.05.2014	DAPIX Mixed Committee Meeting	Internationale Datentransfers (Kapitel V), One-stop-shop Mechanism
34	15.05.2014	DAPIX Mixed Committee Meeting	Internationale Datentransfers (Kapitel V), One-stop-shop Mechanism
35	12.06.2014	DAPIX Mixed Committee Meeting	Datenportabilität (Revision von Art. 18), Processor (Revision of Art. 26), Data Protection Impact Assessment and Prior Checks, Presidency's Note concerning Profiling
36	10.07.2014	DAPIX Mixed Committee Meeting	Risk based approach, The right to be forgotten
37	11.09.2014	DAPIX Mixed Committee Meeting	Kapitel V, the right to be forgotten
38	30.09.2014	DAPIX Mixed Committee Meeting	Public Sector and Kap. IX
39	21.10.2014	DAPIX Mixed Committee Meeting	Kapitel II, Art. 21 und Kapitel IX
40	28.10.2014	DAPIX Mixed Committee Meeting	Kapitel II, Art. 21 und Kapitel IX
41	06.11.2014	DAPIX Mixed Committee Meeting	One-Stop-Shop Mechanism, Kapitel IX
42	20.11.2014	DAPIX Mixed Committee Meeting	One-Stop-Shop Mechanism

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Nr.	Datum	Akteur	Thema
43	15.01.2015	DAPIX Mixed Committee Meeting	Kapitel II
44	26.01.2015	DAPIX Mixed Committee Meeting	The one-stop-shop mechanism, Kapitel III sections I and II
45	05.02.2015	DAPIX Mixed Committee Meeting	The one-stop-shop mechanism, Kapitel II
46	23.03.2015	DAPIX Mixed Committee Meeting	Kapitel III und VIII
47	30.03.2015	DAPIX Mixed Committee Meeting	Acceptability of the GDPR to the activities of the International Committee of the Red Cross (ICRC),Kapitel III und VIII, Article 76
48	21.04.2015	DAPIX Mixed Committee Meeting	Kapitel VIII
49	06.05.2015	DAPIX Mixed Committee Meeting	Relationship Chapters II and IX, Chapters I and XI
50	18.05.2015	DAPIX Mixed Committee Meeting	Delegated and implementing acts, Chapters I and XI, Chapter III and horizontal issues, including Chapter II Art. 6, International Committee of the Red Cross
51	01.07.2015	DAPIX Mixed Committee Meeting	Articles 3(2), 4(14) and 25 and Chapter V - Preparation of the trilogue on 14 July 2015 9985/1/15 REV 1
52	02.09.2015	DAPIX Mixed Committee Meeting	Chapter III, preparation of trilogue 11082/15

Tabelle Anhang 8: Liste aller mit der DSGVO befassten DAPIX-Ratsarbeitsgruppensitzungen (eigene Zusammenstellung auf Grundlage der Sitzungsprotokolle und Tagesordnungen)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

Datum	# der Sitzung	Themen
24.06.2015	1. Trilog-Sitzung	• Package approach: Objective of Luxembourg Presidency for the proposed directive • Agreement on the overall roadmap for Trilogue negotiations • General method and approach for delegated and implementing acts
14.07.2015	2. Trilog-Sitzung	• Territorial scope (Article 3), Representative (Article 25) • International transfers (Chapter V), related definitions
16./17.09.2015	3. Trilog-Sitzung	• Data protection principles (Chapter II) • Data subject rights (Chapter III) • Controller and Processor (Chapter IV)
29./30.09.2015	4. Trilog-Sitzung	• Data protection principles (Chapter II) • Data subjects rights (Chapter III) • Controller and Processor (Chapter IV)
15.10.2015	5. Trilog-Sitzung	• Independent Supervisory Authorities (Chapter VI) • Cooperation and consistency (Chapter VII) • Remedies, liability and sanctions (Chapter VIII)
28.10.2015	6. Trilog-Sitzung	• Independent Supervisory Authorities (Chapter VI) • Cooperation and consistency (Chapter VII) • Remedies, liability and sanctions (Chapter VIII)
11./12.11.2015	7. Trilog-Sitzung	• Objectives and material scope (Chapter I) • Specific regimes (Chapter IX)
24.11.2015	8. Trilog-Sitzung	• All open issues from Chapter I to IX
10.12.2015	9. Trilog-Teilsitzung 1 von 2	• Delegated and Implementing Acts (Chapter X) • Final provisions (Chapter XI) • Remaining issues
15.12.2015	9. Trilog-Teilsitzung 2 von 2	• Delegated and Implementing Acts (Chapter X) • Final provisions (Chapter XI) • Remaining issues

Tabelle Anhang 9: Überblick aller Trilog-Sitzungen und der Themen (EPP 2015)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

1.6 Vollständige Akteurslisten der Datenschutz-NGOs

#	**Akteur**
1	Advocacy for Principled Action in Government
2	Center for Digital Democracy
3	Center for Media and Democracy
4	Consumer Action
5	Consumer Federation of America
6	Consumer Watchdog
7	Consumers Union
8	Cyber Privacy Project
9	Electronic Privacy Information Center
10	Essential Information
11	The FoolProof Initiative
12	Friends of Privacy USA
13	Liberty Coalition
14	National Association of Consumer Advocates
15	National Consumers League
16	Patient Privacy Rights
17	Privacy Journal
18	Privacy Rights Clearinghouse
19	Privacy Rights Now
20	Privacy Times
21	Public Citizen
22	U.S. PIRG

Tabelle Anhang 10: Unterzeichner-Organisationen des TACD-Briefes an die Rapporteure Albrecht und Comi vom 5. September 2012 (US-Consumer Organizations 2012)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

#	**Akteur**
1	Access (International)
2	Article 19 (International)
3	Bits of Freedom (The Netherlands)
4	Digitalcourage (Germany)
5	Digitale Gesellschaft e.V. (Germany)
6	Electronic Frontier Finland (Finland)
7	European Digital Rights (Europe)
8	Europe-v-facebook.org (Austria)
9	Initative für Netzfreiheit (Austria)
10	IT-Political Association of Denmark (Denmark)
11	La Quadrature du Net (France)
12	Net Users' Rights Protection Association (NURPA) (Belgium)
13	Open Rights Group (ORG) (United Kingdom)
14	Panoptykon Foundation (Poland)
15	Privacy International (International)
16	Statewatch (United Kingdom)
17	VIBE (Austria)
18	Vrijschrift (The Netherlands)

Tabelle Anhang 11: Unterzeichner-Organisationen des NGO-Briefes an die griechische Ratspräsidentschaft vom 28. Januar 2014 (Civil Rights Organisations 2014)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

#	**Akteur**
1	EDRi (Europe)
2	Access (Interntaional)
3	Association for Progressive Communications – APC (International)
4	Privacy International (International)
5	World Wide Web Foundation (International)
6	ALES - Alumni of European Studies (Croatia)
7	Aktion Freiheit statt Angst e.V. (Germany)
8	AKVorrat.at - Arbeitskreis Vorratsdaten Österreich (Austria)
9	Arbeitskreis Vorratsdatenspeicherung (Germany)
10	Asociatia pentru Tehnologie si Internet - ApTI (Romania)
11	BEUC - The European Consumer Organisation (Europe)
12	Bits of Freedom (Netherlands)
13	Consumentenbond (Netherlands)
14	Danish Consumer Council (Denmark)
15	Deutsche Vereinigung für Datenschutz e.V. (Germany)
16	DFRI (Sweden)
17	Digitalcourage (Germany)
18	Digitale Gesellschaft e.V. (Germany)
19	EU-Logos Athèna (Belgium)
20	European Information Society Institute - EISi (Slovakia)
21	FIfF - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (Germany)
22	Forum Datenschutz (Austria)
23	Fundamental Rights European Experts Group - FREE (Europe)
24	GeneWatch UK (United Kingdom)
25	GreenNet (United Kingdom)
26	Hungarian Civil Liberties Union (HCLU)
27	Initiative für Netzfreiheit (Austria)
28	International Modern Media Institute (Iceland)
29	Iuridicum Remedium (Czech Republic)
30	IT-Pol (Denmark)
31	Liberty – NCCL (United Kingdom)
32	medConfidential (United Kingdom)
33	Norwegian Consumer Council (Norway)
34	One World Platform (Bosnia Herzegovina)
35	Open Rights Group (United Kingdom)
36	Panoptykon Foundation (Poland)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

37	SHARE Foundation (Serbia)
38	#StopWatchingUs Cologne (Germany)
39	VZBV - Federation of German Consumer Organisations (Germany)
40	VIBE - Verein für Internet-Benutzer Österreichs (Austria)
41	JONCTION (Senegal)
42	KICTANet (Kenya)
43	Unwanted Witness Uganda (Uganda)
44	Bytes for All (Pakistan)
45	CIS India (India)
46	Digital Rights Foundation (Pakistan)
47	Foundation for Media Alternatives (Philippines)
48	Australian Privacy Foundation (Australia)
49	Asociación para una Ciudadanía Participativa - ACI-Participa (Honduras)
50	Fundación Acceso (Costa Rica)
51	IPANDETEC – Instituto Panameño de Derecho y Nuevas Tecnologías (Panama)
52	British Columbia Civil Liberties Association (Canada)
53	Center for Digital Democracy (United States)
54	Consumer Federation of America (United States)
55	Consumer Watchdog (United States)
56	Electronic Privacy Information Center – EPIC (United States)
57	Horizontal (Mexico)
58	Open Government Project (Canada)
59	Red en Defensa de los Derechos Digitales - R3D (Mexico)
60	Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic - CIPPIC (Canada)
61	ADC - Asociación por los Derechos Civiles (Argentina)
62	DATA (Uruguay)
63	Fundacion Karisma (Colombia)
64	Fundación Vía Libre (Argentina)
65	Hiperderecho (Peru)
66	TEDIC (Paraguay)

Tabelle Anhang 12: Unterzeichner-Organisationen des NGO-Briefes an den Kommissionspräsidenten Juncker vom 21. April 2015 (EDRi und Access (International) 2015)

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – (cc) BY-NC-SA - https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748915898, am 12.07.2024, 12:52:10
Open Access – BY-NC-SA - https://www.nomos-elibrary.de/agb