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.

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).

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.

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

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.

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).

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-

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]

	N	Mean	Std. Deviation	Missing	
Item				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,

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-

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

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)

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.

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)		

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)

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

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.

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

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-

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/12684.htm https://be.linkedin.com/in/christopher-kuner-888500

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.

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.).

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

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

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.

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

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

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

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.

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

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

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

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.

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)

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-

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

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)

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
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	2	1	2	3	4	4		2	1	3	4	34
B2 Staatl./Private Aktivität	5	4	2	2	2	2	2	1	2	1	1	2	2	1	1	2	2	1	2	2	2	2	2	3	2	4	2	2	3	2	2	1	2	3	2	1	2	2	2	2	1	39
B3 Policy-Orientierung	4	2	2	2	2	2	2	1	2	1	1	2	2	1	1	2	2	1	2	2	1	1	1	2	2	2	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	4	5			4	5	4	4	5	4		4		4	5	5	5	4	5	4	4	4		29
B8 Globalisierung	4			4	2	2	2	2	2	2		2	2	1		2				2				2		2	2	2	1				2			2						20
B12 Reformwunsch	5		4	2	2	2	2	2	2	2		3	3		1	2	2	1	2	1	2		1	2	1		2	2	3	2	1	3	2	3	1	2	4	2	2	2		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								1	1								2			2	2							2	2		2			2					18
C 3 D Einwilligung	4	3								2					2		2			3			2				3	2		2						2					16
C 5 A Transparenz	3	3	2								1		3				2				2	4	2				2							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																																							1
C 5 G Recht auf Datenübertragb.	5	1																																							0
C 5 I Automat. Verarb./Profiling		3																						1																	2
C 5 L Meldung v. Verletzungen	4	1											2									3								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										1		2	2	2	2	2			2	3		2	2			3				2	2		2	2		2	2	2			17
C 6 H Datensicherheit	4	3																				4													3						2

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	1	2	33
C 7 Drittstaatentransfers	4	3			2	2	2	2	2	2		2	2			1	3		2	1			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			2	3	1		2		1		2			1	1				26
C 13 A Verhaltensregeln	3	3			2	2	2	2	2									2		2			2	2				2								2						13
C 13 B Zertifizierungen/Gütesiegel	3	1																					1	2						2	2						2					6
C 13 C Bestellung eines DSB	4	2								2		4				2						2							3													7
C 13 D DSFA	4	1																			4	4						4			4											2
C 15 B Datenschutzbehörden	4	3											4									4						4			4						1				7
C 16 C Art. 29-Datenschutzgruppe		2								2					1	1				2	1					1	2				2	2		4			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)

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.

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

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)

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-

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

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.

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).

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).

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

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

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-

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

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).

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	

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

Item	Cluster 1	Cluster 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	

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 vertretenen Positionen als eine Art Zwischenposition

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.

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

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

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

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)

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

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

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).

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).

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

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

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

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.

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

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

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.

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

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.

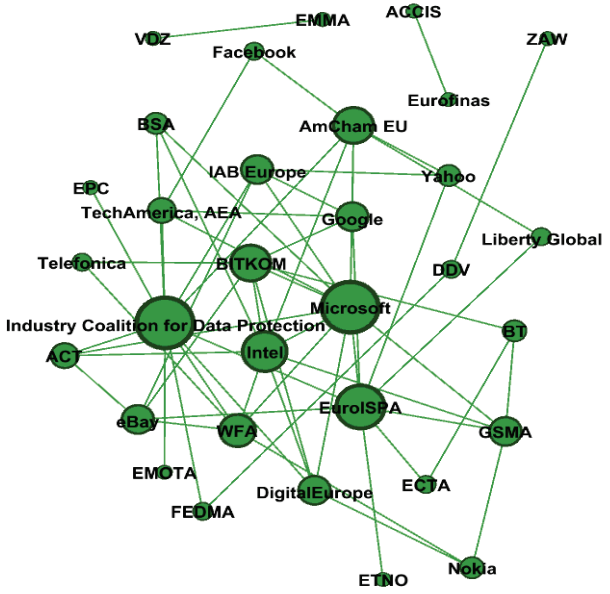

Abbildung 7: Netzwerk der Flexibilitätsbefürworter (eigene Darstellung und Berechnung)

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).

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

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

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.

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)."

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.

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).

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).

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).

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

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)

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).

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

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

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 Zertifizierungs*pflicht* 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)

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).

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.

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 Identitäsdiebstahl, 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.

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).

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)

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).

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).

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.

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		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

Häufigkeit d. Nennung	32	19	31	25	6	24	6	28	28	20
ZAW	2 2	3 3	2 2					2 2	1 1	
Yahoo	1 1	3 3	2 2	2				2 2	1 1	2 2
WFA	2 2	3 3	2 2					1 1	2 2	2 2
VDZ	1 1	3 3		2 2		2 2		1 1		2 2
UEAPME	2 2					1 2			2 2	2 2
Telefonica	2 2	3 3	3 3	2 2				2 2	2 2	2 2
TechAmerica (formerly AeA)	1 1	2 2	2 2	2 2		1 2		2 2	2 2	2 2
Nokia	2 2	3 3	1 1	2 2		2 2		1 1	1 1	1 1
Microsoft	2 2	3 3	1 1	2 2		1 2		2 2	2 2	1 1
Liberty Global			2 2			2 2		2 2		1 1
Intel	2 2							2 2	2 2	2 2
Industry Coalition for DP	2 2	3 3	3 3	1 1			1 1	2 2	2 2	2 2
ICO		4 4	2 2		2 2	3 3	3 3	3 3	2 2	2 2
ICC	1 1		2 2	2 2		2 2		2 2	2 2	2 2
IAB Europe	3 3	3 3	2 2	2 2		3 3		2 2		
GSMA	2 2		3 3	2 2					1 1	2 2
GDV	3 3	3 3	2 2	2 2	2 2	3 3		2 2	2 2	
FTC	3 3	2 2				4 4	3 3	4 4		
FEDMA	1 1		2 2		2 2					
FBF	3 3			2 2		3 3			2 2	2 2
Facebook	3 3		3 3	2 2		2 2			2 2	2 2
EuroISPA	2 2		3 3	2 2	2 2	2 2			2 2	
Eurofinas	1 1	3 3	2 2		1 1	1 1		2 2		1 1
ETNO	2 2		3 3	2 2			1 1	2 2	2 2	
EPC	2 2		1 1	2 2		3 3		2 2		
ENPA & FAEP	2 2	3 3	1 1	2 2				2 2	1 1	
EMOTA		3 3		3 3					2 1	
ECTA			3 3	2 2	1 1	3 3	1 1	1 1	2 1	
EBF	2 2					1 1		2 2	2 1	
eBay			2 2							
DIGITALEUROPE	2 2	2 2	2 2	2 2		3 3		1 1	1 1	2 2
DDV	2 2	3 3	3 3	2 2				3 3	2 1	
BT	2 2		2 2					1 1	1 1	
BSA			3 3	2 2		2 2		2 2	2 1	2 2
BITKOM	2 2		3 3	1 1		2 2				
BDIU										
AmCham EU	1 1		2 2	2 2		2 2	2 2	2 2	3 3	1 1
ACT	2 2		2 2			2 2				
ACCIS	2 2	2 2	3 3	2 2		2 2		2 2	2 2	
DSGVO-E 2012	4 4	4 4	4 4	5 5	4 4	4 4	4 4	4 4	4 4	4 4
DSGVO-E 2011	4 4	4 4	5 5	5 5	5 5	5 5	4 4	4 4	4 4	5 4
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

Häufigkeit d. Nennung	28	25	26	21	26	20	11	20
ZAW		1 1	2		1			2
Yahoo	2	1 1	1 2	1	2	2		1
WFA		1 1	2					
VDZ		1 1	2 2	1	1			
UEAPME	2	2	2	2 1	2	2		
Telefonica	2 2	1 2	1 2	1 2	2	2	4 4	2
TechAmerica (formerly AeA)	1 1	2 2	2 2	2 2			4 4	2 2
Nokia	1 1	2 2	2	2 2	2	2		2 2
Microsoft	1 1	1		1 1			4	2
Liberty Global	2 2	2	1	1 1	2 2	2		4
Intel	2 2	1		1 1	2 2	2		
Industry Coalition for DP	2 2		1	1	2 2	1		
ICO	2 2	4			2 2	3	4	4
ICC	2 2		2	2 2	2 2	2		
IAB Europe			2 2	2 2	2 2	2		2 2
GSMA	1	1	2 2	4	2 2			2 2
GDV	2 2	4	2	3	3	2		
FTC	3						4	
FEDMA	2 2							
FBF	2 2				1			
Facebook			1 2	1 2		2		3
EuroISPA	2	2	1	1 2		2 2		2 3
Eurofinas						2		
ETNO	2	1	2		3			2
EPC		2	1	2	2 2	2	3	2 2
ENPA & FAEP		1	1	2	2 2		3	2 2
EMOTA		2	2		2			
ECTA	1		1				4	2
EBF	2 2	2						
eBay	2 2	2 2						
DIGITALEUROPE	2 2	1 1	1	1	2	2	4	2
DDV	2 2	1 1	1		1			
BT	2 2							
BSA	1 2	1	2	2	2 2	3 2		2
BITKOM	2				3	3		
BDIU							2	
AmCham EU	1	2	1	2	2 2	2		2
ACT					2			
ACCIS	2 2		2	2 2	2 2	2	2	2 2
DSGVO-E 2012	4 4	3 3	4 4	3 3	4 4	4 4	4 4	3 3
DSGVO-E 2011	4	3	4	3	4	4	4	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

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)

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

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.

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.

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

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).

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).

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).

> *„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

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-

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-

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

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.

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

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.

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.

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.

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-

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-

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-

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

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.

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-*

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

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

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.

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-

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-

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).

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)

(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.

Item	Flexibilitätsbefürworter	DSGVO-E	Datenschutzbefürworter	Kompromissswillige
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)

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.).

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.

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)

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.

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)

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)

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

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

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-

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-Berichtsent-wurf	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).

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.

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)

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

	Extreme Datenschutzbefürworter											Gemäßigte Datenschutzbefürworter									
Item / Akteur	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

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).

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

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).

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).

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

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)

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).

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

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.).

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).

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).

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)

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.).

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
FI	Mitgliedstaatl. Regierung
GDD	Zivilgesellschaft/Wirtschaft

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.

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)

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).

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".

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

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.

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).

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).

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

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).

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-

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).

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

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-

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

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).

Name	B3 Grundlegende Policy-Orientierung im Falle staatlicher Interventionen	C1B Räumliche Anwendungsbereich	C1C Definition personenbezogener Daten	C 2 C Grundsatz der Datenminimierung	C3A Bedingungen für die Rechtmäßigkeit einer Verarbeitung	C3C Verarbeitung zu anderen Zwecken	C3D Bedingungen für die Einwilligung	C4A Besondere Kategorien personenbezogener Daten	C 4 D Datenschutz bei Kindern	C5A Transparenz
Häufigkeit d. Nennung	29	10	13	21	17	14	26	13	8	21
NO - Norway	2	3						4	5	2
SE	1	3	4	3	2	1	2	1		2
Fl	3			3			2			2
Sl	2		4	3		1	2	3	1	2
NL	3			3	2	1	2	4		2
MT	2			3		3	2			2
LU - Ratsvorsitz 2015-2	2		2	4			3	4		2
LT - Ratsvorsitz 2013-2	2	3		3	4	3	2	2		2
LV - Ratsvorsitz 2015-1	3			3			2			
HR	3			3			2			
ES	2		3	3	2	3	2			2
IE - Ratsvorsitz 2013-1	2	3	2	3	2		2	3		2
EE	2		3	3			2	2		2
DE	1	4	3	3	2	1	2	2	3	2
DK - Ratsvorsitz 2012-1	1			3			2			1
CZ	2	2		3	2		2	1	1	1
BG	2			3	2	3	2			
BE	2	2	3	3	1	3	2	2		2
JURI-Bericht	3		3	2	1	1	4	4	3	3
FEDMA	2				3	2				
Intel	2				2					
IMCO-Bericht	2	3	3	2	1	1	2	4	4	2
FBF 12-08	2	4		1			2			2
Microsoft 12-07	2				2		2			
GDD	3		3		2	1	3			3
ACCIS 12-04	2			2	2	1	2			
Facebook 12-03	2						2		3	4
CDT 12-03	3		3				3		4	
Google	2	4	2		2		2			3
DS-RL 95/46/EG	3	3	3	3	3	4	3	3	3	3
Vorschlag 2012/001 COD	4	4	4	4	3	2	5	4	5	4
Ratsposition	2	4	3	4	4	1	3	3	3	2
Parlamentsposition	5	5	5	4	2	5	5	5	5	4
Gesamtkonzept für DS in EU	4		4		4		4	4		4
Ver 2016/679	3	4	4	4	3	3	4	4	4	3

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		3	2	3	3	2	2	2
Fl	3	3		2				4	2	1
Sl	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
EE	3	2	2							1
DE	3	3	2	3	2	4	2	2	3	1
DK - Ratsvorsitz 2012-1	2	2	2	2		3	3			1
CZ	3	3		3	3			2	2	1
BG	2	2	2	2				4		2
BE	2	2	3	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	4	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

Name	C 13 B Zertifizierungen/Gütesiegel	C 13 C Bestellung eines bDSB	C 13 D Datenschutz-Folgenabschätzung	C 15 C Datenschutzbehörden	C 17 D Verbands- /Sammelklagerecht	C 17 E Sanktionen und Geldbußen
Häufigkeit d. Nennung	9	2 2	2 0	1 1	1 2	2 0
NO - Norway		3		2 3	3	2 2
SE		2	3	2 3	2 3	2 2
Fl		1	2 2			3
Sl	2 2	2	2 2	2 2	1 1	2
NL	2 2	2	3	2 2	1	
MT						3 3
LU - Ratsvorsitz 2015-2		3	2	2		3 3
LT - Ratsvorsitz 2013-2		2				
LV - Ratsvorsitz 2015-1		2	4			3
HR						
ES	3 2	2	2		3	3
IE - Ratsvorsitz 2013-1	3	2 2	2 2	2		3 3
EE		2	2 2	3 2	1	2
DE	2	4	3 3	4	3	3 3
DK - Ratsvorsitz 2012-1		2	3			3
CZ	1	3	2	2	1	
BG		4				
BE	3 2	2 2	2 2	3		3 3
JURI-Bericht	3	2	2		2	3
FEDMA						
Intel						
IMCO-Bericht		3 2	3		1 1	2 2
FBF 12-08		3	2 2		1 1	2 2
Microsoft 12-07	2		2 2			2 2
GDD		2 3	2 2			
ACCIS 12-04		2	2 2		1	2 2
Facebook 12-03				3		3 2 2
CDT 12-03		2	2			3
Google						
DS-RL 95/46/EG	1	2	1	3	1	1
Vorschlag 2012/001 COD	3	4	4	4	4	4
Ratsposition	2	2	2		2	3
Parlamentsposition	5	5	5	5	5	5
Gesamtkonzept für DS in EU	4	4	4	4	4	4
Ver 2016/679	4	3	3	4	3	5

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

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	2	1	2	2							2				1		1			1	3	2	1		16
C 2 C Grundsatz der Datenminimierung					2											1	2		2		1				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			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				15
C5C Modalitäten für die Wahrnehmung von Betroffenenrechten		2	1		1	2		1					3			2	2	2	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				2			1	2	1				1		1	1	2			14
C5L Benachrichtigung bei Datenschutzverletzungen	2		2		2			1	2	1	1	1	2	3	2	1	1	2				2		1	2		2		18

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	1		2	1		1	1		1		17
C 6 C Dokumentation		1	2					1	2	2	2	2	1		1	1		1				1	1	1			1		16
C 7 Übermittlung in Drittstaaten	2		2							2	2	2			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	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)

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

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

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.

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

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-

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).

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).

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).

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.

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)

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).

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).

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).

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

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).

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)

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

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-

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).

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).

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).

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).

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

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).

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

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).

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.

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*

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).

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.

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.

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).

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

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.).

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).

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).

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).

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).

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.

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).

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.

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)

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

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

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

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.

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,

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-

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 unterschtätzt werden, dass sich

431 Rede Viviane Redings auf der CPDP 2016.

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.