Anforderungen an die automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal: eine Multi-Stakeholder-Perspektive auf Motivation und Umsetzung

Lars Pfeiffer, Stefanie Astfalk, Lorenz Baum, Björn Hanneke, Christian H. Schunck und Matthias Winterstetter

Zusammenfassung

In der Digitalwirtschaft besteht ein erhebliches Bedürfnis nach sowohl effektiven als auch effizienten Lösungen, um datenbasierte Geschäftsmodelle mit den hohen europäischen Datenschutz-Standards in Einklang zu bringen. Hierbei stellen einerseits die Förderung von Transparenz und Intervenierbarkeit für die betroffenen Personen sowie andererseits der Ressourcenaufwand zur Einhaltung der rechtlichen Vorgaben für – insbesondere kleine und mittlere – Unternehmen wesentliche Herausforderungen dar. Personal Rights Management (PRM)-Systeme können bei der Adressierung dieser Herausforderungen unterstützen, indem sie auf einen vermittelnden Ansatz abzielen, der den Interessen aller Stakeholder gerecht wird. Dieser Beitrag beschreibt aus einer datenschutzrechtlichen, sozioökonomischen und technischen Perspektive die Motivation für und die Multi-Stakeholder-Anforderungen an die Komponente des Transaktionsjournals zur automatisierten Protokollierung von Datenverarbeitungstätigkeiten im Rahmen eines PRM-Systems. Betroffene erhalten durch das Transaktionsjournal eine nachvollziehbare Darstellung dessen, was mit ihren Daten geschieht, was die jeweilige Verarbeitungstätigkeit legitimiert und welche Interventionsmöglichkeiten ihnen zur Verfügung stehen. Unternehmen profitieren von einem besseren Überblick ihrer Datenverarbeitungstätigkeiten und der Förderung ihrer Fähigkeit zum Nachweis der Einhaltung ausgewählter datenschutzrechtlicher Anforderungen.

1. Einführung – Fortbestehende Datenschutzprobleme in der Praxis

In der Digitalwirtschaft besteht ein erhebliches Bedürfnis nach technischen sowie ökonomischen Lösungsansätzen, um die seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) hohen europäischen Standards zum Privatsphärenschutz mit datengetriebenen Geschäftsmodellen in Einklang zu bringen. Gerade in der Plattformökonomie[1] kann die ressourcenbindende Einhaltung der Vorgaben aus der DSGVO, insbesondere für kleinere Plattformbetreiber,[2] eine Hürde bedeuten. Allerdings sehen sich nicht nur kleine Unternehmen Schwierigkeiten gegenüber – selbst große digitale Plattformen haben Probleme, ihre Datenbestände und deren rechtmäßige Verarbeitung zu kontrollieren, sich der Rechtskonformität ihrer Tätigkeiten zu vergewissern und ihren Dokumentationspflichten nachzukommen.[3] Neben dieser unternehmenszentrierten Perspektive führt die Vielzahl der über eine Plattform interagierenden Akteure zu zahlreichen unterschiedlichen Datenströmen und Möglichkeiten der Datenweitergabe, was aus Sicht der betroffenen Personen die Nachvollziehbarkeit der Datenverarbeitung erschwert. Dabei sind selbst abseits der Plattformökonomie die datenschutzrechtlichen Transparenzprobleme in der Praxis immer noch nicht zufriedenstellend gelöst – beispielsweise werden regelmäßig weder Einwilligungen „in Kenntnis der Sachlage" (ErwGr. 42 DSGVO) erteilt, noch wird die Nachvollziehbarkeit der gesamten Datenverarbeitung gewährleistet, womit es auch an der Voraussetzung für eine effektive Nachprüfbarkeit von deren Rechtmäßigkeit (ErwGr. 63 DSGVO) mangelt.

Um die von den Plattformkunden gewünschten Services anzubieten, können Plattformbetreiber in der Regel nicht auf die Verarbeitung personenbezogener Daten verzichten, weshalb auch die Anwendung des in der Privacy-Forschung besonders intensiv betrachteten Konzepts der Anonymisierung (z.T. auch als Schutzziel der „Unverkettbarkeit[4] bezeichnet) weitgehend impraktikabel ist. Aus diesem Grund hat das vom *Bundesministerium für Bildung und Forschung* (*BMBF*) geförderte Forschungsprojekt

1 Für eine ausführliche Darstellung von Charakteristika, Funktionen und Herausforderungen digitaler Plattformen s. *Engert*, AcP 2018, 304 (304 ff.).

2 In diesem Beitrag wird aus Gründen der Vereinfachung und besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich eingeschlossen.

3 S. exemplarisch zu Facebook *Lang*, Facebook hat keine Kontrolle über seine Daten, Netzpolitik v. 30. Apr. 2022.

4 *Zibuschka u. a.,* in: Roßnagel u. a. (Hrsg.), Open Identity Summit, 2019, 71-82.

PERISCOPE[5] das Ziel, „privatsphärenfreundliche Geschäftsmodelle für die Plattformökonomie“ insbesondere durch die Stärkung von Transparenz und Intervenierbarkeit zu ermöglichen. Dabei wird dieses Problemfeld u. a. durch die Implementierung eines Transaktionsjournals adressiert, das über die Transparenzanforderungen aus der DSGVO hinausgehend eine tatsächliche Informiertheit der betroffenen Personen herstellen und damit die Nachvollziehbarkeit aller relevanten Datenverarbeitungstätigkeiten fördern soll. Durch Anreicherung der dargestellten Verarbeitungsvorgänge mit weiteren Informationen wie Zweck und Rechtsgrundlage der jeweiligen Datenverarbeitung sowie auch der den betroffenen Personen jeweils zustehenden Interventionsmöglichkeiten, wird zugleich auch eine Förderung des Schutzziels der Intervenierbarkeit verfolgt.

In diesem Beitrag stellen wir erste Ergebnisse von Studien zur Motivation für und zu Multi-Stakeholder-Anforderungen an den Einsatz eines solchen Transaktionsjournals vor. Dabei ist der Beitrag folgendermaßen strukturiert: In den Abschnitten 2 und 3 werden wichtige Praxisprobleme bei der Umsetzung der DSGVO – vor allem, aber nicht ausschließlich – in der Plattformökonomie diskutiert. Der Fokus liegt dabei auf Transparenz und Intervenierbarkeit für die betroffene Person und einem potenziell die Wettbewerbsfähigkeit bedrohenden Ressourcenaufwand für kleinere Unternehmen. In Abschnitt 4 gehen wir darauf ein, wie diese Herausforderungen mit Hilfe eines Personal Rights Management (PRM)-Systems, das eine automatische Protokollierung von Verarbeitungstätigkeiten umfasst, angegangen werden können. Die dazu erhobenen Multi-Stakeholder-Anforderungen werden auszugsweise in Abschnitt 5 vorgestellt. Der Beitrag schließt mit einem Fazit und Ausblick.

2. *Praxisproblem I: Transparenz und Intervenierbarkeit für die betroffene Person*

Gemäß dem „grundrechtlich determinierten“[6] Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a Alt. 3 DSGVO ist die Verarbeitung personenbezogener Daten in einer für die betroffenen Person nachvollziehbaren Weise vorzu-

5 Förderkennzeichen: 16KIS1479K; für mehr Informationen s. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope.

6 *Greve*, in: Sydow/Marsch (Hrsg.), DSGVO | BDSG, 3. Aufl. 2022, Art. 12 DSGVO Rn. 5.

nehmen. Die Aufnahme des Transparenzgrundsatzes an dieser prominenten Stelle der Verordnung spiegelt damit die Bedeutung, die Transparenz im Allgemeinem zugeschrieben wird. So wird sie etwa als Grundvoraussetzung für das Recht auf informationelle Selbstbestimmung[7] oder sogar als „konstitutiv für das gesamte Datenschutzrecht"[8] angesehen. Wie auch die anderen in Art. 5 DSGVO enthaltenen Grundsätze der Datenverarbeitung entfaltet das Transparenzgebot Wirkung für alle nachfolgenden Vorschriften der DSGVO und ist bei deren Anwendung zu beachten – anderenfalls ist die entsprechende Datenverarbeitung rechtswidrig.[9] Insofern handelt es sich zwar um eine unmittelbar geltende Pflicht für den Datenverarbeiter,[10] zugleich wird allerdings die Konkretisierungsbedürftigkeit des Transparenzgrundsatzes wegen seines hohen Abstraktionsgrades und insofern sein Charakter als „Optimierungsvorgabe"[11] hervorgehoben, der dadurch bedingt ist, dass die Grundsätze mittels Zielvorgaben die Beschreibung eines Idealzustands vornehmen, für dessen Erreichung es keine klar definierten Grenzen gibt.[12]

Gleichwohl findet sich eine Konkretisierungsleistung dieser abstrakten Vorgabe sowohl in den Erwägungsgründen, als auch in zahlreichen weiteren Vorschriften der DSGVO.[13] In erster Linie können hier die allgemeinen Transparenzanforderungen aus Art. 12 DSGVO sowie ErwGr. 39 DSGVO genannt werden, die weiteren Aufschluss darüber geben, was eine transparente Datenverarbeitung gegenüber der betroffenen Person voraussetzt. So findet sich in Art. 12 Abs. 1 DSGVO etwa das Erfordernis, geeignete Maßnahmen zu treffen, um die der betroffenen Person bereitzustellenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. In Anbetracht der Menge und des Umfangs der beispielsweise gem. Art. 13 und 14

7 *Husemann/Pittroff,* in: Roßnagel u. a. (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, 337 (340).

8 *Tribess*, ZD 2020, 440 (441) m. w. N.

9 *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO Rn. 1; eindeutig auch der *EuGH*, Urt. v. 16.01.2019 – C-496/17, EU:C:2019:26, Rn. 57.

10 *Reimer*, in: Sydow/Marsch (Hrsg.), DSGVO | BDSG, 3. Aufl. 2022, Art. 5 DSGVO Rn. 1; *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO, Rn. 1.

11 *Roßnagel/Hornung*, MMR 2018, 197 (198).

12 *Roßnagel/Hornung*, MMR 2018, 197 (198); *Roßnagel*, ZD 2018, 339 (342).

13 S. etwa *Roßnagel*, ZD 2018, 339 (340), demzufolge der Grundsatz „seinen Ausdruck in den Rechten der betroffenen Person auf Information und Auskunft und in den korrespondierenden Pflichten des Verantwortlichen" findet.

DSGVO bereitzustellenden Informationen zeigt sich schon am Kriterium der Präzision die sich für den Verantwortlichen ergebende Schwierigkeit, den rechtlichen Anforderungen gerecht zu werden. So sollen die Informationen zwar möglichst knappgehalten, „auf eine einfache Formel gebracht und griffig formuliert“[14] sein, gleichzeitig darf dieses Bestreben nicht zu Lasten der inhaltlichen Richtigkeit und Vollständigkeit der Informationen gehen.[15]

Empirische Studien deuten allerdings darauf hin, dass die geltenden Transparenzanforderungen aus der DSGVO und die derzeitigen Versuche der Verantwortlichen, diesen Anforderungen gerecht zu werden, nicht darin resultieren, dass in der Praxis eine tatsächliche Informiertheit der betroffenen Personen geschaffen wird. So gaben etwa bei einer Umfrage der *Europäischen Kommission* im Jahr 2015 lediglich 20% der Studienteilnehmer an, immer über die Bedingungen der Datenerhebung und die weiteren Verwendungsmöglichkeiten informiert zu werden, wenn sie online darum gebeten werden, persönliche Informationen bereitzustellen.[16] Vier Jahre später und damit bereits nach Inkrafttreten nach der DSGVO hat sich diese Situation nicht verbessert – 2019 gaben lediglich 22 % der Befragten an, immer informiert zu werden.[17] Die Bereitschaft zum vollständigen Lesen von Datenschutzerklärungen (DSE) nahm von 2015 bis 2019 sogar ab. Während 2015 noch 18 % der Befragten angaben, DSE vollständig zu lesen, waren es 2019 nur noch 13 %.[18] Weitere Studien geben Hinweise auf mögliche Gründe dafür: So gaben in einer Studie von *Bitkom Research* im Jahr 2015 90 % der Befragten an, dass sie DSE in der Regel unverständlich finden und 86 % gaben an, dass die Erklärungen schlicht zu lang sind.[19] Diese Ergebnisse decken sich mit denen aus den Umfragen der *Europäischen Kommission*. So gaben im Jahr 2015 67 % der Befragten an, dass sie DSE zu lang finden und 38 % hoben die Unverständlichkeit als Hinderungsgrund hervor,[20] 2019 waren es 66% respektive 31 %.[21] Diese Ergebnisse sind nicht weiter

14 *Artikel-29-Gruppe*, WP 260 rev.01, Rn. 8.
15 *Paal/Hennemann*, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 3. Aufl. 2021, Art. 12 DSGVO Rn. 28.
16 *European Commission*, Special Eurobarometer 431, 2015, S. 81.
17 *European Commission*, Special Eurobarometer 487a, 2019, S. 15.
18 *European Commission*, Special Eurobarometer 431, 2015, S. 84; *European Commission*, Special Eurobarometer 487a, 2019, S. 16.
19 *Bitkom*, Datenschutz in der digitalen Welt, 2015, S. 11.
20 *European Commission*, Special Eurobarometer 431, 2015, S. 87.
21 *European Commission*, Special Eurobarometer 487a, 2019, S. 17.

verwunderlich, wenn man berücksichtigt, dass die DSE der 50 umsatzstärksten Internethändler in Deutschland im Mittel aus 444,5 Sätzen mit jeweils 17,85 Wörtern bestehen,[22] die Lektüre jeder einzelnen DSE daher im Durchschnitt rund 44 Minuten benötigen würde[23] und die Erklärungen zuletzt nach vier gängigen Lesbarkeitsindizes als schwer verständlich zu bewerten sind.[24] Doch selbst dieser Umfang scheint nicht zwangsläufig zur Vollständigkeit der dargestellten Informationen beizutragen. *Freye* hat Form, Sprache und Inhalte der DSE von Gesundheits-Apps analysiert und auf Rechtskonformität im Einklang mit den Transparenzleitlinien der *Artikel-29-Datenschutzgruppe* (*Art.-29-Gruppe*),[25] die vom *Europäischen Datenschutzausschuss* (*EDSA*) ausdrücklich angenommen wurden,[26] überprüft.[27] Dabei ist sie zu dem Ergebnis gekommen, dass keine der zehn untersuchten DSE vollumfänglich überzeugt. Beispielsweise bestehen erhebliche Kritikpunkte hinsichtlich der korrekten Angabe der Rechtsgrundlage der Datenverarbeitung und der korrekten Information über die Betroffenenrechte.[28]

Im Unterschied zur Transparenz hat der Begriff der Intervenierbarkeit keinen expliziten Einzug in die DSGVO erhalten, insbesondere nicht als Datenschutzgrundsatz gem. Art. 5 DSGVO.[29] Dennoch ergibt sich auch dieses Schutz- bzw. Gewährleistungsziel[30] aus den Vorschriften der DSGVO[31] und wird dort in zahlreichen Normen konkretisiert – in erster Linie in den Betroffenenrechten in Art. 15-22 DSGVO.[32] Gleichwohl umfasst das Schutzziel der Intervenierbarkeit nicht lediglich die individuelle Fähigkeit zur Geltendmachung von Betroffenenrechten, sondern deckt

22 S. dazu die Studie von *Gerpott/Mikolas*, MMR 2021, 936 (938).
23 *Gerpott/Mikolas*, MMR 2021, 936 (938).
24 *Gerpott/Mikolas*, MMR 2021, 936 (940).
25 *Artikel-29-Gruppe*, WP 260 rev.01.
26 *EDSA*, Endorsement 01/2018.
27 *Freye*, DuD 2022, 762.
28 *Freye*, DuD 2022, 762 (765 f.).
29 Dies als Versäumnis bezeichnend *Roßnagel*, ZD 2018, 339 (341).
30 Die sechs Schutzziele der Transparenz, Intervenierbarkeit, Nichtverkettbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit dienen der systematische Konkretisierung der abstrakten datenschutzrechtlichen Anforderungen in technische und organisatorische Maßnahmen. S. dazu u. a. *Rost/Pfitzmann*, DuD 2009, 353; *Bock/Meissner*, DuD 2012, 425; ebenso – allerdings unter Rückgriff auf den Begriff der Gewährleistungsziele und erweiternd um das Ziel der Datenminimierung – *DSK*, Standard-Datenschutzmodell, Version 2.0b, 2020, S. 9 f.
31 So auch *Roßnagel*, in: Roßnagel (Hrsg.), HDSIG, 2021, Einleitung, Rn. 65.
32 S. dazu die Ausführungen der *DSK*, Standard-Datenschutzmodell, Version 2.0b, 2020, S. 28.

auch weitere Perspektiven ab.[33] Hier sind u. a. die Möglichkeit der Aufsichtsbehörden zur Kontrolle der Rechtmäßigkeit der Datenverarbeitung durch die Verantwortlichen,[34] die Möglichkeit der Verantwortlichen zur Einwirkung auf bestehende Systeme, etwa indem die Option zur Deaktivierung einzelner Funktionalitäten ohne negative Auswirkungen auf die Funktionalität des Gesamtsystems gegeben ist,[35] sowie auch die Fähigkeit der Verantwortlichen einer Datenverarbeitung, auf ihre Weisungen hin agierende Auftragsdatenverarbeiter kontrollieren zu können,[36] zu nennen. Für diesen Beitrag und auch für die Aktivitäten im PERISCOPE-Forschungsprojekt liegt der Fokus jedoch auf der Fähigkeit der betroffenen Personen zur Wahrnehmung der ihnen gem. DSGVO zustehenden Interventionsmöglichkeiten – in erster Linie die Betroffenenrechte aus den Art. 15-22 DSGVO sowie das Recht auf Widerruf der Einwilligung gem. Art. 7 Abs. 3 DSGVO.

Diese Fähigkeit zur Intervention ist eng verknüpft mit der Funktion der Transparenzanforderungen aus der DSGVO. Denn erst durch die Einhaltung der Transparenzanforderungen wird die betroffene Person in die Lage versetzt, die Verarbeitung der sie betreffenden personenbezogenen Daten nachzuvollziehen, den Verantwortlichen dadurch gegebenenfalls zur Rechenschaft ziehen zu können sowie informiert in bestimmte Datenverarbeitungen einzuwilligen oder aber auch ihre Einwilligung zu widerrufen.[37] Diese enge Verbindung zeigt sich auch am Auskunftsrecht der betroffenen Person aus Art. 15 DSGVO, dessen unmittelbarer Zweck die Schaffung von Informiertheit ist: Die betroffene Person soll erkennen können, was mit den sie betreffenden personenbezogenen Daten geschieht und dadurch die Rechtmäßigkeit der Datenverarbeitung bewerten können.[38] Mittelbar hängt jedoch die Fähigkeit zur Wahrnehmung (nahezu) aller anderen Be-

33 S. a. *Rost*, Das Standard-Datenschutzmodell, 2022, S. 85, der Intervenierbarkeit einerseits als auf die Fähigkeit der Verantwortlichen, Änderungsbedarfen nachzukommen, abzielend versteht, andererseits auf die Fähigkeit der betroffenen Personen, ihre Rechte wahrzunehmen und durchzusetzen.

34 *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), HdB IT- und Datenschutzrecht, 3. Aufl. 2019, § 34 Rn. 557.

35 *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), HdB IT- und Datenschutzrecht, 3. Aufl. 2019, § 34 Rn. 557; *Scheja u. a.,* in: Leupold u. a. (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 6.6, Rn. 324.

36 So etwa die *ENISA*, Privacy and Data Protection by Design – from policy to engineering, 2014, S. 7.

37 Vgl. auch *Artikel-29-Gruppe*, WP 260 rev.01, Rn. 4.

38 *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1.

troffenenrechte vom Auskunftsrecht ab,[39] weshalb es regelmäßig als „das zentrale subjektive Datenschutzrecht"[40] eingeordnet wird. Ein weiteres Beispiel für die enge Verbindung von Transparenz und Intervenierbarkeit zeigt sich auch darin, dass den Betroffenen keine falsche Interventionsmöglichkeit suggeriert werden darf, indem beispielsweise eine Datenverarbeitung aus Absicherungsgründen sowohl auf die Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO als auch auf die Erforderlichkeit zur Vertragserfüllung gem. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gestützt wird. In diesem Fall würde der betroffenen Person ansonsten fälschlicherweise die Möglichkeit zur Intervention durch Ausübung des Widerrufsrechts aus Art. 7 Abs. 3 DSGVO suggeriert werden.[41]

Wenngleich empirisch weniger umfangreich belegt als die unverändert bestehenden Transparenzprobleme des Datenschutzrechts, so zeigt sich doch auch hinsichtlich der Fähigkeit zur Wahrnehmung von Betroffenenrechten ein Problem in der Praxis. So zeigen etwa *Kozyreva u. a.* in einer Studie, dass sich zwar 82% der Deutschen hinsichtlich ihrer Privatsphäre besorgt zeigen, zugleich jedoch nur 37% ihre Privatsphären- und Werbeeinstellungen auf Online-Plattformen ändern.[42] Diese Ergebnisse werden durch eine im Rahmen des PERISCOPE-Projekts durchgeführten quantitativen Online-Umfrage grundsätzlich bestätigt. Hierbei gaben 81% der Befragten an, im vergangenen Jahr über eine Veränderung ihre Privatsphäreeinstellungen nachgedacht zu haben, wobei als häufigster Grund dafür die „Angst/Sorge vor unbefugtem Zugriff auf persönliche Daten" genannt wurde. Insofern ist es auch nicht verwunderlich, dass Transparenz bei den Befragten grundsätzlich einen hohen bis sehr hohen Stellenwert einnimmt und sich dabei 71% der Befragten fragen, wer Zugriff auf ihre persönlichen Daten hatte und 60%, auf welcher Rechtsgrundlage ihre Daten verarbeitet werden. Im Missverhältnis dazu steht mit 64% allerdings der Anteil der Befragten, die tatsächlich aktiv ihre Privatsphäreeinstellungen verändert haben. Als wesentliche Hinderungsgründe wurden Angst vor Servicever-

39 *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, 3. Aufl. 2022, Art. 15 DGSVO Rn. 1 f.; *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1; *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, 3. Aufl. 2022, Art. 15 DSGVO Rn. 1.

40 *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1; ähnlich *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, 3. Aufl. 2022, Art. 15 DGSVO Rn. 1.

41 *Engeler*, ZD 2018, 55 (58).

42 *Kozyreva u. a.*, Artificial Intelligence in Online Environments, 2020, S. 12.

schlechterung (45 %), Komplexität bzw. Unwissenheit (32 %) und Zeitaufwand (30 %) genannt (jeweils % der Befragten, Mehrfachauswahl zulässig). Insbesondere für vulnerable Gruppen, etwa ältere Menschen sowie Bevölkerungsgruppen mit geringerer Bildung, fällt dabei eine mangelnde Fähigkeit zur Intervention auf: Viele Befragten dieser Gruppen haben ihre Privatsphäreeinstellungen noch nie geändert. Darüber hinaus gaben 49% der Befragten an, dass sie sich über ihre Betroffenenrechte aus der DSGVO bewusst sind, wobei sich lediglich 42 % der Befragten in der Lage sehen, diese auch in Anspruch zu nehmen.

Insgesamt weisen empirische Erkenntnisse daher darauf hin, dass die Betroffenen in der Praxis weder ausreichend informiert noch ausreichend dazu befähigt sind, die ihnen zustehenden Rechte wahrzunehmen und dadurch auf die Datenverarbeitung Einfluss zu nehmen.

3. Praxisproblem II: Ressourcenaufwand als Bedrohung für die Wettbewerbsfähigkeit kleinerer Unternehmen

Praxisprobleme des Datenschutzes bestehen nicht nur auf der Seite der betroffenen Personen, sondern auch auf Seiten der für die Datenverarbeitung Verantwortlichen. Schon seit dem Inkrafttreten der DSGVO wurden sie von Wirtschaft und Politik in erster Linie als Innovationshindernis gesehen.[43] Wenngleich diese „typische Datenschutz-Ausrede" nicht immer der tatsächlichen Sachlage entspricht,[44] weisen zumindest die Selbsteinschätzungen der Unternehmen auf einen wahren Kern dieser Aussage hin: So gaben beispielsweise 2019 in einer Umfrage von *Bitkom Research* rund 14 % der Befragten an, dass in ihren eigenen Unternehmen bereits innovative Projekte wegen der DSGVO gescheitert seien und 29 % der Befragten betonten darüber hinaus, dass durch die DSGVO Innovationen innerhalb der EU verhindert würden.[45] 2020 bejahten bereits 56 % der befragten Unternehmen das Scheitern neuer, innovativer Projekte aufgrund der DSGVO[46]

43 Anschaulich und leicht polemisch dazu *Pettinger*, Datenschutz als Spaßbremse? Weniger Fakt als Ausrede.

44 Exemplarisch statt vieler *Kelber*, Digitalisierung und Datenschutz - Schluss mit Ausreden!, Netzpolitik v. 04. Feb. 2023.

45 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 6-8.

46 *Bitkom*, DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, 2020, S. 5.

und 2022 berichteten gar 98 % der Studienteilnehmer „von mindestens einem gescheiterten Innovationsprojekt."[47]

Größerer Konsens herrscht hingegen bezüglich der Feststellung, dass es sich bei der DSGVO um ein „Bürokratiemonster"[48] handle. Dies ist in Anbetracht dessen, dass die DSGVO – je nach Zählweise – rund 46 Pflichten für die Verantwortlichen bereithält und die Verantwortlichen daher nachweisen können müssen, „welche mindestens 46 Maßnahmen [sie] zur Erfüllung dieser 46 Pflichten ergriffen [haben]",[49] wenig überraschend. So bestätigten 2019 rund 95 % der im Rahmen einer Studie befragten Unternehmen einen eher hohen bis sehr hohen personellen Aufwand und 94 % einen eher hohen bis sehr hohen finanziellen Aufwand, der mit der Umsetzung der DSGVO-Pflichten einhergehe.[50] Als wesentlichste Gründe werden dabei mit jeweils 97 % die Erfüllung von Informationspflichten sowie die Erfüllung von Dokumentationspflichten ausgemacht.[51] Diese hohen Umsetzungsaufwände werden auch von anderen Studienergebnissen gestützt. So gingen beispielsweise bei 36 % der im Rahmen einer Studie von *Capgemini Research* befragten deutschen Unternehmen im ersten Geltungsjahr der DSGVO über 1.000 Betroffenenanfragen ein[52] und der Anteil an Unternehmen, die zur Einhaltung der Datenschutzvorgaben mehr als 1.000.000 Euro in den Bereichen „legal fees", „consulting fees" und „technology upgrade costs" ausgegeben haben, stieg von 2019 auf 2020 deutlich an (Steigerungen von jeweils 8 %, 3 % und 8 %).[53]

Insbesondere kleine und mittelständische Unternehmen haben oft nicht die notwendigen Ressourcen und Expertise, um die regulatorischen Anforderungen korrekt und vollumfänglich umzusetzen.[54] Zusätzlich haben *Chen u. a.* gezeigt, dass die negativen Auswirkungen der DSGVO auf den Gewinn der Unternehmen, die in den Anwendungsbereich der Verordnung

47 *Bitkom*, Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, 2022, S. 8; s. dazu *Jakobs*, ZD-Aktuell 2022, 01404; vgl. auch *Karaboga u. a.,* in: Friedewald/Roßnagel (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 2022, S. 49 (50 f.).

48 Diese Frage aufwerfend etwa *Heidrich/Maekeler*, Bürokratiemonster EU-Datenschutz?, c't Magazin 19/2018, S. 162.

49 *Veil*, ZD 2018, 9 (9).

50 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 4.

51 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 5.

52 *Capgemini Research*, Championing Data Protection and Privacy, 2019, S. 15.

53 *Capgemini Research*, Championing Data Protection and Privacy, 2019, S. 12.

54 S. beispielhaft die Studie von *Freitas/Mira da Silva*, J Inform Systems Eng 3(4), Article No: 30.

fallen, abhängig von Unternehmensgröße und Branche zu sein scheinen. So fallen die negativen Auswirkungen auf den Gewinn bei kleinen Unternehmen aus dem IT-Sektor doppelt so stark aus, wie der durchschnittliche negative Effekt auf die Gesamtuntersuchungsmenge. Bei großen IT-Unternehmen konnten hingegen keine wesentlichen Auswirkungen festgestellt werden.[55]

Die Ergebnisse deuten darauf hin, dass zumindest das Potenzial für Markteintrittsbarrieren von KMUs bestehen. Dieser Befund ist aus zwei Gründen gerade in der Plattformökonomie nachteilig. Zum einen besteht aufgrund ihrer ökonomischen Charakteristika ohnehin bereits die Tendenz zur Monopolbildung, was sich – etwas verkürzt dargestellt – aus dem Zusammenspiel aus Netzwerkeffekten, Lock-In-Effekten infolge hoher Wechselkosten sowie auch den sog. „Datennetzwerkeffekten" ergibt.[56] Zum anderen wird gerade in der Plattformökonomie der Erfüllungsaufwand zur Gewährleistung eines (nicht nur datenschutz-)rechtskonformen Geschäftsbetriebs weiterhin zunehmen. Als Reaktion auf die zunehmende Bedeutung digitaler Plattformen für die Gesamtwirtschaft hat die *Europäische Kommission* in den vergangenen Jahren insbesondere die bedenkliche Marktmacht digitaler Plattformen, „vor allem die der mächtigsten […], denen andere Marktteilnehmer kaum noch ausweichen können"[57], herausgestellt und dabei betont, dass ein „bedarfsgerechtes Regulierungsumfeld für Plattformen und Mittler"[58] zu etablieren sei. In der Folge wurden u. a. mit der VO (EU) 2019/1150 (Platform-to-Business-Verordnung; P2B-VO) sowie der VO (EU) 2022/2065 (Digital Services Act; DSA) neue plattformspezifische Rechtsakte erlassen, die auch für kleine und mittlere Plattformbetreiber neue Transparenzverpflichtungen vorsehen - etwa Art. 5 P2B-VO in Bezug auf Rankingparameter, Art. 7 Abs. 3 lit. a und Art. 9 P2B-VO in Bezug auf

55 *Chen u. a.*, Privacy Regulation and Firm Performance, 2022, S. 24; s. a. *Goldberg u. a.*, Regulating Privacy Online: An Economic Evualuation of the GDPR, 2019, S. 4, die gezeigt haben, dass die DSGVO bei kleinen E-Commerce-Webseiten zu etwa doppelt so hohen Umsatzverlusten (-16,7 %) wie bei größeren Webseiten (-7,9 %) geführt hat.

56 S. etwa *Schweitzer u. a,* Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, S. 12 ff; *OECD,* An Introduction to Online Platforms and their Role in the Digital Transformation, 2019, S. 11; *Eisenmann*, Calif. Manag. Rev. 2008, 31 (36 f.).

57 COM (2015) 192 final, S. 10.

58 COM (2015) 192 final, S. 12.

Datenzugangsmöglichkeiten sowie Art. 14 und 15 DSA in Bezug auf die Moderation von Inhalten.[59]

Zusammenfassend sehen sich kleine und mittlere Plattformbetreiber mehreren Faktoren gegenüber, die ihre Wettbewerbsfähigkeit im europäischen Markt beeinträchtigen. Der insofern offenkundige Unterstützungsbedarf wurde auch durch eine im Rahmen des PERISCOPE-Projekts durchgeführten qualitativen Studie mit neun Plattformbetreibern identifiziert. Dabei gaben alle Interviewten an, dass insbesondere der Kosten- und Zeitaufwand eine sehr große wirtschaftliche Herausforderung bei der Umsetzung der DSGVO darstelle und bestätigten damit die oben aufgezeigten Ergebnisse. Ausschlaggebend dafür war die gerade bei kleinen Unternehmen oftmals fehlende Expertise, das Erfordernis zur Einbindung verschiedener Mitarbeiter aus nahezu allen Unternehmensbereichen, sowie die Unsicherheit sowohl bzgl. der Rechtskonformität der von ihnen etablierten Strukturen und Prozesse als auch bzgl. etwaiger Sanktionen bei mangelnder oder mangelhafter Umsetzung einzelner Pflichten aus der DSGVO.

4. Problembehandlung mittels Personal-Rights-Management-System

Bislang wurde zum einen aufgezeigt, welche Defizite für die betroffenen Personen derzeit in der Praxis sowohl bezüglich der Nachvollziehbarkeit der Datenverarbeitung als auch bei der Wahrnehmung der Möglichkeiten zur Intervention hinsichtlich der Verarbeitung sie betreffender personenbezogener Daten bestehen. Zum anderen wurde auf die unterschiedlichen Auswirkungen, die die zur Gewährleistung von DSGVO-Konformität notwendigen finanziellen und personellen Belastungen auf Unternehmen haben, hingewiesen. Insbesondere KMU-Plattformbetreiber wünschen sich deshalb ein technisches Werkzeug, das ihnen bei der Einhaltung der DSGVO-Pflichten hilft.

Das Forschungsvorhaben PERISCOPE widmet sich unter anderem der Entwicklung technischer Komponenten für ein PRM-System. Mit deren Hilfe sollen zum einen die tatsächliche Nachvollziehbarkeit der Datenverarbeitung und die Fähigkeit zur Wahrnehmung der Betroffenenrechte für die betroffenen Personen gefördert werden, sowie zum anderen KMU-Platt-

59 Die ebenfalls digitale Plattformen adressierende VO (EU) 2022/1925 (Digital Markets Act) kann an dieser Stelle vernachlässigt werden, da diese sich lediglich an die größten Betreiber digitaler Plattformen, sog. Gatekeeper, richtet.

formbetreiber bei der Umsetzung und Wahrnehmung einzelner Pflichten aus der DSGVO unterstützt werden. Dieses PRM-System besteht aus einer Reihe unterschiedlicher Komponenten, namentlich den Transaktionsjournalen, Komponenten zur Ausübung von Betroffenenrechten und zur Verwaltung von Einwilligungen sowie einem Datenverarbeitungsassistenten (s. Abb. 1). Im Zusammenspiel sollen diese Komponenten die genannten Schwerpunkte der Datenschutz-Schutzziele der Transparenz und Intervenierbarkeit für die betroffene Person bestmöglich fördern und zugleich die Ressourcenlast für Plattformbetreiber verringern.

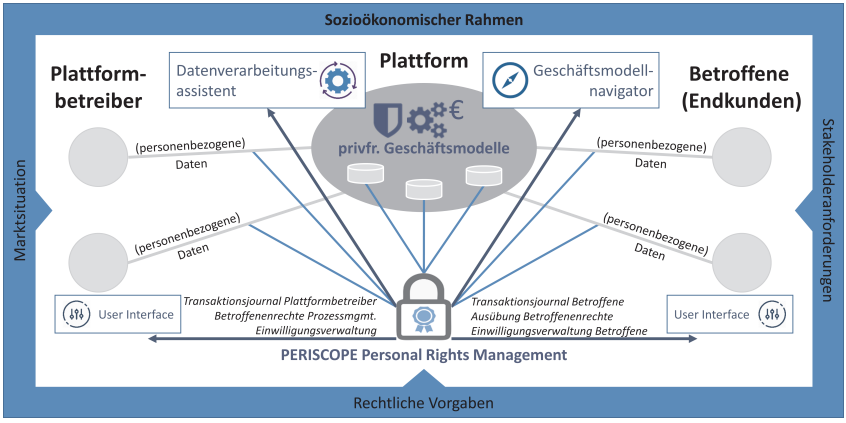

Abb. 1: Überblick über die Herangehensweise des PERISCOPE Projekts

Nachfolgend liegt der Schwerpunkt dieses Beitrags auf der Komponente des Transaktionsjournals, dessen Funktionalitäten sowie den Anforderungen, die sich aus multidisziplinärer Perspektive an ein solches ergeben.

4.1 Das PERISCOPE-Transaktionsjournal

Die oben skizzierten Unzulänglichkeiten in der heutigen Datenschutzpraxis sollen im Rahmen des PRM-Systems in erster Linie durch das sogenannte Transaktionsjournal adressiert werden.

Für die betroffene Person soll durch das Transaktionsjournal primär die Nachvollziehbarkeit der bei einem Plattformbetreiber stattfindenden Datenverarbeitung sichergestellt werden. Dies geschieht durch die Protokollierung von drei unterschiedlichen Aktivitäten. Erstens werden ausgewählte und als besonders privatsphäreninvasiv empfundene Datenverarbeitungs-

tätigkeiten protokolliert und der betroffenen Person angezeigt. Zweitens werden sämtliche Vorgänge rund um die Ausübung von Betroffenenrechten protokolliert, also beispielsweise von welchem Recht zu welchem Zeitpunkt Gebrauch gemacht wurde, wie viel Zeit dem Verantwortlichen noch zur fristgerechten Reaktion verbleibt sowie ob und mit welchem Ergebnis der Anfrage nachgekommen wurde. Drittens erfolgt eine „aktionsbasierte" Darstellung der „Veränderungen" bestimmter Rechtsgrundlagen, auf die der Verantwortliche seine Datenverarbeitungen stützt, also etwa das Entfallen einer Verarbeitung aufgrund berechtigter Interessen gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO infolge eines erfolgreichen Widerspruchs gem. Art. 21 Abs. 1 DSGVO oder auch das Hinzukommen einer neuen Datenverarbeitung auf Basis einer Einwilligung gem. Art. 6 UAbs. 1 lit. a DSGVO.

Zudem soll dem Transaktionsjournal in Verbindung mit anderen Komponenten des PRM-Systems für den Plattformbetreiber in erster Linie die Funktion zukommen, ihn bzgl. der Einhaltung ausgewählter Dokumentations- und Rechenschaftspflichten zu unterstützen. Dies erfolgt u. a. durch die Erfassung und Archivierung der Prozesse im Zusammenhang mit der Ausübung von Betroffenenrechten, das Vorhalten der nötigen Nachweise rund um die Einwilligung sowie die Protokollierung der Datenweitergabe an Empfänger, damit der Plattformbetreiber in der Lage ist, dem Auskunftsrecht so nachzukommen, wie es der *EuGH* jüngst konkretisiert hat.[60]

4.2 Automatische Protokollierung von Verarbeitungstätigkeiten

Nachfolgend wird der Fokus auf lediglich eine der soeben skizzierten Funktionalitäten gelegt, nämlich die automatische Protokollierung ausgewählter Datenverarbeitungstätigkeiten zum Zweck der Gewährleistung der Nachvollziehbarkeit der Datenverarbeitung für die betroffene Person.

Hierbei sollen nicht undifferenziert sämtliche Verarbeitungsvorgänge des Verantwortlichen protokolliert werden, sondern vielmehr lediglich solche, die durch ein besonders hohes Risiko charakterisiert sind. Die Identifizierung solcher Vorgänge sollte dabei sowohl durch den Rückgriff auf anerkannte Risikobemessungskriterien – etwa jene, die von der *Artikel-29-Datenschutzgruppe* im Rahmen der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO entwickelt wurden, um festzustellen, ob ein Verarbeitungs-

60 *EuGH*, Urt. v. 12.01.2023 – C-154/21, EU:C:2023:3, Rn. 46.

vorgang wahrscheinlich ein hohes Risiko mit sich bringt[61] – als auch durch eine Orientierung daran, welche Verarbeitungen die betroffenen Personen selbst als besonders risikoreich empfinden, erfolgen. Anderenfalls würde in Anbetracht der Vielzahl und Vielfalt der unterschiedlichen in Betracht kommenden Datenverarbeitungstätigkeiten lediglich eine Situation gefördert, die erneut zu einem Informationsüberschuss (Information Overload) auf Seiten der betroffenen Person führen könnte. Die so verbleibenden Verarbeitungsvorgänge werden protokolliert und für die betroffene Person angezeigt – jeweils ergänzt um weitere Informationen zur einschlägigen Rechtsgrundlage gem. Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO, zum mit dem Verarbeitungsvorgang verfolgten Zweck sowie der den Vorgang durchführenden Stelle. Zuletzt wird jeder dieser Verarbeitungsvorgänge angereichert um die der betroffenen Person im Einzelfall jeweils konkret zustehenden Interventionsmöglichkeiten, die sich aus Zweck und Rechtsgrundlage der Datenverarbeitung ergeben, um so eine möglichst niedrigschwellige Möglichkeit zur Wahrnehmung der Betroffenenrechte zu gewährleisten und damit die Fähigkeit der Betroffenen zur Intervention zu stärken.

5. Multi-Stakeholder Anforderungen an die automatisierte Protokollierung von Verarbeitungstätigkeiten

Aus einer solchen automatischen Protokollierung von Datenverarbeitungstätigkeiten ergeben sich eine ganze Reihe an Anforderungen aus multi- und interdisziplinärer Perspektive, im Konkreten aus Blickwinkel des (Datenschutz-)Rechts, der Sozio-Ökonomie sowie der technischen Machbarkeit und Funktionalität. Welche Herausforderungen und Anforderungen sich dabei jeweils stellen, wird nachfolgend erörtert.

5.1 Ausgewählte datenschutzrechtliche Anforderungen

Bei der automatisierten Protokollierung von Verarbeitungstätigkeiten handelt es sich nicht nur um eine Datenschutzmaßnahme, sondern zugleich auch selbst um eine Verarbeitungstätigkeit, die ein Sicherheitsrisiko darstellen kann.[62] Da zur vollständigen Überprüfbarkeit der Rechtmäßigkeit

61 *Artikel-29-Datenschutzgruppe*, WP 248 rev.01, S. 10 ff.

62 *Bedner*, Cloud Computing, 2013, S. 217; ähnlich *Rost*, Das Standard-Datenschutzmodell, 2022, S. 137 f.

einer erfolgten Verarbeitung auch die Instanz, die eine bestimmte Aktivität ausgelöst hat, zu protokollieren ist,[63] werden auch hier regelmäßig personenbezogene Daten verarbeitet, sodass darauf zu achten ist, die Protokollierungsaktivitäten selbst im Einklang mit den datenschutzrechtlichen Anforderungen aus der DSGVO auszugestalten.

Hier findet sich lediglich Platz für die Nennung einiger ausgewählter datenschutzrechtlicher Anforderungen, die sich zum Großteil aus den Datenschutzgrundsätzen in Art. 5 Abs. 1 lit. a-f DSGVO ergeben. So bedarf es auch bei der Protokollierung personenbezogener Daten einer entsprechenden Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO (enges Verständnis[64] des Rechtmäßigkeitsgrundsatzes aus Art. 5 Abs. 1 lit. a DSGVO), und die Datenverarbeitung muss den Transparenzanforderungen aus Art. 5 Abs. 1 lit. a i. V. m. Art. 12 ff. DSGVO genügen. Zur Einhaltung des Zweckbindungsgrundsatzes bedarf es bereits vor Beginn der Protokollierungstätigkeiten der Festlegung eines eindeutigen und legitimen Zwecks und es muss darauf geachtet werden, dass die jeweiligen Protokolldaten in aller Regel nur für die Zwecke, die Anlass für ihre Speicherung gewesen sind, ausgewertet werden,[65] beispielsweise dürfen für Datenschutzzwecke generierte Protokolldaten nicht zur Leistungsmessung verwendet werden.[66] In Bezug auf den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO ist darüber hinaus sicherzustellen, „dass die jeweiligen Daten hinsichtlich ihrer Verarbeitungszwecke angemessen und erheblich sowie auf das notwendige Maß beschränkt [sind]"[67], sodass insbesondere keine Inhaltsdaten im Transaktionsjournal dargestellt werden sollten. Zusätzlich müssen die verarbeiteten personenbezogenen Daten gem. Art. 5 Abs. 1 lit. d DSGVO sachlich richtig sowie erforderlichenfalls auf dem neuesten Stand sein. Bei Verarbeitung unrichtiger oder nicht aktueller personenbezogener Daten käme es dabei in der Regel nicht nur zu einem Verstoß gegen Art. 5 Abs. 1 lit. d DSGVO, sondern auch zu einem Verstoß gegen den Datenminimierungsgrundsatz, da unrichtige Daten insbesondere nicht erheblich für

63 So im Einklang mit *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 2 f.
64 So etwa bei *Pötters*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, 3. Aufl. 2022, Art. 5 DSGVO Rn. 7.
65 *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 2.
66 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (47).
67 *Spindler/Dalby*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 5 DSGVO Rn. 12.

die Erreichung eines bestimmten Zwecks sein können.[68] So ist insbesondere bei der hier angestrebten automatischen Generierung der Protokolldaten durch regelmäßige Überprüfung die Richtigkeit der generierten Daten zu überprüfen.[69] Der Speicherbegrenzungsgrundsatz gem. Art. 5 Abs. 1 lit. e DSGVO bringt darüber hinaus die Notwendigkeit mit sich, ein Löschkonzept für die Protokolldaten festzulegen, bei dem sich die Speicherdauer ebenfalls wieder anhand der Erforderlichkeit für die Zweckerreichung bemisst.[70] Und zuletzt bedarf es zur Einhaltung des Grundsatzes der Integrität und der Vertraulichkeit gem. Art. 5 Abs. 1 lit. f DSGVO der Sicherstellung, dass die Protokolldaten nicht nachträglich verändert werden können und zugleich nur Berechtigten zugänglich sind. Dies kann u. a. dadurch erreicht werden, dass bei der Generierung der Protokolldaten kryptographische Hashwerte verwendet werden,[71] dass die Protokolldaten verschlüsselt gespeichert und übermittelt werden[72] sowie durch die Festlegung im Rollen- und Berechtigungskonzept, wer zu welchen Zwecken auf die Protokolldaten zugreifen kann.[73]

5.2 Sozio-ökonomische Aspekte

Die sozio-ökonomischen Herausforderungen leiten sich anhand eines Multi-Methods-Designs ab, welches eine Untersuchung der Anforderungen seitens der Endanwender und seitens der Plattformbetreiber ermöglicht. Das Multi-Method-Design setzt sich aus einer quantitativen Studie mit Endanwendern (N = 589) als Online-Befragung inkl. Präferenzmessung, sowie qualitativen, halbstrukturierten Interviews (N = 9) mit kleinen und mittelständischen Plattformbetreibern verschiedener Branchen, zusammen. Die durchgeführte quantitative Studie ist repräsentativ für die deutsche Internetbevölkerung. Die Präferenzen der Endanwender wurden durch ein dis-

68 *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO Rn. 138.
69 *Ammon u. a.*, Protokollierung und Protokollierungskonzept, 2020, S. 6.
70 *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 3.
71 So auch *Ammon u. a.,* Protokollierung und Protokollierungskonzept, 2020, S. 24; *DSK*, Standard-Datenschutzmodell, S. 32; s. a. *BSI*, IT-Grundschutz-Kompendium, 2023, in dem unter "CON.1 Kryptokonzept" Maßnahmen zur Sicherung der Integrität und Vertraulichkeit von Datenbeständen und Kommunikationsverbindungen ausgewiesen sind.
72 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (46).
73 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (47).

kretes Entscheidungsexperiment (Choice-based Conjoint Experiment) erhoben und anschließend mittels eines hierarchisch bayesianischen Schätzverfahrens geschätzt. In der Online-Befragung der Studie wurden mittels Fragebogen ergänzende Informationen erhoben.

Im Hinblick auf die Ausgestaltung eines Transaktionsjournals zur Verbesserung der Transparenz und Intervenierbarkeit, haben Endanwender klare Präferenz bezüglich der Ausgestaltung ihrer Transparenzanforderungen. Die große Mehrheit der Endanwender bevorzugt einen digitalen Zugriff auf das Transaktionsjournal, einschließlich eines detaillierten Verzeichnisses der über sie gesammelten Daten und Datenkategorien. Dabei sollte das Transaktionsjournal aufzeigen, mit wem, zu welchem Zweck und in welchem Umfang Daten geteilt und verarbeitet werden. Grundsätzlich stehen die Befragten der Weitergabe von Daten für Marketingzwecke sehr restriktiv gegenüber und bevorzugen keine bzw. anonymisierte Datenweitergabe, zumindest insofern dies der Serviceverbesserung dient oder, z. B. in Form von Rabatten, incentiviert wird. Um für Endanwender Transparenz zu schaffen, sollte das Transaktionsjournal über Datenverarbeitungstätigkeiten und deren entsprechenden Rechtsgrundlagen informieren. Außerdem sollte in den Einträgen im Transaktionsjournal darauf hingewiesen werden, welche Betroffenenrechte den Endanwendern im Einzelfall zustehen, um so gegen eine Datenverarbeitung zu intervenieren oder beispielsweise weitere Informationen erhalten zu können. Weitere sozio-ökonomische Anforderungen aus Endanwender-Sicht umfassen, dass das Transaktionsjournal über robuste Sicherheitsmaßnahmen verfügt, benutzerfreundlich und leicht zugänglich ausgestaltet ist und laufend im Rahmen von Zertifizierungsmaßnahmen durch unabhängige Dritte geprüft wird.

Die durchgeführten qualitativen Interviews wurden anhand einer qualitativen Inhaltsanalyse nach *Mayring*[74] ausgewertet. Die Ergebnisse zeigen auf, dass für kleine und mittelständische Plattformbetreiber verschiedene Herausforderungen bezüglich der Umsetzung und Einhaltung der DSGVO bestehen, welche die in Abschnitt 3 aufgeführten Erkenntnisse bestätigen. Für alle neun interviewten Plattformbetreiber stellt die Umsetzung der DSGVO eine sehr große wirtschaftliche Herausforderung in Form eines Kosten- und Zeitaufwands dar. Infolgedessen resultiert diese Ressourcenbindung in einer fehlenden Kapazität für die Weiterentwicklung der Produkte und Services der Plattformbetreiber, was die Wettbewerbsfähigkeit

74 *Mayring,* in: Mey/Mruck (Hrsg.), Handbuch Qualitative Forschung in der Psychologie, 2020, 3 (17).

und erforderliche Time-to-Market verringert. Daher sehen die Plattformbetreiber ein Transaktionsjournal vor allem in Bezug auf die Dokumentationspflichten als „sehr hilfreich" und die damit verbundene Rechtssicherheit und Nachweisbarkeit als „essenziell". Hierbei gaben zwei Drittel der Interviewten an, einige Aspekte hinsichtlich der rechtssicheren Protokollierung bereits intern in einem dem Transaktionsjournal ähnlichen System umgesetzt zu haben, was dessen Bedeutung für die Plattformbetreiber weiter untermauert. Hieraus leitet sich die Anforderung eines modularen Aufbaus für das Transaktionsjournal bzw. die Komponenten des PRM-Systems ab, um eine ökonomisch vorteilhafte Integration in die vorliegenden Systeme der Plattformbetreiber zu ermöglichen. Denn bei sieben der neun interviewten Plattformbetreiber liegt eine hohe Bereitschaft zur Nutzung eines solchen modularen Angebots vor. Hinsichtlich der Funktionsweise steht für die Interviewten insbesondere der Protokollierungsmechanismus des Transaktionsjournals zur Ermöglichung einer erhöhten Rechtssicherheit im Fokus. Darüber hinaus ist eine Anwendbarkeit des Transaktionsjournals bzw. der anderen Komponenten für verschiedene, heterogene Kundengruppen, Geschäftsmodelle und Datenarten sowie eine schnelle Anbindung und Integration an Schnittstellen und vorliegende Systeme essenziell, um einen möglichen Wettbewerbsvorteil für Plattformbetreiber zu ermöglichen.

Zusammenfassend stellt die Transparenz-Dimension sowohl aus Plattformbetreiber-Sicht als auch aus Endanwender-Sicht einen wichtigen Aspekt dar. Während für die Plattformbetreiber die Protokollierungsfunktion des Transaktionsjournals aufgrund der Nachweisfähigkeit und der erhöhten Rechtssicherheit im Vordergrund steht, ist für Endanwender die Möglichkeit zur Intervention essenziell. Diese Erkenntnisse fließen in der weiteren Entwicklung des Transaktionsjournals ein.

5.3 Technisch-funktionale Anforderungen und Limitationen

Basierend auf den Ergebnissen der rechtlichen und sozio-ökonomischen Anforderungsanalyse lassen sich eine Reihe technischer Anforderungen für die automatisierte Protokollierung von Verarbeitungstätigkeiten im Rahmen eines Transaktionsjournals ableiten. Dazu gehört die Notwendigkeit für eine zweifache Umsetzung des Transaktionsjournals in der Referenzarchitektur: erstens als Komponente für Plattformbetreiber, die der Erfüllung einzelner Dokumentationspflichten der Plattformbetreiber dient, zweitens als eine separate Komponente zur Erhöhung der Transparenz für Betroffene. Dies berücksichtigt einerseits, dass eine Umsetzung von

beiden Stakeholdergruppen gewünscht wird und trägt andererseits den unterschiedlichen Zwecken, die mit den jeweiligen Komponenten verfolgt werden, durch eine technisch getrennte Umsetzung Rechnung.

Die automatisierte Protokollierung von Datenverarbeitungstätigkeiten durch ein Transaktionsjournal setzt zudem unvermeidlich eine Integration mit den Datenverarbeitungs- und Datenspeicherungssystemen des Plattformbetreibers voraus. Dabei liegt eine eventbasierende Architektur für den Datenaustausch mit der Steuerungskomponente des Transaktionsjournals ("Datenverarbeitungsassistent", s. Abb. 1) nahe. Dadurch wird eine unkomplizierte Anbindung an ein existierendes System möglich.

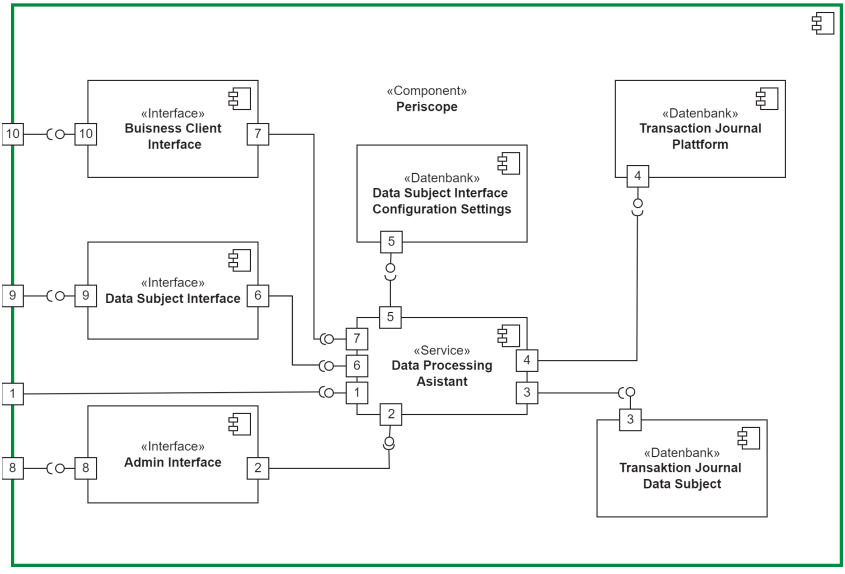

Abb. 2: Die PERISCOPE System-Architektur und -Schnittstellen

Das hat allerdings den Nachteil, dass die Aussagekraft des Transaktionsjournals vom Umfang der Integration in das System abhängt. Sollte bei der Integration beispielsweise die Entscheidung getroffen werden, bestimmte Verarbeitungsprozesse nicht zu protokollieren und an PERISCOPE weiterzuleiten, können diese an den Verbraucher nur über den Plattformbetreiber mitgeteilt werden. Dementsprechend ist der Grad der Transparenz, die das Transaktionsjournal ermöglicht, vom Plattformbetreiber abhängig.

Die Umsetzung des Transaktionsjournals als flexible und modulare Komponente benötigt mehrerer technischer Berücksichtigungen. Durch die Umsetzung des Transaktionsjournals als separate Komponente wird eine separate Datenbank benötigt. Diese kann zwar auf derselben physikalischen Datenbank laufen, sollte darüber hinaus allerdings logisch getrennt sein. Trotz der separaten Datenstruktur müssen die enthaltenen Daten des integrierenden Systems und des Transaktionsjournals gekoppelt sein, um die Verbindung der Daten auf dem Transaktionsjournal zu den Daten des Nutzers auf dem integrierenden System des Plattformbetreibers zu erhalten.

Außerdem muss das Transaktionsjournal durch ein sicheres Authentifizierungsverfahren geschützt sein, da personenbezogene Daten verarbeitet und gespeichert werden. Hierbei sollte kein separates Authentifizierungssystem erstellt werden, da dies zur Verwirrung bei Nutzern und reduzierter Usability führt. Stattdessen sollte für den Zugriff auf das Transaktionsjournal die Authentifizierung der integrierenden Plattform verwendet werden. Dadurch ist es dem Nutzer möglich, dieselben Zugangsdaten, die er beim Zugriff auf das integrierende System verwendet, auch bei der Einsicht seiner Daten im Transaktionsjournal verwenden. Diese Umsetzung wird daher im PERISCOPE Projekt verfolgt.

6. Fazit und Ausblick

Die Diskussion und Forschung um Möglichkeiten, die Nachvollziehbarkeit der Verarbeitung personenbezogener Daten für die betroffenen Personen zu fördern,[75] hat in den letzten Jahren ebenso stark zugenommen, wie die um Werkzeuge, die die Betroffenen bei der Ausübung ihrer Rechte sowie bei der Verwaltung ihrer Einwilligungen unterstützen sollen.[76] Das PERISCOPE PRM-System mit der Komponente des Transaktionsjournals reiht

75 Etwa durch mehrschichtige Informationsbereitstellung, s. dazu etwa *EDSA*, Leitlinien 05/2020, Rn. 69; durch kompakte Darstellung mittels „One-Pager", s. dazu u. a. *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 40; sowie auch durch den Rückgriff auf die Vorzüge visueller Methoden zur Informationsbereitstellung, s. dazu *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider u. a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324 (Rn. 17 ff.); *Nocun*, in: Roßnagel u. a. (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 39 (54 f.).

76 Besonders rege diskutiert unter dem Begriff des Personal Information Management Systems (PIMS), s. dazu etwa *Schweitzer/Peitz*, NJW 2018, 275 (278); *EDSB*, Stellungnahme 9/2016 des EDSB zu Systemen für das Personal Information Management (PIM); in jüngerer Zeit zudem vermehrt diskutiert vor dem Hintergrund von sowohl

sich hier ein, fokussiert dabei allerdings einen vermittelnden Ansatz, der einen Mehrwert sowohl für die Betroffenen als auch für die Verantwortlichen der Datenverarbeitung schaffen soll. Die grundlegende Idee dahinter ist, dass nur durch Berücksichtigung der Bedürfnisse aller Stakeholder eine Form von Datenschutz ermöglicht wird, die das Recht auf Schutz bei der Verarbeitung personenbezogener Daten mit dem ebenso legitimen Interesse an der wirtschaftlichen Nutzbarkeit von personenbezogenen Daten ausbalanciert.

Durch die in diesem Beitrag beschriebene automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal soll ein Aspekt dieses vermittelnden Ansatzes adressiert werden. Während für die Betroffenen leicht nachvollziehbar und chronologisch dargestellt wird, was mit denen sie betreffenden Daten geschieht und welche rechtlich zugestandenen Interventionsmöglichkeiten ihnen dabei jeweils zur Verfügung stehen, profitieren Plattformbetreiber von einem besseren Überblick der Datenverarbeitungstätigkeiten, die bei ihrem Geschäftsbetrieb anfallen und von der Förderung ihrer Fähigkeit zum Nachweis der Einhaltung datenschutzrechtlicher Anforderungen (die sich allerdings insbesondere aus dem Zusammenspiel mit den anderen Komponenten des PERISCOPE PRM-Systems, vor allem den anderen im Rahmen des Transaktionsjournals zu protokollierenden Aktivitäten, ergibt).

Besondere Schwierigkeiten, die sich bei der weiteren Entwicklung des Transaktionsjournals hinsichtlich der automatisierten Protokollierung von Datenverarbeitungstätigkeiten ergeben, liegen einerseits in der technischen Anbindung an die Systeme der Plattformbetreiber, andererseits in der angemessenen und an subjektiven Präferenzen orientierten Reduktion der den Betroffenen anzuzeigenden Vorgänge – was zur Vermeidung eines kognitiv nicht mehr verarbeitbaren Information Overloads unerlässlich ist. Hierfür wird im Rahmen des Forschungsprojekts eine Klassifizierung und Gruppierung unterschiedlicher Datenverarbeitungstätigkeiten entworfen, deren Praxistauglichkeit in der Folge durch eine quantitative Umfrage bei Endanwendern erprobt wird – mit einem Fokus auf der Frage, welche Verarbeitungstätigkeiten von Betroffenen als besonders privatsphäreninvasiv empfunden werden.

Art. 10 lit. b DGA, s. dazu u. a. *Ditfurth/Lienemann,* CRNI 2022, 270 (275), als auch § 26 TTDSG, s. dazu *Golland*, NJW 2021, 2238 (Rn. 19 ff.).

Literaturverzeichnis

Ammon, Danny; Backer-Heuveldop, Andrea u.a. (23.09.2020): Protokollierung und Protokollierungskonzept – Eine Einführung in die Thematik. URL: https://gesundheitsdatenschutz.org/download/protokollierungskonzept_2020.pdf (besucht am 24.02.2023).

Artikel-29-Datenschutzgruppe (2017): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt". 17/DE WP 248-rev.01. Brüssel. URL: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html (besucht am 24.02.2023).

Artikel-29-Datenschutzgruppe (2018): Leitlinien für Transparenz gemäß der Verordnung 2016/679. 17/DE WP260rev.01. Brüssel. URL: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html (besucht am 24.02.2023).

Auer-Reinsdorff, Astrid und Conrad, Isabell (Hrsg.) (2019): *Handbuch IT- und Datenschutzrecht*. 3. Aufl. München: C.H.Beck.

Bedner, Mark (2013): *Cloud Computing. Technik, Sicherheit und rechtliche Gestaltung*. Kassel: kassel university press.

Bitkom (22. Sep. 2015): Datenschutz in der digitalen Welt. Berlin. URL: https://www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf (besucht am 24.02.2023).

Bitkom (17. Sep. 2019): DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, Berlin. URL: https://www.bitkom.org/sites/main/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf (besucht am 24.02.2023).

Bitkom (29. Sep. 2020): DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, Berlin. URL: https://www.bitkom.org/Presse/Presseinformation/Jedes-2-Unternehmen-verzichtet-aus-Datenschutzgruenden-auf-Innovationen (besucht am 24.02.2023).

Bitkom (27. Sep. 2022): Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, Berlin. URL: https://www.bitkom.org/sites/main/files/2022-09/Bitkom-Charts %20Datenschutz %2027 %2009 %202022_final.pdf (besucht am 24.02.2023).

Bock, Kirsten und Meissner, Sebastian (2012): Datenschutz-Schutzziele im Recht. Zum normativen Gehalt der Datenschutz-Schutzziele. *Datenschutz und Datensicherheit (DuD),* S. 425-431.

BSI (2023): IT-Grundschutz-Kompendium. Bonn: Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1 (besucht am 24.02.2023).

Capgemini Research Institute (Hrsg.) (2019): Championing Data Protection and Privacy. A source of competitive advantage in the digital century. URL: https://www.capgemini.com/gb-en/insights/research-library/championing-data-protection-and-privacy/ (besucht am 24.02.2023).

Chen, Chinchih; Frey, Carl Benedikt und Presidente, Giorgio (2022): Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *The Oxford Martin Working Paper Series on Technological and Economic Change.* Working Paper No. 2022-1. URL: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf (besucht am 24.02.2023).

Ditfurth, Lukas v. und Lienemann, Gregor (2022): The Data Governance Act: - Promoting or Restricting Data Intermediaries? *Competition and Regulation in Network Industries (CRNI)*, 23(4), S. 270-295.

DSK (2020): Baustein 43 „Protokollieren". Version 1.0a. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf (besucht am 24.02.2023).

DSK (2020): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 2.0b. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf (besucht am 24.02.2023).

EDPB (25. Mai 2018): Endorsement 01/2018. Brüssel: European Data Protection Board. URL: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf (besucht am 24.02.2023).

EDSA (04. Mai 2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Version 1.1. Brüssel: Europäischer Datenschutzausschuss. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (besucht am 24.02.2023).

EDSB (20. Okt. 2016): Stellungnahme 9/2016. Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM). Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten. Brüssel: Europäischer Datenschutzbeauftragter. URL: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (besucht am 24.02.2023).

Eisenmann, Thomas R. (2008): Managing Proprietary and Shared Platforms. *California Management Review (Calif. Manag. Rev.)* 50(4), S. 31-53.

Engeler, Malte (2018): Das überschätzte Kopplungsverbot. Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen. *Zeitschrift für Datenschutz (ZD),* S. 55-62.

Engert, Andreas (2018): Digitale Plattformen. *Archiv für die civilistische Praxis (AcP),* S. 304-376.

ENISA (2014): Privacy and Data Protection by Design – from policy to engineering. Athen, Heraklion und Brüssel: Agentur der Europäischen Union für Cybersicherheit. URL: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (besucht am 24.02.2023).

European Commission (2015): Data Protection. Special Eurobarometer 431. URL: https://europa.eu/eurobarometer/surveys/detail/2075 (besucht am 24.02.2023).

European Commission (2019): The General Data Protection Regulation. Special Eurobarometer 487a, Summary. URL: https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf (besucht am 24.02.2023).

Freitas, Maria da Conceição und Mira da Silva, Miguel (2018): GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4), Article No. 30. https://doi.org/10.20897/jisem/3941.

Freye, Merle (2022): Die Datenschutzerklärungen von Gesundheits-Apps. *Datenschutz und Datensicherheit (DuD),* S. 762-766.

Gerpott, Torsten J. und Mikolas, Tobias (2021): Lesbarkeit von Datenschutzerklärungen großer Internethändler in Deutschland. Ergebnisse einer empirischen Studie. *Multimedia und Recht (MMR)*, S. 936-941.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz*, 3. Aufl. München: C.H.Beck.

Goldberg, Samuel; Johnson, Garrett und Shriver, Scott (2019): Regulating Privacy Online: An Economic Evaluation of the GDPR. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731 (besucht am 24.02.2023).

Golland, Alexander (2021): Das Telekommunikation-Telemedien-Datenschutzgesetz. Cookies und PIMS als Herausforderungen für Website-Betreiber. *Neue Juristische Wochenschrift (NJW)*, S. 2238-2243.

Heidrich, Joerg und Maekeler, Nicolas (2018): Bürokratiemonster EU-Datenschutz? 100 Tage DSGVO – eine erste Bilanz. *c't magazin für Computertechnik*, 19, S. 162.

Husemann, Charlotte und Pittroff, Fabian (2018): Smarte Regulierung in Informationskollektiven – Bausteine einer Informationsregulierung im Internet der Dinge. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden: Springer, S. 337-359.

Jakobs, Madia (2022): Neue Bitkom-Umfrage zur DS-GVO und internationalen Datentransfers in der deutschen Wirtschaft, *Newsdienst ZD-Aktuell*, 01404.

Karaboga, Murat; Martin, Nicholas und Friedewald, Michael (2022): Governance der EU-Datenschutzpolitik: Harmonisierung und Technikneutralität in und Innovationswirkung der DSGVO. In: Friedewald, Michael und Roßnagel, Alexander (Hrsg.): *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt,* Wiesbaden: Springer Vieweg, (DuD-Fachbeiträge), S. 49–90.

Kelber, Ulrich (04. Feb. 2023): Digitalisierung und Datenschutz: Schluss mit Ausreden! URL: https://netzpolitik.org/2023/digitalisierung-und-datenschutz-schluss-mit-ausreden/#netzpolitik-pw (besucht am 24.02.2023).

Kozyreva, Anastasia; Herzog, Stefan u.a. (Februar 2020): Artificial Intelligence in Online Environments. Representative Sturvey of Public Attitudes in Germany. Joint Study by the Max Planck Institute for Human Development and the University of Bristol, supported by the Volkswagen Foundation. URL: https://pure.mpg.de/rest/items/item_3188061_4/component/file_3195148/content (besucht am 24.02.2023).

Lang, Rahel (30. Apr. 2022): Internes Dokument: Facebook hat keine Kontrolle über seine Daten. URL: https://netzpolitik.org/2022/internes-dokument-facebook-hat-keine-kontrolle-ueber-seine-daten/ (besucht am 24.02.2023).

Leupold, Andreas; Wiebe, Andreas und Glossner, Silke (Hrsg.) (2021): *IT-Recht. Recht, Wirtschaft und Technik der digitalen Transformation,* 4. Aufl. München: C.H.Beck.

Mayring, Philipp (2020): Qualitative Inhaltsanalyse. In: Mey, Günter und Mruck, Katja (Hrsg.): *Handbuch Qualitative Forschung in der Psychologie*, Wiesbaden: Springer, S. 3-17.

Nocun, Katharina (2018): Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden: Springer, S. 39-58.

OECD (2019): An Introduction to Online Platforms and Their Role in the Digital Transformation, Paris: OECD Publishing. URL: https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm (besucht am 24.02.2023).

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz.* 3. Aufl. München: C.H. Beck.

Roßnagel, Alexander (2018): Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche Praxis. *Zeitschrift für Datenschutz (ZD),* S. 339-344.

Roßnagel, Alexander (Hrsg.) (2021): *Hessisches Datenschutz- und InformationsfreiheitsG. HDSIG. Handkommentar.* Baden-Baden: Nomos.

Roßnagel, Alexander und Hornung, Gerrit (2018): Die DS-GVO in den Startlöchern: Anfangszauber oder Reise ins Ungewisse? *Multimedia und Recht (MMR),* S. 197-198.

Rost, Martin (2017): Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten. In: Sowa, Aleksandra (Hrsg.): *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell. Neue Ansätze für die IT-Revision.* Wiesbaden: Springer, S. 23-56.

Rost, Martin (2022): *Das Standard-Datenschutzmodell (SDM). Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele.* Wiesbaden: Springer.

Rost, Martin und Pfitzmann, Andreas (2009): Datenschutz-Schutzziele – revisited. *Datenschutz und Datensicherheit (DuD),* S. 353-358.

Schweitzer, Heike; Haucap, Justus u.a. (29. Aug. 2018): Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen. Endbericht. Projekt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Projekt Nr. 66/17. URL: https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=12 (besucht am 24.02.2023).

Schweitzer, Heike und Peitz, Martin (2018): Ein neuer europäischer Ordnungsrahmen für Datenmärkte? *Neue Juristische Wochenschrift (NJW)*, S. 275-280.

Simitis, Spiros; Hornung, Gerrit und Spieker genannt Döhmann, Indra (Hrsg.) (2019): *Kommentar Datenschutzrecht (DSGVO mit BDSG).* Baden-Baden: Nomos.

Specht-Riemenschneider, Louisa und Bienemann, Linda (2020): Informationsübermittlung durch standardisierte Bildsymbole. In: Specht-Riemenschneider, Louisa; Werry, Nikola und Werry, Susanne (Hrsg.): *Datenrecht in der Digitalisierung.* Berlin: Erich Schmidt Verlag, S. 324-344.

Spindler, Gerald und Schuster, Fabian (Hrsg.) (2019): *Recht der elektronischen Medien – Kommentar*, 4. Aufl. München: C.H.Beck.

Stiftung Datenschutz (Hrsg.) (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Studie. Leipzig. URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Video/Fremdveranstaltungen/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf (besucht am 24.02.2023).

Sydow, Gernot und Marsch, Nikolaus (Hrsg.) (2022): *DS-GVO | BDSG, Handkommentar*, 3. Aufl. Baden-Baden: Nomos.

Tribess, Alexander (2020): Datenzugangsrechte in der Plattformökonomie. Auswirkungen der P2B-Verordnung im Bereich datenschutzrechtlicher Transparenzpflichten. *Zeitschrift für Datenschutz (ZD),* S. 440-444.

Veil, Winfried (2018): Accountability – wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, *Zeitschrift für Datenschutz (ZD),* S. 9-16.

Zibuschka, Jan; Kurowski, Sebastian u.a. (2019): Anonymization is Dead - Long Live Privacy. In: Roßnagel, Heiko; Wagner, Sven und Hühnlein, Detlef (Hrsg.): *Open Identity Summit 2019.* Lecture Notes in Informatics, Bd. 293. Bonn: Gesellschaft für Informatik (GI). S. 71-82.