ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Digital Business
& Innovation

fh st.pölten

Masterarbeit

Die Stärken und Schwächen der DSGVO im Vergleich zum DSA

von:
Isabella Haag
mmm211804

Studiengang: Digital Media Management

Begutachter/in:
FH-Prof. Ing. Dr. Harald Wimmer

Zweitbegutachter/in:
FH-Prof. Priv.-Doz. Dr. Michael Litschka

Wien, am 28. August 2023

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Masterarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Masterarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe. Diese Arbeit stimmt mit der vom Begutachter/von der Begutachterin beurteilten Arbeit

überein.

Wien, 28.08.2023 

Ort, Datum Unterschrift

Zusammenfassung:

In dieser Arbeit wird die Datenschutzgrundverordnung (DSGVO) analysiert, die Schwächen, Lücken und Kritikpunkte werden herausgearbeitet sowie analysiert, inwieweit der Digital Services Act den Schutz personenbezogener Daten erweitern kann und ob dabei von nachhaltigem Datenschutz gesprochen werden kann. Dabei wird in erster Linie im Forschungsstand festgestellt, dass es zwar Forschungsarbeiten zur DSGVO gibt und auch schon zum DSA, jedoch noch keine Arbeiten, welche die beiden EU-Rechtsakte in Bezug setzen und das Datenschutzniveau betrachten. Im ersten Theorieteil dieser Arbeit wird geklärt, was nachhaltiger Datenschutz bedeutet und die DSGVO und die Verantwortungsbereiche von Europäischer Union und Staat, von Unternehmen, Betroffenen und Konsument*innen betrachtet, um herauszufinden, in welchem Bereich die größte Verantwortung zum Schutz personenbezogener Daten, liegt. Dann wurde der Digital Services Act (DSA) und seine Neuerungen bezüglich digitaler Dienstleister vorgestellt und herausgearbeitet, inwiefern er den Schutz personenbezogener Daten erweitert und vorantreibt. Weiters werden beide mit ihren Vor- und Nachteilen verglichen und in Bezug zu nachhaltigem Datenschutz gesetzt. Dann wurde im Rahmen des Forschungsdesigns eine Inhaltsanalyse nach Mayring mit der Technik der induktiven Kategorie Bildung, basierend auf Expert*inneninterviews, durchgeführt. Aus diesen Ergebnissen wurden Hypothesen aufgestellt. Dabei kam heraus, dass die Stärken der DSGVO auch gleichzeitig deren Schwächen sind, nämlich allgemeine Formulierungen oder die Öffnungsklauseln. Außerdem wurde hier die Hypothese aufgestellt, dass es bezüglich nachhaltigen Datenschutzes kein einheitliches Verständnis in der Praxis gibt, jedoch die größte Verantwortung zum Schutz personenbezogener Daten den Unternehmen zugeordnet wird. Weiters wurde die Hypothese aufgestellt, dass EU-Rechtsakte wie der DSA das Schutzniveau personenbezogener Daten steigern, aber der EU-Markt durch dessen Restriktionen unattraktiver ist. Kernergebnis dieser Arbeit ist, dass der DSA den Schutz personenbezogener Daten sowohl direkt mit Artikel 26 und Artikel 28 (DSA), als auch indirekt als zweiten EU-Rechtsakt mit hohen Sanktionierungen erweitern wird. Herausforderungen in der Zukunft zum Schutz personenbezogener Daten werden in der Komplexität von Systemen und künstlicher Intelligenz erachtet. Die Grenzen dieser Arbeit liegen an dem Fakt, dass der DSA noch nicht unmittelbar anwendbar ist und deswegen die indirekte Wirkung auf den Schutz personenbezogener Daten schwer prognostizierbar ist. Deswegen sollte in diesem Bereich nach unmittelbarer Anwendung des DSA weiter geforscht werden.

Abstract:

This paper analyzes the General Data Protection Regulation (GDPR), identifies its weaknesses and shortcomings, reviews critique expressed by experts in the field, and analyzes the extent to which the Digital Services Act can enhance the protection of personal data and whether these practices are sustainable. After reviewing the state of research on this topic, it can be said that there is research on the GDPR and also regarding the DSA, yet there have been no publications aiming to relate the two EU acts and to look at the level of data protection. In the first theoretical part of this paper, the definition of sustainable data protection is clarified. In addition, there is a focus on the GDPR and the areas of responsibility of the European Union and the state, companies, and data subjects and consumers, in order to find out in which area the greatest responsibility for the protection of personal data lies. Then, the Digital Services Act (DSA) and its innovations regarding digital service providers are presented and it was worked out to what extent it expands and advances the protection of personal data. Furthermore, both are compared concerning their advantages and disadvantages and related to sustainable data protection. Then, as part of the research design, a content analysis according to Mayring was conducted using the technique of inductive category formation based on expert interviews. From these results, hypotheses were formulated. This revealed that the strengths of the GDPR are also its weaknesses, namely general formulations and the opening clauses. It was also hypothesized that there is no uniform understanding of sustainable data protection in practice, but that the greatest responsibility for protecting personal data lies with companies. Furthermore, it was hypothesized that EU legislation, such as the DSA, increases the level of protection of personal data, but that the EU market loses appeal due to its restrictions. The core result of this work is that the DSA will expand personal data protection both directly with Article 25 and Article 28 (DSA), and indirectly as a second EU legal act with high sanctions. Challenges in the future for the protection of personal data are considered regarding the complexity of systems and artificial intelligence. The limitations of this work lie in the fact that the DSA is not yet directly applicable and therefore the indirect effect on the protection of personal data is difficult to predict. Therefore, further research should be done in this area after immediate application of the DSA.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence / Künstliche Intelligenz
DMA	Digital Markets Act / Gesetz der digitalen Märkte
DSA	Digital Services Act / Gesetz der digitalen Dienste
DSFA	Datenschutz-Folgenabschätzung
DSG 1978	Datenschutzgesetz 1978
DSG 2000	Datenschutzgesetz 2000
DSGVO	Datenschutzgrundverordnung
DS-RL	Datenschutz Richtlinie
EC-RL	E-Commerce Richtlinie
EDSA	Europäischer Datenschutzausschuss
EMRK	Europäische Menschenrechts Konvention
Erwgrd	Erwägungsgrund
EuGH	Europäischer Gerichtshof
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
StGG	Staatsgrundgesetz
VLOP	Very large online platforms / sehr große Online-Plattformen
VLOSE	Very large online search engines / sehr große online Suchmaschine

1. Einleitung

In diesem Einleitungskapitel wird einerseits eine Übersicht zum Thema, also auch der DSGVO und dessen Lücken gegeben und eine kurze Einführung des Digital Services Acts. Angefangen mit der Problemdarstellung wird ein Überblick in die Problematik der Lücken und der Kritik an der DSGVO dargeboten und ein Einstieg in den DSA. Aus der Problemdarstellung heraus entsteht die Überleitung zur Forschungsfrage. Weiters werden die Zielsetzung und Methode dieser Arbeit geklärt und zum Schluss wird noch auf den Aufbau eingegangen.

1.2 Problemdarstellung

Im April 2016 wurde durch das Europäische Parlament und den EU-Rat die Datenschutz Grundverordnung verabschiedet. Sie gilt seit Mai 2018 als Grundlage des allgemeinen Datenschutzes in der EU. Die DSGVO dient zum Schutz personenbezogener Daten bei Verarbeitung dieser und zum freien Datenverkehr in der Europäischen Union.[1] Genauer gesagt wird geregelt, dass Unternehmen Verantwortung für die Verarbeitung von Daten übernehmen müssen. Es müssen Prozesse überprüft, Daten gelöscht, Vorgänge festgehalten und ab 250 Mitarbeiter*innen Datenbeauftragte eingestellt werden. Die DSGVO hat auf jeden Fall für eine notwendige Sensibilisierung des Datenumgangs in der EU gesorgt, doch lässt sie noch Lücken und stößt auf Kritik, wie zum Beispiel das Thema "Auskunft über Empfänger*innen", das besagt, dass Unternehmen über gespeicherte Daten Auskunft geben müssen. Hierbei ist nicht berücksichtigt, in welchem Ausmaß dies zu geschehen hat, da Empfänger*innen oder die Kategorie deren Zugehörigkeit ausreicht und keine Auflistung genauer Firmen notwendig ist (vgl. DSGVO, Art.15, 1c).

Doch nicht nur Verantwortung in einem Unternehmen wird durch die DSGVO gefordert, sondern auch jene von der Europäischen Union, der einzelnen Staaten, als auch der einzelnen Bürger*innen, auch Betroffene in der DSGVO genannt. Denn

[1] vgl. 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) (Text von Bedeutung für den EWR)., 119 OJ L § (2016). Fassung vom 27.04.2016, DSGVO, Art.1

die Annahme des informierten Verbrauchers, der selbst einwilligt, sorgt für enorme Kritik. Verbraucher*innen kreuzen freiwillig an, wem sie ihre Daten geben und wem nicht. Friedrichsen und Wersig hinterfragen hierbei die Verbraucherschutzperspektive, da die informationenpflichtigen Texte nicht gelesen, nicht verstanden werden oder es bei Nicht-Zustimmung zur Einschränkung der Nutzung kommt und trotzdem auf Eigenverantwortung gesetzt wird (vgl. Friedrichsen & Wersig, 2020, S. 149). Nicht nur die Eigenverantwortung von Betroffenen wird gefordert, sondern auch die Verantwortung der Mitgliedsstaaten, welche die Öffnungsklauseln der DSGVO auf nationaler Ebene regeln sollten und müssten. Denn die DSGVO sieht bei Öffnungsklauseln, wie zum Beispiel dem Einwilligungsalter, Ausschluss der Einwilligung bei sensiblen Daten und, ob alle oder nur gewisse Verantwortliche oder Auftragsverarbeitende, bewusst keine konkrete Antwort vor, und das bei über 60 Öffnungsklauseln (vgl. Fargo & Feiler, 2022, S. 7).

Lücken wie diese öffnen großen IT-Unternehmen weiterhin Tür und Tor, den europäischen Markt nach ihren Regeln zu bespielen. Nun wurde im April 2022 der Digital Services Act eingeführt, der digitale Dienstleitungen und digitale Märkte regeln soll. Genauer gesagt soll der DSA Plattformen und Intermediäre weiter regulieren, wie zum Beispiel mit speziellen Plattformregulierungen und Transparenzrechten und -pflichten (vgl. Klementschitz, 2019, S. 67). Hier geht es besonders um die Regulierung von sehr großen Dienstanbietern. Auch die Offenlegung von digitalem Profiling soll darin geregelt werden, also die Offenlegungspflicht von Empfehlungssystemen, sowie das Verbot von Werbung basierend auf personenbezogene Daten. Dabei soll die DSA die DSGVO nicht ersetzen, sondern ergänzen (vgl. Europäische Kommission, 2022, o.S.).

Ein weiteres Problem liegt darin, dass die Gesetzgebung mit dem Tempo des technologischen Wandels nicht mehr mithalten kann. Ein aktuelles Beispiel für dieses Problem ist die sprachbasierte Anwendung namens ChatGPT, die Texte versteht, Entscheidungen trifft und antworten kann. ChatGPT wurde kurzzeitig in Italien von der Datenschutzbehörde Garante gesperrt, da sich der Anbieter nicht an datenschutzrechtliche Verordnungen gehalten hat (vgl. Der Standard, 2022, o. S.). Nun stellt sich auch für Unternehmen die Frage, ob sie ChatGPT verwenden sollen, da die datenschutzrechtliche Beurteilung sehr komplex ist und auch die deutsche

Datenschutzkonferenz sich erst seit April 2023 mit der Einschätzung von ChatGPT beschäftigt.

Gerade bei diesen technologischen Veränderungen soll die Datenschutz-Folgenabschätzung grundsätzlich Abhilfe leisten, indem sie das Risiko bei neuen technischen Entwicklungen einschätzt. Das Prinzip der Technik-Folgenabschätzung dient der Bewertung des Einflusses von neuen Technologien auf Umwelt, Wirtschaft und Gesellschaft. Zu Beginn gab es den Gedanken, einen Schutz gegenüber Kerntechnologien zu gewährleisten und eine Folgenabschätzung bezüglich Automatisierung in der Arbeitswelt durchzuführen (vgl. Friedewald, 2017, S. 66). Seit den 2000ern steht der Datenschutz im Mittelpunkt der Technikfolgenabschätzung, kurz TA. Zudem ist durch die vermehrten Produkte und Dienstleistungen im Internet ein Machtgefälle entstanden, bei dem sich Anbieter*innen entscheiden können, zu welchen Bedingungen sie ihre Produkte und Dienstleistungen vertreiben. Dies bedeutet im Umkehrschluss, dass Nachfrager*innen häufig personenbezogene Daten übermitteln müssen, um einen Dienst nutzen zu können (vgl. Friedewald, 2017, S. 66).
Genau für solche Fälle fehlte eine standardisierte und unabhängige Technikfolgenabschätzung. Hier sollte die DSGVO mit der Datenschutz-Folgenabschätzung -kurz DSFA- Abhilfe leisten, da unter bestimmten Voraussetzungen Unternehmen dazu verpflichtet sind, eine DSFA durchzuführen oder sonst ein Bußgeld zahlen müssen. Ziel dabei ist es, Datenflüsse so umfassend wie möglich zu erfassen, diese so objektiv wie möglich zu bewerten, um Risikoquellen zu erkennen, Gegenmaßnahmen zu setzen und das Risiko gegenüber Rechten von Betroffenen zu minimieren (vgl. Friedewald, 2017, S.67). Friedewald kritisiert selbst, dass mit der DSFA, auch wenn sie durch die DSGVO durchgesetzt wird, noch Lücken offen bleiben, da es problematisch ist, dass Verantwortliche die Überprüfung selbst durchführen. Außerdem limitiert die DSGVO die DSFA auf Individuen, was bedeutet, dass Datenschutz bezüglich Gruppen und Organisationen ausgeschlossen wird. Dies führt zu einer Einschränkung der Bewertung der Technikfolgen bzw. lässt die DSGVO gewisse Rechte und Freiheiten aus, wie zum Beispiel das Recht auf Schutz des Privatlebens oder die Meinungsfreiheit (vgl. Friedewald, 2017, S. 70).

Zwar gilt die DSFA als eine Möglichkeit des Frühwarnsystems, doch stellt sich gleichzeitig die Frage, ob bei der Schnelligkeit der technologischen Veränderung die rechtlichen Grundlagen bzw. Vorschriften zum Schutz von personenbezogenen Daten noch nachkommen und ob der Digital Services Act Lücken der DSGVO schließen und weiteren Schutz gewährleisten wird.

Durch die Problemdarstellung ergeben sich folgende Fragestellungen: Was ist nachhaltiger Datenschutz und gibt es eine einheitliche Definition dafür? Wer trägt in der Praxis die Verantwortung für den Schutz personenbezogener Daten? Welche Lücken gibt es in der DSGVO und welche Folgen ziehen sie nach sich? Kann im Hinblick auf die DSGVO von nachhaltigem Datenschutz gesprochen werden? In welchen Aspekten erweitert der Digital Services Act das Schutzniveau zum Schutz personenbezogener Daten und kann er das überhaupt? Und in welchen Aspekten liegen in Zukunft die größten Herausforderungen zum Schutz personenbezogener Daten?
All diese Fragen lassen sich in folgendem Abschnitt zu einer Frage zusammenführen.

1.2 Ableitung der Forschungsfrage

Durch die ausführliche Problemdarstellung bezüglich der Lücken in der DSGVO und systematischer Probleme bei der Durchsetzung dieser erschließt sich folgende Forschungsfrage:

> Inwieweit ergänzt die DSA die DSGVO in Bezug auf den Schutz personenbezogener Daten aus Sicht der Konsument*innen und ist dieser ausreichend, um von nachhaltigem Datenschutz zu sprechen?

1.3 Zielsetzung und Methode der Arbeit

Diese Arbeit versucht die Lücken der DSGVO herauszuarbeiten und prüft, inwieweit der DSA den Schutz personenbezogener Daten ergänzen kann. Außerdem ist es ein Unterziel dieser Arbeit, herauszufinden, ob die gesetzlichen Grundlagen einerseits ausreichen, um personenbezogene Daten auch bei der Geschwindigkeit der technologischen Veränderungen zu schützen und wer in der Praxis die größte Verantwortung für den Schutz personenbezogener Daten trägt. Deswegen gilt es herauszufinden, worin die Stärken und Schwächen in der DSGVO liegen und in welchen Aspekten der Digital Services Act weitere Abhilfe leisten wird, personenbezogene Daten zu schützen.

1.4 Aufbau der Arbeit

Diese Arbeit versucht im Rahmen des Forschungsstandes herauszufinden, in welchen Bereichen und Kontexten in den letzten fünf Jahren zum Datenschutz, zur Datenschutzgrundverordnung und zum Digital Services Act geforscht wurde, welche Aspekte kritisiert werden und wie viel Bürger*innen über Datenschutz wissen. Danach wird im Theoriekapitel 3 dieser Arbeit erforscht, wo die Anfänge des Datenschutzes in Österreich lagen, wer in der Praxis die Verantwortung für Datenschutz hat und ob dies derzeit mit nachhaltigem Datenschutz vereinbar ist. Dabei werden anhand der DSGVO die verschiedenen Standpunkte der Verantwortungen von Union und Staat, von Unternehmen und Betroffenen und von Konsumenten*innen beleuchtet und im Anschluss die Sanktionierungen besprochen. In Kapitel 4 widmet sich diese Arbeit dem Digital Services Act und beleuchtet, welche Neuerungen er bringt und wie sich diese auf den weiteren Schutz personenbezogener Daten auswirken. Am Ende des Theorieteils wird eruiert, welche Fragen in der DSGVO offen bleiben, wo der DSA weitere Maßnahmen zum Datenschutz setzt und welche Punkte beide ungeklärt lassen. In Kapitel 5 beginnt der methodische Teil dieser Arbeit, welcher sich mit der Methode und dem Forschungsdesign befasst. In diesem Kapitel werden auch die Vor- und Nachteile von empirischer Sozialforschung, von Expert*inneninterviews und Gütekriterien in der qualitativen Forschung näher beleuchtet. Im gleichen Kapitel wird weiters die qualitative Inhaltsanalyse nach Mayring mit all ihren Vor- und

Nachteilen, sowie eine Technik davon, nämlich die induktive Kategorienbildung nach Mayring diskutiert. In Kapitel 6 werden die Expert*inneninterviews anhand der induktiven Kategorienbildung ausgewertet und basierend auf den Ergebnissen Hypothesen gebildet. Dann wird die Forschungsfrage beantwortet und daraus werden Handlungsempfehlungen formuliert. Zum Schluss werden in einem Fazit die Erkenntnisse dieser Arbeit zusammengefasst, auch die Limitationen beleuchtet, und mit einem Forschungsausblick werden Empfehlungen für zukünftige Forschungsprojekte gegeben.

2. Forschungsstand

Der folgende Abschnitt schafft einen Überblick der Forschungsergebnisse von ausgewählten Arbeiten der letzten fünf Jahre. Der Zeitraum wurde aus dem Grund gewählt, da es vor der unmittelbaren Anwendung der DSGVO kaum Forschungsarbeiten gibt und noch weniger über den DSA. Im Folgenden werden Ergebnisse von juristischen Arbeiten, Vergleichsarbeiten von unterschiedlichen Datenschutzansätzen, als auch internationale Arbeiten zum Verständnis von Datenschutzbegriffen präsentiert. Zudem werden die Ergebnisse von Journals, welche sich mit dem DSA auseinandersetzten besprochen und rechtliche, mediale und wirtschaftliche Aspekte beleuchtet.

Zwei aus juristischer Perspektive geschriebene Literaturarbeiten gehen auf den Vergleich zwischen dem österreichischen Datenschutzgesetz, kurz DSG, und der DSGVO der EU ein. Die erste Literaturarbeit aus juristischer Perspektive ist jene von Klementschitz (2019), der sich mit dem Einfluss der DSGVO auf den internationalen Datenverkehr befasste. Der Autor hat in einer qualitativen Analyse Rechtsquellen zum Thema Datenschutz verglichen. Hauptfragestellungen dieser Arbeit waren, wie sich die Regelungen zum internationalen Datenverkehr ändern, die Judikatur sich verändert hat und die Auswirkungen und Problemdarstellungen für den internationalen Datenverkehr, die dadurch entstanden sind. Dabei arbeitete er Veränderungen durch die DSGVO im Vergleich zur vorherigen DS-RL und dem österreichischen Datenschutzgesetz heraus. Zum Beispiel geht er auf die begrifflichen Veränderungen zwischen dem DSG 2000 und der DSGVO ein. Außerdem befasst er sich mit dem Marktortprinzip, das die räumliche Anwendung auf Unternehmen erweitert, welche Waren und Dienstleistungen die Unternehmen in der EU anbieten können, ohne einen Sitz innerhalb der EU haben zu müssen. Klementschitz erwähnt ebenfalls, dass das österreichische DSG im Gegensatz zur DSGVO neben natürlichen Personen auch juristische Personen erfasst. Die Kontrollinstrumente des DSG wurden außerdem mit der DSGVO durch Selbstkontrolle von verantwortlichen Personen ersetzt. Die Einhaltung der rechtmäßigen Verarbeitung wird durch Art. 5 (DSGVO), die Rechenschaftspflicht ermöglicht. Weiters verpflichtet die DSGVO zur Risikoeinschätzung, zu einer Datenschutz-Folgeneinschätzung und es gilt, Datenschutzbeauftragte zu ernennen.

Zudem können durch die verstärkte Zusammenarbeit durch die DSGVO auf nationaler Ebene betroffene Unternehmen und natürliche Personen Beschwerde bei einer Aufsichtsbehörde im eigenen Land einlegen. Zum Erreichen eines einheitlichen Datenschutzrechts in der EU gibt es den Europäischen Datenschutzausschuss, welcher aus den Leitungen der nationalen Aufsichtsbehörden besteht und die verbindlichen Beschlüsse fassen kann. Der Autor erwähnt auf der einen Seite, dass es in der DSGVO beinahe 70 Öffnungsklauseln gibt, die absichtlich einen weiten Rahmen haben und die jeder Mitgliedsstaat teilweise individuell umsetzen kann. Auf der anderen Seite kritisiert er, dass Österreich zum Beispiel viele der Klauseln nicht genutzt hat und somit nicht unbedingt die Rechtssicherheit verbessert. Im Vergleich zum DSG hob Klementschitz Detailregelungen hervor, wie zum Beispiel, dass durch das DSG genehmigungspflichtiger Datenverkehr nun ausnahmslos genehmigungsfrei ist, der aber weniger die Grundprinzipien des internationalen Datenverkehrs beeinflusst. Zudem fallen die Ausnahmeregelungen des DSG für indirekte personenbezogene Daten durch die DSGVO weg. Unternehmen müssen auch zum internationalen Datenverkehr ausdrücklich Einwilligungen einholen sowie zu Risiken informieren. Die Regelung der Übermittlung an Drittländer, wenn zwingendes und berechtigtes Interesse von Verantwortlichen gegeben ist, hebt Klementschitz als völlig neue Regelung hervor, die durchaus unter Kritik steht. Außerdem kritisiert der Autor, dass in der DSGVO das Wort der Übermittlung nicht definiert ist. Als sehr ungewiss definiert der Autor das EU-US-Datenschutzschild, da die Umsetzung der US-Administration gravierende Defizite zeigt. Zum Schluss hebt der Autor noch die Sanktionierungen hervor, die vom DSG zur DSGVO verschärft wurden. Zusammenfassend bejaht der Autor den verbesserten Rechtsschutz, die schnellere Durchsetzung durch die DSGVO und die Vereinfachung des internationalen Datenverkehrs, da dieser genehmigungsfrei ist (vgl. Klementschitz, 2019, S. 7-67). Diese Dissertation zeigt, gemäß der Verfasserin dieser Arbeit gut auf, welche positiven und negativen Veränderungen die DSGVO zum internationalen Datenverkehr geschaffen hat. Dennoch wurde kein methodischer Zugang oder eine konkrete Methode genannt.

In der zweiten aus juristischer Perspektive geschriebene Arbeit, beschäftigte sich Tagwercher (2019) in ihrer Diplomarbeit mit der Fragestellung des persönlichen Schutzbereichs des § 1 (DSG) unter Einwirkung der DSGVO und, ob tatsächlich nur natürliche Personen in den Schutzbereich fallen oder auch juristische Personen. Ausgangsposition ihrer Arbeit ist die Fragestellung, ob trotz unmittelbarer Anwendung der DSGVO juristische Personen durch das österreichische Datenschutzgesetz trotzdem ein Grundrecht auf Datenschutz haben. Zur Beantwortung ihrer Forschungsfrage analysiert die Autorin die bestehende und ältere Rechtsgrundlage und hebt Veränderungen bezüglich des grundrechtlichen Schutzes hervor. Außerdem erklärt die Autorin, wie das österreichische Datenschutzgesetz an die DSGVO angepasst wurde und, dass die DSGVO nicht unbedingt zu einer gänzlichen Vereinheitlichung des Datenschutzrechts im europäischen Raum geführt hat, da es 69 Öffnungsklauseln gibt, die dafür sorgen, dass nationale Gesetzgeber Freiheiten in der Ausgestaltung haben. Kernergebnisse dieser Arbeit waren, dass in unterschiedlichen Rechtsquellen der persönliche Anwendungsbereich oft unterschiedlich und unpräzise, dennoch definiert ist. Sie ist außerdem zu keinem konkreten Schluss gekommen, wer Grundrechtträger*in ist und wer nicht. Was den persönlichen Schutzbereich des § 1 DSG betrifft, ist die Autor*in zu folgendem Ergebnis gekommen: Da es jedem Mitgliedsstaat selbst überlassen ist, Regelungen zum persönlichen Schutzbereich von juristischen Personen zu finden, fällt nach § 1 (DSG) „jedermann“ in den persönlichen Schutzbereich, und somit auch juristische Personen (vgl. Tagwercher, 2019, S. 7-57). Diese Arbeit hat den Ursprung des Datenschutzes gemäß der Autorin sehr gut beleuchtet und konkret formuliert, woher welcher Aspekt des Datenschutzrechts kommt. Ein Kritikpunkt an dieser Arbeit ist, dass die Arbeit als reine Literaturarbeit mit 60 Seiten sehr kurz erscheint und dass die Autorin keine konkrete Methode für eine Analyse genannt hat.

Die Forschung von Haber und Tamò-Larrieux (2020) versucht hingegen, Regulierungsstrategien zum Schutz der Privatsphäre von Bürger*innen zu vergleichen. In ihrem Fall vergleichen sie die Versuche der EU mit der DSGVO mit jenen Versuchen der israelischen Gesetzgebung. Dabei legen sie den Fokus auf die Implementierung von Privacy by Design und Privacy by Security in die

Gesetzgebung. Weiters untersuchen die Autor*innen die Vor- und Nachteile der jeweiligen Gesetzgebung und was diese für Ingenieur*innen als auch für den Schutz der Privatsphäre bedeutet. Der Ausdruck Privacy by Design bedeutet, dass sowohl in Hard- als auch in Software von Anfang an Datenschutzmaßnahmen berücksichtigt, entwickelt und eingebaut werden. Zum einen haben sie herausgefunden, dass die EU mit der DSGVO sehr viel strengere Maßnahmen hat, indem Privacy by Design vorgeschrieben ist, jedoch kritisieren sie gleichzeitig, dass Ingenieur*innen technische Voraussetzungen bieten müssen, die allen Anforderungen der DSGVO genügen müssen, jedoch ohne einen Leitfaden anzubieten. Damit ist die Verpflichtung gegeben, sich an die technischen Voraussetzungen zu halten, aber nicht erklärt, wie. Das bedeutet: Ingenieur*innen haben keine konkreten Anweisungen, was genau neue Geräte datenschutzrechtlich schon in der Entwicklung implementiert haben müssen. Für Ingenieur*innen ist demnach der israelische Ansatz angenehmer, weil sie konkretere Anweisungen bekommen, unter denen sie eine Datenbank implementieren und eine Risikobewertung machen müssen. Bei der Datensicherheit ist die DSGVO jedoch genauer und gibt Verantwortlichen Angaben, wo die Prioritäten liegen. Zwar sind in der DSGVO auch organisatorische Maßnahmen wie Datenschutz-Folgenabschätzung und Datenschutzbeauftragte geregelt, jedoch geht der israelische Ansatz viel mehr ins Detail und regelt genau, welche Maßnahmen bei welcher Art der Datenbank zu setzen sind, was das Bewusstsein und das Schutzlevel für Organisationen erhöht. Haber und Tamò-Larrieux empfehlen deshalb in ihrer Analyse, rechtlich eine Mischung aus starren Normen, wie einer Bauanleitung, für datenschutzgerechte sichere Systeme und flexiblen Normen, die es ermöglichen, passende Maßnahmen für bestimmte Produkte und Dienstleistungen zu finden(vgl. Haber& Tamò-Larrieux, 2020, S. 1-10), anzubieten. Nach der Autorin hätte die Analyse auch durch Expert*inneninterviews mit Entwickler*innen genauer darauf eingehen können, was sie sich zur Umsetzung von Privacy by Design und Privacy by Security von der Gesetzgebung wünschen würden. Grundsätzlich ist gründlich recherchierte Arbeit, die verschiedene Privacy- und Security by Design-Ansätze vergleicht und versucht herauszufiltern, welche Mischung am besten wäre.

Pleger, Guirguis und Mertes (2021) haben in ihrer empirischen Studie die Wahrnehmung von Datenschutz und Datensicherheit von deutschen Bürger*innen mit der Wahrnehmung von Bürger*innen aus dem Vereinigten Königreich verglichen. Dabei hatten sie den Fokus auf E-Regierungsdienste, also Digitalisierungsdienste im öffentlichen Sektor, gelegt. Leitfragen waren dabei, warum Bürger*innen reserviert gegenüber E-Government Diensten sind und wie sehr Wissen über Datenschutz und Datensicherheit damit in Zusammenhang stehen. Weitere Leitfragen waren, was genau Bürger*innen unter Datensicherheit und Datenschutz verstehen, und inwieweit die individuellen Definitionen der beiden Begriffe mit den rechtlichen und technischen Definitionen übereinstimmen. Zuletzt war eine Leitfrage, wie vertraut Bürger*innen mit den Begriffen sind, die in Medien im Zusammenhang mit Datenschutz und Datensicherheit verwendet werden. Die Autor*innen erhoben die Daten anhand eines Methodenmixes, einerseits mittels einer Medienanalyse anhand von Artikeln und andererseits mit einer quantitativen Umfrage mittels Fragebogen. Durch die Umfrage kamen sie auf eine Stichprobe von 1000. Mit der Medienanalyse von deutschen und britischen Tageszeitungen kamen die Autor*innen auf eine Stichprobe von 128 Artikeln, welche die Worte Datensicherheit oder Datenschutz beinhalteten. Von den 128 Artikeln waren 71% aus britischen Zeitungen und 21% aus deutschen, was bedeutet, dass in England viel mehr über datenbezogene Themen berichtet wird, als Deutschland. Durch diese Medienanalyse kam heraus, dass die Begriffe Datenschutz und Datensicherheit oft und regelmäßig verwendet werden, aber die Artikel nicht die richtige Zielgruppe, also die Nutzer*innen, erreichen. Danach folgte die quantitative Umfrage. Diese fand mit der Stichprobe von 1000 heraus, dass Bürger*innen beider Länder die Begriffe Datenschutz und Datensicherheit als sehr wichtig empfinden. Trotzdem konnten von 1000 Teilnehmer*innen nur 13% den Unterschied der beiden Begriffe erklären. Gleichzeitig empfanden aber 82% in Deutschland und 83% im Vereinten Königreich, dass sie als Konsument*innen keine Kontrolle darüber hätten, wie persönliche Daten von Unternehmen gesammelt und verwendet werden. Ein Resultat dieser Studie ist somit, dass der Großteil der Deutschen und Briten wenig über Datenschutz und Datensicherheit weiß und Medien gleichzeitig auf eine zu technische oder zu rechtliche Weise aufklären, um von ihrer Zielgruppe verstanden zu werden (vgl. Pleger et al., 2021, S. 1-17). Diese Arbeit ist nach der Autorin nicht

direkt umlegbar auf Österreich, da keine österreichischen Proband*innen teilgenommen haben. Dennoch gibt sie Aufschluss über den durchschnittlichen Wissenstand über datenbezogene Themen und zeigt, dass ein Großteil der Betroffenen das Gefühl hat, die Kontrolle über seine Daten zu verlieren. Aufgrund dieser Ergebnisse kann weitere Forschung innerhalb der EU zum Verständnis von Datenschutzthemen betrieben werden.

Der Journalbeitrag von Cauffman und Goanta (2021) analysiert den Reformvorschlag des DSA bezüglich der Kohärenz mit dem Unionsrecht, die Verantwortung von Intermediären und die digitale Durchsetzung. Das Ganze versuchen sie anhand der Verbraucher*innenschutzperspektive zu analysieren. Zuerst analysieren die Autor*innen den Anwendungsbereich und klären wichtige Begriffe. Dann untersuchen sie die Veränderungen bezüglich Haftung von Vermittlungsdienstanbieter*innen, und im Anschluss gehen sie auf die Sorgfaltspflichten ein, die im Online Bereich für mehr Transparenz sorgen sollen. Dabei wird zwischen Vermittlerdienstanbieter*innen, großen und sehr großen Online-Plattformen unterschieden. Zum Schluss blicken die Autor*innen auf die nationale und supranationale Umsetzung sowie auf die Sanktionierungen und die Durchsetzung durch die Koordination digitaler Dienste.
Durch die Analyse finden sie heraus, dass der DSA nicht ganz mit früheren Verbraucherschutzvorschriften einhergeht, die eine Offenlegungspflicht bei Online-Verträgen zwischen Händler*innen und Verbraucher*innen vorsehen. Somit müssen Plattformen Informationen über Händler*innen einholen und diese auch überprüfen. Trotzdem müssen Plattformen keiner Offenlegungspflicht nachkommen. Bezüglich der Haftung von Intermediären haben Plattformen einen Vorteil, da sie nicht für die Informationen haften, wenn Empfänger*innen diese abrufen, unter der Voraussetzung, dass z.B. die Plattform von den illegalen Aktivtäten nichts wusste oder Kenntnis zu illegalen Aktivitäten besitzt und diese umgehend unterbindet. Gerade bei der Haftung kritisieren die Autor*innen den Schutz von Konsument*innen, da auch der DSA von durchschnittlich und gut informierten Konsument*innen ausgeht. Diese ungenaue Terminologie könnte im Zweifelsfall dazu führen, dass Konsument*innen rechtlich einen Nachteil haben, da Plattformbetreiber*innen die Kosten guter Anwälte besser tragen können. Die

Autor*innen betonen, dass auch die Durchsetzung von Rechts- und Selbstregulierungsnormen stark in der Hand von privaten Einrichtungen liegt und merken Bedenken zur Rechtsstaatlichkeit an. Zum Beispiel müssen sehr große Online-Plattformen eine jährliche Selbstüberprüfung durchführen, um zu erkennen, ob ihr Service generell systematischen Schaden anrichtet. Da die Erkennung von Risiken von den Plattformen selbst durchgeführt wird und weitere Pflichtprüfungen von profitorientierten privaten Audits auf Kosten der Plattformanbieter*innen gemacht werden, ist dies kritisch zu betrachten. Allgemein betonen die Autor*innen, dass es abzuwarten gilt, ob die im DSA beschriebenen Kommissionen für Untersuchungen und Abhilfe ausreichen werden, um Verbraucher*innen zu schützen. Bei der Durchsetzung des DSA sprechen die Autor*innen ihre Sorgen aus, was auch die Harmonisierungswirkung der digitalen Reform betrifft, da die Durchsetzungspflichten auch technisch jedem EU-Mitgliedsland möglich sein müssen. Um diese Asymmetrie auszugleichen und zur Durchsetzung des DSA raten die Autor*innen dringend zu enger Zusammenarbeit zwischen den Mitgliedsstaaten und der EU-Kommission (vgl. Cauffman & Goanta, 2021, S. 758-773). Die Autorin empfindet die Analyse des Reformvorschlags des DSA von den Autor*innen gut und kritisch begutachtet. Sie bringt vor der unmittelbaren Anwendung des Gesetzesentwurfs schon gute Einblicke, worauf zu achten ist, und bei welchen Aspekten nachgeschärft werden müsste.

Micova (2021) hat sich mit dem DSA im Zusammenhang mit Plattformengröße und dem Schadensprinzip beschäftigt, insbesondere mit der Risikobewertung, welche VLOPs durch den DSA verpflichtend durchführen müssen. Micova analysiert dabei den Zusammenhang zwischen der Größe einer Plattform und dem potenziellen Schaden, der durch sie entstehen kann mit der Fragestellung, woran es liegt, dass der Schaden größer wird, je größer eine Plattform ist und, ob die Größe der Plattform wirklich einen systematischen Einfluss auf Schaden hat. Zu Anfang des Journals geht sie darauf ein, dass es nicht die Aufgabe des Marktes ist, Schaden zu verhindern und Privatsphäre zu schützen. Auf der anderen Seite nimmt Marktmacht Konsument*innen die Autonomie, speziell was Privatsphäre betrifft. Weiters geht sie auf das Schadensprinzip ein und definiert, dass Schaden sowohl aus einer Gruppe kollektiver Macht als auch durch sozialen Druck entstehen kann.

Weiters stellt die Autorin fest, dass man auch zwischen privatem und öffentlichem Schaden unterscheiden muss und lehnt sich an Feinbergs (1973) Konzept des öffentlichen Schadensprinzips an, welches besagt, dass Schaden öffentlich sein kann, wenn es öffentliche Institutionen, auf die viele angewiesen sind, betrifft. Die Autorin untersucht die genaue Definition großer Plattformen, um zu bestimmen, welche Eigenschaften sie haben müssen, um systematischen Schaden zu verursachen. Sie kritisiert zugleich, dass der DSA nicht definiert, in welchem System er versucht, Schadensrisiken zu minimieren, da er grundsätzlich nur auf EU-Ebene gedacht ist. Dennoch geht der Schaden von VLOPS wegen ihrer Reichweite weit darüber hinaus. Danach geht sie auf die Teilbereiche des Schadens ein, die im DSA erwähnt werden, und die Koordinatoren digitaler Dienste durchsetzen müssen. Die Risikobewertungen müssen in den Bereichen Verbreitung illegaler Inhalte, negative Auswirkungen auf die Grundrechte, sowie Manipulation oder Automatisierung des Dienstes mit negativen Auswirkungen auf die öffentliche Sicherheit, durchgeführt werden. Weiters macht sie darauf aufmerksam, dass schon länger bekannt ist, dass Konsument*innen durch die Größe einer Plattform und deren Marktmacht, eingeschränkt werden, basierend auf Datenschutzvorkehrungen zu entscheiden, was zu massenhaften individuellen Schaden führen kann, da diese Unternehmen oft am meisten in die Monetarisierung von persönlichen Daten investieren. Dieser Tauschhandel mit persönlichen Daten und Privatsphäre könnte ein systemisches Risiko darstellen, das die Verpflichtung des Staates zum Schutz von Privat- und Familienleben untergräbt und digitale Dienste mitschuldig macht. Zusammenfassend erklärt die Autorin, dass es ein Problem darstellt, wenn der DSA kein System definiert, in dem Schadensrisiko verhindert werden soll. Die Bewertung von Schaden betrifft derzeit nur öffentliche Institutionen, sozialen Kontext und gesellschaftliche Systeme. Deswegen empfiehlt Micova, dass die Systeme der einzelnen Mitgliedsstaaten in der Definition von VLOPs eine Rolle spielen müssen, da selbst, wenn die offiziellen Kriterien einer VLOP nicht erfüllt wurden, der öffentliche Charakter einer Plattform öffentliche Einrichtungen eines Staates gefährden kann.. Auch der Grad der Vernetzung sollte bei der Definition von VLOPs eine Rolle spielen, um Schaden in einem sozialen System besser widerzuspiegeln und nicht nur Schaden rein auf ein Plattformökosystem zu beziehen. Zum Schluss bemerkt die Autorin, dass der DSA Medienpluralismus als eigene Risikokategorie

bei der Risikobewertung von VLOPs einstufen müsste, da digitale Dienste einen starken Einfluss auf die Auffindbarkeit von Medieninhalten haben, indem Inhalte personalisiert gezeigt werden. Die Gatekeeper Funktion von digitalen Plattformen hat dementsprechend einen großen gesellschaftlichen als auch wirtschaftlichen Einfluss (vgl. Mikova, 2021, S.1-18). Die Autorin hat sehr gut erschlossen, was Schaden sowohl auf individueller Seite als auch im öffentlichen Sinne alles bedeuten kann und was in neuen Rechtsakten wie dem DSA berücksichtigt werden müsste. Trotzdem hat sie in ihrer Analyse keine konkrete Methode angewandt.

Die Studie von Corman, Canaway, Culnane und Teague (2022) hat getestet, nach welchen Prinzipien Menschen ihre gesundheitsbezogenen Daten für Forschungszwecke an Zweite weitergeben und wollte damit herausfinden, wonach Menschen beurteilen, ob die technische Wirksamkeit zum Schutz ihrer Daten und Privatsphäre gegeben ist. Außerdem wollten die Autor*innen herausfinden, ob es einen Zusammenhang zwischen demografischen Daten, Gesundheitszustand und Bereitschaft, die Daten zu teilen, gibt. Die webbasierte Umfrage hat vier Methoden des Datenaustausches abgefragt, die unterschiedliche Niveaus zum Schutz der Privatsphäre bieten. Außerdem wurden Fragen zum derzeitigen Gesundheitszustand als auch zum allgemeinen Empfinden des gemeinsamen Nutzens von Daten abgefragt. Obwohl die kreuzsektional durchgeführte Umfrage aus Australien stammt, kommt sie mit einer Stichprobe von 317 Menschen auf ähnliche Ergebnisse wie jene von Pleger, Guirguis und Mertes, in der es um die Verständlichkeit der Zustimmung zur Datenverwendung ging. Speziell handelte es sich um das Verständnis des technischen Wortes „De-identifizierung“ bei der Einverständniserklärung. Dabei kam einerseits kein einheitliches Verständnis des Begriffs, als auch kein Zusammenhang zwischen der Bereitschaft, Daten weiterzugeben und der vorherigen Anonymisierung dieser, heraus. Trotzdem stellen Befragte ihre Daten zur Sekundärnutzung eher zur Verfügung, wenn besserer Schutz der Privatsphäre gegeben ist. Das fehlende Verständnis für die in Einverständniserklärungen verwendeten Terminologien zur Sekundärnutzung von Gesundheitsdaten lässt die Autor*innen zu dem Schluss kommen, dass allgemein besser verständliche Einverständniserklärungen formuliert werden müssen, um ein klares Einverständnis von Personen zu erlangen (vgl. Corman, et al., 2022, S. 1-7).

Die Ergebnisse dieser Studie sind nicht unbedingt auf die EU ummünzbar, da die DSGVO nicht in Australien gilt. Dennoch ist es spannend, dass die Problematik des Verständnisses von Einwilligungserklärungen weit verbreitet ist. Weiters wurden Befragte nicht direkt gefragt, wie gut sie die Begrifflichkeiten der Umfrage wirklich verstehen.

Turillazzi, Taddeo, Floridi und Casolari (2023) haben den Digital Services Act anhand akademischer Literatur und Policy Papers analysiert und die ethischen, sozialen und rechtlichen Bedeutungen des DSA herausgearbeitet. Dies haben die Autor*innen mittels Stichwortabfrage über drei große Repositorien gemacht und dabei die drei Stichworte „Wettbewerbsrecht“ „Ethik“ und „digitale Wirtschaft“ abgefragt, um den DSA zu beschreiben. Sie haben sich auf Publikationen, die zwischen 2016 und 2021 veröffentlicht wurden, beschränkt, und dabei 80 identifiziert, die dann weiter analysiert wurden. Dabei arbeiteten sie vier Kerngebiete heraus, die in der Literatur zur Umsetzung des DSA herausstachen. Einerseits der Versuch der Harmonisierung von EU-Praktiken, der Umgang mit schädlichen oder illegalen Inhalten, die Haftungsregelungen, was Intermediäre betrifft, sowie der Verbraucherschutz in Zusammenhang mit dem Kartellrecht. Die Forschungsgruppe hatte den Fokus auf Probleme, die sich durch digitale Dienstleistungen ergeben, für welche EU-Einrichtungen zuständig sind. Zuletzt hinterfragen sie, wie der DSA die Förderung von Wettbewerb mit dem Schutz von grundlegenden europäischen Werten vereint. Damit meinen sie die Abwägung zwischen dem Schutz von Grundrechten von User*innen und dem Umstand, als Online Plattform innovativ und konkurrenzfähig bleiben wollen. Sie heben hervor, dass Unternehmen sich, wie bei der DSGVO, an den Digital Services Act halten müssen, ob sie einen Sitz in der EU haben oder nicht. Trotzdem richtet sich der DSA nur an Intermediäre. Dies könnte dazu führen, dass europäische Plattformen einen Vorteil haben und deswegen den europäischen digitalen Markt unattraktiv machen. Kernergebnisse der Analyse waren unter anderem, dass der DSA für Gatekeeper zu Herausforderungen führen wird, da Aufsichtsbehörden direkt in Geschäftsmodelle von Gatekeepern eingreifen können, wenn Gatekeeper kleinere Anbieter hindern könnten, größer zu werden, da sie mehr Ressourcen haben. In Bezug auf Inhaltsregulierungen und deren Moderation sind die Autor*innen nicht sicher, ob der DSA die Grundrechte richtig

abbildet. Sie stellen auch fest, dass die bisherigen Rechtsvorschriften für eine digitale Weltwirtschaft nicht mehr ausreichen, da sich die Gesellschaft in einem komplexen System der Plattformwirtschaft befindet. Zum Schluss stellen sie fest, dass Diskussionen zum DSA zu widersprüchlichen Interpretationen führen und dass je nach Interessensgruppe vorgestellte Verpflichtungen auch als ungerechtfertigt empfunden werden. Widersprüchliche Meinungen in der Umsetzung können wiederum die Harmonisierung in der EU behindern. Zum Beispiel verlangt der DSA nicht, dass Dienstanbieter illegale Inhalte überwachen oder verweigern, und Mitgliedsstaaten dürfen dies auch nicht verlangen. Auf der anderen Seite verhindert der DSA auch nicht, dass Mitgliedsstaaten von Anbieter*innen verlangen können, dass Verstöße verhindert oder beendet werden. Auch bei Regulierung von Inhalten schlägt der DSA vor, dass alle Internetuser*innen jeglichen Inhalt als illegal melden dürfen. Die Autor*innen heben deshalb Bedenken bezüglich der Grundrechte hervor, vor allem, was die terminologische Unsicherheit zwischen illegal und schädlich betrifft. Bezüglich der Haftung von Intermediären wird angemerkt, dass der DSA zwar Ausnahmen bei Dienstleister*innen vorsieht, aber nicht, unter welchen Bedingungen. Weiters gehen sie noch auf Transparenz und das Vertrauen von Konsument*innen ein, und zwar insofern, dass Unternehmen Informationen sowohl gegenüber Plattformen als auch Konsument*innen offenlegen müssen. Zum Schluss heben die Autor*innen die Wahrscheinlichkeit hervor, dass der DSA einen ähnlichen Effekt haben könnte wie die DSGVO, nämlich, dass er die Regulierung digitaler Dienste auch außerhalb der EU mitgestalten und vorantreiben wird (vgl. Turillazzi et al., 2023, S. 83-106). Die Autor*innen legen ihre Methode und ihre Ergebnisse klar und offen dar, was den Beitrag gut verständlich und nachvollziehbar macht. Der kurze Ausblick bezüglich der ähnlichen Wirkung zwischen DSGVO und DSA geben der Autorin dieser Masterarbeit einen weiteren Anhaltspunkt.

Auch Leerssen (2023) sieht aus juristischer Perspektive auf den Digital Services Act und untersucht dabei die Transparenzrechte, welche neue Moderationsregelungen von Inhalten bieten. Seine Forschungsfrage bezieht sich dabei auf den Umgang mit Shadowbanning und ob der DSA dafür sorgen wird, dass es diese Praxis der Contentmoderation nicht mehr geben wird. Diese Forschungsfrage versucht der Autor zu beantworten, indem er Shadowbanning seitens der Terminologie Technik

und dessen politischen Einfluss betrachtet und im Anschluss darauf eingeht, welche Details des DSA mit dem Transparenzgesetz verändert werden. Somit betrachtet er, ob die Diskrepanz zwischen Transparenz und Geheimhaltung ausgeglichen wird. Shadowbanning war bisher eine Maßnahme von Plattformen, die Sichtbarkeit von usergenerierten Inhalten zu drosseln, ohne dass die Verursacher*innen davon wissen und ohne dass sie komplett von einer Plattform gesperrt werden. Dies kann bedeuten, dass Inhalte nicht gezeigt werden oder niedrig gereiht werden, damit eine geringere Anzahl an User*innen diese Inhalte sieht. Nun ist laut Autor Shadowbanning schon vor der Einführung von Transparenzgesetzen eine viel kritisierte Praxis der Contentmoderation gewesen, da es von einigen als undemokratisches Manöver gesehen wird, Meinungen nicht zuzulassen und von anderen als Schutzstrategie gegenüber Täter*innen auf Social Media gesehen wird. Deswegen versucht das Transparenzgesetz die Frage des Einsatzes von Shadowbanning zu klären, nämlich, ob und wenn ja, wann die Moderation von Inhalten geheim bleiben darf. Denn auf der einen Seite soll Shadowbanning Hassreden und Falschinformationen daran hindern, viral zu werden, doch setzt der Autor auch Argumente entgegen, dass User*innen mit Shadowbanning heimlich sanktioniert werden und das wiederum dem Anspruch der Transparenz von Plattformen widerspricht. Bezüglich des DSA spricht der Autor besonders stark die „notice and action“-Regelung in Art 14 (DSA) an, welche die erste Contentmoderations-Regelung ist, die über bloßes Verbannen und Sperren von Accounts hinausgeht und Sichtbarkeiten beschränken und Inhalte niedrig listen soll. Voraussetzung dafür ist, dass die Regeln der Contentmoderation in den Allgemeinen Geschäftsbedingungen stehen und auf sorgfältige und verhältnismäßige Art implementiert werden müssen, sodass betroffene Interessen und Grundrechte beachtet werden.

Der Autor kritisiert die Umsetzung des Verbots von Shadowbanning, da sie zu wenig Ausnahmen beinhaltet und somit Shadowbanning mehr oder weniger verboten ist. Plattformen müssen dadurch die Verwendung von Shadowbanning nachweisen und wenn sie tatsächlich Shadowbanning als Contentmoderation verwenden, dies offenlegen. Somit legt der DSA in Bezug auf Contentmoderation hohen Wert auf Transparenz, schafft aber kein Gleichgewicht zwischen den gegensätzlichen Meinungen mit der Praxis des Shadowbannings. Zum Schluss kritisiert der Autor

den generellen Ausdruck der Herabstufung als Sanktionierung im Digital Services Act, da auf technischer Seite mit binären Kategorien gearbeitet wird. Das heißt, es wird gelistet oder nicht gelistet, ohne technische Alternativen. Deswegen kritisiert Leerssen, dass jeder Inhalt individuell behandelt werden muss, da es keinen Standard- oder Mittelwert gibt, nachdem sich das System richten kann (vgl. Leerssen, 2023, S. 1-13). Leerssen hat in seiner detaillierten Aufarbeitung von Shadowbanning im Digital Services Act der Autorin einen Denkanstoß gegeben, die Art und Weise des Schutzes personenbezogener Daten im DSA herauszuarbeiten. Seine Analyse ist sehr gut nachvollziehbar und gibt Einblicke in die Diskrepanz zwischen juristischen Ausdrücken und technischer Realität.

In der nachstehenden Tabelle werden überblicksmäßig die Arbeiten aus dem Forschungsstand und dessen Kernergebnisse noch einmal präsentiert.

Autor / Jahr	Ziel/Forschungsfrage	Methodik	Stichprobe	Kernergebnisse	Kritik
Klementschitz/ 2019	Die Regelung des internationalen Datenverkehrs im DSG und DSGVO. Die jeweilige Judikatur dazu sowie besondere Problemdarstellungen im Internationalen Datenverkehr unter Einfluss der DSGVO sind Kern der Arbeit.	Qualitativ: Vergleich von Gesetzestexten	-	Der internationale Datenverkehr wurde vom Sprung vom nationalen DSG zur DSGVO vereinfacht, da er weitestgehend genehmigungsfrei ist. Dennoch erfahren auch hier die Öffnungsklauseln der DSGVO Kritik. Auch die Selbstkontrolle Verantwortlicher und das EU-US Datenschutzschild stehen unter Kritik.	Es wurde in dieser Dissertation keine Methode genannt.
Tagwercher/ 2019	Das österreichische Datenschutzgesetz DSG im Vergleich zur DSGVO in Bezug auf das Grundrecht auf Datenschutz und den persönlichen Schutzbereich.	Qualitativ: Vergleich von Gesetzestexten	-	Die Öffnungsklauseln in der DSGVO verhindern gänzliche Vereinheitlichung des Datenschutzrechts Der persönliche Anwendungsbereich ist je nach Gesetzeslage unpräzise definiert. Genauso unpräzise ist, wer Grundrechts-träger*in ist und wer nicht. In Österreich fällt „jedermann“ in den persönlichen Schutzbereich und somit auch juristische Personen.	Die Diplomarbeit ist eher kurz gehalten und keine konkrete Methode wurde genannt.
Haber& Tamò-Larrieux / 2020	Analyse der Umsetzung von Security und Privacy by Design und anschließender Vergleich zwischen dem israelischen und dem europäischen Ansatz. Welcher Ansatz enthält mehr Anleitung für Entwickler*innen zur Umsetzung von Privacy und Security by Design?	Qualitativ: Analyse und Vergleich der Gesetzgebungen	-	Im Gegensatz zur israelischen Regulierung schreibt die DSGVO Privacy by Design zwar vor und gilt deswegen als strenger, dafür bekommen Ingenieur*innen jedoch keine konkreten Anweisungen. Beim israelischen Ansatz bekommen Ingenieur*innen genaue Bauanleitungen bei der Implementierung von Privacy by Design, doch ist die Datensicherheit nach DSGVO höher, da Verantwortliche Anweisungen geben, wo Prioritäten liegen.	Expert*inneninterviews wären bei der Analyse ein Mehrwert gewesen, dennoch ist es eine gute Vergleichsarbeit, welche die beste Mischung aus verschiedenen Gesetzestexten hervorhebt.
Pleger, Guirguis & Mertes / 2021	Datenschutz und Datensicht aus Sicht der Bürger*innen. Wie müssen E-Government, Datenschutz und Datensicherheit kommunizieren, um Bedenken von Bürger*innen bezüglich Datenweitergabe zu minimieren?	Methodenmix Qualitative Methode: Medien-Analyse	1000	Bürger*innen verstehen die Begrifflichkeiten Datensicherheit und Datenschutz in Medienartikeln nicht vollständig. Die Wichtigkeit von Datensicherheit und Datenschutz ist abhängig von Dienstleistung und bei Banken als sehr wichtig angesehen.	Es wurden nur deutsche und britische Bürger*innen befragt. Die Studie ist nicht direkt anwendbar auf Österreich. Trotzdem kann basierend auf den Ergebnissen Forschung zu

		Quantitative Methode: Umfrage			dem Thema in der EU empfohlen werden.
Cauffman & Goanta / 2021	Die Autor*innen untersuchen den Reformvorschlag des DSA bezüglich Haftung von Intermediären, Verbraucherschutz, Vereinbarkeit mit dem Unionsrecht sowie die Herausforderungen, welche die Durchsetzung mit sich bringen wird.	Qualitativ: Analyse von Gesetzestexten	-	DSA sorgt bezüglich der Haftbarkeit für mehr Rechtsschutz gegenüber Intermediären als gegenüber Konsument*innen. Pflichtüberprüfungen werden von gewinn-orientierten Unternehmen gemacht, deren Kund*innen die gleichen großen Plattformen sind, die sie überprüfen. Außerdem müssen für die Durchsetzung des DSA die Mitgliedsstaaten und die EU-Kommission eng zusammenarbeiten.	Die Analyse des DSA Reformvorschlags bietet der Autorin gute Einblicke in Lücken und offene Fragen, auf die zu achten ist.
Micova / 2021	Die Autorin hinterfragt in ihrem Journalbeitrag die verpflichtende Risikobewertung durch den DSA, welche sehr große Plattformen durchführen müssen. Sie untersucht dabei den Zusammenhang zwischen der Größe einer Plattform und den davon ausgehenden potentiellen Schaden.	Qualitativ: Analyse von Fachliteratur und dem Reformvorschlag des DSA	-	DSA sollte bezüglich Risikobewertung von VLOPs auch die Vernetzbarkeit mitdenken und nicht nur die Anzahl der User*innen. Medienpluralismus sollte eine eigene Risikokategorie zur Bewertung sein. Der DSA sollte ein System definieren, in dem das Schadensrisiko minimiert werden soll. Außerdem sollten die einzelnen Systeme der Mitgliedsstaaten eine Rolle spielen, da der öffentliche Charakter einer Plattform auch ohne Zugehörigkeit zu den VLOPs einen massiven Schaden bei öffentlichen Einrichtungen anrichten kann.	Die Analyse des DSA war gut strukturiert und definiert das Ausmaß, das Schaden bezüglich großer Plattformen haben können. Keine Anwendung einer konkreten Methode.
Corman et al. / 2022	Sie versuchen herauszufinden, wie genau die Menschen die Wirksamkeit von Techniken zum Schutz der Privatsphäre bei gemeinsam genutzten Gesundheitsdaten wahrnehmen.	Quantitativ: kreuzsektionale Umfrage	317	Große Toleranz bei Verwendung von Gesundheitsdaten, wenn Forscher sie bekommen sollen. Uneinigkeit bei Abfragung von Begrifflichkeiten „de-identified“.	Ergebnisse sind nicht direkt umlegbar auf die Population in der EU, da dies eine australische Studie ist.
Turillazzi et al. / 2023	Eine Stichwortanalyse anhand von Policy Papers und akademischer Literatur, um die sozialen, ethischen und rechtlichen Bedeutungen des DSA herauszuarbeiten.	Qualitativ: Stichwortanalyse	-	Gatekeeper könnten durch den DSA einen Nachteil haben, da Aufsichtsbehörden künftig in das Geschäftsmodell direkt eingreifen	Die Methode ist gut nachvollziehbar und gut dargelegt. Der Vergleich der Wirkung des DSA mit der

				dürfen. In Bezug zu Contentmoderation sind sich die Autor*innen nicht sicher, ob der DSA die Grundrechte richtig abbildet. Je nach Interessensgruppe werden die Verpflichtungen des DSA teils unfair empfunden. Auch hier werden wieder terminologische Unsicherheiten bezüglich Content Moderation angemerkt.	DSGVO gibt der Autorin einen Anhaltspunkt für diese Arbeit.
Leerssen/ 2023	Eine Analyse, wie sich die Transparenzrechtregelungen im Digital Services Act auf Content Moderation und Shadowbanning auswirken. Er untersucht dazu verschiedene Passagen des DSA und deklariert die Vor- und Nachteile bzw. offene Fragen und Konflikte, die durch die Transparenzregelungen entstehen können.	Qualitativ: Analyse von Gesetzestexten	-	Der DSA schafft mit dem Transparenzrecht zwar mehr Transparenz, aber dafür weniger Sichtbarkeit und verbietet Shadowbanning mit wenigen Ausnahmen. Außerdem sind einige Terminologien, die im technischen Kontext schwer umzusetzen sind, kritisiert worden	Der Autor hat aus dem DSA die Vor- und Nachteile der Praxis von Shadowbanning herausgearbeitet und die Diskrepanz zwischen juristischen Formulierungen und technischer Realität erläutert.

Tab. 1: Überblick Forschungsstand (Eigendarstellung)

Forschungslücke:

Die Literaturarbeiten aus juristischer Sichtweise auf das DSG und die DSGVO von Tagwercher (2019) mit Blick auf den persönlichen Schutzbereich und Klementschitz (2019) auf den internationalen Datenverkehr verfolgen den Vergleichsansatz, den auch diese Arbeit verfolgt. Hier wird der Blick jedoch primär auf Lücken in der DSGVO und Erweiterungen des DSA zum Schutz personenbezogener Daten geworfen, da diese Aspekte noch unbekannt sind. Auch der Vergleichsansatz von Privacy by Design zwischen dem israelischen Konzept und dem EU-Konzept von Haber und Tamò-Larrieux (2020) gibt Aufschluss darüber, dass bei dem Privacy by Design-Konzept der DSGVO Unklarheiten bestehen, denen hier auf den Grund gegangen wird. Es gibt einige internationale Forschungsarbeiten, die bezüglich des Verständnisses von Datenschutzbestimmungen aus Konsument*innenperspektive geforscht haben, mit der Erkenntnis, dass der Großteil der Befragten genaue Bedeutungen von datenschutzrechtlichen Begrifflichkeiten nicht kennt, wie die Forschung von Pleger, et al. (2021), aber auch die Forschung von Coreman et al. (2022) gezeigt hat, weswegen hier das Verständnis von Einwilligungserklärungen hinterfragt wird. Cauffman und Goanta (2021) analysieren den Reformvorschlag des DSA, die neuen Haftungsbedingungen, die verpflichtende Bewertung von Unternehmen und die Vereinbarkeit des DSA mit dem Unionsrecht. Aspekte, wie Pflichtbewertungen gewisser Plattformen, werden in dieser Arbeit näher untersucht, aber der Blick auf den DSA wird hier eher auf den Schutz personenbezogener Daten gerichtet. Das Gleiche gilt für die Arbeit von Micova (2021), welche hinterfragt, ob großer Schaden tatsächlich nur von sehr großen Plattformen ausgeht. Dies wird in der Arbeit auch näher beleuchtet. Auch Turillazzi et al. (2023) untersuchen den DSA aus verschiedenen Blickwinkeln, um die sozialen, ethischen und rechtlichen Aspekte zu analysieren, und Leerssen (2023) untersucht die Transparenzrechte des DSA genauer, besonders die Aspekte bezüglich Shadowbanning. Leerssen spricht speziell die Diskrepanz zwischen juristischen Formulierungen und technischer Praxis an, welche in dieser Arbeit eine Rolle spielen wird. Zudem gibt es noch keine Forschungsarbeiten bezüglich konkreter Lücken in der DSGVO und inwieweit der DSA den Schutz personenbezogener Daten ergänzen kann.

Deswegen wird sich diese empirische Arbeit mit der Forschungslücke zwischen DSGVO und DSA beschäftigen und versuchen, herauszufinden, an welchen Stellen

sie einander in Bezug auf personenbezogene Daten ergänzen oder wo sie sogar Schwächen beim jeweils anderen Gesetz verursachen. Außerdem versucht diese Arbeit zu eruieren, ob Regelungen wie die DSGVO oder der DSA dem technologischen Wandel hinterherkommen und an welchen Stellen die Verantwortungen zu nachhaltigem Datenschutz liegen.

Im folgenden Kapitel startet das erste Theoriekapitel über nachhaltigen Datenschutz, die DSGVO und die Verantwortung zum Schutz personenbezogener Daten in der Praxis.

3. Die DSGVO und nachhaltiger Datenschutz

Die folgenden Kapitel beschäftigen sich mit den Anfängen des Datenschutzes in Österreich und wie sich die Judikatur in Richtung Datenschutz-Grundverordnung verändert hat. Dazu wird zuerst ein kurzer Rückblick auf die Anfänge und Entwicklungen des Datenschutzes in Österreich geworfen. Dann geht es weiter zum ersten Datenschutzgesetz bis hin zur Einführung der DSGVO und deren Ziele. Dann wird ein kurzer Einblick gegeben, was nachhaltiger Datenschutz bedeutet. Mit den Kapiteln der Verantwortlichkeiten wird die Durchsetzung der DSGVO heruntergebrochen auf Staat, Unternehmen, Betroffene und Konsument*innen und verglichen, welche Akteure in der Praxis die Verantwortung haben. Im gleichen Zug wird außerdem erarbeitet, welche Lücken oder Schwächen es gibt. Weiters wird verglichen, ob sich die einzelnen Verantwortungen mit nachhaltigem Datenschutz vereinbaren lassen. Zum Schluss wird in diesem Kapitel auch noch darauf eingegangen, wie sich die Sanktionierung zur DSGVO hin bei Verstößen gegen das Datenschutzrecht verändert hat.

3.1 Der Weg zum Datenschutzgesetz

Die Entwicklung eines Datenschutzgesetzes kam das erste Mal in den 1960er Jahren auf, nachdem die Entwicklung von Informationstechnologien voran ging und somit die Schnelligkeit der Verarbeitung großer Datenmengen angestiegen ist. Daraus resultierte zum ersten Mal, dass Betroffene den Überblick über die Verarbeitung ihrer eigenen Daten verlieren und somit die Wahrscheinlichkeit für Missbrauch erheblich ansteigt (vgl. Duschanek, 2009, S. 43). Zwar gab es schon vor dem Datenschutzgesetz Regelungen im Allgemeinen Bürgerlichen Gesetzbuch, kurz ABGB und im Staatsgrundgesetz, kurz StGG, dennoch benötigte es ein allumfassenderes Gesetz.

Zum einen ist im allgemeinen Bürgerlichen Gesetzbuch, kurz ABGB, geregelt, dass jeder Mensch ein angeborenes Recht auf Privatsphäre und deren Schutz hat.[2] Diese Regelung fällt unter die Persönlichkeitsrechte. Persönlichkeitsrechte haben den Zweck, den Menschen ganzheitlich gegenüber Dritten zu schützen. Dieses

[2] Vgl. Allgemeines bürgerliches Gesetzbuch für die gesamten deutschen Erbländer der Österreichischen Monarchie (ABGB), StF: JGS Nr. 946/1811, Fassung vom 15.05.2023, Fassung vom 15.05.2023, § 1328a.

absolute Gesetz, also eines, dass gegen jedermann wirkt, ist schon im Jahr 1812, damals noch als § 16 (ABGB), in Kraft getreten und ist seitdem unverändert geblieben. 1975 traten § 10 und § 10a (StGG) in Kraft, welche schon Ähnlichkeiten zum Datenschutzgesetz hatten, indem sie sich auf das Recht auf Briefgeheimnis und das Recht auf Fernmeldegeheimnis beziehen.[3] Speziell § 10a (StGG) schützt Daten gegenüber Dritten, die über Telekommunikationsnetze verbreitet werden. Dennoch steht bei den Anfängen des Datenschutzes mehr der Schutz von Individuen gegenüber dem Staat im Vordergrund, wie auch Tagwercher in ihrer Diplomarbeit festhält. Die Abwehr gegenüber dem Staat war gut umzusetzen mit der Gesetzgebung im StGG, doch verarbeitet nicht nur der Staat große Datenmengen, sondern auch Bürger*innen und andere Akteur*innen. Um Betroffene auch vor anderen Akteur*innen, welche mit großen Datenmengen arbeiten, zu schützen, und Betroffenenrechte, die auf den Schutz personenbezogener Daten basieren, besser einfordern zu können, trat am 1. Jänner 1980 das Datenschutzgesetz in Kraft. Die erste Version der DSG trat zwar 1980 in Kraft, wurde aber schon 1978 kundgemacht, weshalb diese Version DSG 1978 genannt wird (vgl. Tagwercher, 2019, S. 9f.). Österreich war mit dem Inkrafttreten des Datenschutzgesetzes eines der ersten Länder weltweit. Ab dem Zeitpunkt wurden betroffene Personen, deren personenbezogene Daten verarbeitet wurden, unter Schutz gestellt. Nun gab im Datenschutzgesetz 1978 das Grundrecht auf Geheimhaltung, welches als eines beschrieben wird, das unabhängig von der Automatisierung der Verarbeitung davon, greift.[4] Nach diesem Paragraphen haben sowohl natürliche als auch juristische Personen ein Grundrecht auf Geheimhaltung. Dies bedeutete, dass nicht nur natürliche Personen, sondern auch Betriebsgeheimnisse von juristischen Personen geschützt wurden. Dies steht im Gegensatz zur DSGVO, die nur Daten von natürlichen Personen schützt (vgl. Tagwercher, 2019, S. 10).

[3] Vgl. Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger. StF: RGBl. Nr. 142/1867, Fassung vom 26.08.2023, § 10 und § 10a.
[4] Vgl. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG), StF: BGBl. Nr. 565/1978, Fassung vom 18. Oktober 1978, § 1.

Im Jahr 1995 trat die Datenschutz-Richtlinie in Kraft, welche in den Mitgliedsstaaten innerhalb von drei Jahren bis zum 13. Jänner 1998 umgesetzt werden musste.[5] Dies setzte weitere Schritte zum Schutz personenbezogener Daten und zum freien Datenverkehr voraus. In Österreich wurde besagte Richtlinie im DSG 2000 schlussendlich am 1. Jänner 1998 umgesetzt[6], woraus sich Änderungen ergaben. Eine der wichtigsten Veränderungen war, dass nun die Verarbeitung von manuell eingegeben Daten auch erfasst wurde und nicht nur die ganz oder teilweise automatisierten Daten (vgl. Duschanek, 2009, S. 49). Weiters wurden die Zuständigkeit der Datenschutzkommission sowie Sanktionierungen erweitert. Außerdem wurde der Begriff der Schutzwürdigkeit weiter präzisiert, da diese eine Voraussetzung für den Geltungsbereich des Grundrechts ist. Zudem wurde im DSG 2000 der persönliche Schutzbereich auf „jedermann“ erweitert, was bedeutet, dass in Österreich juristische Personen auch ein Recht auf Datenschutz haben. Diese Regelung widerspricht nicht der Datenschutzrichtlinie und auch nicht der später eingeführten DSGVO (vgl. Tagwercher, 2019, S. 14f.). Damals schon wurde nach Tagwercher (2019) die Wirkung der Harmonisierung hinterfragt, weil abermals alle Mitgliedsstaaten sich frei entscheiden durften, ob zum Beispiel juristische Personen beim Schutz der Verarbeitung von Daten einbezogen werden sollten oder nicht.

Aus diesem Grund wurde mit 25. Mai 2018 die DS-RL von der Datenschutzgrundverordnung ersetzt, die im Gegensatz zu der vorherigen Richtlinie eine Rechtsnorm darstellt, die nicht national umgesetzt werden muss, sondern unmittelbar anwendbar ist (vgl. Feiler & Forgó, 2022, S. 1).

[5] Vgl. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr., 281 OJ L § (1995). Fassung vom 23.11.1995, Art. 32.

[6] Vgl. Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.), Fassung vom 17. August 1999, § 59.

3.1.2 Die Datenschutzgrundverordnung – die Hoffnung auf Datenhoheit

Im April 2016 wurde die DSGVO beschlossen und stellte die neue Grundlage des Datenschutzrechts in der EU dar. Diese ist seit dem 25. Mai 2018 unmittelbar in 28 Mitgliedsstaaten inklusive Österreich anwendbar und löste damit die DS-RL ab. Ziel ist es, das Datenschutzrecht in der EU zu harmonisieren und für mehr Transparenz zu sorgen. In Art. 1 (DSGVO) werden die Grundrechte und Ziele geklärt, dass der Schutzbereich bei Verarbeitung personenbezogener Daten nur für natürliche Personen gilt. Außerdem werden der Schutz zum freien Datenverkehr, sowie der Schutz der Grundfreiheiten und Grundrechte geklärt. Wichtig dabei ist, dass der freie Datenverkehr weder eingeschränkt oder verboten werden darf. Weiters wird auch ein räumlicher und sachlicher Anwendungsbereich definiert. Der sachliche Anwendungsbereich bezieht sich darauf, dass auf jede Art der Verarbeitung von personenbezogenen Daten, ob automatisiert oder nicht-automatisiert, die DSGVO anzuwenden ist (vgl. DSGVO, Art 2, Abs. 1). Das heißt, dass Betroffene auch bei manueller Verarbeitung und Sammlung von personenbezogenen Daten geschützt sind (vgl. Fargo & Feiler, 2022, S. 51). Fast noch wichtiger ist der räumliche Anwendungsbereich, der festlegt, dass Verantwortliche und Auftragsverarbeitende sich an die Verordnung halten müssen, wenn sie eine Niederlassung innerhalb der Europäischen Union haben und auch, wenn sie keine Niederlassung in der Europäischen Union haben. Es sind somit alle Betroffenen in der EU geschützt, auch vor Verantwortlichen außerhalb der EU (vgl. DSGVO, Art. 3). Demnach ist es egal, ob Verantwortliche eine Hauptniederlassung, ein Zweigstelle oder auch gar keine örtliche Niederlassung in der EU haben, denn die DSGVO hat die räumliche Anwendung an die Betroffenen gebunden, die sich in der EU befinden müssen. Dies hat den Zweck, dass Betroffene der EU den gleichen Schutz gegenüber ihren personenbezogenen Daten erwarten können, egal aus welchem Land Anbieter*innen ihre Produkte und Dienstleistungen anbieten. Außerdem ist die räumliche Anwendung wichtig, um Anbieter*innen im Netz, welche Daten von EU-Bürger*innen verarbeiten, die gleiche rechtliche Basis zu bieten, indem innerhalb der EU die gleichen Datenschutzvorgaben einhalten werden müssen wie außerhalb der EU. Dadurch ist der Markt fairer gegenüber Online-Anbieter*innen innerhalb der EU und dadurch konkurrenzfähig gegenüber Anbieter*innen von außerhalb der EU (vgl. Fargo & Feiler, S. 60). Weiters wird im Art. 5 (DSGVO) definiert, dass

personenbezogene Daten rechtmäßig und nach Treu und Glauben transparent verarbeitetet werden müssen und an einen legitimen Zweck gebunden sein müssen mit dem Hintergrund der Datenminimierung (vgl. Fargo & Feiler, 2022, S. 101ff.).

Da die DSGVO zum Schutz personenbezogener Daten eingeführt wurde, muss zuerst geklärt werden, was laut DSGVO überhaupt unter personenbezogene Daten fällt. Unter personenbezogene Daten werden alle Informationen verstanden, die dazu dienen, eine natürliche Person, auch betroffene Person genannt, zu identifizieren, wie zum Beispiel Namen, Kennnummer, Daten zum Standort oder Online Identifizierung. Es reichen jedoch auch Daten, die indirekt auf eine Person hinweisen, wie zum Beispiel besondere Merkmale, die auf die Identität einer natürlichen Person hinweisen können (vgl. DSGVO, Art. 4, Abs.1).

Für diese Arbeit müssen auch die Begriffe für Verantwortliche und Auftraggeber*innen geklärt werden. Mit Verantwortlichen sind laut DSGVO sowohl natürliche, juristische Personen, als auch Behörden oder Einrichtungen gemeint, die über die Zwecke und Mittel verfügen, um über die Verarbeitung von personenbezogenen Daten zu entscheiden. Auftraggeber*innen sind jene natürlichen oder juristischen Personen, welche personenbezogene Daten im Auftrag der Verantwortlichen verarbeiten. Unter dem Begriff „Dritter“ wird nach der DSGVO jemand definiert, der außerhalb der Betroffenen, Auftragsverarbeitenden und Verantwortlichen Zugang zu personenbezogenen Daten hat (vgl. DSGVO, Art. 4).

Um nun einen Bezug zu Nachhaltigkeit und dem Zusammenhang mit Datenschutz zu bekommen, wird im folgenden Abschnitt geklärt, was nachhaltiger Datenschutz bedeutet. Es wird auf die einzelnen Verantwortlichkeiten eingegangen und geklärt, welche Akteure in der Praxis die größte Verantwortung zum Schutz personenbezogener Daten haben.

3.2 Verantwortlichkeiten: Nachhaltiger Datenschutz

Durch die DSGVO wurden auch Verantwortlichkeiten stärker definiert, die sich auf Verantwortliche, Auftragsverarbeitende und Betroffene zusammenfassen lassen. Dennoch wird der Blick in dieser Arbeit mehr auf die Verantwortung in der Praxis zum Schutz personenbezogener Daten gelenkt. In diesem Kapitel werden die Verantwortungen des Datenschutzes kritisch analysiert und es wird erschlossen, wie gut dies mit nachhaltigem Datenschutz einhergeht. Zuerst muss hier geklärt werden, was nachhaltiger Datenschutz bedeutet.

Nachhaltigkeit ist ein Prinzip, um mit begrenzten Ressourcen schonend umzugehen, damit der Mensch Ressourcen langfristig zur Verfügung hat. In der Digitalökonomie darf jedoch eine Ressource nicht als Persönlichkeitsrecht, das nicht verbraucht werden kann, gedacht werden. Es geht um die Verfügungs- und Entscheidungsmacht über personenbezogene Daten, welche die Ressource hier darstellt, die nicht unbegrenzt zur Verfügung steht. Sobald nämlich Nutzer*innen zum Beispiel Informationen über sich auf sozialen Medien preisgeben, können Dritte darauf zugreifen. Somit verlieren Nutzer*innen Stück für Stück die Möglichkeit, den Weg der Datenverarbeitung zu verfolgen und in weiterer Folge auch den Einfluss auf den Zweck der Verarbeitung (vgl. Amort et al., 2022, S. 201-203). Die DSGVO gilt hier als Mittel, um nachhaltigen Datenschutz zu gewährleisten und somit mit der Ressource, Verfügungs- und Entscheidungsmacht über personenbezogene Daten schonend umzugehend. Kern des Schutzes der informationellen Selbstbestimmung ist somit die Fragestellung, inwieweit Einzelne noch autonom über Zweck, Art und Umfang ihrer eigenen personenbezogenen Daten entscheiden können (vgl. Amort et al., 2022, S. 212).

Dieser angestrebte schonende Umgang mit Verfügungs- und Entscheidungsmacht wird hier in Bezug auf die Verantwortungen der Union und des Staates, von Unternehmen und Betroffenen gesetzt. Auch wenn die Rollen in der DSGVO genau definiert werden, wie zum Beispiel die Rolle von Auftragsverarbeitenden, Verantwortlichen und Betroffenen, geht die Autorin hier eher auf die Verantwortung der Union und der Mitgliedsstaaten, von Unternehmen und von Betroffenen und Konsument*innen ein, um einen Fokus darauf zu richten.

3.2.1 Verantwortung: Union und Mitgliedsstaaten

Als übergeordnete Verantwortung des EU-Staates in Bezug auf Datenschutz steht das Recht auf Achtung des Privat- und Familienlebens in der Europäischen Menschenrechtskonvention. Darin wird geregelt, dass jedermann Anspruch auf die Achtung des Familien- und Privatlebens hat, inklusive Wohnung und Briefverkehr.[7] Da dieses Recht auch informationelle Selbstbestimmung umfasst, ist der Staat dazu verpflichtet, die Daten von Bürger*innen zu schützen (vgl. Europäische Menschenrechtskonvention, 2023, o.S.). Dies sind Handlungs- und Unterlassungspflichten, denen der Staat nachgehen muss. Dabei hat der Staat oft eine doppelte Stellung, wie im Falle von Richtlinienumsetzung, wo er einerseits verpflichtet ist, sie umzusetzen, als auch selbst Adressat der Richtlinienregelung wird. Mitgliedsstaaten in der EU setzen nicht nur nationales Recht um, sondern sind oft selbst Adressaten von EU-Verhaltensnormen, die national umgesetzt werden müssen, wenn es sich um mittelbare Anwendung handelt. Wenn es sich um unmittelbare Anwendung handelt, dann müssen Mitgliedsstaaten der EU es direkt anwenden, ohne es in nationales Recht umsetzen zu müssen, wie zum Beispiel im Falle der DSGVO (vgl. Stöggl, 2019, S. 467). Wenn jedoch der Staat seinen Handlungs- und Unterlassungspflichten nicht nachkommt, muss auch der Staat haften, wenn zum Beispiel Richtlinien von Mitgliedsstaaten nicht rechtzeitig umgesetzt werden. Bei Falschumsetzung von Richtlinien greift der EuGH ein, da Bürger*innen einen Nachteil durch die mangelhafte Umsetzung haben können (vgl. Furrer & Epiney, 1995, S. 21f.).

Nicht nur bei Richtlinien haben Mitgliedsstaaten die Verantwortung, diese in nationales Recht umzusetzen. Es werden auch in unmittelbar anwendbaren Rechtsakten, wie zum Beispiel der DSGVO, Öffnungsklauseln festgelegt, welche Mitgliedsstaaten die Möglichkeit einräumen, außerhalb der DSGVO Tatbestände zu erlauben. Das heißt wiederum auch, dass Tatbestände in der DSGVO absichtlich sehr offen formuliert wurden, und wenn Mitgliedsstaaten sie nicht strenger formulieren, führt das zu Rechtslücken und Grauzonen und kann das Schutzniveau,

[7] Vgl. Konvention zum Schutz der Menschenrechte und Grundfreiheiten StF: BGBl. Nr. 210/1958 (NR: GP VIII RV 459 AB 509 S. 63. BR: S. 137., § 8 Abs. 1.

welches die EU vorgesehen hat, aufweichen (vgl. Amort et al., 2022, S. 207). Doch was umfasst die Öffnungsspielräume der DSGVO?

Wie weit Teile einer Verordnung abweichen dürfen, kommt auf die Wortwahl an, denn eine unmittelbare Geltung umfasst einen vollständigen territorialen als auch inhaltlichen Geltungsbereich und ist verbindlich (vgl. Weiß, 2022, S. 42). Dennoch gibt es immer häufiger Durchführungsmaßnahmen von Verordnungen, bei denen vom EuGH entschieden wird, ob Mitgliedsstaaten Maßnahmen treffen dürfen, sollen oder müssen. Diese Maßnahmen müssen in jedem Fall mit der Verhältnismäßigkeit übereinstimmen und sind Entscheidungen, die einzeln geprüft werden. Dieser Öffnungsspielraum wird stark kritisiert, da dies grundsätzlich etwas ist, was Richtlinien ausmacht und nicht zum Charakter von Verordnungen gehört. Nun wird von Weiß festgestellt, dass Richtlinien in den letzten Jahren seltener beschlossen werden und dafür vermehrt Verordnungen, die wiederum Öffnungsklauseln beinhalten und somit den Charakter der Verordnung auflockern und einen Richtliniencharakter bekommen. Die DSGVO ist laut Weiß dafür ein Paradebeispiel, da sie den Wortlaut der DS-RL sogar großteils übernommen hat. Nun hat die Verordnung den Charakter, dass man sie nicht umsetzen muss, dennoch gibt es in der DSGVO viele beabsichtigte Öffnungsklauseln und implizite Durchsetzungsmaßnahmen, welche die harmonisierende Wirkung schwächen (vgl. Weiß, 2022, S. 45f.). Mitgliedsstaaten müssen sowohl die Grenzen und Ziele, als auch Grundrechte und Grundfreiheiten beachten und Durchführungsmaßnahmen keinen allzu großen Spielraum lassen. Sie werden eher als Unterstützungs- und Hilfsmaßnahmen gesehen, da über jede Anpassung der EuGH wacht. Im Gegensatz dazu haben die exklusiven Öffnungsklauseln in der DSGVO einen größeren Anpassungsspielraum, bei dem die nationale Gesetzgebung entweder alte Regelungen beibehalten oder neue erlassen kann. Diese stellt in den meisten Fällen keine Pflicht, sondern lediglich eine Option dar. Sie dienen explizit dazu, nationale Abweichungen und Modifizierungen zuzulassen und konkreter zu formulieren (vgl. Weiß, 2022, S. 51). Nun ist der Begriff der Öffnungsklausel sehr allgemein formuliert und muss, um deren Eigenschaften und Reichweite zu erschließen, differenziert werden. Müller erschließt somit fünf Kategorien der Öffnungsklauseln. Die erste wird als Anpassungsklausel beschrieben, die für Mitgliedsstaaten verpflichtend umzusetzen ist und als Regelungsauftrag mit

Zielvorgaben zu sehen ist. Solche Anpassungsklauseln finden sich in der DSGVO im Verwaltungsbereich. Aus diesem Grund lassen sich in der DSGVO im Bereich unabhängiger Aufsichtsbehörden zum Beispiel häufig nur Ziele und Leitlinien finden, da diese in nationales Recht umzusetzen sind. In Art 51 Abs. 1 (DSGVO) wird bezüglich der Aufsichtsbehörden nur definiert, dass die einzelnen Mitgliedsstaaten zur Überwachung und Anwendung eine oder mehrere Behörden einrichten müssen, die unabhängig sind, alles Weitere ist den Mitgliedsstaaten überlassen. Solche Anpassungsklauseln sind ein Grund, weshalb die DSGVO als Hybridform zwischen Verordnung und Richtlinie Kritik erfährt. Dann gibt es die Verstärkungsklausel, die es den Mitgliedsstaaten erlaubt, strenger zu regeln, und zusätzliche Anforderungen erlässt, um das Schutzniveau national zu erhöhen. Die Gestaltungsklausel ermöglicht es Mitgliedstaaten, Rechtsakte zu erlassen, die es ermöglichen, dass sowohl Anwendung als auch Durchsetzung von Unionsrecht erleichtert werden. Dies sind vor allem Bestimmungen, die spezifizieren und konkretisieren. Wie auch die Verstärkungsklausel ist auch diese nicht verpflichtend. Die bedeutendsten Gestaltungsklauseln befinden sich in der DSGVO in den Bereichen der DSFA und der Datenschutzbeauftragten. Die Verweisungsklauseln verweisen auf nationale Rechtsakte und sind für die Harmonisierungswirkung besonders bedeutend, da Mitgliedsstaaten sie selbst ausgestalten müssen und dies die harmonisierende Wirkung schwächen kann. Ein Beispiel dafür wäre die Verarbeitung von sensiblen Daten im Gesundheitsbereich, bei dem ein Artikel auf den nächsten verweist, um schlussendlich auf die nationale Gesetzgebung zu verweisen. Verweisklauseln lassen sich in der DSGVO auch bei Aufsichtsbehörden finden. Zum Schluss gibt es noch die Ausnahmeklauseln, die dafür sorgen, dass unter bestimmten Voraussetzungen Mitgliedsstaaten von zwingenden Regelungen abweichen dürfen (vgl. Weiss, 2022, 57-61). Es werden hier nicht alle Öffnungsklauseln bis ins Detail behandelt, da es sich in der DSGVO um fast 70 Öffnungsklauseln handelt.

Eine bekannte Durchführungsverordnung befindet sich im Anwendungsbereich des Datenschutzrechts, hierbei geht es um die Einwilligung zur Verarbeitung personenbezogener Daten. Nach Art 8 Abs.1 (DSGVO) ist eine Einwilligung zur Verarbeitung von personenbezogenen Daten von Kindern vor der Vollendung des 16. Lebensjahres nicht zulässig. Weiter wird formuliert, dass jeder Mitgliedsstaat die

Altersgrenze auf 13, 14 oder 15 Jahre herabsetzen darf. In Zusammenhang mit der Einwilligung gibt die DSGVO auch vor, dass die Verarbeitung von sensiblen Daten nur zugelassen wird, wenn in einer ausdrücklichen Einwilligung zugestimmt wird. Ausnahme: Es gibt in Mitgliedsstaaten ein besonderes Verbot zur Verarbeitung von Daten besonderer Kategorien. Dies bedeutet wiederum, dass die Gültigkeit der Einwilligung zur Verarbeitung personenbezogener Daten auf nationales Recht hin geprüft werden muss (vgl. Feiler & Fargo, 2022, S. 473). Österreich hat in diesem Fall im DSG (2018) das Einwilligungsalter auf die Vollendung des 14. Lebensjahres herabgesetzt (vgl. DSG § 4, Art. 2, Abs. 1). Eine Regelung, die Österreich zum Beispiel nicht umgesetzt hat, ist, dass Datenschutzorganisationen auch ohne Auftrag eines Betroffenen gegen Verantwortliche und Auftraggeber*innen mittels Klage vorgehen könnten.

Nun gehört zu den wichtigsten Öffnungsklauseln, die individuell umgesetzt werden können, das Profiling und automatisierte Entscheidungen. Speziell, ob Profiling und automatisierte Entscheidungen, die für Abschluss eines Vertrags nicht notwendig sind, auch ohne Einwilligung der Betroffenen erlaubt sind, oder ob für Betroffenenrechte zusätzliche Beschränkungen bestimmt werden, wird festgelegt Weiters ist auch wichtig, ob alle oder nur einzelne Verantwortliche einen Datenschutzbeauftragten bestellen müssen oder, ob gegen öffentliche Stellen genauso Geldbußen verhängt werden können. Außerdem wird den Mitgliedsstaaten weitestgehend selbst überlassen, die Verarbeitung von personenbezogenen Daten zu Zwecken wie Journalismus, Kunst, Wissenschaft oder Literatur zu regeln. Die Anzahl der Öffnungsklauseln führt dazu, dass die DSGVO nicht ohne die nationalen Umsetzungen gelesen werden kann. Dies führt wiederum zu einem weiteren Problem, dem Kollisionsrecht, welches regelt, welche Norm anzuwenden ist, wenn zwei Staaten aufeinandertreffen, wie zum Beispiel, wann welches Recht eines jeden Mitgliedsstaates anzuwenden ist. Problem dabei ist, dass in der DSGVO kein Kollisionsrecht geregelt ist (vgl. Feiler & Fargo, 2022, S. 7f.). Dies führt dazu, dass sich zum Beispiel Aufsichtsbehörden vorerst einmal einig werden müssen, welches Recht anzuwenden ist, was in einem Beschwerdefall Betroffenen schaden kann (vgl. Feiler & Fargo, 2022, S. 477).

Wenn nun von der Autorin darauf geachtet wird, dass die Verantwortung des Staates darin liegt, die Daten seiner Bürger*innen zu schützen, dann gilt es die Öffnungsklauseln so gut wie möglich zu nützen und im besten Fall strenger zu regeln. Dies hat Österreich zum Beispiel nicht ausreichend gemacht, indem es das Einwilligungsalter zur Verarbeitung personenbezogener Daten von 16 auf 14 herabgesetzt hat. So argumentiert Weiss, dass die Öffnungsklauseln zwar mehr Spielraum für die Mitgliedsstaaten einräumen, jedoch die Vollharmonisierung des Datenschutzrechts in der EU auf der Strecke bleibt und dass nationales Umsetzungsrecht zu einer enorm hohen Komplexität führt. Außerdem argumentiert Weiss, dass einige Öffnungsklauseln in der DSGVO derart vage formuliert sind, dass bei der nationalen Umsetzung große Rechtsunsicherheit herrscht (vgl. Weiss, 2022, S. 275f.).

Vage Formulierungen treten zum Beispiel bei der Privacy by Design und der Privacy by Default- Regelung auf. Diese sind Datenschutzregelungen in der DSGVO, die präventiv Produkte und Verfahren schon in der Gestaltung nach datenschutzrechtlichen Bestimmungen ausstatten soll. Diese Regelung beeinflusst Technikgestaltung unionsweit und bietet Kontrolle über Datenverarbeitung. Dennoch führt die Formulierung zu Problemen, da sich die Einhaltung der Pflicht an die Verantwortlichen richtet und nicht an die technischen Entwickler*innen oder Hersteller*innen, gerade bei der Privacy by Design-Regelung (vgl. Hentschel, Hornung & Jandt, 2020, S. 261). Genau diesen Kontext kritisieren Haber und Tamò-Larrieux, denn mit der bloßen Anmerkung, dass sowohl technische als auch organisatorische Maßnahmen allen Voraussetzungen der DSGVO gerecht werden müssen, ist keine Anweisung für Techniker*innen gegeben. Auch wenn die DSGVO genau formuliert, welche Risiken geschützt werden sollen und wo die zu schützenden Prioritäten liegen, ist die DSGVO weniger eine technische Anleitung für Ingenieure, sondern eher ein organisatorisches Instrument. Da die Privacy by Design-Regelung im § 25 Abs. 1 (DSGVO) Verantwortliche

> „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen (…) geeignete technische und organisatorische Maßnahmen(…)“,

entscheiden lässt, wird mit dem Wortlaut der gesamte Paragraf relativiert. Das bedeutet, dass der implementierte Datenschutz in den Händen der Verantwortlichen liegt, um Unternehmen eine Handlungsflexibilität zu gewährleisten, da jedes Produkt und jede Dienstleistung andere Anforderungen hat. Dies hat jedoch zur Folge, dass Techniker*innen selbst herausfinden müssen, wie sie datenschutzfreundliche und sichere Systeme konstruieren müssen (vgl. Haber & Tamò-Larrieux, S. 8f.).

Die Privacy by Design-Bestimmung und die Öffnungsklauseln der DSGVO zeigen laut Verfasserin dieser Arbeit, wie wichtig konkrete Formulierungen in der Judikatur sind, damit alle Akteur*innen diese auch richtig umsetzen und befolgen können. Diese konkreten Formulierungen zu finden liegt in der Verantwortung der Union, wenn es um die Formulierung der DSGVO geht und in der Verantwortung der Mitgliedsstaaten, wenn es um die Inanspruchnahme der Öffnungsklauseln und um die nationalen Anpassungsgesetze geht. Wenn nun die Verantwortlichkeit des Staates auf nachhaltigen Datenschutz bezogen wird, ist die DSGVO ein teilharmonisierendes Gerüst, das versucht, Individuen die informationelle Entscheidungsmacht wiederzugeben. Dennoch entstehen durch die vagen Formulierungen und Öffnungsklauseln derart viele Ausnahmen und ein derart hohes Maß an Komplexität, dass das Schutzniveau herabgesetzt ist. Deswegen argumentiert die Autorin der Arbeit, dass Union und Mitgliedsstaaten eine wichtige Rolle zu nachhaltigem Datenschutz spielen, die DSGVO jedoch diese Verantwortung besser widerspiegeln könnte.

3.2.2 Verantwortung: Unternehmen

Die nächste Verantwortungsinstanz sind nach Meinung der Autorin Unternehmen, die seit Einführung der DSGVO die Verantwortung übertragen bekommen haben, sich an die DSGVO zu halten und diese ordnungsgemäß anzuwenden. Hier wird auf die Verantwortung von Verantwortlichen, Auftragsverarbeitenden und auf die Rolle von Datenschutzbeauftragten eingegangen. Weiters wird ein Blick auf die Datenschutzfolgen-Abschätzung und auf Datenlecks geworfen.

Grundsätzlich müssen alle Auftragsverarbeitenden und Verantwortlichen ein Register über Verarbeitungstätigkeiten führen. Dies kann schriftlich oder

elektronisch sein. Dennoch sind Unternehmen, die weniger als 250 Mitarbeitende haben, davon ausgenommen, wenn es sich um keine sensiblen Daten handelt oder Daten nur hin und wieder verarbeitet werden, oder wenn es sich um keine strafrechtlich wichtigen Daten handelt. Wenn also ein Verzeichnis oder Register geführt werden muss, wird außerdem bei den Verzeichnissen unterschieden in welche, die, Verantwortliche führen müssen und welche, die Auftragsverarbeitende führen müssen (vgl. Feiler & Fargo, 2022, S. 22f.). Verantwortliche und Auftragsverarbeitende müssen einen Datenschutzbeauftragen bestellen, wenn die Verarbeitung von personenbezogenen Daten Teil der Kerntätigkeit ist und regelmäßige Überwachung dieser Daten erforderlich ist, oder wenn es sich um eine Behörde handelt. Zusätzlich kann es auch weitere Kategorien geben, Datenschutzbeauftragte zu bestellen, wenn es das nationale Recht vorsieht. Nichtsdestotrotz müssen auch nach den Kategorien der DSGVO alle Unternehmen, die ein datengetriebenes Geschäftsmodell haben, einen Datenschutzbeauftragten bestellen, da die Datenverarbeitung Kerngeschäft ist (vgl. Feiler & Fargo, 2022, S. 25f.). Diese besagte Öffnungsklausel im Art. 37, Abs. 4 (DSGVO) wäre nach den Definitionen von Weiss eine Verstärkungsklausel, weil die Mitgliedsstaaten strenger regeln dürften. Diese Öffnungsklausel hat Österreich im Gegensatz zu Deutschland nicht genutzt.

Doch was gehört überhaupt zu den Aufgaben von Datenschutzbeauftragten? Datenschutzbeauftragte haben eine beratende Funktion für Verantwortliche und Auftragsverarbeitende und sollen somit dafür sorgen, dass die DSGVO und individuelle interne Datenschutzregeln, insbesondere die Datenschutz-Folgenabschätzung, eingehalten werden. Dies kann jedoch eine intern beschäftigte Person oder auch eine externe Person, jeweils mit entsprechendem Fachwissen sein (vgl. Feiler & Fargo, 2022, S. 26f.) Zu den Aufgaben der Datenschutzbeauftragten gehört dass sie mit den zu zur Verfügung gestellten Ressourcen Verantwortliche und Arbeitnehmer*innen beraten, die Einhaltung der DSGVO überwachen, interne Strategien zum Schutz personenbezogener Daten sowie Schulungen prüfen (vgl. DSGVO, Art. 39). Außerdem müssen sie die Überwachung der Ausführung der DSFA begutachten und mit der jeweiligen Aufsichtsbehörde zusammenarbeiten und sie konsultieren. Der Datenschutzbeauftragte ist aber klar definiert, also weder für die Verzeichnisse noch

für die Ausführung der DSFA zuständig, sondern lediglich für die Überwachung und die Beratung (vgl. Feiler & Fargo, 2022, S. 27). Da die Anpassung der DSGVO in Unternehmen vor allem zu Beginn eine Herausforderung darstellte, waren gerade externe Datenschutzbeauftragte am Anfang kritisch zu betrachten. Denn Unternehmen tendieren dazu, sich zu sehr auf die Erfahrung von externen Datenschutzbeauftragten zu verlassen, ohne sich intern mit der Thematik auszukennen (vgl. Kremer, 2020, S. 333).

Neben dem Datenschutzbeauftragten spielt auch die Datenschutz-Folgenabschätzung eine große Rolle. Sie ist an und für sich kein Konzept, das erst durch die DSGVO entstanden ist. Denn das Konzept hatte unter dem Namen Technikfolgenabschätzung in den 1970er und 1980er Jahren seine Hochphase zur Einschätzung von neuen Großtechnologien. Es diente dazu, den Einfluss von technischen Innovationen auf die Gesellschaft und die Umwelt zu eruieren und die Risiken einzuschätzen. Seit den 1990ern wurde im Hinblick auf automatisierte Prozesse in Fabriken auch elektronische Datenverarbeitung zur Technikfolgenabschätzung ins Auge gefasst. Doch erst seit den 2000ern, durch die Zunahme von vernetzten Produkten und Dienstleistungen, die mit personenbezogenen Daten funktionieren, stehen Datenschutzanliegen im Fokus der Technikfolgenabschätzung. Durch vernetzte Produkte ist auch ein Machtgefälle entstanden, sodass User*innen diese nur zu Bedingungen der Anbieter*innen verwenden dürfen. Darum wurden DSFAs eingeführt, bei denen aber nie einheitliche Anforderungen festgesetzt oder großteils keine Verpflichtung dazu eingeführt wurden. Erst die DSGVO hat für bestimmte Unternehmen eine verpflichtende Datenschutzfolgenabschätzung eingeführt, die dazu dient, Datenflüsse und ihre Folgen nach genauen Kriterien zu untersuchen, zu bewerten und Gegenmaßnahmen zu ergreifen, um das Risiko für Betroffene so gering wie möglich zu halten. Eine DSFA hilft auch Ingenieur*innen und Entwickler*innen bei der Umsetzung der Privacy by Design-Regelungen, da sie dadurch Risiken einer technischen Entwicklung besser erkennen und anpassen können (vgl. Friedewald, 2017, S. 66f.). Doch wann muss eine DSFA durchgeführt werden?

Es muss eine DSFA hauptsächlich dann durchgeführt werden, wenn

> „(…) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (…)“ hat (DSGVO, Art. 35, Abs. 1).

Es gibt aber noch weitere Kategorien, wann eine DSFA durchzuführen ist. Wenn eine hohes Risiko besteht, wie zum Beispiel die systematische Erfassung persönlicher Teilbereiche durch automatisierte Verarbeitung, ausführliche Verarbeitung von besonderen Kategorien personenbezogener Daten und systematischer Überwachung von öffentlichen Orten, dann besteht ebenfalls die Notwendigkeit, eine DSFA zu machen (vgl. DSGVO, Art. 35, Abs. 3). Friedewald kritisiert auch hier die Wortwahl des hohen Risikos, weil dadurch Unternehmen enorm große Spielräume eingeräumt werden, was ein hohes Risiko ist und was nicht und dadurch große Unsicherheit herrscht. Ebenfalls kritisiert der Autor den Interessenskonflikt, der dadurch entsteht, dass selbst, wenn es zu DSFA kommt, sie von den gleichen Verantwortlichen und Auftragsverarbeitenden durchgeführt wird, die gleichzeitig ein wirtschaftliches Interesse and der Verarbeitung personenbezogener Daten haben und am Ergebnis das niedrige Risiko haben (vgl. Friedewald, 2017, S. 68). Doch was wird überhaupt genau gemacht bei einer DSFA?

Eine korrekte DSFA hat fünf Phasen und startet mit der Vorbereitungsphase, in der die Relevanz des Gegenstands geprüft wird, inklusive eines Prüfplans und der Zusammenstellung eines Teams. An dieser Stelle werden alle relevanten Akteure und der Rechtsgegenstand definiert. In der nächsten Phase, der Bewertungsphase, werden Betroffene konsultiert, da ihre Sichtweise besonders wichtig ist, da rein technische Expert*innen eine zu enge Sicht auf die Risiken hätten. In dieser Phase werden auch Schutzziele identifiziert. Weiters werden potentielle Angreifer*innen identifiziert und eingeschätzt, sowie der Schutzbedarf bestimmt. In dieser Phase wird das Risiko bestimmt, auf das in der nächsten reagiert wird. In der dritten Phase, der Maßnahmenphase, werden basierend auf vorherigen Erkenntnissen passende Schutzmaßnahmen ausgesucht, implementiert, dann werden sie getestet und dokumentiert. Auch die Bewertungsrisiken und deren Restrisiken werden dokumentiert. An dieser Stelle wird auch darauf geachtet, ob alle Anforderungen der DSGVO eingehalten wurden. Die Berichtphase ist die vierte, bei der die

Erstellung und Veröffentlichung des Berichts im Mittelpunkt steht (Friedewald, 2017, S. 67). Dennoch ist nach der DSGVO die Veröffentlichung der Ergebnisse nicht verpflichtend. Damit Unternehmen sicher sein können, dass die DSFA auch sinngemäß und korrekt durchgeführt wurde, sollten sie diese von einer unabhängigen Stelle prüfen lassen, um auch vorher beschriebene Interessenskonflikte zu vermeiden. Die letzte Phase ist die des Fortschreibens und Prüfens, da die DSFA eines Projekts ein laufender Prozess ist, der durchgehend überwacht werden muss. Wenn sich nämlich das Risiko ändert, muss eine neue DSFA durchgeführt werden. Verantwortliche sollten mindestens alle 3 Jahre prüfen, ob die ursprünglichen Ergebnisse mit der DSFA übereinstimmen und zusätzlich laufend kontrollieren, ob sich die Rahmenbedingungen verändert haben und somit die Schutzmaßnahmen angepasst werden müssen (vgl. Friedewald, 2017, S. 70). In einer Publikation drei Jahre später und zwei Jahre nach Einführung der DSGVO, im Jahr 2020, kritisieren Friedewald und Kolleg*innen, dass die DSFA nur etwas zum Datenschutz beitragen kann, wenn sie seriös von Verantwortlichen umgesetzt wird. Dies hängt von zwei Komponenten ab, einerseits von den Ressourcen, die Verantwortliche zu Verfügung haben und andererseits von der Bereitwilligkeit, die Ergebnisse ernst zu nehmen und Maßnahmen zu setzen, auch wenn sie negativ ausfallen (vgl. Martin et al., 2020, S. 153). Nach Meinung der Autorin bedeutet dies aber auch, dass der Schutz von personenbezogenen Daten zu großen Teilen von der Gutmütigkeit der Verantwortlichen abhängt, die auch ein wirtschaftliches Interesse an personenbezogenen Daten haben. Zum Thema nachhaltiger Datenschutz, wie er in Kapitel 3.2 definiert wurde, sieht die DSGVO zwar vor, Betroffenen informationelle Entscheidungsmacht zu geben, indem Betroffene in der Bewertungsphase konsultieren werden (vgl. DSGVO, Art. 35 Abs. 9). Dennoch müssen dies Unternehmen nicht wahrnehmen, wenn es zum Schutz öffentlicher und gewerblicher Interessen dient (vgl. Friedewald, 2017, S.69f.).

Nun wurde anhand von Datenschutzbeauftragten und der Datenschutzfolgen-Abschätzung kurz angeschnitten, welche Verantwortung Unternehmen haben, um personenbezogene Daten zu schützen. Hier wird ein Blick darauf geworfen, welche Verantwortungen Unternehmen haben, wenn es wirklich zu einem Datenleck kommt. Nach Artikel 33 Abs. 1 (DSGVO) müssen Verantwortliche bei Verletzung von Schutz personenbezogener Daten dies umgehend, im besten Fall innerhalb von

72 Stunden, an die zuständige Aufsichtsbehörde melden. Auch Auftragsverarbeitende sind dazu verpflichtet, dies sofort nach Erkenntnis der Verletzung den Verantwortlichen zu melden (DSGVO, Artikel 33, Abs. 2). Diese auch Data Breach Notification genannte Meldung muss getätigt werden, wenn ein Risiko besteht, dass Rechte und Freiheiten von natürlichen Personen gefährdet sind. Zudem müssen Betroffene nur informiert werden, wenn ein hohes Risiko besteht (vgl. Fargo und Feiler, 2022, S. 264). Rechte und Freiheiten werden dann als gefährdet eingestuft, wenn es zu einem Kontrollverlust von personenbezogenen Daten kommt und somit immaterieller, materieller oder physischer Schaden für die natürliche Person entstehen kann (vgl. Fargo und Feiler, 2022, S. 267). Kritik an der Data Breach Notification Regulierung der DSGVO kommt von einer niederländischen Studie aus dem Jahr 2018, welche die Effektivität der Data Breach Notification aus wirtschaftlicher und juristischer Perspektive untersucht hat. Dabei haben sie den sozialen Nutzen und die Kosten der Durchführung der Data Breach Notification gemessen, als auch den privaten Nutzen und die privaten Kosten. Sie kritisieren, dass Datenlecks erst ab einem gewissen datenverletzenden Schwellenwert gemeldet werden müssen und, dass Verantwortliche Datenlecks ungern melden werden, solange es keine Offenlegungspflicht gibt. Denn die Wahrscheinlichkeit, dass Behörden von selbst hinter nicht gemeldete Datenlücken kommen, ist sehr gering. Wenn Datenlecks jedoch gemeldet werden, kann dies für ein Unternehmen derart rufschädigend sein, dass sie in Konkurs getrieben werden. Die Autoren argumentieren, dass, solange der gesellschaftliche Nutzen für ein Unternehmen geringer ist als die privaten Kosten, sich daran nichts ändern wird. Sie appellieren deswegen, dass der datenverletzende Schwellenwert auf ein sozial verträgliches Niveau herabgesetzt werden sollte und somit Verantwortliche zu Meldungen veranlasst werden sollen. Weiters argumentieren sie, dass die Abschreckung durch die Sanktionierungen, die in der DSGVO beschrieben sind, nicht abschreckend genug sind, im Gegensatz zu potentiellem Rufmord. Zum Schluss empfehlen sie, dass die Schwelle zur Offenlegung gegenüber Betroffenen hoch und klar formuliert sein muss, weil die Information von geringen Datenschutzverletzungen für Individuen hohe zeitliche und finanzielle Kosten beinhaltet, um Gegenmaßnahmen zu setzen. Dafür könnte die Schwelle zur Offenlegungspflicht gegenüber Aufsichtsbehörden viel niedriger angesetzt werden,

damit schon kleinere Datenschutzverletzungen einer Aufsichtsbehörde gemeldet werden und somit die Transparenz gesteigert wird (vgl. Nieuwesteeg & Faure, 2018, S. 1232-1246).

Zusammenfassend liegt nach der Verfasserin die Verantwortung von Unternehmen darin, die Datenschutzvorkehrungen ernst zu nehmen, eventuell ernster als es die DSGVO vorschreibt. Im Falle von Österreich wäre das zum Beispiel, auch Datenschutzbeauftragte in Unternehmen einzuführen, die unter 250 Mitarbeiter*innen haben. Auch wenn sie nur eine beratende Funktion haben, wären auch externe Datenschutzbeauftragte eine gute Lösung, da die Gefahr von Interessenskonflikten geringer ist. Auch die Datenschutzfolgen-Abschätzung in die gleichen Hände zu legen, derer, die ein wirtschaftliches Interesse haben, personenbezogene Daten zu verarbeiten, ist an sich ein hohes Risiko und ist auf viel Ehrlichkeit angewiesen. Das Gleiche gilt für die Data Breach Notification-Regelung, welche so geregelt ist, dass Unternehmen derzeit größere Nachteile haben, wenn sie Datenlecks offenlegen, als wenn sie geheim halten und dafür eine Sanktionierung riskieren würden. Dementsprechend ist es noch ein langer Weg, um von nachhaltigem Datenschutz zu sprechen, da die einzige informationelle Selbstbestimmung hier in der Konsultierung im Prozess der DSFA liegt, welche Unternehmen jedoch leicht umgehen können. Ein weiterer Punkt, in dem User*innen noch selbstbestimmt über ihre Daten entscheiden können, ist die Einwilligung zur Verarbeitung personenbezogener Daten, welche im folgenden Kapitel behandelt wird.

3.2.3 Verantwortung: Konsument*innen und Betroffene

Da nicht nur Union und Staat, sowie Unternehmen eine Verantwortung gegenüber Verarbeitung personenbezogener Daten haben, sondern jede*r auch zu gewissen Teilen für die eigenen Daten verantwortlich ist, ist auch hier ein gewisses Maß an Verantwortung anzusiedeln. Doch hat diese Verantwortung Grenzen, wie in diesem Abschnitt beleuchtet wird.

Um auf die Verantwortung von Betroffenen und Konsument*innen einzugehen, muss vorher das unionsrechtliche Verbraucherleitbild geklärt werden, um zu wissen, von welchen Bürger*innen oder in dem Fall Verbraucher*innen die EU in

der Gesetzgebung ausgeht. Nach Schmitt gibt es verschiedene Kontexte, in denen das Verbraucherleitbild definiert wird, doch in der Rechtswissenschaft kommt das Verbraucherleitbild aus den Rechtsprechungen des EuGH zu den Grundfreiheiten. Damit wird ein Rollenbild definiert und mit Werten aufgeladen, welches einen Personenkreis widerspiegeln soll, dem wiederum der Verbraucherschutz gilt. Es dient dazu, Eigenschaften, Merkmale und Kompetenzen von Konsument*innen zusammenzufassen, um Regulierungsniveaus zu bestimmen. Aus diesem Grund hat im Jahr 1998 der EuGH den Durchschnittsverbraucher definiert, der sowohl durchschnittlich informiert als auch durchschnittlich aufmerksam und verständig ist. Dies stellt in der EU die Verbraucherleitbildformel dar (vgl. Schmitt, 2018, S. 52f.). Diese Definition wird jedoch von der Verhaltensökonomie stark kritisiert, da sie auf Annahmen basiert, dass es sich um Konsument*innen handelt, die selbstverantwortlich sind und die sich mit der Information, welche sie zur Verfügung gestellt bekommen, stets rational verhalten. Das bedeutet, dass davon ausgegangen wird, dass Konsument*innen die Informationen nutzen und dann eine Entscheidung treffen. Forschungen der Verhaltensökonomie zeigen, dass Konsument*innen Informationen nicht unbedingt genau beachten, wahrnehmen oder verstehen. Gerade in der jetzigen Zeit ist die Informationsflut derart hoch, dass die Annahme von rational entscheidenden Verbraucher*innen fragwürdig ist, da sie eher unterdurchschnittlich informiert sind und das Schutzniveau somit höher sein müsste. Das bedeutet also, dass der unionsrechtliche durchschnittliche Verbraucher nicht mit dem Verbraucher*innenverhalten aus Forschungsergebnissen der Verhaltensökonomie zusammenpasst (vgl. Schmitt, 2018, S.102f.). Mit dieser Klarstellung wird nun ein genauerer Blick auf eine der Datenverarbeitungsvoraussetzungen geworfen: Die Einwilligung.

Einer der Gründe, wann personenbezogene Daten rechtmäßig verarbeitet werden dürfen, ist, die Einwilligung für einen oder mehrere gewisse Zwecke (vgl. DSGVO. Art. 6, Abs. 1). Dabei müssen die einzelnen Zwecke müssen genau beschrieben werden. Die Einwilligung ist auch nur dann gültig, wenn sie auf freiwilliger Basis geschieht, auf informierende Art und Weise, und sie muss jederzeit widerrufbar sein. Dabei sollte für jeden Verarbeitungsvorgang eine eigene Einwilligung eingeholt werden, was bedeutet, dass es in einer Einwilligung für jeden einzelnen Vorgang eine Checkbox geben muss. Eine allgemeine Einwilligung ohne Zweckbindung ist

außerdem ungültig (vgl. Fargo & Feiler, 2022, S. 13). Weiters bedarf es für die Verarbeitung von sensiblen Daten nochmals einer ausdrücklichen Einwilligung. Diese Daten sind nach Art. 9 Abs.1 (DSGVO) eine besondere Kategorie, unter die, zum Beispiel ethnische Herkunft, Weltanschauung, politische Einstellung sowie Sexualleben und Gesundheitsdaten, oder auch biometrische Daten fallen. Besonders kritisch zu betrachten ist, dass die Einwilligung „in informierter Weise und unmissverständlich“ (DSGVO, Art. 9, Abs. 32) erteilt wird. Nicht nur das schon besprochene erforderliche Mindestalter zur Einwilligung spielt eine Rolle, sondern auch der Wissensstand ist hier zu hinterfragen. Deshalb muss eine Einwilligung, damit sie Gültigkeit erlangt, Betroffene aufklären, warum, von wem, zu welchem Zweck und Umfang personenbezogenen Daten verarbeitet werden, welche Risiken damit verbunden sind und welche Rechte Betroffene haben. In Artikel 13 und 14 (DSGVO) werden außerdem Unterrichtungspflichten festgelegt, die Verantwortliche gegenüber Betroffenen haben, da es für Betroffene meist auch schwer zu erfassen ist, in welchem Ausmaß ihre personenbezogenen Daten verarbeitet werden (vgl. Bunnenberg, 2020, S. 40f.). Wegen dieses Risikos des mangelnden Wissenstandes muss eine Einwilligung auch in klarer und leicht verständlicher Sprache formuliert sein (vgl. Feiler & Fargo, S. 13). Für Bunnenberg ist die Einwilligung der Schlüssel, um durch anderweitige Verbote der DSGVO personenbezogene Daten zu verarbeiten. So wird argumentiert, dass die Einwilligung durch die von Verantwortlichen ausgesuchten Angaben in der Erklärung ihnen nahezu unbeschränkter Zugang zu personenbezogenen Daten gibt. Gerade in der Wirtschaft und zu kommerziellen Zwecken wird die Einwilligung kritisiert, da sie auf einem Machtgefälle basiert, bei dem Anbieter*innen entscheiden können, Betroffenen den Zugang zu Produkten und Dienstleistungen zu verwehren. Damit wird einerseits das Prinzip der Selbstbestimmung und auch das der Freiwilligkeit zunichte gemacht (vgl. Bunnenberg, 2020, S.69f.). Auch diese Problematik findet ihre Ursprünge in der vagen Formulierung in der DSGVO, denn demnach muss geprüft werden,

> „(…) ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“(DSGVO, Abs 7. Art. 4)

Erst in den Erwägungsgründen der DSGVO wird genau formuliert, dass die Einwilligung bei einem Machtverhältnis nicht gültig ist (vgl. DSGVO, Erwgrd. 43). Bunnenberg legt diese Regelung streng aus und kommt zu dem Schluss, dass, wenn Leistung und Verarbeitung durch die DSGVO nicht gekoppelt sein dürfen, sich auch datenlastige Geschäftsmodelle nicht auf Einwilligungen stützen können, weil die mangelnde Freiwilligkeit sie ungültig werden lässt. Eine derart strenge Auslegung wäre jedoch auch für Betroffene nicht gut, da sich Verantwortliche im Notfall auf „berechtigte Interessen“ (DSGVO, Art 6, Abs. 1f) zur Verarbeitung personenbezogener Daten stützen könnten. Dadurch wären die Schutzvorgaben und die inhärente Transparenz der Einwilligung zunichte gemacht (vgl. Bunnenberg, S. 72ff.). Auch wenn die Einwilligung für Transparenz sorgt, indem Unternehmen jede Art der Verarbeitung angeben müssen, inklusive den Zweck deren Verarbeitung, ist, nach der Autorin dieser Arbeit, der durchschnittliche Verbraucher als Verbraucherleitbild auf EU-Ebene fragwürdig. Gerade im Hinblick auf die schon in Kapitel 3. 2. 1 erwähnte Altersgrenze von 16 Jahren, die national auch auf 13 Jahre herabgesetzt werden darf (vgl. DSGVO, Art. 7) ist es kritisch zu betrachten, inwieweit 13 - Jährige nach unionsrechtlicher Definition nämlich als durchschnittlich informiert, aufmerksam und verständig gelten können. Hierbei könnte das Schutzniveau auch im Sinne der Ergebnisse der Verhaltensökonomie erhöht werden. Gerade wenn es um die Kontrolle der eigenen personenbezogenen Daten und informationelle Selbstbestimmung geht, ist es wichtig, dass die Kontrolle der eigenen Daten auch in einem Verbraucherschutzkontext zu sehen ist.

Die Problematik des Verbraucherschutzleitbildes geht auch in die Privacy by Design-Regelung hinein. Denn seit Einführung der DSGVO und dem Wunsch nach datenschutzkonformen Produkten nutzen Plattformbetreiber*innen wie Meta und Google dies aus, um damit zu werben, User*innen Kontrolle über ihre Daten zu geben. Da viele User*innen weder Software noch Hardware in ihrer Gänze verstehen, wird ihnen oft nur Kontrolle über ihre eigenen Daten vorgespielt, wie zum Beispiel Fitnessuhren, die oft lokale Speicherung der Daten nicht erlauben. Das bedeutet, dass zusätzliche Apps und andere Hardwareprodukte der Anbieter*innen verwendet werden müssen, um die Daten zu übermitteln. User*innen sollte deswegen die Kontrolle ihrer Daten gegeben werden und nicht darauf vertrauen müssen, dass Hersteller*innen Daten nicht unrechtmäßig verarbeiten (vgl.

Hentschel et al., 2020, S. 261ff.). Mehr Kontrolle über die eigenen Daten wäre, nach der Verfasserin der Arbeit, auch im Sinne des nachhaltigen Datenschutzes, wie er in der Arbeit definiert wurde. Gerade bei Dienstleistungen, bei denen es nicht notwendig ist, Daten in einer Cloud zu speichern, sollten Unternehmen im Sinne der Datenminimierung das auch tun und sich nicht Software einfallen lassen, damit sie an personenbezogene Daten gelangen. Auch hier müsste das Verbraucherschutzniveau hinauf gesetzt werden.

Ein weiteres Beispiel für den Wissensstand von Verbraucher*innen zeigt auch die Studie von Pleger et al. (2021), welche 1000 Deutsche und Briten nach ihrer Wahrnehmung zu Datenschutz und Datensicherheit befragt haben. Dabei kam heraus, dass sich Deutsche und Briten große Sorgen darüber machen, dass ihre Daten betrügerisch verwendet werden, gestohlen werden und dass Unternehmen Daten ausbeuten, um damit Profit zu machen. Sowohl bei den Deutschen als auch bei den Briten haben bei der Aussage, dass Konsument*innen die Kontrolle über ihre persönlichen Informationen, welche von Unternehmen gesammelt und verwendet werden, behalten wollen, über 80% zugestimmt. Gleichzeitig hat die Medienanalyse zum Verständnis von Datensicherheit und Datenschutz gezeigt, dass die rechtlichen und technischen Definitionen stark von denen der Bürger*innen, abweichen. Die Medienanalyse hat auch gezeigt, dass viel Information über Datensicherheit und Datenschutz auf eine Weise berichtet wird, die Bürger*innen nicht verstehen. Daraus schließen die Autor*innen, dass der Staat die Verantwortung trägt, Informationen zu Datenschutz und Datensicherheit Bürger*innen zur Verfügung zu stellen, die auch verstanden werden (vgl. Pleger, Guirguis und Mertes, S. 9f.). Zwar ist Großbritannien nicht Teil der EU und vom sachlichen Geltungsbereich ausgenommen, doch spielen die Ergebnisse der 479 Deutschen eine Rolle, da Deutschland sich auch an die sachliche Anwendung der DSGVO halten muss. Auch aus diesen Ergebnissen schließt die Verfasserin dieser Arbeit, dass der durchschnittlich informierte Bürger eher unterdurchschnittlich informiert ist und deswegen, wie schon erwähnt, das Schutzniveau und der Grad der Information seitens des Staates gehoben werden müssten.

An dieser Stelle muss noch erwähnt werden, dass Betroffene ein gewisses Maß an Kontrolle haben, einerseits, in dem, was sie an Daten zur Verfügung stellen, und sie

haben stets ein Widerrufsrecht. Betroffene dürfen jederzeit das Recht in Anspruch nehmen, die Einwilligung zu widerrufen. Dazu muss die Person auch in Kenntnis gesetzt sein und der Widerruf muss einfach durchführbar sein (vgl. DSGVO, Art. 7, Abs.3). Neben diesem Recht werden in der DSGVO Betroffenen auch noch weitere Rechte gegenüber Verantwortlichen zugesprochen, wie das Recht auf Auskunft (vgl. DSGVO, Art. 15), welches bedeutet, dass Verantwortliche innerhalb eines Monats Betroffenen Auskunft geben müssen, ob personenbezogene Daten verarbeitet werden und welche. Außerdem gibt es das Recht auf Datenübertragung, wobei betroffene Personen unter bestimmten Voraussetzungen das Recht haben, ihre eigenen personenbezogenen Daten zu erhalten und diese auch anderen Verantwortlichen übermitteln zu können (vgl. DSGVO, Art. 20). Weiters haben Betroffene auch ein Recht darauf, dass ihre Daten unverzüglich berichtigt werden (vgl. DSGVO, Art.16) und ein Recht auf Löschung der Daten, wenn dies erwünscht ist. Speziell wenn es um den Widerruf der Einwilligung geht, ist das wichtig, da sich Verantwortliche auch unverzüglich darum kümmern müssen, dass die Daten auch gegenüber Dritten gelöscht werden (vgl. DSGVO, Art. 17). Die Einschränkung der Verarbeitung gibt außerdem Betroffenen das Recht, ihre Daten vor weiterer Verarbeitung zu schützen (vgl. DSGVO, Art. 18). Zum Schluss haben, wie schon erwähnt, Betroffene auch ein Recht auf Widerspruch (vgl. DSGVO Art. 21), was besonders dann wichtig ist, wenn Verantwortliche die Verarbeitung von personenbezogenen Daten nicht mit einer Einwilligung durchführen, sondern mit dem Argument des öffentlichen Interesses (vgl. Fargo & Feiler, 2022, S. 17f.).

Trotz der vielen eingeräumten Betroffenenrechte, welche die DSGVO eingeräumt hat, muss bedacht werden, dass diese Paragraphen von einem juristischen Verbraucherleitbild ausgehen und nicht von einem verhaltensökonomischen.

Die Ergebnisse der drei Verantwortungskapitel zeigen, dass die Grenzen bei der Verantwortung von Betroffenen recht schnell erreicht sind. Zwar haben sie eine Kontrolle darüber, wem und in welchem Kontext sie ihre Daten zur Verfügung stellen, aber sobald sie ihre Daten zur Verfügung gestellt haben, haben Betroffene eine mangelnde Kontrolle über die eigenen Daten, da oft das Wissen und die Informationen fehlen. Die einzige wirklich Verantwortung bei Betroffenen liegt darin, sich zu informieren, und hier muss die Information auf eine Weise bereitgestellt

werden, dass sie durchschnittliche informierte Bürger*innen wirklich versteht. Dies liegt wiederum in der Verantwortung von Plattformen und Unternehmen. Eine große Verantwortung haben Unternehmen und Verantwortliche, welche die rechtlichen Anweisungen befolgen und ihnen nachgehen müssen. Die Verantwortung ist deswegen groß, da sie entscheiden können, ob mit Daten konform oder nicht konform umgegangen wird. Es sollten daher nicht die Grauzonen in der Judikatur oder der Interpretationsspielraum der Wortwahl ausgenutzt werden, um wieder wirtschaftliche Vorteile durch übermäßige Datenverarbeitung zu erlangen. Diese Spielräume zu schaffen liegt, wenn man es genauer betrachtet, wiederum in der Verantwortung der Union und der Mitgliedstaaten. Die Europäische Union und die Mitgliedsstaaten haben auch eine große Verantwortung, nämlich, bestmöglichen Schutz den Betroffenen und bestmögliche Anweisung den Verantwortlichen und Auftragsverarbeitenden gegenüber zu bieten. Dies ist nach der Analyse nicht unbedingt geschehen, was sowohl der stark interpretierbaren Wortwahl geschuldet ist, als auch den vielen Öffnungsklauseln.

3.3 Sanktionierung bei Verstoß gegen die DSGVO

Ein großer Unterschied zu den Vorgängern der DSGVO ist die Sanktionierung, die allein schon für eine größere Sensibilisierung mit dem Umgang mit Daten geführt hat, da diese auch wirklich Verantwortliche zu Verantwortung ziehen (vgl. Feiler & Fargo, 2022, S. 1). Grundsätzlich hat

> „ (1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.
>
> (2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.“ (DSA, Art. 77)

Das bedeutet, dass sich jede Person bei einer Aufsichtsbehörde im eigenen Mitgliedsstaat über den Missbrauch der eigenen personenbezogenen Daten beschweren kann und diese Aufsichtsbehörde die betroffene Person über den Verlauf der Beschwerde auf dem Laufenden hält. Dies bedeutet aber gleichzeitig, dass die Beschwerde nur im Nachhinein eingebracht werden kann und nicht auf

Verdacht, dass jemand Daten unrechtmäßig verarbeiten könnte (vgl. Feiler & Fargo, 2022, S. 422). Wichtig zu erwähnen ist außerdem noch, dass

> „(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller, Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“ (DSGVO, Art. 82)

Das heißt, Personen, denen Schaden durch unrechtmäßige Verarbeitung von Daten zugefügt wurde, sollen von den Verantwortlichen also auch einen Schadensersatz bekommen. Mit materiellem Schaden ist hier entweder Gewinnverlust, oder wenn der Wert von Vermögensgütern vermindert wird, auch positiver Schaden genannt, gemeint. Mit immateriellem Schaden ist vor allem das persönliche Befinden gemeint, wie zum Beispiel negative Gefühle, die ausgelöst wurden, sowie eine persönliche Kränkung. Nach diversen Rechtsprechungen bezüglich immateriellen Schadens des Obersten Gerichtshofes hat sich die Höhe der Geldbuße zwischen 500 und 2000 Euro etabliert (vgl. Feiler & Fargo, 2022, S. 438). Wichtig zu erwähnen ist, dass sich an die Bestimmungen der DSGVO sowohl natürliche als auch juristische Personen halten müssen, dennoch werden gegenüber natürlichen Personen vor allem bei geringfügigen Verstößen und bei unverhältnismäßiger Belastung auch Verwarnungen ausgesprochen. Trotzdem wurden Sanktionierungen und Geldbußen durch Einführung der DSGVO stark angehoben. Wenn also die Pflichten von Verantwortlichen und Auftragsverarbeitenden der Zertifizierungs- oder Überwachungsstelle nicht eingehalten werden, dann kann dies eine Geldbuße von 10 Millionen Euro oder 2% des Jahresumsatzes im Falle eines Unternehmens bedeuten. Wenn gegen die Grundsätze der Datenverarbeitung inklusive Einwilligung, Rechte des Betroffenen, die Übermittlung von Daten an ein Drittland, alle Pflichten nach den Rechtsvorschriften der Mitgliedsstaaten oder bei Nichteinhalten von Anweisungen oder Beschränkungen der Aufsichtsbehörde verstoßen wird, kann dies zu Geldbußen von bis zu 20 Millionen Euro oder im Falle eines Unternehmens 4% des Jahresumsatzes bedeuten. Bei der Abwägung des Verstoßes wird je nach Schwere, Vorsätzlichkeit oder Fahrlässigkeit, Maßnahmen, Grad der Verantwortung, frühere Verstöße und die Art der personenbezogenen Daten entschieden. Auch die Zusammenarbeit mit der Aufsichtsbehörde, die Art und Weise des Verstoßes, die Einhaltung von Maßnahmen und Verhaltensregeln, oder ob durch den Verstoß

finanzielle Vorteile erzielt wurden, spielt eine Rolle. Basierend auf den genannten Aspekten wird individuell entschieden, welches Ausmaß der Verstoß hatte und darauf basierend wird eine Geldbuße verhängt (vgl. Feiler & Fargo, 2022, S. 440-443).

Durch diese empfindlichen Geldbußen hat der Konzern Meta im Mai 2023 mit 1.2 Milliarden Euro die höchste Geldbuße seit Einführung der DSGVO bekommen. Die Begründung dafür ist, dass Facebook mit einer Standardvertragsklausel personenbezogene Daten von EU-Bürger*innen seit Juli 2020 an die USA übermittelt hat. Meta wurde dazu aufgefordert, seinen Datentransfer mit der DSGVO zu vereinbaren. Dieser Fall ist nach Andrea Jelinek, der Vorsitzenden der Europäischen Datenschutzbehörde, besonders schwerwiegend, da diese Datenübermittlung mit Millionen von Nutzer*innendaten systematisch, wiederholt und kontinuierlich durchgeführt wurde (vgl. European Data Protection Board, 2023, o.S.). Aber nicht nur Meta musste große Summen wegen Verstoßes gegen die DSGVO zahlen. Laut Statista gehören zu den 10 Firmen mit den höchsten Geldstrafen, die seit Einführung der DSGVO verhängt wurden, die Unternehmen Meta, Amazon und Google, wobei Meta mit einzelnen verhängten Geldbußen gegen Facebook, Instagram und WhatsApp weitaus dominiert (vgl. Statista, 2023, o.S.).

Im Gegensatz zum DSG 2000 sind die Geldbußen und Sanktionierungen durch die DSGVO deutlich intensiver geworden. Im DSG 2000 müssen sich jene, die sich widerrechtlichen Zugang zu Daten verschafft haben oder vorsätzlich Daten vermittelt haben oder die gegen das Datengeheimnis verstoßen haben, verantworten und mit Sanktionierungen rechnen. Außerdem gilt dies auch für jene, die Daten auch bei einem Urteil oder Bescheid nicht richtiggestellt haben, weiter verwendet oder nicht gelöscht haben, oder jene, die Daten vorsätzlich löschen. All diese Fälle mussten mit einer Geldbuße von bis zu 25.000 Euro rechnen. Zudem wurde im DSG 2000 auch Datenermittlung, -vermittlung oder -übermittlung ohne die Meldepflicht zu erfüllen oder Datenübermittlung ins Ausland ohne Genehmigung der Datenschutzbehörde mit bis zu 10. 000 Euro sanktioniert. Auch bei einem Verstoß gegen die Offenlegungs- und Informationspflichten, oder Außerachtlassen der Sicherheitsmaßnahmen oder beim Nichtlöschen von Daten trotz Löschfrist, konnte dies zu einem Bußgeld von 10. 000 Euro führen. Wer nicht zeitgerecht richtigstellte,

Auskunft gab oder löschte, musste mit einer Verwaltungsstrafe von bis zu 500 Euro rechnen.[8] Da jedoch im Art. 83 (DSGVO) auch Öffnungsklauseln enthalten sind, hat Österreich beschlossen, sie zu nutzen und im DSG weitere Bedingungen der unrechtmäßigen Datenverarbeitung zu definieren, worin unter anderem definiert wird, dass auch widerrechtlicher Zugang zu Datenverarbeitung oder der Zugang zu Daten unter Vortäuschung falscher Tatsachen Geldstrafen von bis zu 50. 000 Euro ergibt. Neben dem Lob, dass die Sanktionierungen der DSGVO wirken, wird die Diskrepanz zwischen Österreich und der DSGVO auch kritisiert. Denn einerseits sieht die DSGVO vor, schon erstmalige Vergehen hart zu bestrafen, wohingegen Österreich im § 11 (DSG) definiert hat, dass die Datenschutzbehörde bei Erstvergehen in erster Linie eine Verwarnung aussprechen soll (vgl. Holzer, 2019, S. 27).

Dies waren in den Fällen der DSGVO, des DSG 2000 und des DSG nur die Verwaltungsstrafen, und allein daran kann schon erkannt werden, dass die Höhe der Strafen der DSGVO deutlich abschreckender ist.. Dennoch ist es auch hier wieder problematisch, dass Mitgliedsstaaten selbst die DSGVO und deren Wirkung schwächen können. Auf der anderen Seite könnte argumentiert werden, dass Österreich diesen Weg der Verwarnung gewählt hat, um klein- und mittelständische Unternehmen zu entlasten, da diese weniger Ressourcen, aber den gleichen Aufwand haben, im Vergleich zu großen Unternehmen, um die Maßnahmen der DSGVO umzusetzen (vgl. Schmidhofer, 2019, S, 68).

[8] Vgl. Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl. I Nr. 165/1999, Fassung vom 17. August 1999, § 52, Abs. 1-2a.

3.4 Zwischenfazit DSGVO

Zusammenfassend war es eine lange Reise zwischen den Anfängen und ersten Ideen des Datenschutzes in Österreich bis zur EU-weiten Regelung, der DSGVO. Dabei wurde geklärt, dass sich die Anfänge des Datenschutzes im ABGB und im StGG in Österreich finden ließen, bis dann im Jahr 1980 das Datenschutzgesetz in Kraft trat, welches durch die EU- Datenschutzrichtlinie erweitert wurde. Dann trat im Jahr 1995 die Datenschutz-Richtlinie in Kraft und über 20 Jahre später im Jahr 2018 wurde die DSGVO eingeführt, die seitdem unmittelbar anwendbar ist. Weiters wurde geklärt, was überhaupt nachhaltiger Datenschutz ist, und es wurde in einzelnen Kapitelabschnitten eruiert, dass zum Schutz personenbezogener Daten Union und der Staat eine Verantwortung haben, die Daten von EU-Bürger*innen zu schützen, indem im Fall der DSGVO, Öffnungsklauseln national geregelt und vage Formulierungen vermieden werden. In diesem Zusammenhang wurde auch geklärt, welche Arten von Öffnungsklauseln es gibt und vereinzelt wurde eruiert, wie Österreich sie umgesetzt hat. Bei den Verantwortungen von Unternehmen wurde näher auf die Rollen des Auftragsverarbeiters und die der Verantwortlichen eingegangen und vor allem auf die Privacy by Design- Bestimmungen sowie auf den Ursprung und die Datenschutzfolgenabschätzung und deren Schritte. Außerdem wurde auch die Rolle von Datenschutzbeauftragten sowie das Handeln bei Datenlecks geklärt. Weiters wurde auch die Verantwortung seitens der Betroffenen und Konsument*innen angeschnitten, indem analysiert wurde, woher das EU-Verbraucherleitbild kommt und ob dies der Realität entspricht. In diesem Zusammenhang wurde auch auf die Vor- und Nachteile der Einwilligungserklärung eingegangen. Zum Schluss wurden die Sanktionierungen der DSGVO im Vergleich zum DSG 2000 herausgearbeitet, die gezeigt haben, dass die DSGVO eine größere Abschreckung durch die Höhe der Geldbußen hat. Doch wie sich hier herausgestellt hat, zeigt die DSGVO nicht unbedingt eine abschreckende Wirkung auf millionenschwere Plattformanbieter*innen wie Meta.

Deswegen wird in den folgenden Abschnitten der Digital Servies Act näher beleuchtet, angefangen mit der Entwicklung der E-Commerce Richtlinie bis zum Digital Services Act.

4. Von der E-Commerce Richtline zum Digital Services Act

In diesem Kapitel werden juristische Veränderungen, welche der Digital Services Act verursacht, beleuchtet, angefangen mit seinem Ursprung in der E-Commerce Richtlinie. Weiters wird erläutert, was die Ziele des Digital Services Acts sind und wie der EU Akt aufgebaut ist. Dabei wird hauptsächlich der durch den DSA entstehende Verantwortungsbereich der Online-Plattformen betrachtet. Weiteres wird eruiert, welche Arten von Intermediären die EU definiert hat und wer welche Regelungen einhalten muss. Dann wird noch kurz auf die neuen Sanktionierungen durch den DSA eingegangen. Zum Schluss wird erklärt, in welchen juristischen Aspekten der DSA die DSGVO zum Schutz personenbezogener Daten ergänzt. Anschließend wird am DSA auch Kritik geübt und ein Vergleich zwischen der DSGVO und dem DSA gezogen.

4.1 Die E-Commerce Richtlinie

Die E-Commerce Richtlinie wurde im Jahr 2000 auf Rat der EU-Kommission eingeführt. Diese hatte das Ziel, die Dienste der Informationsgesellschaft weiterzuentwickeln und ohne Binnenmarktgrenzen einen EU-weiten Rechtsrahmen im digitalen Markt zum freien Verkehr von Waren und Dienstleistungen in der EU zu schaffen.[9] Diese Richtlinie war bis zum 17. Jänner 2002 nach Art. 22 (EC-RL) in nationales Recht umzusetzen. Wichtig zu erwähnen ist hierbei noch der räumliche und sachliche Anwendungsbereich, denn der räumliche Anwendungsbereich betraf nur Anbieter*innen, welche auch einen Sitz in der EU hatten, mit dem Plan, sich trotzdem mit dem nicht-europäischen Wirtschaftsräumen abzustimmen (vgl. EC-RL, Erwgrd. 61). Beim sachlichen Anwendungsbereich steht in der EC-RL hingegen der freie Verkehr von digitalen Diensten zwischen Mitgliedsstaaten im Vordergrund (vgl. EC-RL, Erwgrd. 8). In Österreich wurde die Richtlinie in das E-Commerce Gesetz im Jahr 2002 umgesetzt und es wurde vorwiegend übernommen.[10] Da es seit dieser

[9] Vgl. Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Amtsblatt Nr. L 178, Fassung vom 17.07.2022, Erwgrd. 1.

[10] Vgl. Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), BGBl I Nr 152/2001 idF BGBl I Nr 148/2020., Fassung vom 21. Dezember 2001, § 28.

Richtlinie nur geringe Anpassungen in der Judikatur gab, aber sich digitale Dienste in den letzten 20 Jahren rasant weiterentwickelt haben, wird der DSA schon lange erwartet, welcher nicht nur Anpassungen an der EC-RL vornimmt, sondern ein völlig neues Regelwerk schafft. Es regelt die Verantwortung von Anbieter*innen digitaler Dienste somit neu (vgl. Juranek, 2022, S. 79).

4.2. Der Digital Services Act

Der Digital Services Act wird auf Deutsch das Gesetz der digitalen Dienste genannt. Der DSA gilt für alle Vermittlungsdienste, die einen Einfluss auf die EU haben, unabhängig davon, ob sie einen Sitz in der EU haben oder nicht. Das Regelwerk besteht aus zwei Teilen, auf der einen Seite dem Digital Services Act, welcher digitale Vermittlungsdienste reguliert und andererseits aus dem Digital Markets Act, kurz DMA, welcher digitale Märkte reguliert. Zusammen verfolgen sie zwei Hauptziele, nämlich auf der einen Seite das Erreichen eines sicheren digitalen Raums, indem die Grundrechte aller Nutzer*innen geschützt werden. Auf der anderen Seite steht das Ziel, gleiche Wettbewerbsbedingungen sowohl in der EU als auch auf der restlichen Welt zu schaffen und somit Innovation und Wettbewerbsfähigkeit zu fördern. Nun ist der Begriff der digitalen Dienste ein großer und kann von Website bis zu ausgeklügelter Online-Infrastruktur alles bedeuten. Der DSA bezieht sich klar hauptsächlich auf Plattformen und Online-Vermittlerdienste wie zum Beispiel soziale Netzwerke, Reise- sowie Unterkunftsplattformen. Der DMA hingegen bezieht sich auf Gatekeeper-Online-Plattformen, welche den Zugang zu Inhalten steuern und beeinflussen können. Dies ist notwendig, da digitale Dienstleistungen auch den Handel von illegalen Waren, Dienstleistungen und Inhalten international erleichtert haben und wenige große Plattformen über den digitalen Markt bestimmen. Im Juli 2022 wurde dann das Gesetz über den DSA und den DMA beschlossen, ab 17. Februar 2024 ist der DSA und seit 2. Mai 2023 ist der DMA unmittelbar in allen Mitgliedsstaaten anwendbar (vgl. EU-Kommission, 2023a, o. S.). Auch wenn der DMA wichtige Regulierungen schafft, wird er in dieser Arbeit nicht in der Intensität behandelt wie der DSA, da dies sonst den Rahmen der Arbeit sprengen würde. Doch auch vor der unmittelbaren Anwendung gab es schon Etappen, die einzuhalten waren, weswegen im Februar 2023 Online-Plattformen und Suchmaschinen die Anzahl ihrer aktiven Nutzer*innen

veröffentlichen mussten. Dies dient dazu einzuschätzen welche Plattformen sehr große Online-Plattformen sind, kurz VLOPs und welche Suchmaschinen sehr große Online-Suchmaschinen sind, kurz VLOSE genannt. Diese sehr großen Anbieter*innen müssen eine Risikobewertung schon am 25. August 2023, vor der gänzlichen unmittelbaren Anwendung, durchgeführt haben (vgl. EU-Kommission, 2023a, o. S.). Für alle anderen Vermittlerdienste gilt die vollständige Anwendung erst ab dann. Genauso wie bei der DSGVO spielt im Anwendungsbereich der Sitz des Vermittlungsdienstes keine Rolle mehr, er muss nur eine ausschlaggebende Verbindung zur Europäischen Union haben (vgl. Rössel, 2023, S. 93).

4.3 Der DSA: Intermediäre in der Verantwortung

Das Gesetz der digitalen Dienste bietet einen neuen Rahmen für Online-Plattformen und Online-Suchmaschinen und überträgt ihnen mit neuen Sorgfaltspflichten auch die größte Verantwortung. Was der Digital Services Act schafft, ist vier Unterteilungen der Dienstanbieter*innen je nach Größe, Rolle und Auswirkungen. Die erste Kategorie sind Vermittlungsdienste, die über eine Infrastruktur im Netz verfügen, was Internetanbieter*innen wie zum Beispiel Hot Spots, VPN oder Emails sind. Als zweite Kategorie wurden Hostingdienste definiert, wie zum Beispiel Webhosting Dienste oder Cloudcomputing. Dann kommen Online-Plattformen, welche Verkäufer*innen und Konsument*innen miteinander verbinden. Darunter fallen Social Media Plattformen, Online-Marktplätze sowie Plattformen mit kollaborativer Wirtschaft, welche auf der Partizipation der Gesellschaft basieren. Zum Schluss kommen die sehr großen Online-Plattformen, also die VLOPS und VLOSE, welche sich dadurch auszeichnen, dass sie mehr als 10% von 450 Millionen Verbraucher*innen erreichen. Durch diese Größe werden sie als besonders risikoreich für illegale Inhalte und als potentiell schädlich für die Gesellschaft eingeschätzt. Wenn Suchmaschinen jedoch nicht in die Kategorie der ganz großen Plattformen fallen, gehören sie automatisch zu der Kategorie der Vermittler. Wie in Abbildung 1 visualisiert, sind die durch die Kategorie beschlossenen Regulierungen kumulierend, was bedeutet, dass sich der innerste Bereich, die VLOPs und die VLOSE an die meisten und strengsten Regelungen halten müssen (vgl. Rössel, 2023, S. 94). Welche Regelungen müssen nun Intermediäre einhalten?

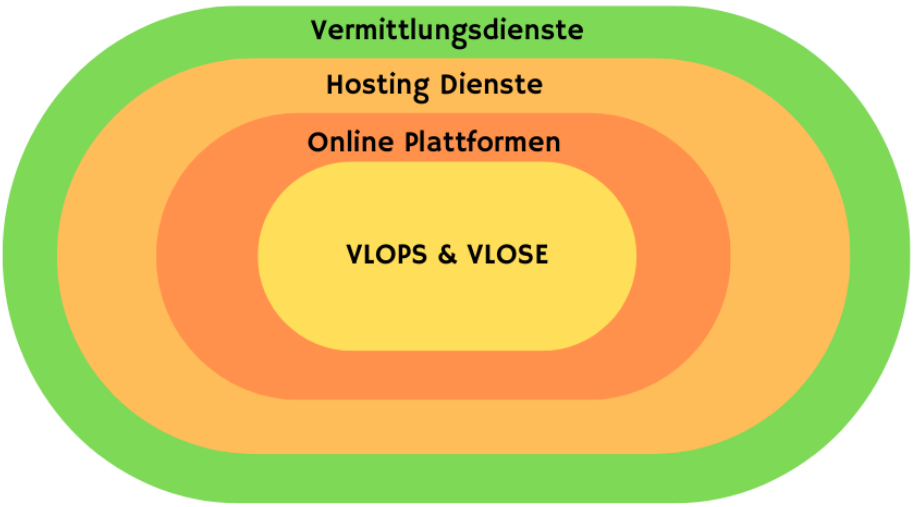

Abb. 1: Kategorien von Digitalen Dienstleistern des DSA (Eigendarstellung angelehnt an EU-Kommission, 2023b, o. S.)

4.3.1 Vermittlungsdienste, Hostingdienste, Online-Plattformen und VLOPS

In diesem Abschnitt wird geklärt, welche Pflichten auf die vier verschiedenen Kategorien der Intermediären zukommen und was sich dahingehend verändern wird, angefangen mit Vermittlungsdiensten.

Vermittlungsdienste:

Alle Vermittlungsdienste müssen sich an Transparenzpflichten halten, die, je nachdem, in welcher der vier Kategorien sich der Vermittlungsdienst befindet, aufbauend sind. Dabei müssen alle Vermittlungsdienste einmal im Jahr einen Bericht über die Moderation von Inhalten veröffentlichen. [11] Ein weiterer Punkt ist die Berücksichtigung der Grundrechte in den Nutzungsbedingungen, welche von allen eingehalten werden müssen (vgl. DSA, Art. 4, Abs.4) . Insbesondere auf die Meinungs-, Informations- und Medienfreiheit wird hoher Wert gelegt. Außerdem müssen auch alle Informationen zu Nutzungseinschränkungen, Inhalten, Moderation, Filterverfahren und Kündigungsrechten in den Nutzungsbedingungen

[11] Vgl. Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), 277 OJ L § (2022). Fassung von 19.10.2022, Art. 55.

transparent und eventuell auch grafisch dargestellt werden. Alle Vermittlungsdienste müssen auf Anordnung mit nationalen Behörden zusammenarbeiten. Außerdem müssen nach Art. 43 (DSA) alle Vermittler eine Kontaktstelle für Nutzer*innen einrichten, das heißt, Vermittler*innen ohne Sitz in der EU müssen eine gesetzliche Vertretung mit Sitz in der EU einrichten, um die Kommunikation mit Behörden zu verbessern (vgl. DSA, Erwgrd. 44).

Hostingdienste:

Für Hostingdienste gibt es zusätzliche Regelungen, die auf den bisher genannten aufbauen, wie das Melde- und Abhilfeverfahren, welches Hostingdienste nach Art. 16 (DSA) dazu verpflichtet, rechtswidrige Inhalte zu melden und nach Bewertung womöglich auch zu sperren. Sie müssen außerdem diese Melde- und Abhilfemaßnahmen Rechteinhaber*innen zur Verfügung stellen und diese informieren. Um die Grundrechte zu schützen, kann dies zu einer Inhaltsblockade führen. Diese Blockade-Entscheidung kann je nach Bewertung auch nur zu einer Teilsperre, Teilentfernung, Herabsetzung im Ranking, oder zu Shadowbanning, dem heimlichen Ausschluss führen (vgl. DSA, Erwgrd. 50). Hierbei fällt die Beweislast auf die Hostinganbieter, wenn sie solche Einschränkungen durchführen (vgl. DSA, Erwgrd. 55). Außerdem ist für Hostingdienste nach Art. 18 (DSA) die Meldung von Straftaten verpflichtend, wenn der Verdacht besteht, dass eine Straftat gegenüber dem Leben oder der Personensicherheit begangen wurde oder begangen wird. Bei dieser Meldungspflicht muss der Hostingdienst alle Informationen zur Identifizierung und zum Ausfindigmachen der Verdächtigen preisgeben. Bei der Kategorie der Online-Plattformen werden die Regelungen nochmals deutlich strenger. Diese Zusatzpflichten für Online-Plattformen dienen vor allem dazu, zwischen Klein- und Mittelunternehmen und den Großen zu unterschieden und die kleineren Betriebe weniger zu belasten. Deswegen gelten die Pflichterweiterungen erst für Unternehmen ab 50 Beschäftigten oder 10 Millionen Euro Jahresumsatz. Trotzdem müssen alle Online-Plattformen genauso ihre Nutzer*innenzahlen melden, da die Ausnahmen nicht für VLOPs gelten (vgl. Rössel, 2023, S. 100).

Online-Plattformen:

Eine Regelung für Online-Plattformen ist nach Art. 20 (DSA), das interne Beschwerdemanagement, welches Nutzer*innen kostenlos zur Verfügung gestellt werden muss und der außergerichtlichen Streitbeilegung dient. Das Beschwerdemanagementsystem hat nach Erwgrd. 58 (DSA) den Zweck, Nutzer*innen bestimmte Entscheidungen zu überlassen und z.B. rechtswidrige Inhalte auf einfache Weise beanstanden zu können. Das außergerichtliche Schlichtungsverfahren nach Art. 21 (DSA) dient dazu, Ungereimtheiten, die über das Beschwerdemanagementsystem nicht geklärt werden können, trotzdem außergerichtlich über zertifizierte Stellen zu verhandeln (vgl. DSA, Erwgrd. 59). Trotzdem haben Nutzer*innen jederzeit die Möglichkeit, die Streitigkeiten vor Gericht zu tragen. Bei Meldungen von rechtswidrigen Inhalten werden diese nach Art. 22 (DSA) von vertrauenswürdigen Hinweisgeber*innen vorrangig behandelt. Diese sind keine Einzelpersonen, sondern Einrichtungen, die nachweislich besondere Kenntnis über besagte rechtswidrige Inhalte haben (vgl. DSA, Ewgrd. 61). Weiters können nach Erwgrd. 64 im Falle von offensichtlich rechtswidrigen und missbräuchlichen Inhalten Online-Plattformen den Dienst für beteiligte Personen, welche dafür verantwortlich sind, auch aussetzen. Dies gilt auch für Personen, die häufig unbegründet Beschwerde einreichen oder Meldungen vornehmen.

Außerdem gelten für Online-Plattformen weitere Transparenzpflichten, zum Beispiel für die Moderation von Inhalten. Nach Art. 15 (DSA) wird die EU-Kommission eine Datenbank veröffentlichen, in der aktuelle Entscheidungen anonym zu illegalen Inhalten und deren Moderation veröffentlicht werden. Auch im Transparenzbericht gibt es für Online-Plattformen weitere Pflichten, vor allem zu Missbrauchs- und Schlichtungsverfahren (vgl. DSA, Erwgrd. 66). Außerdem ist die Transparenz für Empfehlungssysteme nach Art. 27 (DSA) einzuhalten, sodass z.B. bei nutzerverhaltensbasierten Empfehlungssystemen in den Nutzungsbedingungen über die Funktionsweise dieser Systeme in einfacher Sprache aufgeklärt werden muss. Hauptsächlich geht es darum, Nutzer*innen zu informieren, nach welchen Prinzipien Inhalte gezeigt und gereiht werden (vgl. DSA, Erwgrd. 70). Auch sogenannte Dark Patterns bei Benutzer*innenschnittstellen sind verboten, da sie potentiell oder tatsächlich die Entscheidungsfindung von Nutzer*innen

beeinflussen. Gerade bei Kündigungs- oder Auswahlentscheidungen dürfen solche akustische, visuelle oder anderweitige Elemente nicht verwendet werden. Dark Patterns werden im DSA als Praktiken definiert, welche das Verhalten von Nutzer*innen potentiell oder tatsächlich beeinflussen, was über bloße Werbung hinausgeht (vgl. DSA, Ewgrd. 67).

Eine relevante Regelung, welche eine Schnittstelle zur DSGVO bildet, ist die der Online-Werbung. Nach Art. 26 (DSA) müssen Online-Plattformen Nutzer*innen genau die Hauptparameter, also den Kontext, aufzeigen, nach denen ihnen eine Werbung gezeigt wird. Zudem ist Werbung, die auf Profiling von besonderen Kategorien von Daten beruht, für Online-Anbieter*innen verboten (vgl. DSA, Art 26. Abs. 3). Hier muss vorher der Begriff des Profiling definiert werden, welcher in der DSGVO ausführlich beschreiben wurde. Profiling ist

> „(...) jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;(…)“ (DSGVO, Art.4 Abs. 4).

Besondere Kategorien von Daten sind jene, die Auskunft über die ethische Herkunft, sexuelle Orientierung, politische und religiöse Meinung, also auch Weltanschauung Auskunft bieten. Auch Gesundheitsdaten, biometrische und genetische Daten zählen zu dieser Kategorie (vgl. DSGVO, Art. 9 Abs. 1). Die Entscheidung des Verbots von Online-Werbung basierend auf besonderen Kategorien von Daten und Profiling wird begründet mit dem Argument, dass derart personalisierte Werbung zu negativen Auswirkungen für Nutzer*innen und zu gesellschaftlichem Schaden führen kann (vgl. DSA, Erwgrd. 69).

Der Schutz von Minderjährigen wird hier auch ganz besonders ins Auge gefasst. Nach Art. 28 Abs. 1 (DSA) müssen Online-Plattformen Maßnahmen setzen, um Kindern Sicherheit und Privatsphäre zu gewährleisten, um ihnen einen hohen Schutz zu bieten. Auch hier kommen wieder personenbezogene Daten ins Spiel, da Anbieter*innen, wenn sie wissen, dass Nutzer*innen minderjährig sind, keine Werbung verwenden dürfen, die durch Profiling oder personenbezogene Daten ermittelt wurde (vgl. DSA, Art 28, Abs. 2). Um zu prüfen, ob Nutzer*innen

minderjährig sind, sollen Anbieter*innen im Sinne der Datenminimierung nicht zusätzlich personenbezogene Daten verarbeiten (vgl. DSA, Art 28, Abs. 3). Dieses Vorgehen wird als Ziel der Union definiert, Minderjährige auf Online-Plattformen weiter zu schützen. Es wird auch definiert, dass es nicht wichtig ist, ob die Plattform unbedingt auf Minderjährige ausgelegt ist, denn es reicht der Judikatur, wenn Anbieter*innen bekannt ist, dass Minderjährige die Plattform nutzen (vgl. DSA, Ewgrd. 71)

Für Marktplätze im Business to Customer-Bereich, die einen Fernabsatz ermöglichen, gibt es in der Kategorie der Online-Plattformen nochmals strengere Regelungen. Dies dient unter anderem dem Schutz von Verbraucher*innen, indem nämlich nach Art. 30 (DSA) Unternehmen, welche ihre Produkte und Dienstleistungen über einen Online-Marktplatz vertreiben, nachverfolgt werden können. Neben der Privacy by Design-Regelung in der DSGVO kommt für Marktplätze im DSA die Compliance by Design Regelung hinzu, welche nach Art. 31 Abs. 1 (DSA) besagt, dass Plattformen sicherstellen müssen, dass Online-Schnittstellen auf eine Weise funktionieren, dass Unternehmen, welche über die Plattform Verträge im Fernabsatz abschließen, den Informationspflichten, der Konformität und den Produktsicherheitsinformationen auch nachkommen können. Die Schnittstellen von Online-Plattformen müssen dabei so gestaltet sein, dass Unternehmen Informationen über Produkte und Dienstleistungen zur Verfügung stehen, Mittel zur Identifikation des Unternehmens wie z.B. ein Logo und Etikettierung nach Unionsrecht (vgl. DSA, Art 31, Abs. 2). Diese vorangehende Compliance by Design-Regelung, bevor ein Unternehmen auf einer Plattform etwas im Fernabsatz verkaufen darf, muss auch von Online-Plattformen nach Art. 31 Abs. 3 (DSA) stichprobenartig geprüft werden. Sollten Marktplatzbetreiber von rechtswidrigen Produkten oder Dienstleistungen Kenntnis haben, müssen sie Käufer*innen darüber informieren, inklusive Unternehmensidentität sowie Rechtsbehelfe (vgl. DSA, Art. 32).

VLOPS bzw. VLOSE

Zusätzlich zu den bisher genannten einzuhaltenden Regelungen gelten für VLOPS durch ihre Größe und Reichweite noch zusätzliche Bestimmungen, da sie besonders großen Einfluss auf die Gesellschaft, Informationsbeschaffung und

Meinungen haben. Wie schon erwähnt, müssen seit Februar 2023 alle VLOPS und VLOSE ihre durchschnittlichen Nutzer*innenzahlen öffentlich zur Verfügung stellen. Als Nutzer*innen gelten diejenigen, welche die Online-Plattform einmal im Monat aktiv benutzen. Dabei wird über sechs Monate das arithmetische Mittel der aktiven Nutzer*innen herangezogen, welche Suchanfragen eingeben, aktiv etwas veröffentlichen oder diese Inhalte konsumieren. Dabei kommt es aber nicht darauf an, ob Nutzer*innen registriert sind oder nicht, da sonst Anbieter*innen ihren Pflichten ausweichen können. Zu den Pflichten, welche die ganz großen Plattformbetreiber*innen einhalten müssen, gehört, ähnlich wie die DSFA bei der DSGVO, die Risikobewertung (vgl. Rössel, 2023, S.102f.). Diese Risikobewertung müssen VLOPS einmal im Jahr und auf jeden Fall vor Einführung einer neuen kritischen Funktion durchführen, um systematische Risiken nach Schwere und Wahrscheinlichkeit zu ermitteln, zu bewerten und Maßnahmen zu setzen. Dabei muss bewertet werden, ob rechtswidrige Inhalte verbreitet werden und ob durch die Einführung der Funktion Nachteile zur Ausübung der Grundrechte entstehen. Außerdem werden Nachteile auf gesellschaftliche Diskussionen und Wahlprozesse, Nachteile für Minderjährige, auf geschlechterspezifische Gewalt und das allgemeine Wohlbefinden, die sowohl psychisch als auch physisch entstehen, geprüft (vgl. DSA, Art. 34, Abs.1). Außerdem wird nach Art 34 Abs. 2 (DSA) der Einfluss von neuen Funktionen auf Empfehlungssysteme, die Moderation von Inhalten, die AGBs, das Anzeigen von Werbung und die datenbezogenen Praxen geprüft. Die Dokumente der Risikobewertung müssen der EU-Kommission und dem Koordinator für digitale Dienste übermittelt und für drei Jahre aufbewahrt werden (vgl. DSA, Art. 34, Abs.3). Maßnahmen zur Risikominimierung müssen von Anbieter*innen von VLOPS auch getroffen werden, welche besonders zu den systemischen Risiken in Art. 34 (DSA) passen und verhältnismäßig sind. Dabei ist es wichtig, dass Empfehlungssysteme und Werbesysteme so getestet und modifiziert werden, dass keine Anreize für Verbreitung illegaler Inhalte geschaffen werden, welche Minderjährige nutzen (vgl. DSA, Art. 35). In Krisensituationen, welche die öffentliche Sicherheit gefährden, wie zum Beispiel Kriege, kann die EU-Kommission VLOPs dazu auffordern, Maßnahmen zu treffen, um Risiken zu verringern, wie zum Beispiel bei Desinformation (vgl. DSA, Art. 36). Eine weitere Schwelle, die für VLOPS hinzukommt, sind die externen und unabhängigen Audits, welche einmal im Jahr

durchgeführt werden müssen und dies auf eigene Kosten. In diesen Audits werden alle Sorgfaltspflichten für Transparenz und Sicherheit sowie die Verpflichtungszusagen zu Verhaltenskodizes und Krisenprotokollen geprüft. Es müssen dafür Zugang zu Räumlichkeiten inklusive EDV und die Beantwortung aller Anfragen im Rahmen des Audits ermöglicht werden. Weiters wird der umfassende Bericht zu Risikominderungsmaßnahmen und der Bewertung an den Koordinator digitaler Dienste und an die Kommission übermittelt (vgl. DSA, Art 37). Im daraus entstehenden Prüfbericht muss argumentiert werden, welche Maßnahmen zur Erfüllung aller Pflichten gesetzt wurden. Wenn VLOPs ihre Pflichten nicht erfüllen, bekommen sie von Prüfer*innen einen negativen Vermerk (vgl. DSA, Erwgrd. 93). Zusätzlich gilt bei den Regelungen zu Empfehlungssystemen, dass nach Art. 38 (DSA) VLOPs eine Option zur Verfügung stellen müssen, die nicht auf dem Prinzip von Profiling beruht. Weiters muss Transparenz geschaffen werden bezüglich der Werbesysteme von VLOPS, die das Ziel haben, Nutzer*innenverhalten zu analysieren. Außerdem VLOPS müssen zusätzlich ihre Archive für Werbung zur Überwachung und Forschung zugänglich machen für den Zeitraum von einem Jahr (vgl. DSA, Art. 39). Koordinator*innen digitaler Dienste bekommen, um ihren Pflichten nachzukommen, Zugang zu allen notwendigen Daten, Algorithmen, zu Inhalten, Moderationen, zu Empfehlungssystemen sowie zu Werbearchiven und Systemen. Davon sind Nutzer*innendaten jedoch ausgenommen. Wichtig zu erwähnen ist auch noch, dass Koordinator*innen digitaler Dienste Forschungseinrichtungen den Zugang zu Plattformdaten ermöglichen können, damit systemische Risiken für die Union besser bewertet, eingeschätzt und am Ende des Tages auch verhindert werden können (vgl. DSA, Art. 40).

Da die Transparenzberichtspflichten für VLOPS nochmals steigen und sie nach Art 42 (DSA) zusätzlich zu den genannten Transparenzpflichten weitere einhalten müssen, wie personelle Ressourcen und deren Qualifikationen, dürfen Aufsichtsbehörden für den zusätzlichen Aufwand eine Gebühr verlangen (vgl. DSA, Art. 43). Im Gegensatz zu den kleineren Intermediären gilt die unmittelbare Anwendung des DSA für VLOPS und VLOSE schon ab dem 25. August 2023. In diesem Zug müssen sie bis zu diesem Tag schon die erste Risikobewertung durchgeführt haben und ihre Plattformen regelkonform gestalten (vgl. EU-Kommission, 2023a, o. S.).

Im nächsten Abschnitt werden kurz Compliance Beauftragte und Koordinator*innen digitaler Dienste beleuchtet. Nachdem grob die Pflichten angeführt werden, an die sich die vier Kategorien der Intermediäre halten müssen, wird im folgenden Abschnitt noch erklärt, welche Rollen es zur Überwachung im DSA gibt.

4.3.2 Von Compliance Beauftragten bis zum Europäisches Gremium der digitalen Dienste

Genau wie der Datenschutzbeauftragte in der DSGVO nach Art. 37 gibt es im Gesetz für digitale Dienste auch den Compliance-Beauftragten. Alle VLOPS müssen eine unabhängige Compliance-Abteilung einrichten inklusive Leiter*innen derer, welche das Einhalten des DSA überwachen müssen. Genauso wie Datenschutzbeauftragte haben Leiter*innen der Compliance-Abteilung eine beratende und informierende Funktion, besonders was die Risikobewertung, Pflichten und Krisenprotokolle betrifft (vgl. DSA, Art. 41).

Ähnlich wie bei der Datenschutzbehörde der DSGVO werden Koordinator*innen für digitale Dienste eingeführt. In jedem Mitgliedsstaat wird eine Behörde zum Koordinator digitaler Dienste ernannt, dessen Aufgabe es ist, Fragen zur Verordnung digitaler Dienste zu beantworten und auf nationaler Ebene die Überwachung und Umsetzung der Verordnung zu koordinieren (vgl. DSA, Art. 49). Aus einer ausgewählten Gruppe der Koordinator*innen wird das Europäische Gremium für digitale Dienste zusammengestellt, welches die einheitliche Anwendung kontrollieren und koordinieren soll (vgl. DSA, Art. 61). Eine vergleichbare Rolle zum Europäischen Gremium der digitalen Dienste hat der Europäische Datenschutzausschuss, welcher eine unabhängige Kontrollbehörde ist, die aus den Leiter*innen einer Datenschutzbehörde aus jedem Mitgliedsstaat besteht und die einheitliche Durchsetzung der DSGVO fördern soll (vgl. DSGVO, Art. 68). Der 2019 gewählte europäische Datenschutzbeauftragte ist Wojciech Wiewiórowski, welcher für eine fünfjährige Amtszeit gewählt wurde (vgl. European Data Protection Supervisor, o.S.). Nun zu den Sanktionierungen wenn der DSA nicht eingehalten wird.

4.3.3 Sanktionierung nach dem DSA

Die Sanktionierung von Vermittlungsdiensten gilt in allen vier Kategorien. Mitgliedsstaaten müssen Sanktionierungen selbst erlassen, wenn es in ihren Zuständigkeitsbereich fällt. Ziel ist es, dass die Sanktionen wirksam, abschreckend und trotzdem verhältnismäßig sind. Dennoch werden Mitgliedsstaaten dazu angehalten, auch Höchststrafen zu verhängen, welche bis zu 6 % des Jahresumsatzes des Vorjahres darstellen. Diese maximalen 6 % des Jahresumsatzes sind dann zu verhängen, wenn Verpflichtungen der Verordnung nicht eingehalten werden. Bei Informationen, die irreführend, nicht richtig oder unvollständig sind oder wenn Berichtigung verlangt und dem Auftrag nicht nachgekommen wird, sollen Mitgliedsstaaten bis zu 1% des Jahresumsatzes aus dem Vorjahr verhängen. Wenn eine dieser Sanktionen beschlossen wird, kann ab dem Datum des Beschlusses ein Zwangsgeld von 5% des Tagesumsatzes oder der Tageseinnahmen des Vorjahres berechnet werden. Dies müssen Mitgliedsstaaten sicherstellen (vgl. DSA, Art. 52). Auch wenn die Sanktionen in Art 83 (DSGVO) schon mit 20 Millionen Euro oder 4% des Jahresumsatzes als Höchststrafe eine verändernde Wirkung hatten, wird der Schutz der Konsument*innen beim DSA noch einmal höher angesetzt und verschärft.

Zusammenfassend lässt sich aus den Vorschriften der vier Kategorien von Online-Vermittlungsdiensten des Digital Services Acts sagen, dass versucht wird, notwendige Transparenz über Empfehlungssysteme, Werbungsschaltung, Inhalte-Moderation und Schutz von Grundrechten zu schaffen. Außerdem kann der DSA mit den strengen Verpflichtungen und Sanktionen gegenüber Online-Plattformen und VLOPs, die schon die DSGVO nicht eingehalten haben, ein klares Zeichen setzen.

4.4 Aspekte, welche die DSGVO ergänzen

Nachdem ausführlich behandelt wurde, was sich für Intermediäre ändern wird, wird an dieser Stelle noch einmal genau darauf eingegangen, wie der DSA den Schutz personenbezogener Daten erweitert. Zwar bleiben durch den DSA die Verordnungen der DSGVO unberührt, dennoch erweitert der Digital Services Act den Schutz personenbezogener Daten direkt um zwei Aspekte (vgl. DSA, Erwgrd. 10).

Wenn Werbung auf Personalisierung beruht, kann sich das negativ auf die Gesellschaft auswirken, da die Gefahr und ein Risiko für Manipulation und Desinformation besteht. Dies ist der Grund, weshalb Online-Werbung nach Artikel 26 (DSA) basierend auf Profiling (vgl. DSGVO, Art. 4. Abs. 4) besonderer Kategorien personenbezogener Daten verboten ist (vgl. DSA, Erwgrd. 69). Weiters wurde in Art 28 (DSA) der Schutz gegenüber Minderjährigen ausgeweitet, welches ein priorisiertes Ziel in der Union war. Deswegen ist es Anbieter*innen verboten, Werbung auf Basis von Profiling auszuspielen, wenn ihnen bewusst ist, dass Nutzer*innen minderjährig sind. Vermittlerdienste, die für Minderjährige zugänglich sind, werden daran festgemacht, wenn es in den AGBs steht, wenn sie sich an Minderjährige richten oder wenn diese Dienste von einer großen Anzahl Minderjähriger genutzt werden. Es reicht jedoch auch, wenn Anbieter*innen bekannt ist, dass Minderjährige den Dienst verwenden. Außerdem müssen Anbieter*innen Maßnahmen treffen, um Minderjährige zu schützen, wie zum Beispiel Standards für Online-Schnittstellen mit der höchsten Art und Weise an Privatsphäre und Sicherheit. Um keinen Anreiz zur weiteren Beschaffung von personenbezogenen Daten zu geben, dürfen Anbieter*innen auch keine neuen personenbezogenen Daten verarbeiten, nur um herauszufinden, ob Nutzer*innen minderjährig sind (vgl. DSA, Erwgrd. 71).

Im Allgemeinen tragen die Transparenzpflichten und Sorgfaltspflichten zu Empfehlungssystemen, Profiling, Inhalten, Moderationen und Online-Werbung im Internet dazu bei, dass Nutzer*innen sich bewusst sind, auf welchen Daten diese basieren und weshalb ihnen Inhalte gezeigt werden. Nutzer*innen wird nach der Autorin mit dem DSA und den Pflichten, die er mit sich bringt, das Werkzeug in die Hand gegeben, zu informierten Bürger*innen zu werden. Sie werden direkt informiert, was Löschungen von Inhalten betrifft und können sich dagegen auch wehren. Innerhalb ihres Mitgliedsstaates bekommen sie Zugang zu Streitbeilegungsmaßnahmen. Durch einige Informationspflichten bekommen sie auch mehr Information zu Verkäufern, die Produkte und Dienstleistungen im Fernabsatz verkaufen. Auch Nutzungsbedingungen für Plattformen müssen transparent dargelegt werden. Außerdem werden konkrete Krisenmanagementmaßnahmen für mehr öffentliche Sicherheit und Gesundheit eingerichtet. Und Wissenschaftler*innen wird der Zugang zu Plattformdaten

ermöglicht, damit die Forschung ein besseres Verständnis von Risiken und Gefahren für die Gesellschaft und zu Grundrechten gegenüber diesen Intermediären bekommt (vgl. EU Kommission, 2023c, o. S.). Allein die Transparenz- und Informationspflichten geben laut Autorin den Nutzer*innen ein besseres bzw. greifbares Verständnis, wie auch ihre personenbezogenen Daten von Plattformen verwendet werden und erweitern somit indirekt auch den Schutz personenbezogener Daten. Die Autorin merkt an dieser Stelle an, dass die Ermächtigung durch Information und Transparenz zunimmt, Nutzer*innen mehr über die Verwendung ihrer Daten erfahren und somit auch mehr Kontrolle darüber bekommen. Dies wäre wiederum eine Verbesserung gemäß des hier in Kapitel 3 formulierten nachhaltigen Datenschutzes.

4.5 Kritik am Digital Services Act

Doch der Digital Services Act erfährt nicht nur Lob, sondern schon vor seiner verpflichtenden Umsetzung Kritik, welche im folgenden Abschnitt durchleuchtet wird. Der erste Kritikpunkt fängt nach Micova (2021) bei der Einschätzung des Risikos einer Plattform anhand der aktiven Nutzer*innen an. Da es beim DSA stark um systemische Risiken geht, geht sie speziell darauf ein, dass nicht nur die Nutzer*innenzahl aussagekräftig ist, ob eine Plattform systemische Risiken verursacht. Sie argumentiert, dass Plattformen sehr wohl auch mit größerem Schadensrisiko eingeschätzt werden müssen, wenn sie öffentlich sind. Damit meint sie, wenn der Schaden die Gesellschaft, öffentliche Systeme und die Möglichkeit des Staates, Schutzmaßnahmen bereitzustellen, beeinflusst. Außerdem sind Plattformen auch dann ein größeres Schadensrisiko, wenn Anhäufungen von Schäden ein Ausmaß erreichen, das sich auf das soziale Umfeld auswirkt über Nutzer*innenzahlen und Inhalte hinaus. Deswegen empfiehlt Micova, dass die Systeme der Mitgliedsstaaten mitbedacht werden, da auch Plattformen unter 45 Millionen Nutzer*innen einen öffentlichen Charakter haben und systemische Risiken für die gesellschaftlichen Systeme einzelner Mitgliedsstaaten haben können. Zu den Nutzer*innenzahlen sollte es ihrer Meinung nach ein Maß an Vernetzung zur Definition von VLOPs geben, da nicht nur die Plattformökonomie eine Rolle spielt, sondern für systemische Risiken auch die Beziehungen zu Werbetreibenden, Softwareentwickler*innen, Geräteherstellern und die Vernetzung mit anderen

Diensten relevant sind. Für die Risikobewertung sieht es die Autorin auch als essentiell, dass Medienpluralismus in einer eigenen Kategorie aufgelistet wird. Allgemein vertritt die Autorin zur verpflichteten Bewertung von Risiken die Meinung, dass die Einstufung von Plattformen als VLOPs dann sinnvoll ist, wenn dadurch tatsächlich systemische Risiken entdeckt werden. Dafür müssen VLOPs jedoch über eine interne Prüfung hinausgehen und plattformübergreifende Aktivitäten, soziales Umfeld und andere Dienste miteinbeziehen (vgl. Micova, 2021, S. 16ff.). Zudem ist es nach der Autorin fragwürdig, dass VLOPs die verpflichtenden Audits im Rahmen der Risikobewertung selbst bezahlen, da dies ein Risiko für missbräuchliches Verhalten auslösen könnte. Die Sorgen der nicht allumfassenden Einschätzung von systemischen Schaden ist gut nachvollziehbar, da vor allem der Zugang von Forschungseinrichtungen zur Erforschung von systemischen Risiken im DSA nur bei VLOPs ermöglicht wird (vgl. DSA, Art. 40, Abs. 4). Das heißt: Ob andere Online-Plattformen ein systemisches Risiko darstellen können, wird hier auch in der Erforschung systemischer Risiken ausgelassen.

Weiters wird auch die Praxis des Shadowbannings, auch Schattenverbot genannt, von Leerssen (2023) kritisiert. Der Autor wirft einen Blick auf die Regelungen zur Moderation von Inhalten im DSA und die Sichtbarkeitsbeschränkungen von Inhalten als Schutzmaßnahme. Grundsätzlich wird der DSA gelobt als erste Rechtsvorschrift im Bereich der Sichtbarkeit und er thematisiert somit das Schattenverbot. Plattformen müssen nämlich nach Erwgd. 55 (DSA) begründen, wenn sie Shadowbanning als Form der Inhaltemoderation anwenden. Die einzigen Ausnahmen der Begründung betrifft irreführende kommerzielle Inhalte, die durch manipulative Nutzung von Diensten verbreitet werden, wie zum Beispiel durch Bots. Hier wird argumentiert, dass die Ausnahme möglicherweise mehr nuanciert formuliert werden sollte, wann Plattformen keine Begründung für Shadowbanning liefern müssen, wie zum Beispiel wegen gewisser Akteure und Normen. Der Autor befürchtet bei zu vager Formulierung, dass Plattformen dies als Schlupfloch nützen könnten, um nicht begründen zu müssen, warum sie Inhalte heimlich herabstufen. Trotzdem lobt der Autor den DSA im Allgemeinen für seine Transparenzpflichten für Plattformen (vgl. Leerssen, 2023, S. 11). Hier bemerkt man, wie bei der DSGVO, dass zu vage Formulierungen einerseits für Rechtsunsicherheit sorgen können,

andererseits auch zu missbräuchlichem Verhalten seitens der Plattformen und Unternehmen führen können.

Turillazi et al. (2023) haben die Unterschiede zwischen der E-Commerce Richtlinie und dem Nachfolger, dem Digital Services Act, analysiert. Sie loben den Digital Services Act und seine Transparenzpflichten. Trotzdem merken sie an, dass es im Hinblick auf Harmonisierung wichtig ist, dass es keine Ungereimtheiten zwischen den Mitgliedsstaaten gibt. Die Hauptverantwortung der Durchsetzung des DSA den Mitgliedsstaaten zu überlassen statt der EU-Kommission, könnte dies erschweren. Im Zusammenhang mit illegalen Inhalten und Content Moderation kritisieren die Autor*innen, dass der DSA das Grundrecht auf freie Meinungsäußerung untergraben könnte, da er nicht klar definiert, was illegale schädliche Inhalte sind und was nicht. Sie kritisieren auch hier die Informationspflicht, welche bei den Nutzer*innen liegt und empfinden es als fragwürdig, ob man wirklich von durchschnittlichen und informierten Bürger*innen ausgehen kann. Sie betonen, dass es absolut notwendig ist, ein Mittelmaß zwischen Schutz von Privatsphäre und Wahrung von demokratischen Rechten zu finden.

Dem muss entgegengehalten werden, dass der DSA im Gegensatz zur DSGVO keine Öffnungsklauseln beinhaltet, was die Harmonisierung erleichtert. Trotzdem wird auch hier die Moderation von Inhalten kritisiert, da diese mit Grundrechten wie Meinungsäußerung aneinandergeraten könnte. Hier wird abermals betont, dass auch beim DSA die Bringschuld seitens der Konsument*innen, sich zu informieren, fragwürdig ist, da diese von durchschnittlich informierten Bürger*innen ausgeht. Trotz der Kritikpunkte können diese erst durch die gänzliche unmittelbare Anwendbarkeit des DSA bestätigt oder widerlegt werden.

4.6 Zwischenfazit

In diesem Kapitel wird ein Fazit aus der Analyse der DSGVO und des DSA gezogen, Aspekte aufgezeigt, in denen sie einander ergänzen und Lücken, welche beide offen lassen, werden zusammengefasst.

Wie auch die DSGVO, soll mit dem DSA ein einheitliches Schutzniveau in der EU geschaffen werden. Die DSGVO hat das Ziel, personenbezogene Daten zu schützen und der Digital Services Act zielt darauf ab, Vermittlungsdienste zu regulieren, um für mehr Transparenz zu sorgen. Beide zielen darauf ab, EU-Bürger*innen zu schützen und haben einen Harmonisierungsanspruch. Dabei ist interessant, dass die erfolgreiche Harmonisierung der DSGVO oft wegen der Öffnungsklauseln kritisiert wurde, da diese das Schutzniveau senken können und für große Rechtsunsicherheit gesorgt haben. Nun wurde im Jahr 2020 der Digital Services Act vorgestellt, welcher keine Öffnungsklauseln mehr beinhaltet und somit keine Verpflichtungen und Ausnahmen in nationales Recht umgesetzt werden müssen (vgl. Härting& Adamek, 2023, S. 318).

Ein weiterer Punkt, bei dem der Digital Services Act unterschiedlich zur DSGVO agiert, ist, die Größe von Unternehmen zu unterschieden. Zwar müssen in der DSGVO auch nur Unternehmen ab 250 Mitarbeiter*innen ein Verzeichnis der Verarbeitungstätigkeiten führen (vgl. DSGVO, Art. 30). Dennoch müssen auch ganz kleine Unternehmen die meisten Verordnungen der DSGVO strikt befolgen, da auch sie harte Sanktionen treffen können. Der Digital Services Act hingegen nimmt hier strengere Unterscheidungen vor und sieht in Online-Plattformen und sehr großen Plattformen klar ein größeres Risiko für systemischen Schaden, weswegen Online-Plattformen und VLOPS auch sehr viel strengere Regeln befolgen müssen (vgl. DSA, Art.3). Trotzdem erwarten bei der Sanktionierung jedoch alle Unternehmen die gleichen Strafen. Beim DSA findet demnach eine bessere Kategorisierung statt, welche auf der Verhältnismäßigkeit zwischen potentiellem Schaden und der Größe der Plattform basiert.

Gewisse Kritikpunkte in der DSGVO werden auch in den Digital Services Act mitgenommen, wie zum Beispiel die Problematik der Einwilligungen, und dass auch sie wieder ein Rolle spielen werden. Gerade zum Schutz von Minderjährigen wurde die Einwilligung als Instrument im Kapitel 3.2.3 zur Verantwortung von User*innen

und Betroffenen schon ausreichend kritisiert. Da der DSA eine ergänzende Wirkung zur DSGVO hat, wird auch die gültige Einwilligung der betroffenen Person ab dem 16. Lebensjahr aus Art. 8 Abs. 1 (DSGVO) herangezogen. Je nach Regelung der Mitgliedsstaaten auch jünger. Hierbei wird in Erwgrd. 68 (DSA) erklärt, dass vor Verarbeitung personenbezogener Daten für gezielte Werbung inklusive Profiling die Einwilligung von Betroffenen eingeholt werden muss. Wie schon erwähnt, kann jeder Mitgliedsstaat das Alter für eine gültige Einwilligung bis auf 13 Jahre herabsetzen (vgl. DSGVO, Art.8 Abs. 2). Gleichzeitig ist nach Art. 28 Abs 2 (DSA) das Zeigen von Online-Werbung basierend auf Profiling der Personendaten Minderjähriger verboten und als minderjährig wird jeder Person unter 18 bezeichnet. Dennoch muss auch für Online-Werbung für die Verarbeitung von personenbezogenen Daten inklusive Profiling, wie auch in Erwgrd. 68 geschrieben, eine Einwilligung eingeholt werden. Hier stellt sich die Autorin die Frage, ob bei dieser Schutzregelung des DSA der Minderjährigenschutz von 18 herangezogen wird, oder das Einwilligungsalter, das in Mitgliedsstaaten auf bis zu 13 Jahre herabgesetzt werden darf, herangezogen wird. Dies erscheint, als könnte es zu Unklarheiten führen bezüglich des Online Schutzes Minderjähriger in § 28 Abs. 2 (DSA).

Neben dem Einwilligungsalter steht auch hier das EU-Verbraucherleitbild zur Debatte, welches mit dem verhaltensökonomischen nach Schmitt (2018) nicht übereinstimmt. Denn sowohl die Informationspflichten, die Einwilligungen als auch die Transparenzpflichten sind zwar auf der einen Seite gut, da sie Konsument*innen und Betroffenen die Möglichkeit zur Kontrolle über ihre Daten geben. Auf der anderen Seite basiert diese Kontrolle, über die eigenen Daten zu bestimmen, auf einem Verbraucherleitbild, welches nicht der Realität entspricht und auf einem Machtverhältnis basiert. Schon 2013, also vor der Einführung der DSGVO haben Kamp & Rost festgestellt, dass Einwilligungen eine Transparenz-Fiktion sind und keine nachhaltige Schutzwirkung vorweisen können, da sie nicht mehr Kontrolle oder Vertrauen erzeugen, sondern Unternehmen eine Gestaltungsmacht über personenbezogene Daten geben. Zwar ist es nach Erwgrd. 42 (DSGVO) verboten, dass Betroffene Nachteile haben, wenn sie nicht einwilligen, dennoch fängt das Machtverhältnis schon beim informationellen Ungleichgewicht an (vgl. Kamp & Rost, 2013, S.80-84).

Ein weiterer Kritikpunkt, welcher sowohl die Datenschutz-Folgenabschätzung nach Art. 35 (DSGVO) als auch die Risikobewertung nach Art. 34 (DSA) tragen, ist, dass beide intern durchgeführt werden. Das heißt, Betroffene und Konsument*innen sind auf die seriöse Durchführung von Verantwortlichen und Anbietern dieser Bewertungen angewiesen. Bei Art. 37 (DSA) kommt hinzu, dass sich VLOPs auf eigene Kosten einmal im Jahr einer unabhängigen Prüfung unterziehen müssen, ob sie die beschriebenen Pflichten einhalten. Nach der Autorin ist es an dieser Stelle fraglich, ob die Durchführung auf eigene Kosten nicht Missbrauch begünstigt, indem VLOPs sich für Prüfstellen entscheiden, die zu ihren Gunsten prüfen.

Anhand all dieser Beispielen kann erkannt werden, dass die Verantwortung zu großen Teilen in der Hand der Unternehmen und Plattformen liegt, Betroffene und Konsument*innen zu schützen und ihre Interessen ernst zu nehmen. Zwar haben Union und Staat die Verantwortung, die Judikatur vorzulegen, dennoch ist es eine Herausforderung, Formulierungen zu finden, wie man an der Kritik an der DSGVO und dem DSA sieht. Viel wichtiger wäre es nach Meinung der Autorin, dass Plattformen und Unternehmen den Schutz personenbezogener Daten ernst nehmen und nicht juristische Lücken suchen, um Daten am besten monetarisieren zu können. Wenn man dies in Bezug zur Definition von nachhaltigem Datenschutz nach Amort et. al (2022) setzt, überlassen die DSGVO und der DSA zwar die Entscheidungsmacht und die Kontrolle, einzuwilligen, den Betroffenen und Konsument*innen und geben ihnen Information und Transparenz, um sich zu entscheiden. Dennoch bietet die Einwilligung in Kombination mit einem Machtverhältnis und Informationsungleichgewicht Unternehmen die Möglichkeit, Betroffenen und Konsument*innen die Kontrolle über ihre personenbezogenen Daten zu nehmen.

Nun wird im empirischen Teil dieser Arbeit erforscht, wo die Verantwortlichkeiten zum Schutz personenbezogener Daten liegen, ob es ein einheitliches Verständnis von nachhaltigem Datenschutz gibt und was der Digital Services Act zum Schutz personenbezogener Daten seitens Expert*innen beitragen kann und worin die Herausforderung in Zukunft zum Schutz personenbezogener Daten liegen. Für diesen Teil wird jedoch vorerst die Methodik dieser Forschungsarbeit geklärt.

5. Methodik

In diesem Kapitel wird der empirische Zugang erklärt, um eine Antwort auf die Forschungsfrage zu erarbeiten. Zuerst wird noch einmal ein Blick auf die Forschungsfrage geworfen und erklärt, warum diese von Bedeutung ist. Dann wird die Methode der Inhaltsanalyse nach Mayring erklärt. Weiters wird auf die Bedeutung von empirischer Sozialforschung für die Beantwortung der Forschungsfrage eingegangen. In weiterer Folge werden die Inhalte und die Ziele des Interviewleitfadens beleuchtet, da der Leitfaden die Grundlage für die Expert*inneninterviews darstellt. Nachfolgend wird das Forschungsdesign geklärt. Danach werden noch die Eigenschaften von Expert*inneninterviews erklärt und es wird auf deren Vor- und Nachteile eingegangen, um daraufhin auf die Gütekriterien der Interviews dieser Arbeit eingehen zu können.

5.1 Forschungsfrage

In Zusammenarbeit mit den Theoriekapiteln und der empirischen Untersuchung versucht diese Arbeit nun folgende Forschungsfrage zu beantworten:

> Inwieweit ergänzt der DSA die DSGVO in Bezug auf den Schutz personenbezogener Daten, aus Sicht der Konsument*innen und ist dieser ausreichend, um von nachhaltigem Datenschutz zu sprechen?

Aus den Ergebnissen von Expert*inneninterviews werden Hypothesen aufgestellt, mit denen die Forschungsfrage beantwortet werden kann. Außerdem geben diese Hypothesen Anhaltspunkte zu weiterer Forschung und dienen dazu, Handlungsempfehlungen geben zu können. Hypothesen stellen grundsätzlich Vermutungen dar, die einerseits wissenschaftlich begründet sind. Sie bestehen zu einem Teil aus bestätigtem Wissen und zum anderen Teil aus Vermutungen, die noch nicht bestätigt sind (vgl. Häder, 2015, S. 33). Im folgenden Abschnitt wird das Forschungsdesign erklärt und grafisch dargestellt, Grundgesamtheit und Stichprobe erklärt.

5.2 Forschungsdesign, Grundgesamtheit und Stichprobe

Das Forschungsdesign ist der Untersuchungsrahmen, in welchem geforscht wird. Innerhalb des Forschungsdesigns werden die Methoden und Techniken der Forschung dargelegt. Außerdem wird argumentiert, wie die Daten aufbereitet und ausgewertet werden. Ziel des Forschungsdesigns ist es, anhand dieses konkreten Plans eine Karte zu entwickeln und die Forschungsfrage beantworten zu können (vgl. Mayring, 2020, S. 5).

Nach Mayring gibt es ein allgemeines Forschungsdesign, welches sowohl qualitativ als auch quantitativ angewandt werden kann. In Abbildung 2 wird das Forschungsdesign dieser Arbeit anhand einer eigenen Darstellung dargelegt, angelehnt an Mayrings Darstellung. Wie in der Abbildung ablesbar ist, beginnt jede Forschung mit einer Forschungsfrage und einer Forschungslücke, wie in dieser Arbeit in Kapitel 1 und 2 geklärt wurde. Im 2. Schritt werden Theoriekapitel gebildet, um eine theoretische Basis und den Hintergrund der Arbeit darzustellen, wie auch hier in den Theoriekapiteln 3 und 4 zur DSGVO und dem DSA. Weiters wird im 3. Schritt der methodische Ansatz geklärt, zum Beispiel, auf welche Art die Stichproben zusammengestellt sind, und es wird auf die gewählte Methode, deren Vor- und Nachteile und auf die Techniken dieser Methode näher eingegangen. Im 4. Schritt wird die empirische Untersuchung der Durchführung von Expert*inneninterviews, die Erstellung eines Kodierleitfadens und die Durchführung der induktiven Kategorienbildung gezeigt und in Kapitel 6 durchgeführt. Im 5. Schritt werden die Ergebnisse der induktiven Kategorienbildung dargestellt und darauf basierend Hypothesen gebildet. Dieser Schritt findet hier ebenfalls in Kapitel 6 statt. Weiters wird im letzten Schritt die Forschungsfrage anhand der Ergebnisse, hier anhand der Hypothesen, beantwortet und basierend darauf wird in Kapitel 7 ein Fazit gebildet. Wie man in Abbildung 2 sieht, finden zwei Rückkopplungsschleifen statt, wobei der linke Pfeil dazu dient, die Ergebnisse, hier die Hypothesen, in Verbindung zur Theorie zu setzen und der rechte Forschungsfrage und -lücke darstellt (vgl. Mayring, 2020, S. 8f.).

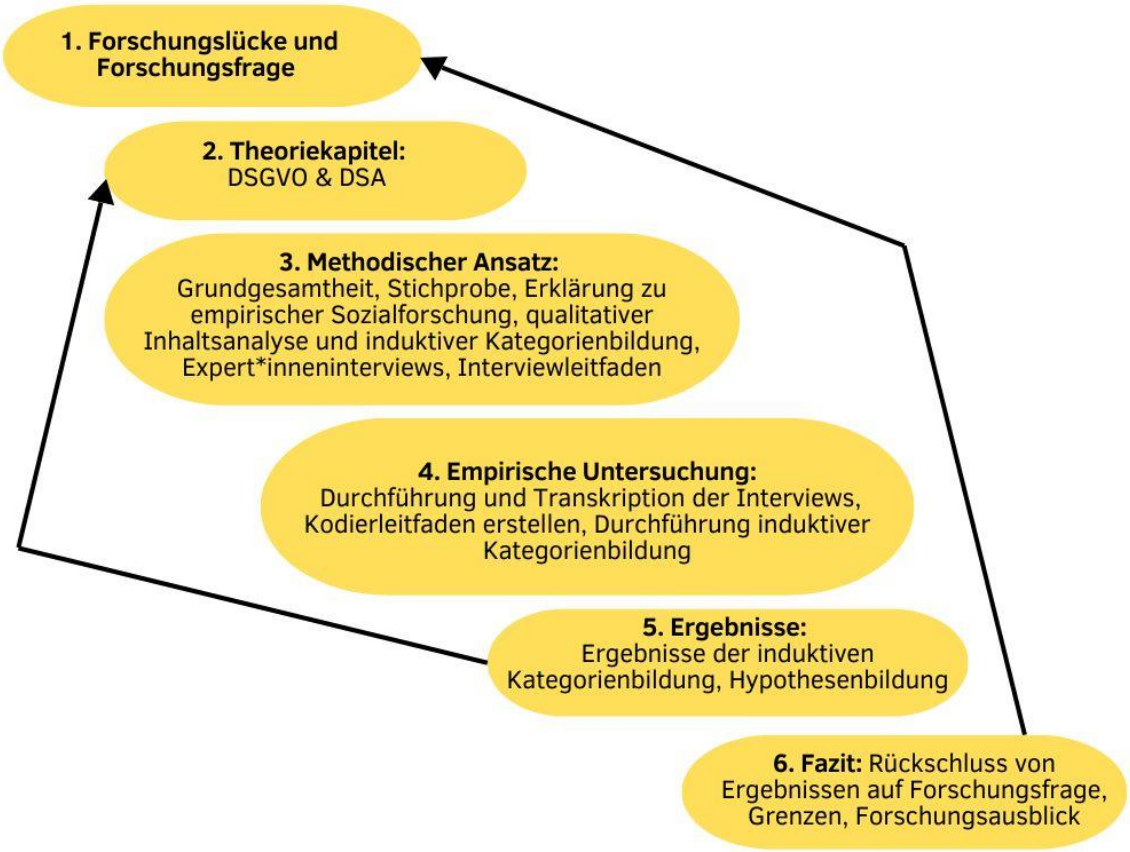

Abb. 2 Forschungsdesign (Eigendarstellung angelehnt an Mayring 2020, S.8)

Grundgesamtheit, Stichprobe

Die Grundgesamtheit ist die Anzahl, welche für die Forschung Gültigkeit besitzt und über die eine Aussage getroffen werden kann. Das können echte und potentielle Proband*innen oder in diesem Fall Expert*innen sein. Dabei geht es nicht um eine richtige Anzahl, sondern nur darum, ob es für die Forschung zweckmäßig ist (vgl. Heidig & Dobbelstein, 2021, S. 53f.). In der qualitativen Sozialforschung spielt jedoch weniger die Repräsentativität der Grundgesamtheit eine Rolle, sondern viel mehr die Stichprobenziehung. In erster Linie spielt in dieser Arbeit die bewusste Stichprobenziehung eine Rolle. Dabei werden die Fälle nicht nach Zufall ausgewählt wie bei einer Zufallsstichprobe, sondern gezielt so, dass der Erkenntnisgewinn so hoch wie möglich ist (vgl. Schreier, 2020, S. 23f.). Da unter den Expert*innen zu Datenschutz die Grundgesamtheit wenig Aussagekraft hat, wurde hier der Fokus auf die bewusste Stichprobenziehung gelegt. Deswegen wurden für die Expert*inneninterviews folgende Kriterien ausgesucht. Für die bewusste Stichprobe kommen Expert*innen infrage, welche sich beruflich mit der DSGVO oder dem DSA auseinandersetzen, jedoch aus möglichst unterschiedlichen Blickwinkeln. Damit ist

gemeint, dass die Expert*innen alle einen juristischen Hintergrund haben sollten, aber beruflich aus unterschiedlichen Branchen kommen sollten, wie Technik, Politik, Forschung, sowie Consulting zum Thema Datenschutz. Damit kann ein breiter Einblick aus der Praxis auf die DSGVO und den DSA geworfen werden. Aus diesen Kriterien ist eine bewusste Stichprobe aus 8 Expert*innen entstanden. Nach der Autorin ist eine quantitative Erhebung mittels Fragebogen in diesem Fall nicht möglich, da die Bevölkerung zu wenig über das Ausmaß von Datenschutz und das Recht auf den Schutz personenbezogener Daten weiß. Dies ist mitunter ein Grundproblem bei der Umsetzung der DSGVO, welches in dieser Arbeit erforscht wird. Da die Rolle der Konsument*innen und deren Eigenverantwortung in dieser Arbeit dennoch eine Rolle spielt, gibt es einen theoretischen Teil dazu. Dieser spielt in der Befragung von Expert*innen eine Rolle, nämlich die Verantwortung von Betroffenen und User*innen in Kapitel 3.2.3.

Im folgenden Abschnitt wird auf die empirische Sozialforschung und ihre Eigenschaften eingegangen.

5.3 Empirische Sozialforschung

Die Empirie dient dazu, Realitäten und Wirklichkeiten zu beschreiben und stellt eine spezielle Art von Aussagen dar. Die empirische Sozialforschung dient der Erforschung menschlichen Verhaltens und dessen Realitäten und ist eine Querschnittsdisziplin, da sie in vielen verschiedenen Wissensgebieten angewandt wird. Teile der empirischen Sozialforschung sind Methoden und Techniken, wobei Methoden Systeme sind, um bestimmte Erkenntnisse systematisch realisieren zu können. Diese Systeme kann man in quantitative und qualitative Methoden unterscheiden. Die qualitativen Methoden versuchen individuelle Realitäten, Handlungen und Eindrücke zu verstehen, wohingegen die quantitativen Methoden versuchen, Daten standardisiert zu erheben, um allgemeine Aussagen tätigen zu können. Techniken sind dazu da, um Methoden zu konkretisieren und zu gestalten. Die Inhaltsanalyse ist ein Beispiel für Methoden in der empirischen Sozialforschung. Neben den Methoden gibt es auch Techniken, um gewisse Aspekte zu untersuchen. Zum Beispiel gibt es unterschiedliche Arten von Inhaltsanalysen, um konkrete Aspekte zu untersuchen. Bevor es zu einer gewissen Art Inhaltsanalyse kommt, können zum Beispiel auch verschiedene Befragungstechniken angewandt werden

die je nach Forschungsgegenstand angepasst werden. (vgl. Häder, 2015, S. 12-15).

In dieser Arbeit spielt die empirische Sozialforschung eine große Rolle. Anhand der Theoriekapitel in Zusammenhang mit den empirischen Ergebnissen der Expert*inneninterviews wird versucht zu erklären, in welchen Aspekten der DSA den Schutz personenbezogener Daten erweitert, ob dies nachhaltiger Datenschutz ist und wer die größte Verantwortung dafür trägt. Hierzu wurde als empirische Methode eine qualitative Inhaltsanalyse gewählt. Die zu analysierenden Daten wurden mittels Expert*inneninterviews erhoben, und als Technik wurde die Art der Inhaltsanalyse namens induktive Kategorienbildung nach Mayring gewählt. Die Methode und die Technik wurden ausgesucht, da die individuellen Eindrücke von Jurist*innen sowohl das Fachwissen als auch teilweise die Sicht von Betroffenen abdecken, da sie selbst sowohl mit Betroffenen in Kontakt stehen als auch selbst Betroffene darstellen, deren eigene personenbezogene Daten regelmäßig verarbeitet werden. Im nächsten Abschnitt wird die Technik der Expert*inneninterviews näher beschrieben, die hier zur Beschaffung von Analysematerial für die Inhaltsanalyse dient.

5.3.1 Expert*inneninterviews

Zu den qualitativen Methoden gehören häufig Interviews, doch es gibt nicht nur eine Interviewform, sondern verschiedene wie zum Beispiel Leitfadeninterviews, narrative Interviews und Gruppendiskussionen. Expert*inneninterviews gehören zu der Form Leitfadeninterviews. Doch stellt sich schnell die Frage, wer überhaupt Experte oder Expertin ist. Hierbei gibt es verschiedene Definitionen von unterschiedlichen Autor*innen, welche man auf einen gemeinsamen Nenner herunterbrechen kann, denn Expert*innen sind Menschen, die auf die eine oder andere Weise über ein Spezialwissen verfügen, dennoch immer ein Spiegelbild des Forschungsinteresses bleiben (vgl. Bogner, Littig & Menz, 2014, S. 9ff.). Ein Unterschied liegt in der Unterscheidung zwischen Alltagswissen und Expertenwissen. Dies heißt aber nicht, dass Expert*innen zwangsweise Wissenschaftler*innen sein müssen, trotzdem sind sie oft Vertreter*innen von Wissenschaftler*innen. In der Literatur wird weiters in drei verschiedene Expert*innenbegriffe unterschieden. Der erster wäre der voluntaristische

Expertenbegriff, welcher verwendet wird, um Menschen zu beschreiben, die auf Grund ihrer individuellen Erfahrungen besondere Fähigkeiten und Wissen besitzen. Diese Definition bedeutet, dass jeder Mensch dementsprechend auf gewissen Gebieten ein Experte oder eine Expertin ist. Genau aus diesem Grund wird der voluntaristische Expertenbegriff auch stark kritisiert, da er den Unterschied zwischen Laien und Expert*innen nur mehr schwer erkennen lässt. Die zweite wäre die konstruktivistische Definition des Expertenbegriffs, welcher jene zu Expert*innen macht, die durch die Gesellschaft zu Expert*innen gemacht werden. Oft sind dies leitende repräsentative Personen, die sich in der Wissenschaft einen Namen gemacht haben und somit zum Experten ernannt werden. Das heißt aber nicht, dass sie durch gesellschaftlichen Rang und Namen tatsächlich die besten Expert*innen in einem Forschungsgebiet sind (vgl. Littig& Menz, 2005, S. 40f.). Die dritte Art ist die wissenssoziologische Fokussierung von Expert*innen, bei der das reine Wissen der Person im Vordergrund steht. Auch hier werden Expert*innen am Expert*innenwissen gemessen, welches oft im Zusammenhang mit dem Beruf steht, im Gegensatz zum Allgemeinwissen. Bei dieser Definition werden Expert*innen auch vom gesellschaftlichen Status gelöst und sprechen mehr als Wissenskörper und nicht als Privatperson (vgl. Littig& Menz, 2005, S. 41). Expert*innenwissen ist pluralistisch, denn es ist an pluralistisches Wissen gebunden und keinesfalls als objektiv hinzunehmendes Wissen zu erachten (vgl. ebd. S. 16). Es gibt zwei Formen des Expert*inneninterviews, deren Funktion nur ungefähr zu beschreiben ist. Zum einen gibt es die Form der explorativen Expert*inneninterviews, die keine zentrale Funktion, sondern eher eine ergänzende Funktion haben. Gegenüber steht die Form der fundierten Expert*inneninterviews, welche eine zentrale Funktion haben für Begriffserklärung, Begründungen und für Informationen. Basierend auf den zwei Unterscheidungen können drei Varianten der Expert*inneninterviews analysiert werden. Die erste wäre das explorative Expert*inneninterview, welches sich durch die Funktion der Orientierung auszeichnet und mit Hypothesenbildung endet. Expert*innen sind oft selbst Teil des zu erforschenden Umfelds und werden in dem Prozess oft als Informationsquelle zur Zielgruppe eingesetzt. Dann kommt das systematisierende Expert*inneninterview, bei dem es um eine möglichst ausführliche Einschätzung durch das Fachwissen geht und der maximale Informationsgewinn das Ziel ist mit

Expert*innen in der Berater*innenfunktion, wofür auch anschließend eine qualitative Inhaltsanalyse zur Auswertung geeignet ist. Das theoriegenerierende Expert*inneninterview dient dazu, subjektive Einschätzungen abzufragen und daraus Handlungsmuster zu erkennen (vgl. Bogner, Littig & Menz, 2014, S. 22-24). Kritik erfahren Expert*inneninterviews durch den Vorwurf der zu standardisierten Leitfadeninterviews, welche Interviewpartner*innen in eine Denkrichtung lenken und nicht offen genug sind. Außerdem werden Expert*inneninterviews wegen ihrer vagen Definitionen kritisiert, wodurch in der qualitativen Sozialforschung viel Uneinigkeit herrscht (vgl. Bogner, Littig & Menz, 2014, S. 2f.).

Für diese Arbeit eignet sich am besten der wissenssoziologische Expert*innenbegriff, da nur Expert*innen befragt werden, die sich beruflich mit Datenschutz auseinandersetzen und sich mit der DSGVO oder dem DSA beschäftigen. Außerdem handelt es sich um eine Mischung aus explorativem und systematisierendem Expert*inneninterview, darauf abzielend, größtmögliche Einschätzung und Wissen zu erlangen, was juristische Stärken und Schwächen in der DSGVO und dem DSA betrifft.

Im folgenden Abschnitt werden die Gütekriterien in der qualitativen Sozialforschung diskutiert.

5.3.2 Gütekriterien qualitativer Forschung

Gütekriterien dienen sowohl in der quantitativen Forschung als auch in der qualitativen Forschung als Qualitätsmerkmal. Trotzdem steht nach Sonntag (2023) immer wieder zur Diskussion, ob die gleichen Gütekriterien für qualitative und quantitative Forschung verwendet werden können, da zum Beispiel die Objektivität in der qualitativen Forschung schwer einzuhalten ist, wenn es um subjektive Einschätzungen geht (vgl. Sonntag, 2023, S. 7-25). Deswegen definiert Burkart Gütekriterien in der qualitativen Forschung anders. Gütekriterien haben in der qualitativen Forschung den Anspruch auf Verlässlichkeit, Gültigkeit, Geltung aber auch auf den Gültigkeitsbereich. Dabei kann es sein, dass die Ergebnisse zu Beginn der Auswertung nicht sehr reliabel sind, wenn Personen, verschiedene Ansichten haben. Wenn zum Schluss aber die Analyse dies ausgleicht, ist die Reliabilität nach Burkart gegeben. Auch die Validität kommt bei der Auswertung, wenn nach

Gemeinsamkeiten gesucht wird und mit ihnen die 100% angestrebt werden. Bei der Gültigkeit der Ergebnisse entstehen häufig auch Grenzen. Diese Grenzen geben Aufschluss für Handlungsempfehlungen und weitere Forschung (vgl. Burkart, 2020, S. 51).

Für die Inhaltsanalyse hat Krippendorf eigene Gütekriterien aufgestellt. Dabei gibt es die zwei Überkriterien Validität und Reliabilität. Zur Validität gehören folgende Gütekriterien: Die semantische Gültigkeit, welche sich auf das Material im Zusammenhang mit den Definitionen, Ankerbeispielen und Kodierregeln bezieht. Dazu muss auch die Stichprobengültigkeit passen. Mit der korrelativen Gültigkeit sind valide Ergebnisse durch eine Korrelation gemeint. Die Vorhersagegültigkeit ist jedoch nur gegeben, wenn stringente Prognosen aus dem Material entstehen. Die Konstruktvalidität lässt sich mit Erfolgen in ähnlichen Konstrukten, Kontexterfahrung mit dem Material, Theorien, Interpretationen und Expert*innen erreichen. Zur Reliabilität gehören die Stabilität, Reproduzierbarkeit und die Exaktheit. Die Stabilität wird durch eine weitere Anwendung des Instruments auf die Analyse bestätigt. Die Reproduzierbarkeit ist der Grad an Wiederholbarkeit, welcher zu gleichen Ergebnissen führt, und die Exaktheit ist der Grad, bis zu welchem die Analyse den Standards entspricht (vgl. Mayring, 2020, S. 125-128).

Nun wird auf die Technik dieser Arbeit näher eingegangen und deren Vor- und Nachteile geklärt.

5.3.3 Qualitative Inhaltsanalyse nach Mayring

Nach Mayring verfolgt die qualitative Inhaltsanalyse das Ziel, Kommunikationsmaterial zu bearbeiten und zu analysieren. Dabei steht weniger im Vordergrund, dass es unbedingt Textmaterial ist, sondern mehr, dass es protokollierbar ist. Nach dieser Definition darf es also auch Bild-, Ton- oder jegliches anderes Kommunikationsmaterial sein, solange es festgehalten werden kann (vgl. Flick, 2005, S. 468).

Die Inhaltsanalyse findet ihren Ursprung in den USA im 20. Jahrhundert. Besonders stark wurde sie erstmals in den 1920ern angewandt, um große Datenmengen vor allem Texte, Zeitungs- und Radiobeiträge auswerten zu können. Häufig zur Anwendung kamen dabei Häufigkeitsanalysen, Valenz-, Intensitäts- und

Kontingenzanalysen. Diese versuchten in Texten Häufigkeiten von Merkmalen auf Skalen einzuordnen und nach Zusammenhängen zu analysieren (vgl. Mayring, 1991, S. 209.).

Doch wie wendet man eine qualitative Inhaltsanalyse nun an? Eine qualitative Inhaltsanalyse verlangt das Zerteilen von Analyseeinheiten, damit sie in einzelnen Schritten erarbeitet werden können, um eine Systematik vorzuweisen. Nach Mayring gibt es ein allgemeines Ablaufmodell, welches für jede Inhaltsanalyse verwendet werden kann. Der erster Schritt ist es, das Material festzulegen, um einen Untersuchungsgegenstand zu haben. Im nächsten Schritt ist es wichtig, sich anzuschauen, in welchem Kontext das Material entstanden ist und die formalen Kriterien und Charakteristika herauszuarbeiten. Danach muss bestimmt werden, in welche Richtung die Analyse überhaupt gehen soll, was das Ziel der Analyse überhaupt ist und ob es im Text um eine Personengruppe oder um die Produktion des Textes geht. Jetzt kann man zu einer konkreten Fragestellung übergehen und zum Ablaufmodell, das zum tatsächlichen Gegenstand passt. Da dieses Ablaufmodell stark vom Gegenstand abhängt, gibt es nur Techniken zur Orientierung. Die erste Technik ist die zusammenfassende Inhaltsanalyse, bei welcher das Textmaterial auf das Wesentliche reduziert wird. Hierbei wird zwischen einzelnen reduktiven Prozessen unterschieden wie Auslassung, Generalisierung, Konstruktion, Selektion, Integration und Bündelung, welche zusammen ein Ablaufmodell der zusammenfassenden Inhaltsanalyse darstellen (vgl. Mayring, 1991, S. 211f.). Was kann die qualitative Inhaltsanalyse nun besonders gut und worin liegen ihre Grenzen?

Laut Mayring leistet die qualitative Inhaltsanalyse nicht nur einen Beitrag zur Entwicklung neuer Verfahrensarten in der qualitativen Forschung, sondern bietet auch Vorteile, wie gute Auswertungstechniken, bezogen auf verbales Forschungsmaterial, vor allem bei subjektiven Einschätzungen und Deutungen. Laut Mayring liegt der stärkste Vorteil der qualitativen Inhaltsanalyse in der Systematik. Dieses regelbasierte Vorgehen sorgt dafür, dass es sich nicht um reine Textinterpretationen handelt, sondern dass ein Kategoriensystem entwickelt wird, auf dem basierend Textbausteine analysiert werden können. Diese sind im Rückschluss leichter überprüfbar und die Ergebnisse sind genauer. Außerdem

lassen sich große Datenmengen analysieren und bei Notwendigkeit quantitative Schritte einbauen, welche die Schere zwischen qualitativ und quantitativ schließen.

Trotzdem ist die qualitative Inhaltsanalyse nach Mayring nicht immer geeignet und hat auch Grenzen: Bei Forschungsfragen, die explorativer sind, gibt es Verfahren, wie die Grounded Theory, die geeigneter wären. Das Wichtige bei der Methodenwahl ist, dass sie zur Fragestellung und zum Textmaterial passt (vgl. Mayring, 2020, S.123f.).

Nun wird im folgenden Abschnitt die Technik der induktiven Kategorienbildung besprochen, um eine systematische Inhaltsanalyse der Expert*inneninterviews durchführen zu können.

5.3.4 Induktive Kategorienbildung nach Mayring

In Abbildung 3 ist der Ablauf einer induktiven Kategorienbildung abgebildet, welche im folgenden Abschnitt beschrieben wird. Dabei gibt es die Möglichkeit einer deduktiven Kategorienbildung, bei der die Kategorien schon vor den Interviews festgelegt werden und die Möglichkeit einer induktiven Kategorienbildung, bei der die Kategorien durch das Material entstehen. Hier werden die Kategorien basierend auf dem Interviewmaterial gebildet, weshalb von einer induktiven Kategorienbildung gesprochen wird. Die induktive Kategorienbildung gehört zur Überkategorie der zusammenfassenden Inhaltsanalyse (vgl. Flick, 2005, S. 472f.).

1. Für eine induktive Kategorienbildung müssen zuerst das Material und die Fragestellung definiert werden. Bei dieser Arbeit stand die Fragestellung schon seit Beginn fest und das Material ergab sich aus den Expert*inneninterviews.
2. Danach werden Kategorien basierend auf dem Analysematerial definiert und Selektionskriterien festgelegt in Form eines Kodierleitfadens, wie er in Tabelle 2 einsehbar ist.
3. Im nächsten Schritt werden Kategorien basierend auf dem Untersuchungsmaterial unter der Voraussetzung der Selektionskriterien gebildet. Dies wird durch eine schrittweise Reduktion des Materials durchgeführt.

4. Nach zirka der Hälfte des Materials werden die Kategorien noch einmal überprüft und notfalls ergänzt.
5. Danach wird das restliche Material durchgegangen, reduziert und eingeordnet.
6. Danach kann das Material ausgewertet werden wie zum Beispiel nach Häufigkeiten. Die Ergebnisse werden dann analysiert und interpretiert und noch einmal in Bezug zum Material gesetzt (vgl. Mayring, 2010, S. 83ff.).

Abb. 3 Induktive Kategorienbildung nach Mayring (Eigendarstellung in Anlehnung an Mayring, 2010, S. 84

Für diese Inhaltsanalyse wurde eine induktive Kategorienanwendung gewählt, sie sich gut zur Auswertung von Expert*inneninterviews eignet, da sie das Ziel hat, Material zu reduzieren und zu allgemeinen Aussagen zu gelangen. Ein Nachteil ist, dass die induktive Kategorienbildung sehr komplex werden kann, wenn eine Kategorie pro Interview vergeben wird, jedoch die Kategorie mehrmals in einem Interview erwähnt wird (vgl. Mayring 2020, S. 498). Diese Problematik wurde in dieser Arbeit damit gelöst, dass pro Expert*in jede Kategorie bei den Häufigkeiten

nur einmal gezählt wurde. Das heißt unter den 8 Expert*innen kam eine Kategorie auf eine maximale Häufigkeit von 8.

5.3.5 Interviewleitfaden

Nach Häder (2015) haben Interviews in der Sozialforschung einen wissenschaftlichen Zweck und versuchen ein Ziel, meistens eine Forschungsfrage zu beantworten. Das Interview ist hauptsächlich einseitig und wird durch die Forschenden geleitet und gelenkt, und es entsteht nicht auf natürliche Weise (vgl. Häder, 2015, S.190). Weiters unterscheidet er zwischen intensiven und qualitativen Interviews. Intensive Interviews zeichnen sich dadurch aus, dass auch bei möglicherweise falsch verstandenen Fragen es möglich ist, eine richtige Antwort zu bekommen, indem nochmal Nachfragen gestellt werden. Bei qualitativen Interviews stehen die persönlichen Ansichten im Vordergrund. Dies ist besonders gut, um herauszufinden, ob sich Probleme aus vorhergehender Forschung wiederfinden (vgl. ebd., S. 400f). Die für diese Arbeit geführten Interviews sind qualitativ geführte Interviews, da zum Beispiel die Auswirkungen des DSA auf Datenschutz sich erst einschätzen lassen, aber nicht in die Tiefe bestätigen lassen. Außerdem kann von Expert*innen das Verständnis von Einwilligungen eingeschätzt werden, das auf früheren Forschungen zum Verständnis von Datenschutzbegriffen angestoßen wurde. Auch die persönlichen Ansichten zu Stärken und Schwächen der DSGVO und zukünftige Herausforderungen für den Schutz personenbezogener Daten können dadurch gut eingeschätzt werden.

Der Interviewleitfaden wird vor Interviews vorbereitet und besteht aus drei Fragetypen, der Primärfrage, der Sekundärfrage und dem Nachfragen. Der Vorteil von Interviewleitfäden ist die notwendige Flexibilität. Die Primärfragen beziehen sich auf die Überthemen eines Themenkreises und können durch Sekundärfragen ergänzt werden, die nur gestellt werden, wenn die Antwort nicht die gewünschte Tiefe besitzt. Wenn es auf manche Fragen keine eindeutigen Antworten gibt, dann kann nachgefragt werden (vgl. Lehmann, 2022, S.101f.). Ein Nachteil des Interviewleitfadens kann sein, dass Fragen zu wissenschaftlich formuliert sind und nicht zur Sprache und Begriffswelt der Befragten passen (vgl. Töpfer, 2012, S. 343). Dies lässt sich beim Interviewleitfaden in dieser Arbeit ausschließen, da die juristischen Begriffe den Expert*innen geläufig sind. Dennoch kommt es durch

offene Formulierungen vor, dass Expert*innen nachfragen, ob es einen Schwerpunkt gibt.

Der Interviewleitfaden gibt hier einen Überblick über die gestellten Fragen und wurde bei Anfrage auch im Voraus zugeschickt. Im Zuge der Befragung der Expert*innen wurde nach folgendem Konzept vorgegangen, wie auch in Abbildung 3 ersichtlich ist:

1. **Einleitung:** Die Autorin hat sich im Zuge der Einleitung vorgestellt und den Vorgang des Interviews erklärt. Hier hat die Autorin auch den Hinweis auf Anonymität, Aufnahme und Transkription den Interviewpartner*innen mitgeteilt und die Expert*innen diesem Vorgang verbal zustimmen lassen.
2. **Situation:** In diesem Schritt wurde nach persönlichen Daten gefragt, wie Name und beruflicher Kontext. In diesem Zug wurden auch schon zwei Primärfragen gestellt. Eine davon zum Verständnis von nachhaltigem Datenschutz und die andere zur Einschätzung der Verantwortlichkeit zum Schutz personenbezogener Daten.
3. **Probleme:** Im Zuge dieses Abschnitts wurden Fragen zu den Stärken und Schwächen oder Vor- und Nachteilen der DSGVO abgefragt. In diesem Abschnitt des Interviewleitfadens gab es auch einige Kategorien von Abfragen, die bei Bedarf als Unterfragen gestellt wurden, wie die Beurteilung der Harmonisierung, der Öffnungsklauseln, der Privacy by Design-Regelung, die Beurteilung der DSFA und das Verständnis von Einwilligungserklärungen. Diese Sekundärfragen wurden jedoch nicht allen Expert*innen gestellt.
4. **Auswirkungen von Problemen:** Hier wurden Fragen zu Auswirkungen gestellt, welche durch vorher genannte Probleme entstehen, wenn die Verantwortungen von Staat, Unternehmen und Betroffenen zum Schutz personenbezogener Daten nicht eingehalten werden.
5. **Lösungsansätze:** In diesem Abschnitt wurde abgefragt in welchen Aspekten der Digital Services Act die DSGVO ergänzen kann. Auch hier gab es eher allgemeine Unterkategorien zur Verfügung gestellt, wie Plattformregulierungen und Transparenzpflichten zur Orientierung. Die letzte Frage diente einem Ausblick in die Zukunft und bezog sich auf zukünftige

Herausforderungen zum Schutz personenbezogener Daten mit der Unterkategorie des technologischen Fortschritts.

6. **Ende:** Zum Schluss wurde den Interviewpartner*innen gedankt und bei Bedarf nach weiteren Quellen oder Interviewpartner*innen gefragt.

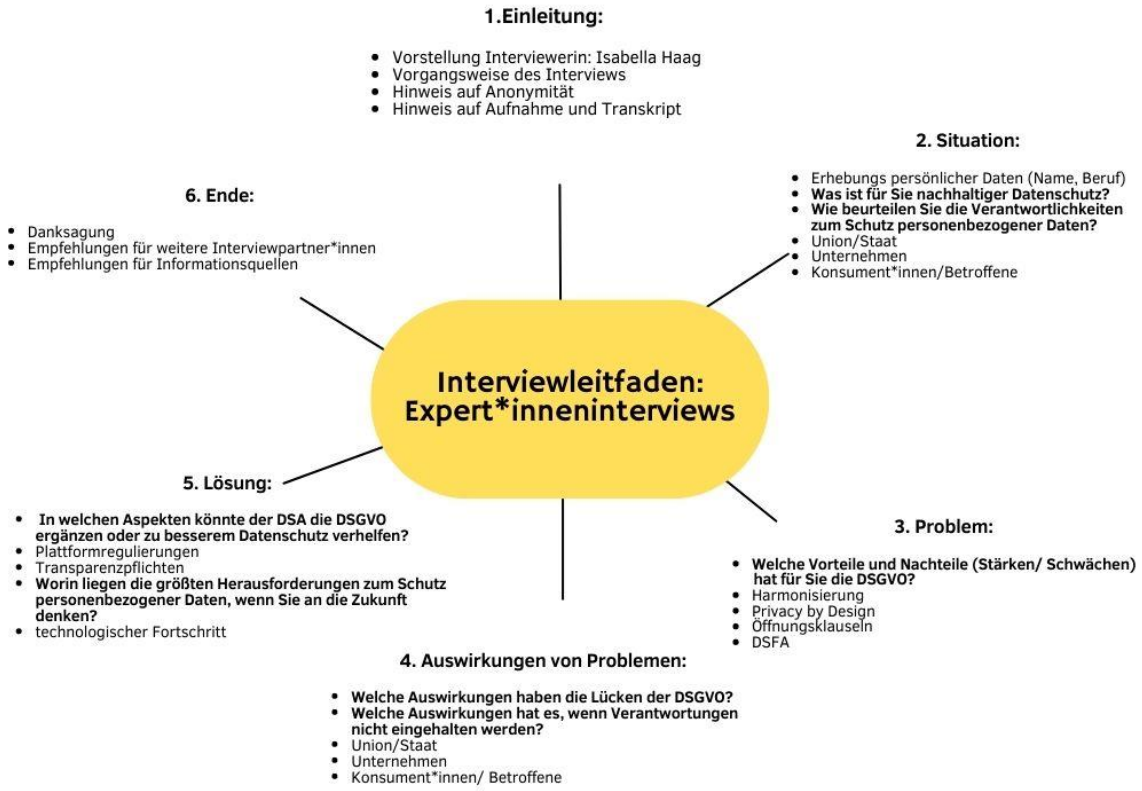

Abb. 3: Darstellung Interviewleitfaden (Eigendarstellung)

6. Empirische Untersuchung

In diesem Kapitel werden die Ergebnisse der Expert*inneninterviews mittels induktiver Kategorienbildung ausgewertet. Die Ergebnisse werden mittels Kodierleitfaden dargestellt und systematisiert. Im Anschluss werden die Ergebnisse der gebildeten Kategorien ausgeführt und erläutert. Basierend auf den Ergebnissen werden Hypothesen aufgestellt. Im Rahmen der Handlungsempfehlungen dieses Kapitels wird dann nahegelegt, in welche Richtung auf diese Ergebnisse reagiert werden kann. In diesem Kapitel wird auch die Forschungsfrage beantwortet, Handlungsempfehlungen werden daraus abgeleitet und letztendlich wird ein Fazit gezogen.

6.1 Deskriptive Ergebnisse / Auswertungen

Angefangen mit diesem Abschnitt, wird der Kodierleitfaden in Tabelle 2 präsentiert. Dann wird näher auf die Stichprobe der Expert*innen eingegangen. Anschließend werden die Ergebnisse der einzelnen Kategorien näher ausgeführt. Die Kategorien sind durch den Vorgang der induktiven Kategorienbildung entstanden, also aus dem Interviewmaterial heraus. Für die Kategorien in der nachstehenden Tabelle wurden folgende Schritte der induktiven Kategorienbildung durchlaufen:

1. Die Interviews wurden transkribiert und überprüft.
2. Es wurden Kategorien selektiert und Selektionskriterien und Ankerbeispiele im Kodierleitfaden festgelegt.
3. Basierend auf den Kategorien wurden die Interviewpassagen mit Farben markiert und anschließend in Tabelle 15 im Anhang festgehalten.
4. Jede Textpassage wurde dann zweimal paraphrasiert und somit zwei Mal zusammenfassend reduziert. Daraus entstanden dann Kategorien oder die Passagen wurden, wenn schon eine bestand, zugeordnet.
5. Bei der Hälfte des Interviewmaterials wurde geprüft, ob die Kategorien zur Fragestellung passen.
6. Dann wurde das restliche Material in Kategorien eingeordnet und anschließend nochmals überprüft, ob die Kategorien zur Fragestellung passen. Bei der Überprüfung der Kategorien wurde hier aus der Überkategorie „Schwächen / Nachteile der DSGVO“, eine eigene Kategorie „Harmonisierungserfolg der DSGVO“ gebildet, da diese nicht nur negativ

bewertet wurde und dementsprechend nicht nur den Schwächen und Nachteilen zugeordnet werden konnte.

7. Das Material wurde an der Stelle nochmal dahingehend überprüft, ob Textstellen, die relevant für die Fragestellung sind, vielleicht nicht zugeordnet wurden.
8. Nachdem alle relevanten Textstellen einer Kategorie in Tabelle 15 im Anhang zugeordnet wurden, werden ab Kapitel 6.1.1 die Ergebnisse ausgewertet.

Doch bevor hier ein Blick auf die Ergebnisse der Kategorisierung geworfen wird, wird im folgenden Abschnitt kurz der Kodierleitfaden präsentiert, in dem festgelegt wurde, an welche Regeln sich die Autorin bei der Zuordnung der Kategorien gehalten hat.

Kodierleitfaden:

Kategorie	Selektions-kriterium	Ankerbeispiel	Kodierregel
Nachhaltiger Datenschutz	Jede Textpassage, unter der deutlich wird, was Expert*innen unter „nachhaltigem Datenschutz“ verstehen.	ID1: „Also nachhaltiger Datenschutz bedeutet für mich, dass man nicht nur pro forma die gesetzlichen Bestimmungen einhält, sondern dass man sich wirklich in die Rolle der betroffenen Personen versetzt, also deren Daten man bearbeitet.(…)“ (ID1: Z. 40-44, durchgeführt am 10.07.2023)	Textstellen müssen definitorische Aspekte beinhalten, was nachhaltigen Datenschutz betrifft.
Verantwortung Union/Staat	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Union und Staat haben zum Schutz personen-bezogener Daten.	ID1: „Also das heißt, daran sieht man schon auch der nationale Gesetzgeber in jedem Mitgliedstaat sollte sich am besten Gedanken machen, wie man die DSGVO idealerweise ergänzt, mit nationalen Gesetzgebungen, also dort, wo ein entsprechender Spielraum ist..” (ID1, Z. 44-50)	Textstellen müssen klar deklarieren, welche Verantwortung Union/Staat zum Schutz personenbezogener Daten haben.
Harmonisierungs-erfolgs der DSGVO	Jede Textpassage, welche Öffnungsklauseln und den Harmonisierungs-effekt von Datenschutzrecht durch die DSGVO bewertet.	ID1: „Ja, es gibt sogenannte Öffnungsklauseln, wie Sie richtig gesagt haben. Ja, ich denke, je besser man die Lücken schließt, die die DSGVO eröffnet, umso besser.” (ID1, Z. 166-168)	Textstellen müssen eine Bewertung von Öffnungsklauseln oder des Harmonisierungs-erfolgs durch die DSGVO beinhalten.

Verantwortung von Unternehmen	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Unternehmen zum Schutz personenbezogener Daten haben.	ID2: „Die Verantwortung die Auflagen einzuhalten und Umzusetzen liegt definitiv bei den Unternehmen.“ (ID2, Z. 364-367)	Textstellen müssen klar deklarieren, welche Verantwortung Unternehmen zum Schutz personenbezogener Daten haben.
Privacy by Design	Jede Textpassage, welche die Privacy by Design-Regelung in der DSGVO bewertet.	ID4: „Und auch dieser Privacy by Design Grundsatz halte ich für absolut sinnvoll. Aber das können andere Unternehmen im internationalen Vergleich halt dann einfach nicht so krass berücksichtigen und haben dadurch vielleicht schneller ein Produkt, das dann doch so überzeugend ist für den Endkunden, dass er sagt okay, das ist mir jetzt relativ egal, ob ich da eine gewisse Anzahl an Daten preisgeben muss oder ob das jetzt optimiert ist auf Privacy by Design oder bei Default.“(ID4, Z. 2143-2148)	Textstellen müssen eine Bewertung der Privacy by Design-Regelung beinhalten.
DSFA	Jede Textpassage, welche die DSFA-Regelung in der DSGVO bewertet.	ID8: „Also eigentlich eine Datenschutzfolgeabschätzung erwarte ich immer bei jedem Start eines Projektes. Irgendwie in einer Form. (…) Es dürfte ja gar nicht zu großem Risiko unterwegs sein. Und da sehe ich zum Teil einen Widerspruch, weil jetzt zum Teil für alles noch Datenschutzfolgenabschätzung gemacht werden. Und das ist vielleicht auch das Instrument nicht immer richtig verstanden oder eingesetzt.“(ID8, Z. 4305-4310)	Textstellen müssen eine Bewertung der DSFA-Regelung beinhalten.
Verantwortung Betroffene / Konsument*innen	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Betroffene & Konsument*innen zum Schutz personenbezogener Daten haben.	ID1: „Die praktische Sicht ist natürlich die, dass selbstverständlich auch Betroffene ihre eigenen Daten unter Anführungszeichen verantwortlich sind.“ (ID1, Z. 98-108)	Textstellen müssen klar deklarieren, welche Verantwortung Betroffene/Konsument*innen zum Schutz personenbezogener Daten haben.

Verständnisses der Einwilligungs-erklärung	Jede Textpassage, welche das Verständnis von Einwilligungserklärungen in der DSGVO bewertet.	ID1: „ (…) Nach Judikatur stellt man auf den Durchschnittsverbraucher ab, das heißt nicht auf einen Analphabeten, der nicht lesen kann, aber eben auch nicht auf den besten Datenschutzexperten, Datenschutzexpertin in der Welt. Aber auch dieser Maßstab, also den Durchschnitt sozusagen, würde ich hier unten anlegen. Also der Durchschnittsverbraucher oder -verbrauchin kennt sich eben nicht so gut aus.“ (ID1, Z. 72-76)	Textstellen müssen das Verständnis von Einwilligungen und den Informationsstand von Bürger*innen beurteilen.
Vorteile/Stärken der DSGVO	Jede Textstelle, welche einen positiven Effekt der DSGVO auf den Schutz personen-bezogener Daten deklariert.	ID1: „Das heißt, die awareness auch bei jemandem, der jetzt vielleicht nicht mit dieser Materie zu tun hat, ist einfach gestiegen. Und auch die Medien in Österreich, aber auch international, berichten immer mehr über datenschutzrechtliche Dinge.” (ID1, Z. 125-131)	Textstellen müssen sich klar zu positiven Effekten der DSGVO äußern.
Nachteile/ Schwächen der DSGVO	Jede Textstelle, welche einen negativen Effekt der DSGVO auf den Schutz personen-bezogener Daten deklariert.	ID1: „(…)es gibt viele Dinge, die ich wahrscheinlich ändern würde. Damit beginnen, dass viele Dinge einfach unpräzise sind und unklar sind.(…)” (ID1, Z. 141-147)	Textstellen müssen sich klar zu negativen Effekten der DSGVO äußern.
Einfluss des DSA auf Schutz personen-bezogener Daten	Jede Textstelle über den DSA, welche einen Effekt auf den Schutz personen-bezogener Daten deklariert.	ID1: „(…) Also kurz gesagt, es gibt natürlich sehr viele, ich nenne sie mal Synergieeffekte. Also das heißt, selbstverständlich wird auch dadurch das Grundrecht auf Datenschutz gestärkt, auch wenn es jetzt nicht primär um Datenschutz geht, sondern sozusagen allgemein um Plattformregulierung. (…)” (ID1, Z. 193-204)	Textstellen müssen klar zu Effekten des DSA auf den Schutz personenbezogener Daten formuliert sein.
Heraus-forderungen in Zukunft für Datenschutz	Jede Textstelle, welche eine Herausforderung in der Zukunft zum Schutz personenbezogener Daten erwähnt.	ID1: „(…) Aber nichtsdestotrotz würde ich trotzdem sagen AI. So die massenhafte Datenverarbeitung innerhalb eines kurzen Zeitraums mit sehr sehr viel Rechenleistung.(…)” (ID1, Z. 216-227)	Textstellen müssen klar definieren, was eine Herausforderung in Zukunft zum Schutz personenbezogener Daten sein kann und was nicht.

Tab. 2: Überblick Kodierleitfaden (Eigendarstellung)

Für die gezielte Stichprobe waren von 8 Expert*innen, 4 Personen männlich und 4 Personen weiblich. 3 davon waren Datenschutzbeauftragte, wovon 2 aus Forschungseinrichtungen sind und eine Person externer Datenschutzconsultant ist. Eine Expertin arbeitet in einer Institution der EU und eine Expertin davon ist Vizedirektorin einer Fachhochschule. Von den 8 Personen hat die Hälfte einen rechtswissenschaftlichen und die andere Hälfte einen technischen Hintergrund. Da bei der DSGVO und dem DSA der Österreichbezug nicht unbedingt gegeben ist, da es EU-Verordnungen sind, mussten die Expert*innen nicht zwangsweise die österreichische Sicht vertreten. Aus diesem Grund wurden 4 Expert*innen aus Österreich befragt, 2 aus Deutschland, eine Expertin aus Belgien und eine aus der Schweiz. Basierend auf dem Interviewmaterial der 8 Interviews wird nun im nächsten Abschnitt die Auswertung durchgeführt. Der genaue Vorgang der induktiven Kategorienbildung befindet sich im Anhang in Tabelle 15 dieser Arbeit.

6.1.1 Kategorie: Nachhaltiger Datenschutz

Die erste Kategorie, die sich erschließen ließ, war die des nachhaltigen Datenschutzes. Alle 8 Expert*innen haben sich zu dem Thema geäußert und erklärt, was für sie nachhaltiger Datenschutz bedeutet. Dabei ist klar geworden, dass es kein einheitliches Verständnis von nachhaltigem Datenschutz gibt. Trotzdem bringen 5 von 8 Expert*innen nachhaltigen Datenschutz mit datenschutzrechtlich konformen Umgang mit personenbezogenen Daten seitens Unternehmen in Verbindung. Grob gesagt sollte der Schutz von personenbezogenen Daten Teil der Unternehmensstrategie sein und Unternehmen sollten den Schutz von Betroffenen ernst nehmen, und das langfristig. Eine Person ist der Meinung, dass Verantwortliche sogar über die gesetzlichen Bestimmungen hinausgehen sollten und eine Person meint, dass der Prozess zur Datenhoheit nachhaltiger Datenschutz wäre, das heißt, die Kontrolle über die eigenen Daten. Eine Person bringt nachhaltigen Datenschutz weder mit Betroffenen, noch mit Verantwortlichen oder Unternehmen in Verbindung, sondern appelliert, dass Datenschutz dauerhaft, effektiv und überprüfbar sein müsse und gleichzeitig auch keine Grundrechte einschränken dürfe.

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Nachhaltiger Datenschutz	Jede Textpassage, unter der deutlich wird, was Expert*innen unter „nachhaltigem Datenschutz“ verstehen.	ID1: „Also nachhaltiger Datenschutz bedeutet für mich, dass man nicht nur pro forma die gesetzlichen Bestimmungen einhält, sondern dass man sich wirklich in die Rolle der betroffenen Personen versetzt, also deren Daten man bearbeitet und sich die Frage stellt: Wäre es für mich in Ordnung, dass meine Daten auch in dieser Form verwendet werden?“ (ID1: Z. 40-44, durchgeführt am 10.07.2023)	Textstellen müssen definitorische Aspekte beinhalten, was nachhaltigen Datenschutz betrifft.

Reduktion 2:

ID1: Nachhaltiger Datenschutz bedeutet nicht nur gesetzliche Bestimmungen, sondern sich in Betroffene hineinversetzen (vgl. ID1, Z. 40-44, durchgeführt am 10.07.2023).

ID2: Nachhaltiger Datenschutz ist die möglichst frühe Integration von Datenschutz in jegliche Prozesse eines Geschäftsmodells (vgl. ID2, Z. 327-342, durchgeführt am 24.07.2023).

ID3: Nachhaltiger Datenschutz ist das Niveau, welches allen zugutekommt und nicht nur denjenigen, die an Privatsphäre einen Preis hängen (vgl. ID3, Z. 859-870, durchgeführt am 25.07. 2023).

ID4: Nachhaltiger Datenschutz ist die schrittweise Hoheit über die eigenen Daten (vgl. ID4, Z. 1902-1917, durchgeführt am 25. Juli 2023).

ID5: Nachhaltig wäre es, wenn Unternehmen nicht nach Grauzonen in der DSGVO suchen und Individuen mehr über den Schutz ihrer Daten nachdenken (vgl. ID5, Z. 2509-2515 und 2519-2521, durchgeführt am 31.07.2023).

ID6: Nachhaltiger Datenschutz ist, wenn er effektiv, dauerhaft und überprüfbar passiert und das Risiko unter Kontrolle hat, ohne Grundrechte einzuschränken (vgl. ID6, Z.3114-3126). Nachhaltiger Datenschutz bedeutet auch die Folgen von Lösungen einzuschätzen und im Gesamtkontext zu sehen (vgl. ID6, Z. 3151-3157).

ID7: Datenschutz muss Teil der Unternehmensstrategie sein und in allen Prozessen und Abläufen gelebt werden (vgl. ID7, Z. 3662-3674, durchgeführt am 07.08.2023).

ID8: Nachhaltiger Datenschutz ist, wenn Organisationen nach dem Recht sorgfältig mit Informationen umgehen (vgl. ID8, Z. 4191-4194, durchgeführt am 10.08.2023).

Tab. 3: Kategorie Nachhaltiger Datenschutz (Eigendarstellung angelehnt an Tab. 15)

6.1.2 Kategorie: Verantwortung Union und Staat

Bei der Kategorie Verantwortung von Union und Staat in Tabelle 4 haben sich 7 von 8 Expert*innen geäußert und sehen einen Teilbereich der Verantwortung zum Schutz personenbezogener Daten bei der Union und beim Staat. Dabei sind sich die Expert*innen einig, dass Union und Staat eine gewisse Verantwortung haben, eine Vorlage zu erarbeiten, nach der auch in der Praxis gearbeitet werden kann. Dies kann sich als schwierig herausstellen, da Formulierungen nicht derart offen formuliert sein dürfen, dass sie Rechtsunsicherheit verursachen können und auch nicht so streng geregelt sein dürfen, dass sie andere Grundrechte und Grundfreiheiten einschränken und somit auch Infrastrukturen. 3 von 8 Expert*innen deuten auch an, dass der Staat Bürger*innen ausreichend schützen muss und an und für sich „Personendaten wie die Person selbst“ (ID8, 4209-4212) gesehen werden müssen. Zusammenfassend hat der Staat die Verantwortung, ein Gleichgewicht zwischen Rechten, Freiheit und Interessen zu finden. Trotzdem sehen Expert*innen die größte Verantwortung zum Schutz personenbezogener Daten nicht bei der Union und beim Staat. Dies fasst ID3 gut zusammen:

> „ (…) es gibt tatsächlich eine Reihe von Anpassungen des Verständnisses der Technologie, die jeder vornehmen muss. Regulierungsbehörden, Gesetzgeber und Durchsetzungsbehörden, Regulierungsbehörden und Durchsetzungsbehörden. Und das ist eine echte Herausforderung, denn wir müssen das richtige Gleichgewicht zwischen Innovation und dem Potenzial, das hinter der Verarbeitung personenbezogener Daten steckt, finden und finden, gleichzeitig aber auch einen angemessenen Schutz gewährleisten und für soziale Güter sorgen.“ (ID3, Z. 1019-1026)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Verantwortung Union / Staat	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Union und Staat zum Schutz personen-bezogener Daten haben.	ID1: „Und natürlich ist das auch eine Rechtsunsicherheit für Unternehmen oder Behörden, weil wenn etwas nicht klar geregelt ist und ich dann vielleicht doch eine Geldbuße bekomme, wenn ich dagegen verstoße, ist es natürlich ein Problem." (ID1, Z. 151-155)	Textstellen müssen klar deklarieren, welche Verantwortung Union und Staat zum Schutz personenbezogener Daten haben.

Reduktion 2:

ID1: Wenn Recht nicht klar geregelt ist, sorgt dies für Rechtsunsicherheit und Nachteile (vgl. ID1, Z. 151-155)

ID2: Die Verantwortung, eine Vorlage zu definieren und somit eine Regulierung zu schaffen, liegt bei der EU und den Mitgliedsstaaten (vgl. ID2, Z. 367-371).

ID3: Die Euphorie der 90er und 2000er hat dazu geführt, dass die Auswirkungen von Sozialen Medien und Datenschutz nicht absehbar waren, weswegen die Politik auch nicht sofort reagieren konnte (vgl. ID3, Z. 987-997). Die Probleme des Internets zu erkennen hat gedauert und für Maßnahmen hat es viel Überzeugung in der Politik und in der Gesetzgebung gebraucht (vgl. ID3, Z. 1000-1016). Es müssen noch einige Verständnisanpassungen geschehen, die ein Gleichgewicht zwischen Innovation, Schutzniveau und Potential schaffen müssen (vgl. ID3, Z. 1019-1026). Große Verantwortung haben Regierungen, welche Datenverarbeitung weiter regulieren müssen (vgl. ID3, Z. 1060-1063). Der Staat muss ein ausgewogenes Verhältnis aus Freiheiten, Rechten und berechtigen Interessen finden und den Zugang zu digitalen Dienstleistungen gewähren (vgl. ID3, Z. 1172-1179).

ID4: Die Verantwortung liegt zu großen Teilen beim Staat, da er Bürger*innen schützt und dort reguliert, wo es notwendig ist (vgl. ID4, Z. 1943-1950)

ID5: Es ist als Staat schwer, Gesetze zu schreiben, die alles schützen und nichts einschränken (vgl. ID5, Z. 2560-2561 und 2565-2566). Eigentlich sollte nicht von einzelnen entschieden werden, ob ihre Daten verarbeitet werden oder nicht, sondern eher von einem Expert*innenpool wie z. B. ein Datenschutzrat (vgl. ID5, Z. 2777-2786)

ID6: Der Staat hat eine Infrastrukturverantwortung wie z.B. Social Media und muss darauf achten, dass diese rechtskonform bestehen bleiben, ohne den Weitblick zu verlieren (vgl. ID6, 3197-3211).

I**D8:** Der Staat muss Personendaten wie die Person selbst sehen (vgl. ID8, Z. 4209-4212).

Tab. 4: Kategorie Verantwortung Union und Staat (Eigendarstellung angelehnt an Tab. 15)

6.1.3 Kategorie: Harmonisierungserfolg der DSGVO

Den Harmonisierungserfolg haben 5 von 8 Expert*innen bewertet, wie in Tabelle 5 ablesbar ist. Anhand der Aussagen der Expert*innen kann herausgelesen werden, dass die Öffnungsklauseln einen direkten Einfluss auf den Harmonisierungserfolg der DSGVO hatten. Durch Öffnungsklauseln ist der Harmonisierungserfolg der DSGVO zwar nicht ganz gegeben, dennoch eröffnen sie Spielräume, welche Rechtsakte wie die DSGVO für die Zukunft besser wappnen und nicht neu novelliert werden müssen, wie ID5 argumentiert. Trotzdem sind sich die Expert*innen hier einig, dass die Vollharmonisierung der DSGVO nicht geglückt ist. Dies betont ID6:

> „Um gleich schon zu sagen, ja, jetzt gibt es natürlich Öffnungsklauseln, es wird eben doch unterschiedlich gelebt. Das heißt, ganz ist diese Einigkeit nicht erreicht worden.“ (ID6, Z. 3234-3236)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Harmonisierungs-erfolgs der DSGVO	Jede Textpassage, welche Öffnungsklauseln und den Harmonisierungs-effekt von Datenschutzrecht durch die DSGVO bewertet.	ID1: „Ja, es gibt sogenannte Öffnungsklauseln, wie Sie richtig gesagt haben. Ja, ich denke, je besser man die Lücken schließt, die die DSGVO eröffnet, umso besser.” (ID1, Z. 166-168)	Textstellen müssen eine Bewertung von Öffnungsklauseln oder des Harmonisierungserfolgs durch die DSGVO beinhalten.
Reduktion 2: **ID1:** Je besser Mitgliedsstaaten die Öffnungsklauseln im nationalen Gesetz regeln, desto weniger Lücken in der DSGVO (vgl. ID1, Z. 166-168). **ID4:** Eine Vollharmonisierung wäre besser gewesen, trotzdem sprechen wir in jedem EU-Staat großteils auf dem gleichen Niveau (vgl. ID4, Z. 2160-2170). **ID5:** Die Harmonisierung ist nicht so gut geglückt, da Österreich die Öffnungsklauseln nicht gut geregelt hat, wie zum Beispiel den Forschungsbereich (vgl. ID5, Z. 2608-2611 und 2613-2618). Eine komplette Harmonisierung wäre am besten gewesen, dennoch sind Öffnungsklauseln nicht schlecht, wenn sie gut geregelt werden (vgl. ID5, Z. 2625-2632). Je schneller sich etwas entwickelt, desto offener sollte es geregelt sein, da sonst Gesetze nicht mehr hinterherkommen (vgl. ID5, Z. 2645-2651). **ID6:** Die komplette Harmonisierung konnte mit den Öffnungsklauseln nicht erreicht werden (vgl. ID6, Z. 3236-3244) **ID7:** Die Offenheit der DSGVO hat in der Praxis für viel Rechtsunsicherheit gesorgt, dennoch sind Öffnungsklauseln, wenn sie gut umgesetzt werden, sinnvoll (vgl. ID7. Z. 3996-4009).			

Tab. 5: Kategorie Harmonisierungserfolg der DSGVO (Eigendarstellung angelehnt an Tab. 15)

6.1.4 Kategorie: Verantwortung Unternehmen

Zu dieser Kategorie haben, wie in Tabelle 6 sichtbar, alle 8 Expert*innen geantwortet. Dabei sehen die meisten von ihnen die größte Verantwortung zum Thema Schutz personenbezogener Daten bei den Unternehmen. Alle 8 Expert*innen formulieren genau, was Unternehmen besser machen müssten, woraus sich ableiten lässt, dass Unternehmen die größte Verantwortung haben, rechtskonform zu arbeiten, die Gesetze einzuhalten und das meiste Wissen bezüglich Datenverarbeitung haben. Dabei stellt ein Problem dar, dass kleinere Unternehmen nicht die gleichen Ressourcen haben wie große, aber trotzdem einen ähnlichen Aufwand, was sie nach ID2 vor Herausforderungen stellt und sie dadurch auch benachteiligt. Unternehmen sollten ihre Verantwortung ernster nehmen und nach ID1 Einwilligungserklärungen besser verständlich gestalten. Auch ID7 und ID8 argumentieren, dass Unternehmen eine Rechenschaftspflicht haben, Informationen bereitzustellen. Zwei Expert*innen geben an, dass viele Unternehmen das wirtschaftliche Interesse über das von Datenschutz stellen und deswegen nicht einmal versuchen, rechtskonform zu arbeiten. Von den Expert*innen wird an die Unternehmen appelliert, sich wegen ihrer großen Verantwortung mehr Gedanken zu ihren Prozessen zu machen. Die große Verantwortung der Unternehmen wird von ID7 folgendermaßen untermauert:

> „Also ich glaube, dass die DSGVO sehr stark diese Verantwortung an die Unternehmen abgegeben hat. (…) Und Unternehmen können sich wieder an einer Aussage oder einer Entscheidung orientieren. Aber im Grunde glaube ich, obliegt es den Unternehmen, also den Verantwortlichen, die halt die Pflichten erfüllen müssen, diese Verantwortung auch wahrzunehmen.“ (ID7. Z. 3700-3201 und 3704-3706)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Verantwortung Unternehmen	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Unternehmen haben zum Schutz personen-bezogener Daten	ID2: „Die Verantwortung die Auflagen einzuhalten und Umzusetzen liegt definitiv bei den Unternehmen." (ID2, Z. 364-367)	Textstellen müssen klar deklarieren, welche Verantwortung Unternehmen zum Schutz personenbezogener Daten haben.

Reduktion 2:

ID1: Unternehmen müssen mehr nachdenken, ob Einwilligungserklärungen verständlich sind, dazu können sie auch Betroffene befragen (vgl. ID1, Z. 76-82).

ID2: Die Verantwortung, die Auflagen einzuhalten und umzusetzen, liegt definitiv bei den Unternehmen (vgl. ID2, Z. 364-367). Unternehmen haben die Verantwortung, sich auf neue Regulatoren frühzeitig vorzubereiten, wobei kleinere Unternehmen dadurch oft wegen geringerer Kapazitäten einen Nachteil haben (vgl. ID2, Z. 375-382). Auch wenn in kleineren Unternehmen die Ressourcen für genaue Prozessdarstellung nicht da sind, muss es ein Bewusstsein dafür in allen Unternehmen geben (vgl. ID2, Z. 555-562). Unternehmen haben die Verantwortung, Prozesse zu haben, dass Daten nicht nach draußen gelangen. Wenn sie das doch tun, kommt es bei der Strafe auf die Schnelligkeit der Benachrichtigung an (vgl. ID2, Z. 608-614).

ID3: Es gibt einige Unternehmen, die nicht einmal Aufsichtsbehörden deutlich sagen können, in welchem Umfang sie personenbezogene Daten verarbeiten, was nicht sehr glaubwürdig wirkt (vgl. ID3, Z. 892-898). Es hängt davon ab, wie groß das wirtschaftliche Interesse von Unternehmen an Daten ist, wie ernst sie Datenschutz nehmen (vgl. ID3, Z. 904-907). Große Verantwortung haben Unternehmen bezüglich Rechenschaftspflichten, und sie sollten deswegen überwacht werden (vgl. ID3, Z. 1063-1065).

ID4: Die Verantwortung ist bei Unternehmen größer als beim Staat, da dort das Wissen zur Verarbeitung von Daten sitzt. Ziel ist es, als Unternehmen nach dem Verhältnismäßigkeitsgrundsatz der DSGVO so konform wie möglich zu arbeiten. (vgl. ID4, Z. 1955-1959). Ziel ist es als Unternehmen nach dem Verhältnismäßigkeitsgrundsatz der DSGVO so rechtskonform wie möglich zu arbeiten (vgl. ID4, Z. 1964-1970). Manche Unternehmen verfolgen nicht einmal das Ziel, compliant zu arbeiten (vgl. ID4, Z. 1964-19709).

ID5: Jeder Mensch nutzt die größten Vorteile für sich, das machen auch Unternehmen und diejenigen, die sich an die DSGVO halten, sind leider oft die Verlierer (vgl. ID5, Z. 2962-2970)

ID6: Unternehmen hätten mit der Anonymisierung viel mit Daten anfangen können und andere nichts mehr, was aber Auswirkungen auf den Markt hätte (vgl. ID6, Z. 3159-3166).

ID7: Unternehmen wurde durch die DSGVO die Verantwortung übergeben und sie müssen sich überlegen, ob ihre Prozesse ok sind oder nicht. Die Hauptverantwortung liegt bei Unternehmen (vgl. ID7, Z. 3698-3704). Unternehmen könnten awareness schaffen, indem sie gewisse Dienste und Services nicht verwenden, dies hat sich aber noch nicht durchgesetzt (vgl. ID7, Z. 3704-3707). Als Unternehmen musst du Informationen über Datenverarbeitung zur Verfügung stellen, und das kann kompliziert sein, das einfach und kurz zu formulieren (vgl. ID7, Z. 3707-3718).

ID8: Unternehmen dürfen Personendaten nicht nehmen ohne eine Berechtigung und haben eine Rechenschaftspflicht (vgl. ID8, Z. 4204-4209).

Tab. 6: Kategorie Verantwortung von Unternehmen (Eigendarstellung angelehnt an Tab. 15)

6.1.5 Kategorie: Privacy by Design

Hierzu haben sich 5 Expert*innen geäußert, weswegen die Kategorie Privacy by Design entstanden ist, wie man in Tabelle 7 sieht. Dabei haben die Expert*innen geäußert, dass Privacy by Design zwar sinnvoll ist, es aber dennoch in der Praxis oft noch technische, aber auch organisatorische Hürden gibt, wie ID8 argumentiert. Wie man in Tabelle 7 erkennt, haben 3 von 5 Expert*innen geäußert, dass gewisse Formulierungen noch unklar sind und dies für Hürden bei der Umsetzung dieser sorgt, vor allem von technischer Seite. ID5 geht sogar so weit zu sagen, dass nicht einmal klar ist, was Anonymisierung oder Privacy by Design in der Umsetzung genau bedeutet. Dieses Problem der Unklarheit fasst ID5 zusammen:

> „Was ist Privacy by Design? Schnellst mögliche Anonymisierung? Überhaupt anonym arbeiten? Was ist Anonym arbeiten? Da wissen Sie, wenn Sie zen ITler fragen, kriegen Sie zwölf Antworten, was Anonymisierung ist dahinter. Und das ist, was einfach fehlt, weil nur weil es für uns vielleicht logisch ist.“ (ID5, Z. 2665-2669)

Auch wird Privacy by Design nicht von allen Unternehmen auf gleiche Weise ernst genommen, vor allem, wenn es um Konkurrenzkampf geht und es darauf ankommt, welches Produkt schneller am Markt ist, meint ID4. ID8 argumentiert so weit, dass die Person angibt, dass eine Datenschutzfolgenabschätzung nicht einmal notwendig ist, wenn Privacy by Design korrekt umgesetzt wird, da eigentlich keine Risiken mehr bestehen sollten.

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Privacy by Design	Jede Textpassage, welche die Privacy by Design-Regelung in der DSGVO bewertet.	ID4: „Und auch dieser Privacy by Design Grundsatz halte ich für absolut sinnvoll. Aber das können andere Unternehmen im internationalen Vergleich halt dann einfach nicht so krass berücksichtigen und haben dadurch vielleicht schneller ein Produkt, das dann doch so überzeugend ist für den Endkunden, dass er sagt okay, das ist mir jetzt relativ egal, ob ich da eine gewisse Anzahl an Daten preisgeben muss oder ob das jetzt optimiert ist auf Privacy by Design oder bei Default.“ (ID4, Z. 2143-2148)	Textstellen müssen eine Bewertung der Privacy by Design-Regelung beinhalten.

Reduktion 2:

ID2: Die Privacy by Design Regelung beschreibt Techniker*innen ganz gut, was zu tun ist. Trotzdem verbessern Beispiele, wie jene, auf die die EU hinweist, die Umsetzung (vgl. ID2, Z. 459-468)

ID4: Privacy by Design ist wichtig, aber das berücksichtigen nicht alle, wenn es darum geht, wer schneller am Markt ist (vgl. ID4, Z. 2143-2148).

ID5: Privacy by Design ist zu offen gestaltet und es gibt wenig Klarheit, was mit Privacy by Design genau gemeint ist (ID5, Z. 2667-2673). Es ist unklar, bei welchem IT Ansatz man bei Privacy by Design ansetzt, denn es gibt allein Unklarheit, was Anonymisierung bedeutet (vgl. ID5, Z. 2689-2695 und 2702-2704).

ID6: Die Privacy by Design-Regelung ist noch unterentwickelt und es fehlt Klarheit, wie zum Beispiel eine Methode zur Privacy by Design (vgl. ID6, Z. 3306-3307 und 3313-3321).

ID8: Grundsätzlich ist Privacy by Design sehr gut, dennoch gibt es in der Praxis oft Hürden, was Einschränkungen von technischer Seite und organisatorischer Seite betrifft (vgl. ID8, Z. 4278-4285). Wenn man Privacy by Design lebt, dann braucht es keine DSFA (vgl. ID8, Z. 4325-4327).

Tab. 7: Kategorie Privacy by Design (Eigendarstellung angelehnt an Tab. 15)

6.1.6 Kategorie: DSFA

Wie in Tabelle 8 dargestellt, haben sich 4 von 8 Expert*innen zur Datenschutzfolgenabschätzung geäußert. Dabei kommt heraus, dass derzeit viel Unklarheit um die Datenschutzfolgenabschätzung herrscht, wie zum Beispiel, wann überhaupt eine durchgeführt werden muss, denn ID4 und ID5 stellen fest, dass dies nicht klar ist. ID8 hingegen deklariert, dass sie eigentlich vor jedem Projekt stattfinden müsste. 3 von 4 Expert*innen deuten außerdem an, dass eine DSFA strenger kontrolliert werden müsste, da nach ID4 unklar ist, wie seriös diese wirklich durchgeführt wird und nach ID5 undurchsichtig ist, was basierend auf den Ergebnissen wirklich technisch umgesetzt wird. ID4 argumentiert dazu folgendes:

> „Problematisch ist es natürlich, wenn ich mich selber eigentlich überwache. Und man könnte natürlich sagen, ja, bei allen Themen, die halt eine Datenschutzfolgenabschätzung bedürfen, also dort, wo es kritisch wird, wäre es sinnvoll, wenn irgendwie eine externe Stelle eingebunden wäre oder eine staatliche Stelle, ist ja dann auch im letzten Schritt vorgesehen.“ (ID4. Z. 3886-3889)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
DSFA	Jede Textpassage, welche die DSFA-Regelung in der DSGVO bewertet.	ID8: „Also eigentlich eine Datenschutzfolgeabschätzung erwarte ich immer bei jedem Start eines Projektes. Irgendwie in einer Form. (…) Es dürfte ja gar nicht zu großem Risiko unterwegs sein. Und da sehe ich zum Teil einen Widerspruch, weil jetzt zum Teil für alles noch Datenschutzfolgenabschätzung gemacht werden. Und das ist vielleicht auch das Instrument nicht immer richtig verstanden oder eingesetzt.“(ID8, Z. 4305-4310)	Textstellen müssen eine Bewertung der DSFA-Regelung beinhalten
Reduktion 2: **ID4:** Wie seriös eine DSFA gemacht wird, variiert stark, wenn es überhaupt zu einer kommt, Unternehmen ist es wichtig, einer Aufsichtsbehörde etwas vorweisen zu können (vgl. ID4, Z. 1991-2006). **ID5:** Wann genau eine DSFA gebraucht wird, ist unklar und was technisch wirklich umgesetzt wird, auch, weswegen strenger kontrolliert werden müsste (vgl. ID5, Z. 2720-2730). **ID7:** Die DSFA ist trotz des großen Aufwands eine gute Sache, um Datenverarbeitungsprozesse systematisch aus allen Blickwinkeln zu prüfen (vgl. ID7, Z. 3837-3846 und 3849-3853). Die Verantwortung liegt bei den Unternehmen, das zu machen und nicht bei Aufsichtsbehörden und ist außerdem ressourcenabhängig (vgl. ID7, Z. 3864-3870). Es ist problematisch, sich bei einer DSFA selbst zu überwachen und es wäre besser, wenn dies externe oder staatliche Stellen machen würden (vgl. ID7, Z. 3886-3893). **ID8:** Eine DSFA muss vor jedem Projekt sein, um das Risiko einzuschätzen und wenn Privacy by Design korrekt gelebt werden würde, dann würde es keine DSFA benötigen (vgl. ID8, Z. 4305-4310).			

Tab.8: Kategorie Datenschutzfolgenabschätzung (Eigendarstellung angelehnt an Tab. 15)

6.1.7 Kategorie: Verantwortung Betroffene und Konsument*innen

In Tabelle 9 ist die Kategorie der Verantwortung von Betroffenen und Konsument*innen abgebildet, zu dieser sich 7 von 8 Expert*innen geäußert haben. Dabei ist aufgefallen, dass eine gewisse Einigkeit besteht, dass die Betroffene und Konsument*innen zwar ein gewisses Maß an Verantwortung haben, welche Daten sie von sich preisgeben und, dass dafür ein größeres Bewusstsein herrschen muss. Dennoch äußert ID3, dass dazu einen digitale Bildung notwendig ist, ID4, dass für Verantwortung eine Informiertheit vorauszusetzen ist und ID1, dass großer Handlungsbedarf besteht. Diese Problematik fasst ID3 im Folgenden zusammen:

> „Ja, auch auf individueller Ebene würde ich persönlich nicht so viel Wert darauf legen. Wir brauchen, in gewisser Weise,(…), digitale Bildung. Wir sollten meiner Meinung nach nicht den Schwerpunkt der Verantwortung auf die Endnutzer und Verbraucher legen. (…).“ (ID3, Z. 1055-1056 und 1058-1060)

Zusammenfassend wird also ein gewisses Maß an Verantwortung zum Schutz personenbezogener Daten bei den Einzelnen gesehen, das aber gleichzeitig gewisses Maß an Informiertheit voraussetzt, welches nicht unbedingt vorhanden ist.

Kategorie	Kriterien	Ankerbeispiel	Kodier Regel
Verantwortung Betroffene/ Konsument*innen	Jede Textpassage, unter welcher deutlich wird, welche Verantwortung Betroffene & Konsument*innen haben zum Schutz personen-bezogener Daten.	ID1: „Die praktische Sicht ist natürlich die, dass selbstverständlich auch Betroffene ihre eigenen Daten unter Anführungszeichen verantwortlich sind." (ID1, Z. 98-108)	Textstellen müssen klar deklarieren welche Verantwortung Betroffene/Konsument*innen zum Schutz personenbezogener Daten hat

Reduktion 2:

ID1: Betroffene haben ein gewisses Maß an Selbstverantwortung und sind für den Schutz ihrer Daten verantwortlich, da ist großer Handlungsbedarf (vgl. ID1, Z. 98-108).

ID3: Die große Verantwortung liegt nicht bei den Verbraucher*innen, dennoch brauchen sie digitale Bildung (vgl. ID3, Z. 1055-1060).

ID4: Betroffene können nicht so stark in der Verantwortung stehen, da Eigenverantwortung Informiertheit voraussetzt (vgl. ID4, Z. 1933-1943). Ein gewisses Maß an Verantwortung liegt auch bei den Betroffenen (vgl. ID4, Z. 1953-1955).

ID5: Betroffene sollten mehr über den Schutz ihrer Daten nachdenken, nicht überall mitmachen und alles preisgeben (vgl. ID5, Z. 2535-2538 und 2541-2544).

ID6: Alle, auch Privatpersonen, die Datenverarbeiten haben eine Verantwortung, aber weniger rechtliche Pflichten und viel Verantwortung kann man nicht bei den Einzelnen einordnen (vgl. ID6, Z. 3190-3195).

ID7: Konsument*innen können steuern, ob sie gewisse Dienste und Services nutzen oder nicht aber das ist in der Praxis unwahrscheinlich (vgl. ID7, Z. 3719-3729).

ID8: Es liegt Verantwortung beim Einzelnen, da sie sensibler mit ihren Daten umgehen und sich auch wehren müssen (vgl. ID8, Z. 4212-2020).

*Tab.9: Kategorie Verantwortung Betroffene / Konsument*innen (Eigendarstellung angelehnt an Tab. 15)*

6.1.7 Kategorie: Verständnis von Einwilligungen

Zum Verständnis von Einwilligungserklärungen haben sich 6 von 8 Expert*innen geäußert, wie in Tabelle 10 nachvollzogen werden kann. Aus den Aussagen der Expert*innen geht hervor, dass Einverständniserklärungen trotz einfacher Sprache nicht unbedingt verständlich sind, was durch die komplexe Prozessbeschreibung unter anderem an der Länge dieser liegt. Zwei Expert*innen argumentieren, dass es ein gutes Mittel sei, um sich als Unternehmen abzusichern. ID3 und ID7 kritisieren gleichzeitig, dass Einwilligungserklärungen nicht unbedingt die Form zur Verarbeitung personenbezogener Daten ist, die Betroffene am besten schützt. Dies deuten 5 von 6 Expert*innen an, indem sie argumentieren, dass Einwilligungserklärungen zu lang und zu komplex sind und, dass sie deswegen nicht gelesen werden. Außerdem wird von ID1 argumentiert, dass unklar ist, was Durchschnittsverbraucher*innen verstehen. Das gleiche deutet ID5 an mit dem Argument, dass unklar ist, wann Menschen einwilligungsfähig sind und gleichzeitig die Inhalte immer komplexer werden.

> „Ich tu mir immer schwer, sie sollen immer einfacher geschrieben werden, die Einwilligung, also Klärungen, Stichwort einfache Sprache, kurzer Sätze und alles. Dann mich juckt es dann immer zu hinterfragen, sind diese Menschen überhaupt einwilligungsfähig(…)? Andererseits erkläre ich, eigentlich müsste man ja jede KI im Hintergrund erklären, was da passiert und wie die verarbeitet. Ich habe jetzt schon einen relativ technischen Hintergrund und wenn mir mein Mann seine KI's erklärt, denke ich mir, ja, was will er von mir eigentlich?“ (ID5, Z. 2743-2745 und 2748-2751)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Verständnisses der Einwilligungs-erklärung	Jede Textpassage, welche das Verständnis von Einwilligungserklärungen in der DSGVO bewertet.	ID1: „Nach Judikatur stellt man auf den Durchschnittsverbraucher ab, das heißt nicht auf einen Analphabeten, der nicht lesen kann, aber eben auch nicht auf den besten Datenschutzexperten, Datenschutzexpertin in der Welt. Aber auch dieser Maßstab, also den Durchschnitt sozusagen, würde ich hier unten anlegen. Also der Durchschnittsverbraucher oder verbrauchin kennt sich eben nicht so gut aus.” (ID1, Z. 72-76)	Textstellen müssen das Verständnis von Einwilligungen und den Informationsstand von Bürger*innen beurteilen.
Reduktion 2: **ID1:** Datenschutzerklärungen bieten Unternehmen Absicherung und Rechtssicherheit, dadurch sind sie aber für Betroffene nicht verständlich (vgl. ID1, Z. 44-50. Durchschnittsverbraucher*innen kennen sich mit Einverständniserklärungen nicht so gut aus, darum müssen sie einfach formuliert sein (vgl. ID1, Z. 72-76). **ID2:** Wenn Unternehmen ihre Prozesse ausführlich in Datenschutzerklärungen beschreiben, sind sie rechtlich abgesichert, jedoch werden sie sehr lang (vgl. ID2, Z. 538-547). Da Einwilligungserklärungen derart lang sind und sie keiner liest, sollten Paragraphen und Absätze zusammengefasst werden (vgl. ID2, Z. 538-547). **ID3:** Für die individuelle Autonomie der Einzelnen muss ein Bewusstsein da sein, was auf dem Spiel steht, und da dies nicht der Fall ist, ist die Zustimmung nicht das beste Instrument (vgl. ID3, Z. 924-934). Unter Datenschutzexpert*innen ist die Einwilligungserklärung nicht die am besten schützende Form, dennoch gewichten sie Gerichte sehr stark (vgl. ID3, Z. 1086-1091 und 1096-1099). **ID5:** Es ist schwer einzuschätzen, wann Menschen einwilligungsfähig sind, und das Ganze wird noch schwerer, wenn erklärt werden muss, wie eine KI funktioniert (vgl. ID5, Z. 2744-2754). **ID7:** Einwilligungen und das Prinzip der Transparenz und der Zustimmung sind gut, doch sind Prozesse manchmal so komplex, dass die Ausgestaltung der derzeitigen Einwilligung nicht das beste Mittel ist (vgl. ID7, Z. 3906-3918). Für ein besseres Verständnis sollte eine Einwilligung vielleicht nur eine A4 Seite mit bestimmten Informationen und mit einer Standardstruktur sein (vgl. ID7, Z. 3924-3933). Die Information muss bereitgestellt werden und dadurch wird die Einverständniserklärung so lang (vgl. ID7, Z. 3943-3947). **ID8:** Einwilligungserklärungen sind nicht gut formuliert und unverständlich. Online könnte die Benutzer*inneneinführung durch Videos verbessert werden (vgl. ID8, Z. 4258-4262).		

Tab.10: Kategorie Verständnis Einwilligungserklärungen (Eigendarstellung angelehnt an Tab. 15)

6.1.8 Kategorie: Vorteile / Stärken der DSGVO

Zu den Vorteilen oder Stärken der DSGVO haben sich alle 8 Expert*innen geäußert und sind sich überwiegend einig, dass ein großer Vorteil ist, dass die DSGVO einen EU-weiten Standard abbildet und dem Datenschutz damit eine nie zuvor dagewesene internationale Prominenz und Aufmerksamkeit verschafft wurde.

Zudem haben 3 der Expert*innen hervorgehoben, dass die offenen Formulierungen dafür sorgen, dass das Gesetz auch in Zukunft anwendbar bleibt und nicht ständig novelliert werden muss. ID6 ging sogar so weit zu argumentieren, dass die offenen Formulierungen der DSGVO auch vor Innovationen wie KI wappnen. ID7 fasst im Folgenden die Stärken zusammen:

> „Ich meine, die Stärke ist schon, man muss schon sagen, das hat sich schon als Standard durchgesetzt weltweit. (…) Ja, die Vorteile für ein Unternehmen, das ist natürlich, (…) Interpretationsmöglichkeiten. (…) Also es soll jetzt nichts sein, wo dann durch Technologieentwicklungen das in zwei Jahren eigentlich obsolet ist oder die Regelungen keinen Sinn mehr machen." (ID7, Z. 3756-3758 und Z. 3780-3782)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Vorteile/Stärken der DSGVO	Jede Textstelle, welche einen positiven Effekt der DSGVO auf den Schutz personen-bezogener Daten deklariert.	ID1: "Das wäre wahrscheinlich falsch, aber es hat einfach nicht diese Aufmerksamkeit bekommen, sage ich einmal. Das hat sich eben mit der DSGVO geändert, allein schon aufgrund der medialen Berichterstattung." (ID1, Z. 125-131)	Textstellen müssen sich klar zu positiven Effekten der DSGVO äußern.

Reduktion 2:

ID1: Die DSGVO hat für Aufmerksamkeit gegenüber Datenschutz gesorgt (vgl. ID1, Z. 120-123). Die DSGVO hat individuell, medial und international für Aufmerksamkeit gegenüber Datenschutz gesorgt (vgl. ID1, Z. 125-131).

ID2: Die Betroffenenrechte wurden in der DSGVO klar und strukturiert formuliert (vgl. ID2, Z. 399-402).

ID3: Die DSGVO ist durch ihre allgemeine Formulierung technikneutral und deswegen langwierig (vgl. ID3, Z. 943-954).

ID4: Vorteile sind die EU-weiten Transparenzpflichten, dass Bürger*innen geschützt werden und sich wehren können und der Sanktionsgedanke in Unternehmen jeder Größe (vgl. ID4, Z. 2019-2035). Durch die DSGVO nehmen Unternehmen Datenschutz ernster (vgl. ID4, Z. 2040-2047).

ID5: Ein einheitliches Rechtssystem in der EU ist die Stärke (vgl. ID5, Z. 2579-2581, 2584-2585 und 2596-2598).

ID6: Die Vereinheitlichung in allen Mitgliedsstaaten und die Gültigkeit auch außerhalb der EU ist ein großer Erfolg (vgl. ID6, Z. 3221-3222 und 3227-3235). Die DSGVO ist ein Fundament, das auch gegen zukünftige Innovationen wie künstliche Intelligenz gewappnet ist (vgl. ID6, Z. 3275-3280).

ID7: Die DSGVO hat sich als Standard im europäischen Raum und als Vorbild durchgesetzt und gilt für alle, die mit EU-Bürger*innen- Daten arbeiten und ist so weit interpretierbar, dass dies einen Spielraum für Unternehmen bietet und auch in Zukunft anwendbar bleibt (vgl. ID7, Z. 3759-3765 und 3770-3785). Die Interpretationsfähigkeit der DSGVO macht sie auch zukunftstauglich (vgl. ID7. Z. 3805-3810). Das Gute ist, wenn man von Datenschutz spricht, dann ist es die DSGVO, trotz all ihrer Interpretationen und auch guter Spielräume ist sie ein guter Standard (vgl. ID7, Z. 3816-3821 und 3323-3229).

ID8: Vorteile der DSGVO sind teils die gute Umsetzung in der EU, als auch die globalen Auswirkungen, die Prominenz von Datenschutz und einen Standard zu finden (vgl. ID8, Z. 4234-4238).

Tab.11: Kategorie Vorteile / Stärken der DSGVO (Eigendarstellung angelehnt an Tab. 15)

6.1.9 Kategorie: Nachteile / Schwächen der DSGVO

Auch bei den Nachteilen der DSGVO haben sich, wie in Tabelle 12 nachvollziehbar, alle 8 Expert*innen geäußert. Dabei haben 6 von 8 Expert*innen geäußert, dass es ein Nachteil ist, dass die vagen Formulierungen für sehr viel Interpretationsspielraum sorgen und somit für viel Rechtsunsicherheit. Aus diesem Grund ist sehr viel Unklarheit darüber entstanden, wie sich Unternehmen rechtskonform zu verhalten haben. 4 von 8 Expert*innen haben sich außerdem dazu geäußert, dass es ein Problem darstellt, dass sich kleine und mittlere Unternehmen genauso an die DSGVO halten müssen, wie ganz große. Dies fasst ID4 im Folgenden zusammen:

> „Also die DSGVO hat überschießende Tendenzen drinnen, die ganz offensichtlich größere Unternehmens sind, die tatsächlich Datenverarbeiter im Hauptgeschäft sind, quasi als Target haben. Und das hat mittelständische und kleinere Unternehmen mitgetroffen, wo das Risiko eine ganz andere ist.“ (ID4, Z. 1970-1973)

Dadurch werden laut ID6 tendenziell Innovationen aus Angst vor Bußgeldern verhindert, wohingegen große Unternehmen mit den Strafen kalkulieren können. Zwei Expert*innen argumentieren, dass manche Regelungen derart streng sind, dass es gerade für kleinere Unternehmen schwer ist,100% rechtskonform zu arbeiten. Zwei Expert*innen argumentieren außerdem, dass der bürokratische Aufwand durch die DSGVO enorm gestiegen sei. ID4 argumentiert, dass die DSGVO den Markt weniger attraktiv macht.

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Nachteile/ Schwächen der DSGVO	Jede Textstelle, welche einen negativen Effekt der DSGVO auf den Schutz personen-bezogener Daten deklariert.	ID1: "Es gibt viele Dinge, die ich wahrscheinlich ändern würde. Damit beginnen, dass viele Dinge einfach unpräzise sind und unklar sind." (ID1, Z. 141-147)	Textstellen müssen sich klar zu negativen Effekten der DSGVO äußern.

Reduktion 2:
ID1: Viele Dinge sind in der DSGVO unklar formuliert, was im Falle der Datenkopie Auswirkungen auf Betroffene haben kann (vgl. ID1, Z. 141-147).

ID2: Ein Nachteil ist die räumliche Anwendung, da dies für Unternehmen außerhalb der EU nicht klar ist (vgl. ID2, Z. 402-405). Der Umgang mit dem räumlichen Anwendungsbereich ist komplex, wie zum Beispiel für EU Unternehmen mit Daten aus Großbritannien (vgl. ID2, Z. 421-428). Für die Verarbeitung von personenbezogenen Daten benötigt man große juristische Kenntnisse (vgl. ID2, Z. 437-441). Ein Nachteil in der DSGVO sind die vagen Formulierungen, wie zum Beispiel die Datenübertragbarkeit, wo es keine Standards gibt (vgl. ID2, Z. 481-484 und Z. 493-500).

ID3: Die Technikneutralität ist auch eine Schwäche, da es Zeit braucht, die DSGVO ständig neu zu interpretieren, um ihr ganzes Potential auszuschöpfen (vgl. ID3, Z. 954-969). Die Schwierigkeit im Datenschutzrecht liegt in der Kreuzung zwischen individuellem und kollektivem Recht, denn die Bedrohung liegt eigentlich in der kollektiven Verarbeitung personenbezogener Daten (vgl. ID3, Z. 1027-1042). Die offenen Formulierungen der DSGVO und der Missbrauch von Unternehmen hat zu unbeabsichtigten Ungleichheiten geführt (vgl. ID3, Z. 1131-1138).

ID4: Die DSGVO hat überschießende Tendenzen, die nicht nur große Unternehmen, sondern auch kleinere und mittlere trifft (vgl. ID4, Z. 1971-1974). Nachteile sind der bürokratische Aufwand seitens der Verantwortlichen und der Informationsoverload seitens Betroffener (vgl. ID4, Z. 2040-2047). Kleine Anbieter können manchmal nicht 100% compliant arbeiten, da hier die DSGVO an der technischen Realität vorbeigeht und es sonst zu einem Verwaltungsalbtraum wird (vgl. ID4, Z. 2081-2093). Ein Nachteil ist, dass die DSGVO Innovationen aufhält und Europa als Markt unattraktiver macht (vgl. ID4, Z. 2137-2143).

ID5: Große Unternehmen kalkulieren, wie groß die Strafe und wie lange das Verfahren ist und nicht die compliance (vgl. ID5, Z. 2566-2571). Zu den Schwächen gehören unklare Formulierungen, bei denen keine Techniker*innen hinzugezogen wurden (vgl. ID5, Z. 2585-2590 und 2593-2596). Wenn Dinge wie durch die DSGVO stark eingeschränkt werden, können Geschäftsmodelle zusammenbrechen, vor allem kleinere Unternehmen (vgl. ID5, Z. 2854-2856 und 2865-2868). Ich als Datenschützerin finde die DSGVO nervig, da diejenigen, die etwas ändern sollten, sie nicht ernst nehmen (vgl. ID5, Z. 2898-2901).

ID6: Sowohl die abstrakten Formulierungen, als auch die anfängliche Umsetzung in den Unternehmen hat sich als schwierig erwiesen (vgl. ID6, Z. 3244-3254). Einige Dinge wurden noch nicht ausformuliert in der DSGVO wie zum Beispiel eine Zertifizierung (vgl. ID6, Z. 3267-3274). Eine Schwäche der DSGVO ist die Fehlentwicklung, dass große Unternehmen sie sabotieren und kleine sich nicht an Innovationen herantrauen aus Angst vor Sanktionen (vgl. ID6, Z. 3282-3290). Viele wissen nicht, was Best Practice beim Datenschutz ist und das führt dazu, dass die Angst vor Innovationen und Bußgeldern groß ist und mehr Klarheit und Untersagungsarten kommen müssen (vgl. ID6, Z. 3371-3376 und 3384-3389). Personendaten wurden zur Zeit der Grundentscheidungen anders verstanden, und die Rolle von Login- und Netzwerkeffekten war nicht absehbar und ist unzureichend definiert (vgl. ID6, Z. 3523-3528).

ID7: In der Praxis sind das Auskunftsrecht und die Informationspflichten für Unternehmen nur schwer machbar(vgl. ID7, Z. 3766-3770). Da die DSGVO noch jung ist, gibt es noch nicht viele Rechtssprechungen, die Interpretationen klären (vgl. ID7, Z. 3794-3799). Stellen mit viel Interpretationsspielraum werden von Unternehmen und Betroffenen zu ihren Gunsten ausgelegt, woraus solange eine Spannung entsteht, bis ein Höchstgericht entscheidet (vgl. ID7, Z. 3955-3962 und 3963-3967). Allgemeine Formulierungen sorgen nun einmal für Interpretationsspielräume und Rechtsunsicherheit (vgl. ID7, Z. 3976-3981).

ID8: Die Standardisierung der DSGVO wurde durch die Öffnungsklauseln geschwächt und manche Zielsetzungen der DSGVO greifen nicht (vgl. ID8, Z. 4224-4250).

Tab.12: Kategorie Nachteile / Schwächen der DSGVO (Eigendarstellung angelehnt an Tab. 15)

6.1.10 Kategorie: Einfluss des DSA auf Schutz personenbezogener Daten

Zum Einfluss des DSA auf den Schutz personenbezogener Daten haben sich 6 von 8 Personen geäußert, wobei 5 von ihnen behaupten, dass der Digital Services Act einen positiven Einfluss auf den Schutz personenbezogener Daten haben wird. Genauer gesagt haben 3 von ihnen behauptet, dass die zusätzlichen Regulierungen für Plattformen den Schutz von Daten indirekt stärken werden und es jene Plattformen am stärksten treffen wird, die am meisten Schaden verursachen. Die indirekte Wirkung fasst ID8 im Folgenden zusammen:

> „Weil, also, weil diese großen Anbieter jetzt auch klare Vorgaben erhalten, wie sie auftreten am Markt, was sie und somit auch klar kommunizieren müssen. Und das hat einen Einfluss auf den Umgang mit personenbezogenen Daten. Und zum Teil müssen sie sich auch zertifizieren oder Rechenschaft abgeben dem Staat gegenüber. Und das hat eine ordnende Wirkung auf den Umgang mit Informationen und somit auch auf personenbezogene Daten.“ (ID8, Z. 4368-4373)

ID7 behauptet hingegen, dass der Datenschutz allein deswegen gestärkt wird, weil das Risiko, nicht rechtskonform zu arbeiten, bei zwei großen Rechtsakten noch größer wird und somit die Strafen auch für große Unternehmen abschreckend sind. Dementgegen stellt sich die Argumentationslinie von ID5, welche behauptet, dass Unternehmen aus den USA durch die EU eingeschränkt werden und dass darauf geachtet werden muss, dass der DSA mit den Grundrechten vereinbar bleibt. Ganz konkret hat sich ID3 geäußert, dass der DSA den Schutz von personenbezogenen Daten erweitert, indem ein Verbot eingeführt wird, dass Minderjährige gezielten Inhalten und gezielter Werbung ausgesetzt werden und dass Online-Werbung, basierend auf sensiblen Daten, verboten wird. Dem Schutz von Kindern als Erweiterung schließt sich auch ID4 an.

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Einfluss des DSA auf Schutz personen-bezogener Daten	Jede Textstelle über den DSA, welche einen Effekt auf den Schutz personenbezogener Daten deklariert.	ID1: „Also kurz gesagt, es gibt natürlich sehr viele, ich nenne sie mal Synergieeffekte. Also das heißt, selbstverständlich wird auch dadurch das Grundrecht auf Datenschutz gestärkt, auch wenn es jetzt nicht primär um Datenschutz geht, sondern sozusagen allgemein um Plattformregulierung." (ID1, Z. 193-204)	Textstellen müssen klar zu Effekten des DSA auf den Schutz personenbezogener Daten haben.

Reduktion 2:

ID1: Der DSA wird mit den Transparenzpflichten und den Plattformregulierungen das Grundrecht auf Datenschutz stärken (vgl. ID1, Z. 193-204).

ID3: Der DSA wird die DSGVO mit zwei Verboten ergänzen, einerseits das Verbot, Kinder gezielter Werbung und Inhalten auszusetzen und andererseits das Verbot, Werbung basierend auf sensiblen Daten auszustrahlen (vgl. ID3, Z. 1205-1216). Der DSA trifft die, die am problematischsten sind und, da Werbung basierend auf sensiblen Daten als sehr gefährlich eingestuft wurde, wurde sie jetzt verboten (vgl. ID3, Z. 1222-1232).

ID4: Es ist gut, dass Provider nun Regeln bekommen, die zum Schutz von Kindern dienen und, dass es auch die trifft, die nicht in der EU sind (vgl. ID4, Z. 2195-2204). Es kann sein, dass sich große internationale Dienstanbieter aus dem EU-Markt zurückziehen, da sie in ihren Ländern an und für sich rechtskonform arbeiten (vgl. ID4, Z. 2012-2025). Auch wenn es für europäische Provider nicht so schlecht wäre, kann es sein, dass der DSA eine gegenläufige Wirkung für Provider hat (vgl. ID4, 2244-2249).

ID5: Fragwürdig bleibt, ob der DSA aus der EU die USA stark einschränkt, und die Vereinbarkeit des DSA mit den Grundfreiheiten, speziell mit der Meinungsfreiheit, ist fraglich (vgl. ID5, Z. 2923-2934).

ID7: Der DSA wird auch für mehr Beachtung gegenüber der DSGVO sorgen, da das Compliance Risiko steigt (vgl. ID7, Z. 4018-4029). Irgendwann ist das Risiko auch für große Unternehmen zu hoch, wenn sie gegen mehr als ein Gesetz verstoßen (vgl. ID7, Z. 4043-4054).

ID8: Der DSA hat durch die neuen Vorgaben einen Einfluss auf personenbezogene Daten, da die klare Kommunikation und die Rechenschaftspflichten eine ordnende Wirkung haben (vgl. ID8, Z. 4371-4376).

Tab.13: Kategorie Einfluss des DSA auf Schutz personenbezogener Daten (Eigendarstellung angelehnt an Tab. 15)

6.1.11 Kategorie: Herausforderungen in Zukunft für Datenschutz

Bei dieser Kategorie haben alle 8 Expert*innen geantwortet, dabei haben 6 von 8 Expert*innen argumentiert, dass künstliche Intelligenz die größte Herausforderung für Datenschutz wird, dennoch waren die Gründe unterschiedlich. Sie argumentieren, dass durch die enorme Datenverarbeitung zunehmende Komplexität entsteht. Dennoch stellen für die Expert*innen die KI-Systeme den Datenschutz vor die größten Herausforderungen, sowohl für Unternehmen als auch für Betroffene. 2 Expert*innen argumentieren, dass auch die Haftung bei KI und Machine-learning-Systemen eine Herausforderung darstellen wird. ID5 argumentiert, dass KI von Menschen angelernt und dadurch auch negativ beeinflusst wird. 2 Expert*innen argumentieren, dass die zunehmenden Daten dazu führen, dass die Komplexität steigt. ID6 behauptet weiters, dass die Herausforderung durch KI auch darin besteht, dass der Unterschied zwischen real und falsch schwerer zu erkennen wird. ID3 ist außerdem der Meinung, dass Datenschutz komplexer wird, wenn die Privatsphäre weiter von Plattformen monetarisiert wird, sodass mehr Geld gleichzeitig mehr Privatsphäre bedeutet und dass dadurch Grundfreiheiten gefährdet werden. Die zunehmende Komplexität technischer Systeme wie KI stellt also für Expert*innen mit unterschiedlichen Argumenten die größte Herausforderung in Zukunft dar und zwar für Staat, Unternehmen und auch für Betroffene. ID1 fasst gut den Standpunkt zu den Herausforderungen der meisten befragten Expert*innen zusammen:

„Aber nichtsdestotrotz würde ich trotzdem sagen AI. So die massenhafte Datenverarbeitung innerhalb eines kurzen Zeitraums mit sehr sehr viel Rechenleistung.“ (ID1, Z. 216.218)

Kategorie	Kriterien	Ankerbeispiel	Kodierregel
Heraus-forderungen in Zukunft für Datenschutz	Jede Textstelle, welche eine Herausforderung in der Zukunft zum Schutz personenbezogener Daten erwähnt.	ID1: „Aber nichtsdestotrotz würde ich trotzdem sagen AI. So die massenhafte Datenverarbeitung innerhalb eines kurzen Zeitraums mit sehr sehr viel Rechenleistung." (ID1, Z. 216-227)	Textstellen müssen klar definieren, was eine Herausforderung in Zukunft zum Schutz personenbezogener Daten sein kann und was nicht.

Reduktion 2:

ID1: Künstliche Intelligenz und deren enorme Datenverarbeitung wird eine technologische und rechtliche Herausforderung (vgl. ID1, Z. 216-227).

ID2: Herausforderungen in der Zukunft werden Technikneutralität und selbstlernende Machine learning-Modelle sein (vgl. ID2, Z. 718-726). Die Repräsentant*innenhaftung wird eine Herausforderung, weil sich die Verantwortung auf das System verschiebt (vgl. ID2, Z. 734-742). Je größer der Reifegrad von KI wird, desto schwieriger wird das in Zukunft mit Personendaten werden (vgl. ID2. Z. 765-769).

ID3: Wenn Privatsphäre weiter monetarisiert wird, dann können sich reichere mehr Privatsphäre und Datenschutz leisten als ärmere (vgl. ID3, Z. 1107-1123). Die sozialen Medien und digitalen Dienste sind entscheidend für Informationsfreiheiten und Zugang zu Information, weswegen der Zugang allen ermöglicht werden muss (vgl. ID3, Z. 1149-1158).

ID4: Neben der Tendenz, sein Leben zu veröffentlichen, wird es eine Herausforderung, mündige Bürger*innen zu schaffen (vgl. ID4, Z. 2281-2284). Je stärker Rechte von Betroffenen und Sanktionen angehoben werden und die Datenflut steigt, desto mehr Missbrauchsfälle dieser Rechte wird es auch geben (vgl. ID4, Z. 2387- 2402). Gerade Datenschutzrecht ist auch anziehend für Betroffene die eine missbräuchliche Agenda haben (vgl. ID4, Z. 2433-2439). Auch wenn es für europäische Provider nicht so schlecht wäre, kann es sein, dass der DSA eine gegenläufige Wirkung für Provider hat (vgl. ID4, Z. 2258-2262). Es kann sein, dass sich große Internationale Dienstanbieter aus dem EU-Markt zurückzeihen, da sie in ihren Ländern an und für sich rechtkonform arbeiten (vgl. ID4, Z. 2214-2226 und 2230-2236)

ID5: Die KI und Gesetze von Jurist*innen ohne Technikerfahrung und der Grad, wie viele Leute selbst entscheiden können, ist eine Herausforderung(vgl. ID5, Z. 2980-2989). KI entscheidet basierend auf Fakten, ist aber von Menschen und deren Weltbild angelernt (vgl. ID5, Z. 2997-3003 und 3005-3012).

ID6: Wir kommen in eine disruptive Phase des Probierens und Scheiterns und wenn das mit Daten passiert, dann kann Identitätsdiebstahl passieren und es geht in Richtung Privacy by Desaster (vgl. ID6, Z. 3470-3478). KI und die Wahrnehmung von real und falsch als auch die Reaktion auf eine immer komplexere und schnellere Welt werden eine Herausforderung (vgl. ID6, Z. 3498-3508). Datenschutz spielt im schnellen Auftreten von Dingen mit der Risikobewertung immer eine große Rolle, vorallem wenn etwas plötzlich eintritt wie die KI dieses Jahr (vgl. ID6, Z. 3092-3103)

ID7: Die Komplexität ist es zu schaffen, Unternehmen dazu zu veranlassen, sich an Regeln wie die DSGVO zu halten, ohne dass sie den Markt verlassen (vgl. ID7, Z. 4067-4073). Mehr technologische Entwicklung bedeutet mehr Daten, mehr Datenschutz, da es auch zu mehr Missbrauch kommt (vgl. ID7, Z. 4082-4094). Die zunehmende Komplexität technischer Systeme macht sie für Unternehmen und Betroffene undurchsichtiger. Ab einem gewissen Punkt kann man nur darauf vertrauen, dass alles richtig läuft (vgl. ID7, Z. 4101-4114).

ID8: Die Herausforderung liegt darin vollends in der digitalen Welt anzukommen (vgl. (ID8, Z. 4406-4410). In einer zunehmend komplexen Welt die immer digitaler wird, stellt die Abstraktion von physisch zu digital eine Herausforderung dar (vgl. ID8, Z. 4430-4437).

Tab.14: Kategorie Herausforderung in Zukunft für Datenschutz (Eigendarstellung angelehnt an Tab. 15)

6.2 Herleitung von Hypothesen

In diesem Abschnitt werden die Ergebnisse der induktiven Kategorienbildung zusammengefasst und Hypothesen aufgestellt. Doch bevor hier aus den Ergebnissen der induktiven Kategorienbildung Hypothesen aufgestellt werden, muss vorerst geklärt werden, was Hypothesen sind. Hypothesen sind Aussagen, die zum Teil aus wissenschaftlichen Fakten und zum Teil aus Vermutungen bestehen. Mit Hypothesen soll grundsätzlich neues Wissen entstehen, dennoch gibt es solche, die durch Empirie geprüft werden und Hypothesen, die, wie in dieser Arbeit, aus empirischer Forschung entstehen. Dabei müssen Hypothesen so formuliert werden, dass sie auch überprüft werden können (vgl. Häder, 2015, S.33f.). Zudem muss in vier verschiedene Arten von Hypothesen unterschieden werden.

1. **Verteilungshypothese:** Diese Art der Hypothese trifft nur Aussagen zur Häufigkeit eines Merkmals, wie zum Beispiel, wie oft ein Objekt vorkommt. Dadurch enthält sie keine Aussage zu Ursache und Wirkung. Bei explorativen Studien dient sie also hauptsächlich der Eruierung, wieviel wovon vorhanden ist. Deswegen können Verteilungshypothesen nicht Prognosen oder Erklärungen für Zusammenhänge liefern.
2. **Zusammenhangshypothese:** Sie kann Aussagen darüber tätigen, wie zwei Variablen miteinander zusammenhängen. Dabei ist der Zusammenhang noch ungerichtet, also ohne Wertung, weshalb die bloße Existenz des Zusammenhangs im Vordergrund steht.
3. **Wirkungshypothese:** Diese Hypothese besteht aus einer abhängigen und einer unabhängigen Variable und kann gerichtete Zusammenhänge, also Abhängigkeiten formulieren. Dies ist eine Ursachen-Wirkungshypothese, die eine Wenn-Komponente und eine Dann-Komponente hat.
4. **Unterschiedshypothese:** Sie kann konkrete Aussagen über Ausprägungen von mehreren Merkmalen machen. Es geht darum, dass sich Untersuchungsobjekte aus verschiedenen Kategorien anhand von Merkmalen unterscheiden. Wenn sich die Unterschiede als signifikant herausstellen, kann es interessant sein, welche Ursache zu dem Unterschied führt. Aus Unterschiedshypothesen können dann Wirkungshypothesen

formuliert werden. Unterschiedshypothesen nutzen die Erkenntnisse aus Verteilungshypothesen und Zusammenhangshypothesen und können daraus Wirkungshypothesen machen (vgl. Töpfer, 2012, S. 201-205).

Aus den Ergebnissen der induktiven Kategorienbildung und den Interviews entstehen folgende Hypothesen: Die erste ist eine Zusammenhangshypothese, die aus der Kategorie des nachhaltigen Datenschutzes aus Tabelle 3 entsteht und zeigt, dass, es in der Praxis kein einheitliches Verständnis von nachhaltigem Datenschutz gibt. Daraus lässt sich folgende Zusammenhangshypothese formulieren:

H1: Wenn es kein einheitliches Verständnis von nachhaltigem Datenschutz in der Praxis gibt, dann kann dieser auch nicht einheitlich umgesetzt werden.

Die folgende Wirkungshypothese entsteht aus den Ergebnissen der Kategorie des Harmonisierungserfolgs der DSGVO aus Tabelle 4, da 5 von 8 Expert*innen argumentiert haben, dass Öffnungsklauseln in Rechtsakten wie der DSGVO einen erheblichen negativen Einfluss auf den Harmonierungserfolg derer haben. Diese zwei Zusammenhangshypothesen können für alle EU-Rechtsakte formuliert werden.

H2: Je mehr Öffnungsklauseln in Rechtsakten enthalten sind, desto schwächer ist die Harmonisierungswirkung der Rechtsakte.

H3: Je genauer Öffnungsklauseln national geregelt werden, desto weniger Rechtsunsicherheit gibt es und desto höher ist deren Schutzwirkung.

Wie die Ergebnisse aus Tabelle 6 zeigen, haben große Unternehmen sowohl gegenüber kleinen Unternehmen mehr Ressourcen für rechtskonformes Verhalten, als auch Betroffenen gegenüber die größte Verantwortung, um personenbezogene Daten zu verarbeiten. Deswegen können sie auch am meisten zum Schutz personenbezogener Daten beitragen, woraus die folgende Zusammenhangshypothese entsteht:

H4: Je größer Unternehmen sind, desto größer ist der Einfluss auf den Schutz personenbezogener Daten.

Die Ergebnisse aus Tabelle 7 zeigen, dass Privacy by Design eine wichtige und sinnvolle Regelung ist, aber für Techniker*innen besser formuliert werden muss, damit sie auch in der Praxis gut umgesetzt werden kann. Dazu haben sich 3 von 5 Expert*innen geäußert, weswegen folgende Zusammenhangshypothese entsteht:

H5: Je genauer die Privacy by Design-Regelung für Techniker*innen formuliert ist, desto höher ist das integrierte Schutzniveau in Systemen und Geräten.

Nachdem es in Tabelle 8 unter 3 von 4 Expert*innen zu einem unklaren Ergebnis kommt, wann eine DSFA durchgeführt werden soll, ob dies vor jedem Projekt oder nicht passieren muss, kommt es zu folgender Wirkungshypothese:

H6: Wenn klarer formuliert wird, wann eine DSFA durchzuführen ist, dann sind die Anwendungsfälle auch für Unternehmen in der Praxis klarer.

Aus den Ergebnissen in Tabelle 9 zeichnet sich ab, dass Betroffene und Konsument*innen ein gewisses Maß an Verantwortung zum Schutz personenbezogener Daten haben, dessen Ausmaß von der Informiertheit abhängt, woraus folgende Zusammenhangshypothese gebildet werden kann:

H7: Je mehr Verantwortung Einzelnen zum Schutz ihrer personenbezogenen Daten zugesprochen wird, desto höher muss auch deren Informationsgrad sein.

Die Ergebnisse aus Tabelle 10 stellen fest, dass 5 von 6 Expert*innen die Einwilligungserklärung als beste Schutzform für die adäquate Verarbeitung personenbezogener Daten infrage stellen, da die meisten davon zu lang, komplex und unverständlich sind und oft unklar ist, wie viel davon Durchschnittsverbraucher*innen verstehen. Daraus entsteht folgende Unterschiedshypothese:

H8: Die Einwilligungserklärung ist im Vergleich zu anderen Methoden eine weniger schützende Form, personenbezogene Daten zu verarbeiten.

Die Ergebnisse in Tabelle 11 zeigen, dass die Vorteile und Stärken der DSGVO in der internationalen Wirkung und der Prominenz gegenüber Datenschutz und den

einheitlichen Standards liegen. Außerdem behaupten 3 von 8 Expert*innen, dass die allgemeinen Formulierungen in der DSGVO dazu führen, dass die DSGVO auch gegenüber Innovationen besser anwendbar bleibt und deswegen nicht derart oft novelliert werden müsse. In den Ergebnissen aus Tabelle 12 haben 6 von 8 Expert*innen argumentiert, dass die DSGVO durch vage und allgemeine Formulierungen zu großen Interpretationsspielräumen führt und dadurch große Rechtsunsicherheit entstanden ist. Aus den beiden Ergebnissen kann folgende Zusammenhangshypothese aufgestellt werden:

H9: Je allgemeiner die DSGVO formuliert ist, desto größer ist die Rechtsunsicherheit, aber desto länger bleibt sie gegenüber zukünftigen Innovationen anwendbar, ohne sie novellieren zu müssen.

Die Ergebnisse aus Tabelle 13 zeigen, dass 3 von 6 Expert*innen argumentieren, dass EU-Rechtsakte zu einem indirekten höherem Datenschutzniveau führen. Außerdem behauptet je eine Person bei den Nachteilen der DSGVO, bei dem Einfluss des DSA auf den Datenschutz personenbezogener Daten und bei der Herausforderung zum Schutz personenbezogener Daten, dass solche EU-Rechtsakte den EU-Markt unattraktiver machen. Aus diesen Aspekten kann folgende Wirkungshypothese aufgestellt werden:

H10: Wenn EU-Rechtsakte eingeführt werden, deren Einschränkungen über die EU-Grenzen hinaus gehen, dann steigt das Schutzniveau bezüglich personenbezogener Daten, während die Attraktivität des EU-Marktes sinkt.

Basierend auf den Ergebnissen aus Tabelle 14 sehen 6 von 8 Expert*innen, sowohl die zunehmende künstliche Intelligenz, als auch zunehmende Komplexität technischer Systeme als große Herausforderung in der Zukunft. Die wird eine Herausforderung für den Staat in der Regulierung, für Unternehmen, diese Regulierungen einzuhalten und über die technischen Systeme die Kontrolle zu behalten, als auch für Betroffene, sie zu verstehen. Aus diesem Grund kann folgende Zusammenhangshypothese aufgestellt werden:

H11: Je komplexer technische Systeme wie Künstliche Intelligenz werden, desto komplexer ist Datenschutz.

6.3 Beantwortung der Forschungsfrage

Basierend auf den Erkenntnissen aus Theorie und Empirie kann hier festgestellt werden, dass der Digital Services Act im Gegensatz zur DSGVO allgemein formuliert, das Datenschutzniveau durch seine bloße Existenz anhebt, da alle Plattformen nun ab Februar 2024, nicht nur die DSGVO einhalten müssen, sondern sich auch an den DSA halten müssen. VLOPS und VLOSE müssen sogar schon seit dem 25. August 2023 die erste Risikobewertung durchgeführt haben und sich an den DSA halten (vgl. EU-Kommission, 2023a, o. S.). Zudem sind dessen Strafen mit bis zu 6% des Jahresumsatzes sogar höher angesetzt als jene der DSGVO (vgl. DSA, Art. 52, Abs. 3). Wie die Daten von Statista (2023) in Kapitel 3.3 zeigen, gehören diejenigen, die sich nicht an die DSGVO halten und weltweit die höchsten Strafen zahlen müssen, gleichzeitig zu der Gruppe der VLOPS und VLOSE, welche die strengsten Regulierungen im Digital Services Act befolgen müssen. Es wurde also tatsächlich da angesetzt, von wo der größte Schaden ausgeht oder wie eine Expert*in gesagt hat „ (…) es wird die treffen, die am problematischsten sind. (…)“ (ID3, Z. 1222). Wie auch andere Expert*innen geäußert haben, müssen diese VLOPS und VLOSE sich überlegen, ob sie wirklich gegen zwei EU-Akte verstoßen und somit hohe Strafen zahlen wollen. Allein deswegen kann es sein, dass die DSGVO zunehmend von VLOPs und VLOSE indirekt Beachtung findet. Was der DSA auch im Gegensatz zur DSGVO verändert hat, ist, zwischen großen und kleinen Plattformen anhand der Nutzer*innenzahlen zu unterscheiden, und dass diese kleineren Plattformen basierend auf der geringeren Größe weniger strenge Regelungen befolgen müssen. Außerdem wurde der DSA auch ohne Öffnungsklauseln gestaltet, weswegen mit einer Vollharmonisierung zu rechnen ist (vgl. Rössel, 2023, S.94). Berechtigt ist aber auch das Argument von 3 Expert*innen, dass der EU Markt bei weiteren stark einschränkenden Rechtsakten, die von der EU ausgehen und darüber hinaus andere Länder regulieren wollen, der EU-Markt unattraktiv wird und sich gewisse Unternehmen und Plattformen aus dem Markt zurückziehen werden.

Nichtsdestotrotz hat der DSA nicht nur eine indirekte Wirkung auf das Schutzniveau der DSGVO, sondern auch eine direkte, denn speziell in zwei Artikeln wird auf

Plattformen das Schutzniveau wie in Kapitel 4. 4 erläutert und von einer Expertin konkret formuliert, bestätigt.

Die erste direkte Erweiterung des Datenschutzniveaus lässt sich in Artikel 26 (DSA) finden, welche unter anderem bestimmt, dass die Werbung basierend auf besonderen Kategorien personenbezogener Daten oder basierend auf Profiling für Online-Plattformen verboten wird. Die zweite direkte Erweiterung lässt sich in Artikel 28 (DSA) finden, welcher deklariert, dass auch Kinder weiter geschützt werden müssen. Speziell in Artikel 28 Abs. 2 (DSA) wird geschrieben, dass minderjährigen auf Online-Plattformen nicht basierend auf personenbezogenen Daten oder Profiling Online Werbung gezeigt werden darf. In Artikel 28 Abs. 3 (DSA) wird zusätzlich festgehalten, dass auch keine zusätzlichen personenbezogene Daten verarbeitet werden dürfen, um festzustellen, ob Nutzer*innen minderjährig sind. Zwei Expert*innen haben die Erweiterung des Schutzes personenbezogener Daten von Kindern auch in Tabelle 13 erwähnt.

Das heißt, der Digital Services Act erweitert die DSGVO und das Schutzniveau für Betroffene und Konsument*innen sowohl direkt als auch indirekt. Doch ob deswegen von nachhaltigem Datenschutz gesprochen werden kann, ist unklar. Denn wie sich herausgestellt hat, gibt es einerseits in der Praxis kein einheitliches Verständnis von nachhaltigem Datenschutz, und gleichzeitig wird die Verantwortung für nachhaltigen Datenschutz den Unternehmen zugeordnet. Amort et al. (2022) definieren nachhaltigen Datenschutz als größtmögliche Kontrolle über die eigenen Daten (vgl. Amort et al. S. 212). Diese Kontrolle ist zwar durch das Prinzip der Einwilligung, welches sowohl in der DSGVO als auch im DSA eine große Rolle spielt, bis zu einem gewissen Teil gegeben. Dennoch können Betroffene und Konsument*innen nie ganz wissen, was Unternehmen mit ihren personenbezogenen Daten tatsächlich machen. Das wird auch der DSA nicht ändern, sondern liegt am Verantwortungsbewusstsein von Plattformen und Unternehmen. Wie auch hier in Tabelle 6 gezeigt wurde, wird Unternehmen zum Schutz personenbezogener Daten am meisten Verantwortung beigemessen. Die Ergebnisse von Tabelle 9 haben zwar gezeigt, dass Betroffenen und Konsument*innen auch ein gewisses Maß an Verantwortung zugesprochen wird, zum Beispiel, was Einzelnen über sich preisgeben. Diese Verantwortung steht

jedoch in Zusammenhang mit einem gewissen Wissensstand und dem Bild der Durchschnittsverbraucher*innen. Auch das Verständnis für Einwilligungen in Tabelle 10 zeigt, dass Einwilligungen und deren Prinzip der Zustimmung wegen deren Komplexität und Länge möglicherweise nicht die beste Möglichkeit sind, obwohl sie größtmögliche Kontrolle über die Verwendung personenbezogener Daten bieten. Beim Konzept des nachhaltigen Datenschutzes besteht eine Diskrepanz zwischen größtmöglicher Autonomie und Kontrolle seitens Betroffener und Konsument*innen und deren Wissensstand und dem Umstand, dass auch Unternehmen mit personenbezogenen Daten auf eine Weise umgehen müssen, dass Betroffene und Konsument*innen diese Kontrolle behalten. Zusammenfassend kann also durch den Umstand, dass die DSGVO und der DSA existieren, nicht von nachhaltigem Datenschutz gesprochen werden. Vielmehr spielt es für nachhaltigen Datenschutz eine Rolle, wie sehr Unternehmen und Plattformen diese Rechtsakte einhalten und das bestehende Machtverhältnis zwischen Wissen ihrerseits und dem Unwissen seitens Betroffener und Konsument*innen ausnützen. Gleichzeitig müssen Betroffene und Konsument*innen für nachhaltigen Datenschutz ermächtigt werden, indem ihnen mehr Wissen und digitale Bildung zur Verfügung gestellt werden. Für nachhaltigen Datenschutz benötigt es dementsprechend neben dem rechtlichen Rahmen der DSGVO und dessen Erweiterungen in EU-Verordnungen wie dem DSA, die Verantwortung der Unternehmen, die personenbezogenen Daten von Betroffenen und Konsument*innen nicht auszunutzen und von Betroffenen ein Verständnis zum Wert ihrer personenbezogenen Daten. Es kann daher durch den rein rechtlichen Rahmen von DSGVO und DSA nicht von nachhaltigem Datenschutz gesprochen werden.

6.4 Handlungsempfehlung

Basierend auf den Ergebnissen hat sich herausgestellt, dass von Gesetzestexten wie der DSGVO die Stärken auch gleichzeitig ihre Schwächen sein können und, dass es für Jurist*innen nicht einfach ist, Gesetze zu formulieren, ohne gewisse, in diesem Fall technische Kenntnisse zu besitzen. Aus diesem Grund ist zu empfehlen, dass bei Entwicklung von Gesetzen Expert*innen aus den jeweiligen Gebieten einbezogen werden, um zum Beispiel bessere Formulierungen bezüglich Privacy by Design oder der Datenschutzfolgenabschätzung zu finden und sich von technischer Seite beraten zu lassen. Eine weitere Handlungsempfehlung wäre es, das EU-Verbraucherleitbild an den Stand der Verhaltensökonomie anzupassen, um eines zu bekommen, welches näher an der Realität ist. Auf dem basierend können auch Gesetze formuliert werden, die den heutigen Durchschnittsverbraucher*innen entsprechen und sie auch in der Judikatur widerspiegeln.

7. Fazit

Im folgenden Kapitel werden die Ergebnisse dieser Arbeit noch einmal zusammengefasst. Weiters wird hier auf die Grenzen dieser Arbeit eingegangen. Zum Schluss wird im Forschungsausblick dargelegt, in welchen Gebieten mehr Forschung betrieben werden sollte.

Der empirische Teil dieser Masterarbeit hat mit einer qualitativen Inhaltsanalyse gestartet. Davor wurden Expert*inneninterviews durchgeführt, basierend auf einem Interviewleitfaden. Dabei hat sich die induktive Kategorienbildung als gute Technik herausgestellt, da die Expert*innen viel über die DSGVO und deren Stärken und Schwächen wussten und viel Material vorhanden war. Auch bezüglich des DSA hat sie sich als gute Technik herausgestellt, weil sich dadurch bestätigt hat, dass noch nicht viel Wissen über den DSA vorhanden ist. Dazu muss gesagt werden, dass die Autorin dementsprechend den Fokus des Interviewleitfadens stärker auf die DSGVO gelegt hat.

Die Ergebnisse haben gezeigt, dass im Falle der DSGVO Stärken auch gleichzeitig Schwächen sein können, denn die größten Lücken in der DSGVO liegen in den unklaren Formulierungen und in den Öffnungsklauseln, die in vielen Bereichen dieses Rechtsaktes vorhanden sind, wie in Tabelle 12 dargestellt wurde. Die unklaren Formulierungen stören zwar die einheitliche Umsetzung und die Schutzwirkung der DSGVO, da sie stark interpretierbar sind und Unternehmen sowie Betroffene in vielen Fällen Artikel frei auslegen können, wie zum Beispiel die Privacy by Design-Regelung, die Datenschutzfolgenabschätzung-Regelung, aber auch das Auskunftsrecht zeigen Auf der anderen Seite wappnen diese offenen Formulierungen den Rechtsakt für die Zukunft, da sie technikneutral sind und nicht auf eine Innovation angewiesen sind, wie in Tabelle 13 gezeigt wurde. Das gleiche Verhältnis gilt für die Öffnungsklauseln, die einerseits die Harmonisierungswirkung der DSGVO geschwächt haben, aber auf der anderen Seite dafür sorgen, dass Mitgliedsstaaten je nach Art der Öffnungsklausel sie sogar strenger umsetzen können und somit konkretere Regeln erstellen können, sodass diese Regelungen auch zu den systemischen Gegebenheiten innerhalb eines Mitgliedsstaates passen. Hier kommt die 3. Hypothese dieser Arbeit ins Spiel, dass, je genauer Öffnungsklauseln national geregelt werden, dadurch gleichzeitig die

Rechtsunsicherheit sinkt und das Schutzniveau steigt. Zudem hat sich herausgestellt, dass die Definition von nachhaltigem Datenschutz für kaum eine Expert*in das Gleiche bedeutet hat. Trotzdem haben die meisten Expert*innen in Tabelle 6 Unternehmen die größte Verantwortung zum Schutz personenbezogener Daten nachgesagt, da sie sich um Information, Verständnis von Einwilligungserklärungen, rechtskonforme Datenverarbeitungsprozesse, Privacy by Design und um die DSFA kümmern müssen und die größten Rechenschaftspflichten haben. Durch die Kategorie des Verständnisses von Einwilligungserklärungen hat sich herausgestellt, dass 5 von 6 Expert*innen behaupten, dass die Länge und die Komplexität das Verständnis beeinflussen. Woraus sich die 8. Hypothese bilden ließ, dass nämlich die Komplexität von Einwilligungen dafür sorgt, dass sie nicht die am besten schützende Form der Zustimmung ist. Da 7 von 8 Expert*innen auch einen gewissen Grad an Verantwortung bei Betroffenen und Konsument*innen sehen, dies aber einen gewissen Grad der Informiertheit voraussetzt, wurde die 7. Hypothese gebildet, dass die Verantwortung Einzelner zum Schutz personenbezogener Daten direkt proportional zu deren Informationsgrad steht.

Zur Beantwortung der Forschungsfrage war die Mischung aus der Analyse der zwei Theoriekapitel in Zusammenhang mit der qualitativen Inhaltsanalyse der Expert*innen notwendig. Denn aus den Theoriekapiteln hat sich zum Teil schon die direkte Wirkung des DSA auf den Schutz personenbezogener Daten herausgestellt, nämlich, dass es zwei Artikel im DSA gibt, welche die DSGVO direkt erweitern werden. Dies hat bei den Interviews nur eine Expertin genau so konkret formuliert. Die anderen Expert*innen sind eher auf die indirekte Wirkung des DSA eingegangen, was wiederum bedeutet, dass bezüglich des Digital Services Acts derzeit noch nicht viel Wissen vorhanden ist, zumindest unter den befragten Expert*innen dieser Arbeit. Was der Prozess der empirischen Forschung auch gezeigt hat, war, dass die Autorin keine Probleme hatte, Expert*innen für ein Interview zu finden, was zeigt, dass das Thema als wichtig und relevant empfunden wird. Praktisch ist zum derzeitigen Zeitpunkt noch schwer absehbar, was der DSA wirklich indirekt bewirken wird, weil für VLOPs durch den DSA noch höhere Transparenzpflichten und Sanktionen eintreten. Dies kann jedoch in zwei Richtungen enden. Einerseits kann es sein, dass der DSA neben der DSGVO dafür

sorgt, dass durch die hohen Sanktionen der DSGVO beide Verordnungen strenger eingehalten werden. Andererseits besteht bei Verordnungen der EU, die Länder über den EU-Raum hinweg einschränken, ebenfalls die Gefahr, dass Marktteilnehmer*innen den EU-Markt verlassen. Daraus konnte die 10. Hypothese gebildet werden, da 3 Expert*innen geantwortet haben, dass das Schutzniveau steigt, und 3 Expert*innen meinten, dass dadurch jedoch Marktteilnehmer*innen den EU-Markt verlassen könnten. Zum Schluss haben 6 von 8 Expert*innen die zunehmende Komplexität von Systemen, wie zum Beispiel künstlicher Intelligenz, als größte Herausforderung zum Schutz personenbezogener Daten in Zukunft erwähnt, woraus die 11. Hypothese entstanden ist, dass die Komplexität von technischen Systemen sich direkt proportional auf die Komplexität von Datenschutz auswirkt.

7.1 Grenzen

Die Grenzen dieser Arbeit zeigen sich am begrenzten Wissen der Expert*innen zum Digital Services Act, da die genauen Auswirkungen unmöglich zu wissen sind, sondern nur eingeschätzt werden können vor der gänzlichen unmittelbaren Anwendbarkeit im 17. Februar 2024 (vgl. DSA, Art. 93, Abs. 2). Dies zeichnete sich vor allem dadurch aus, dass 7 von 8 Interviewpartner*innen nur grob einschätzen konnten, welche Auswirkungen der Digital Services Act auf das Schutzniveau personenbezogene Daten haben kann. Nur eine Expertin konnte hier die genauen Verbote nennen, mit denen der Digital Services Act die DSGVO ergänzen wird. Dies kann aber auch daran liegen, dass die meisten Expert*innen einen datenschutzrechtlichen Hintergrund haben und deswegen nicht ein derart großes Wissen zum Digital Services Act besitzen. Hier hätten vielleicht mehr Expert*innen im Hinblick auf den DSA angefragt werden können, wobei eventuell die Fragen zur DSGVO dafür schlechter beantwortet hätten werden können. Durch die rein qualitativen Aspekte der Forschung konnten die Hypothesen nicht geprüft werden, was beim Verständnis von Einwilligungen einschränkend ist, da die Expert*innen dies nur einschätzen können und nicht aus der Sicht von Durchschnittsverbraucher*innen bewerten. Prinzipiell ist der Datenschutz im Vergleich zu anderen juristischen Disziplinen eine junge Disziplin, die gleichzeitig sehr umfassend ist und immer größer wird, weswegen in dieser Arbeit auch nicht

alle Probleme oder Lücken in der DSGVO aufgegriffen werden konnten, wie zum Beispiel die Verarbeitung von sensiblen Daten im Rahmen von Forschungszwecken. Auch die möglichen Ergänzungen des Datenschutzniveaus durch den Digital Markets Act wurden nicht aufgegriffen, da dies den Rahmen dieser Masterarbeit überstiegen hätte. Auch im Rahmen der Befragung wurde keine Bewertung der Praxis des Shadowbannings ebenso wenig wie der Einfluss des DSA auf andere Grundrechte wie die Meinungsfreiheit abgefragt, da dies den Rahmen und vermutlich das vorhandene Wissen überstiegen hätte. Die Grenzen dieser Arbeit zeigten sich allgemein im Wissen über den DSA, das bei 7 von 8 Expert*innen weniger in die Tiefe und eher oberflächlich ausgeprägt war. Weiters hätten die aus der qualitativen Forschung entstandenen Hypothesen auch mit einem Methodenmix nur quantitativ geprüft werden können, dies hätte jedoch auch den Rahmen dieser Masterarbeit überschritten. Diese Grenzen führen wiederum zum Forschungsausblick dieser Arbeit.

7.2 Forschungsausblick

Prinzipiell sollten alle hier aufgestellten Hypothesen im Rahmen von qualitativer Forschung ausreichend geprüft werden. Trotzdem hat sich vor allem im Bereich nachhaltigen Datenschutzes gezeigt, dass dieses Konzept sowohl von der Bedeutung als auch von der Umsetzung weit entfernt ist. Da das Prinzip des nachhaltigen Datenschutzes auch an die Autonomie und Kontrolle über die eigenen Daten gebunden ist, sollte das Verständnis von Einwilligungserklärungen qualitativ mit Fokusgruppen oder quantitativ geprüft werden. Außerdem könnten, wie Expert*innen in Tabelle 10 vorgeschlagen haben, in diesem Zug auch andere Methoden der Information und Zustimmung getestet werden. So könnten eventuell standardisierte Formulare, die nicht länger als eine A4 Seite sind, oder Benutzer*innen-Einführung mit Onlinevideos oder sogar die Möglichkeit, seine Daten hinterlegen zu können und mit der Zustimmung der Verarbeitung entgeltlich vergütet zu bekommen, angewendet werden. Weiters sollte auch die Wirkung von EU-Rechtsakten auf Unternehmen und Plattformen außerhalb der EU weiter erforscht werden, um das Risiko einschätzen zu können, den EU-Markt unattraktiv zu gestalten. Die Wirkung von Öffnungsklauseln und allgemeinen Formulierungen und deren Interpretationsspielräume in der Praxis könnten weiter erforscht werden,

da darauf basierend in zukünftigen Rechtsakten mehr darauf seitens der EU eingegangen werden könnte und Prognosen zum Marktverhalten getroffen werden könnten. Formulierungen können zum Beispiel qualitativ getestet werden, indem eine gewisse Anzahl an Proband*innen Gesetzestexte interpretieren müssen. Speziell was technische Verordnungen betrifft, bei denen es darum geht, dass Techniker*innen etwas umsetzen sollen könnten diese im Vorhinein qualitativ getestet werden, ob die Formulierungen einerseits genug Anweisungen vorweisen, ob damit ein allgemeineres Verständnis abgedeckt ist und ob andererseits dies auch machbar ist, wie zum Beispiel im Falle der Privacy by Design-Regelung. Ein Aspekt, der bis zum Schluss unklar erscheint, ist, wie in Kapitel 4.5 schon erwähnt, dass einerseits das Anwenden von Online-Werbung, basierend auf Profiling, für Minderjährige verboten ist (vgl. DSA, Art. 28, Abs.2). Auf der anderen Seite ist im Erwgrd. 68 (DSA) erwähnt, dass gezielte Werbung, die auf personenbezogenen Daten basiert, nur dann ausgespielt werden darf, wenn eine Einwilligung vorliegt. Das Einwilligungsalter ist in der EU bei 16 Jahren und kann in den Mitgliedsstaaten auf bis zu 13 herabgesetzt werden (vgl. DSGVO, Art 8). Es scheint, als wäre hier unklar, ob hier das Einwilligungsalter der jeweiligen Mitgliedsstaaten gilt oder ob die Minderjährigkeit für das Verbot des Ausspielens von Online-Werbung basierend auf Profiling, gilt.

8. Quellenverzeichnis

Allgemeines bürgerliches Gesetzbuch für die gesamten deutschen Erbländer der Österreichischen Monarchie (ABGB), StF: JGS Nr. 946/1811, Fassung vom 15.05.2023

Amort, M., Arens, S., Bruckmann, J.-F., Fischer, H.-J., Fischer, F.-A., Helfrich, M., Schmittmann, J. M., & Supernok-Kolbe, M. (2022). Kapitel 7 – Nachhaltiger Datenschutz? In: *Nachhaltigkeit und Recht*. Fachmedien Recht und Wirtschaft. *1*. S. 201-213

APA, (2022), ChatGPT könnte schon bald nach Italien zurückkehren. (2023, April 18). von DER STANDARD website: https://www.derstandard.at/story/2000145606074/chatgpt-koennte-schon-bald-nach-italien-zurueckkehren, abgerufen am 06.06.2023

Austria, & Bresich, R. (Hrsg.). (2018). *DSG: Datenschutzgesetz: Kommentar*. Wien: Linde.

Bauer, L., & Reimer, S. (Hrsg.). (2009). *Handbuch Datenschutzrecht*. Wien: Facultas. wuv.

Bogner, A., Littig, B., & Menz, W. (2014). *Interviews mit Experten: Eine praxisorientierte Einführung*. Wiesbaden: Springer Fachmedien Wiesbaden.

Broughton Micova, S. (2021). What is the Harm in Size: Very Large Online Platforms in the Digital Services Act., *Centre for Regulation in Europe (CERRE)*, S. 1-25

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG), StF: BGBl. Nr. 565/1978, Fassung vom 18. Oktober 1978, Fassung vom 18. Oktober 1978

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl. I Nr. 165/1999, Fassung vom 17. August 1999

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), StF: BGBl. I Nr. 24/2018, Fassung vom 20.01.2023

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz-ECG), BGBl I Nr 152/2001 idF BGBl I Nr 148/2020., Fassung vom 21. Dezember 2001

Bunnenberg, J. N. (2020). *Privates Datenschutzrecht: Über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer*

vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO (1. Auflage). Baden-Baden: Nomos.

Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, *12*, S. 758–774.

Corman, A., Canaway, R., Culnane, C., & Teague, V. (2022). Public comprehension of privacy protections applied to health data shared for research: An Australian cross-sectional study. *International Journal of Medical Informatics*, *167*, 104859.

Erwägungsgründe der EU-Datenschutzgrundverordnung. (2016), https://www.datenschutz-grundverordnung.eu/erwagungsgrunde-der-eu-datenschutz-grundverordnung/, abgerufen am 10.07.2023

EU-Datenschutz-Grundverordnung (EU-DSGVO) – Infos, Schulungen und Kommentar über und zur EU-Datenschutz Grundverordnung. https://www.datenschutz-grundverordnung.eu/, abgerufen am 07.06.203

EU-Kommission (2023a), Das Paket des Digital Services Act | Gestaltung der digitalen Zukunft Europas. https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package, abgerufen am 30.06.2023

EU-Kommission (2023b), Gesetz über digitale Dienste: Mehr Sicherheit und Verantwortung im Online-Umfeld. (o. J.). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de, abgerufen am 27.07.2023

EU-Kommission (2023c), Ein Europa für das digitale Zeitalter – was sich für Nutzerinnen und Nutzer ändert. (o. J.). Abgerufen 27. Juli 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-users_de, abgerufen am 03.08.2023

Europäische Menschenrechtskonvention, 2023, https://www.menschenrechtskonvention.eu/, abgerufen am 01.08.2023

European Data Protection Board (2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision, https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, abgerufen am 09.07.2023

Feiler, L., & Forgo, N. (2022). *EU-DSGVO und DSG* (2. Aufl.). Wien: Verlag Österreich.

Flick, U., Kardorff, E. von, & Steinke, I. (Hrsg.). (2022). *Qualitative Forschung: Ein Handbuch* (14. Auflage, Originalausgabe). Reinbek bei Hamburg: Rowohlts Enzyklopädie im Rowohlt Taschenbuch Verlag.

Friedewald, M. (2017). Datenschutz-Folgenabschätzung: Chancen, Grenzen, Umsetzung. *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, *26*, S. 66-71.

Friedrichsen, M., & Wersig, W. (Hrsg.). (2020). *Digitale Kompetenz: Herausforderungen für Wissenschaft, Wirtschaft, Gesellschaft und Politik*. Wiesbaden: Springer Fachmedien Wiesbaden.

Furrer, A., & Epiney, A. (1995). Staatliche Haftung für quantifizierbare Wettbewerbsnachteile aus nicht umgesetzten Richtlinien: Das „rechtlich geschützte Interesse an Nichtdiskriminierung“ und seine Heranziehung im Rahmen der „Francovich-Grundsätze. *Juristenzeitung*, *50*(21), S. 1025–1034.

Goldberg, F., & Hildebrandt, A. (2020). Experteninterviews: Anwendung, Durchführung und Auswertung in der Politikwissenschaft. In C. Wagemann, A. Goerres, & M. B. Siewert (Hrsg.), *Handbuch Methoden der Politikwissenschaft* (S. 267–284). Wiesbaden: Springer Fachmedien Wiesbaden.

Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. *Computer Law & Security Review*, *37*, 105409. S. 1-10

Häder, M. (2015). *Empirische Sozialforschung: Eine Einführung*. Wiesbaden: Springer Fachmedien Wiesbaden.

Härting, N., & Adamek, M. V. (2023). Lässt der Digital Services Act Raum für ein „Gesetz gegen digitale Gewalt“? *Computer Und Recht*, *39*, S. 316–320.

Heidig, W., & Dobbelstein, T. (2021). Von der Grundgesamtheit zur Stichprobe. In W. Heidig & T. Dobbelstein, *Quick Guide Marktforschung im Mittelstand* (S. 53–73). Wiesbaden: Springer Fachmedien Wiesbaden.

Hentschel, A., Hornung, G., Jandt, S., & Roßnagel, A. (Hrsg.). (2020). *Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft: Festschrift für Alexander Roßnagel zum 70. Geburtstag* (1. Auflage). Baden-Baden: Nomos.

Holzer, D. (2019). *Die Entschärfung der DSGVO durch den österreichischen Gesetzgeber / eingereicht von Daniel Holzer*. (Doctoral dissertation, Universität Linz).

Juranek, N. (2022). *Aktuelle Rechtsfragen von datengetriebenen Geschäftsmodellen unter besonderer Berücksichtigung von datengetriebenem Marketing*, Diplomarbeit, Universität Graz.

Kamp, M., & Rost, M. (2013). Kritik an der Einwilligung: Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen. *Datenschutz und Datensicherheit - DuD*, *37*, S. 80-84.

Klementschitz, R. (2019). *Auswirkungen der DSGVO auf den internationalen Datenverkehr,* Dissertation, Universität Linz.

Konvention zum Schutz der Menschenrechte und Grundfreiheiten StF: BGBl. Nr. 210/1958, Fassung vom 24. September 1958

Kremer, S. (2020). Die Praxis externer Datenschutzbeauftragter unter der DSGVO. *Informatik Spektrum*, *43*, S. 332-333.

Kuckartz, U. (2012). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung*. Weinheim Basel: Beltz Juventa.

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790, S. 1-13

Lehmann, G. (2022). *Die effektive Befragung: Ein Ratgeber für die Datenerhebung in der beruflichen und wissenschaftlichen Arbeit* (3. Aufl.). Stuttgart: utb GmbH.

Martin, N., Mester, B. A., Schiering, I., Friedewald, M., & Hallinan, D. (2020). Datenschutz-Folgenabschätzung: Ein notwendiges‚‚Übel‘‘ des Datenschutzes? *Datenschutz und Datensicherheit - DuD*, *44(3)*, S. 149-153.

Mayring, P. (1991). Qualitative Inhaltsanalyse. In U. Flick, E. v. Kardoff, H. Keupp, L. v. Rosenstiel, & S. Wolff (Hrsg.), Handbuch qualitative Forschung : Grundlagen, Konzepte, Methoden und Anwendungen (S. 209-213). München: Beltz- Psychologie Verl. Union.

Mayring, P. (1994). Qualitative Inhaltsanalyse. In A. Boehm, A. Mengel, & T. Muhr (Hrsg.), *Texte verstehen: Konzepte, Methoden, Werkzeuge* (S. 159–175). Konstanz: UVK Univ.-Verl. Konstanz.

Mayring, P. (2000). Qualitative Inhaltsanalyse. Grundlagen und Techniken (7. Auflage). Weinheim: Deutscher Studien Verlag.

Mayring, P. (2010). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (11., aktual. und überarb. Aufl). Weinheim Basel: Beltz

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12., überarbeitete Auflage). Weinheim Basel: Beltz.

Mayring, P. (2020). Qualitative Forschungsdesigns. In G. Mey & K. Mruck (Hrsg.), *Handbuch Qualitative Forschung in der Psychologie*. Wiesbaden: Springer Fachmedien Wiesbaden. S. 3-17

Netzwerk Menschenrechte (2014, September 29). Privatsphäre und Familienleben | Europäische Menschenrechtskonvention. https://www.menschenrechtskonvention.eu/privatsphaere-und-familienleben-9292/, abgerufen am 25.05.2023

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, *34*, S. 1232-1246.

Noyb, 2021, Irische Datenschutzbehörde gibt Facebooks „DSGVO-Umgehung“ grünes Licht. (o. J.). https://noyb.eu/de/irische-datenschutzbehoerde-gibt-facebooks-dsgvo-umgehung-gruenes-licht, abgerufen am 02.04.2023

Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens’ perception of data protection and data security. *Computers in Human Behavior*, *122*, S.1-17.

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Fassung vom 17.07.2022

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr., 281 OJ L § (1995). Fassung vom 23.11.1995
Rössel, M. (2023). Digital Services Act—Eingehende Analyse und Überprüfung der regulatorischen Neuerungen aus dem Trilog und potentieller Lücken. *AfP*, *54*, S. 93-106.

Schmiedhofer, H. M. (2019). *Die Datenschutzgrundverordnung 2016 und daraus resultierende Anforderungen an Klein- und Mittelunternehmen in Österreich / Helena Schmiedhofer*, Masterarbeit, Karl-Franzens-Universität Graz.

Schmitt, L. (2018). *Das unionsrechtliche Verbraucherleitbild: Rechtsgebietsspezifische Rezeption und Binnendifferenzierung des Leitbilds vom informierten, aufmerksamen und verständigen Durchschnittsverbraucher* (1. Auflage). Baden-Baden: Nomos.

Schnell, M., Schulz, C., Kolbe, H., & Dunger, C. (Hrsg.). (2013). *Der Patient am Lebensende: Eine Qualitative Inhaltsanalyse*. Wiesbaden: Springer Fachmedien Wiesbaden.
Sonntag, N. (2023). Viele Vorschläge zur Güte: Gütekriterien der qualitativen Forschung aus analytisch-empirischer Sicht. *Zeitschrift Für Soziologie*, *52*, S. 7-25.

Staatsgrundgesetz vom 21. Dezember 1867, über die allgemeinen Rechte der Staatsbürger. StF: RGBl. Nr. 142/1867, Fassung vom 26.08.2023

Statista, (2023). Infografik: DSGVO-Bußgelder erreichen 2023 neues Rekordhoch. (2023, Mai 23). Statista Daily Data website: https://de.statista.com/infografik/26629/strafen-auf-grund-von-verstoessen-gegen-die-datenschutz-grundverordnung, abgerufen am 13.06.2023

Stöggl, M. (2019). Der Staat als Adressat des Unionsrechts: Zur Ausdehnung des persönlichen Anwendungsbereichs des EU-Rechts in der Judikatur des EuGH. *Zeitschrift für öffentliches Recht*, *74*, S. 465-518.

Tagwercher, J. (2019). *Das Grundrecht auf Datenschutz unter besonderer Berücksichtigung des persönlichen Schutzbereichs*, Diplomarbeit, Paris Lodron Universität Salzburg.

Töpfer, A. (2012). *Erfolgreich Forschen: Ein Leitfaden für Bachelor-, Master-Studierende und Doktoranden*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*, S. 83-106.

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), Fassung vom 27.04.2016

Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), Fassung von 19.10.2022

Weiß, M. (2022). Kapitel 3: Die Öffnungsklauseln und institutionelle Harmonisierungseffekte der DSGVO. In *Öffnungsklauseln in der DSGVO und nationale Verwirklichung im BDSG* (Bd. 50). Baden-Baden: Nomos Verlagsgesellschaft.

Wojciech Wiewiórowski | European Data Protection Supervisor. (2023, Juli 28). https://edps.europa.eu/about-edps/members-mission/supervisors/wojciech-wiewi%C3%B3rowski_de, abgerufen am 27.07.2023

Zou, Y., Danino, S., Sun, K., & Schaub, F. (2019). You `Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, *194*, S. 1-14.

9. Anhang

9.1 Induktive Kategorienbildung:

Text	Reduktion 1	Reduktion 2	Kategorie
ID1: „ Also nachhaltiger Datenschutz bedeutet für mich, dass man nicht nur pro forma die gesetzlichen Bestimmungen einhält, sondern dass man sich wirklich in die Rolle der betroffenen Personen versetzt, also deren Daten man bearbeitet und sich die Frage stellt: Wäre es für mich in Ordnung, dass meine Daten auch in dieser Form verwendet werden.” (ID1, Z. 40-44, durchgeführt am 10.07.2023)	Für mich ist nachhaltiger Datenschutz nicht nur gesetzliche Bestimmungen, sondern sich zu überlegen, ob die Verarbeitung für Betroffenen wirklich in Ordnung wäre.	Nachhaltiger Datenschutz ist nicht nur gesetzliche Bestimmungen sondern sich in Betroffene hineinversetzen.	Nachhaltiger Datenschutz
ID1: „Meiner Erfahrung nach lesen sich viele Datenschutzerklärungen so, dass man möglichst versucht, einen rechtsicheren Text zu schreiben für den Fall, dass man verklagt wird und weniger, dass man wirklich versucht, den Verbrauchern oder betroffenen Personen jetzt präzise und leichte Informationen zugänglich zu machen. Da Verstehe ich natürlich als anwaltlicher Vorsicht, dass man sich irgendwie absichern möchte, dass man dann sagen kann okay, steht ja in der Datenschutzerklärung“ (ID1, Z. 44-50)	Viele Datenschutzerklärungen sind so geschrieben, dass sie für Unternehmen Rechtssicherheit bieten, aber für Betroffene nicht verständlich sind. Zur Absicherung ist dies verständlich.	Datenschutzerklärungen bieten Unternehmen Absicherung und Rechtssicherheit, dadurch sind sie aber Betroffene nicht verständlich.	Verständnis Einwilligungs-erklärung
ID1: „Aber auch dieser Maßstab, also den Durchschnitt sozusagen, würde ich hier unten anlegen. Also der Durchschnittsverbraucher oder -verbrauchin kennt sich eben nicht so gut aus. Und dann muss ich eben versuchen, durch eine leichte und verständliche Sprache entsprechend mich auszudrücken, was ich mit diesen Daten mache“ (ID1, Z. 72-76).	Durchschnitts-verbraucher*innen kennen sich nicht so gut aus, darum muss die Einverständniserklärung in einfacher Sprache sein, nämlich was mit den Daten passiert.	Durchschnitts-verbraucher*innen kennen sich mit Einverständniserklärung en nicht so gut aus, darum müssen sie einfach formuliert sein.	Verständnis Einwilligungs-erklärung
ID1: „Und am Ende des Tages ist das, glaube ich auch nur positiv für das jeweilige Unternehmen, weil eine mangelnde Informiertheit führt eben zu Ungültigkeit der	Durch mangelnde Information könnten die Einwilligungen ungültig sein, weshalb Unternehmen mehr darüber nachdenken	Unternehmen müssen mehr nachdenken, ob Einwilligungserklärungen verständlich sind, dazu können sie auch betroffene befragen.	Verantwortung Unternehmen

Einwilligung. Das heißt, ich laufe immer Gefahr, dass dann meine Einwilligungserklärungen ungültig sind und dann habe ich viele Probleme. Das heißt, lieber ein bisschen länger nachdenken. Ist das jetzt wirklich verständlich? Und ich kann ja auch zum Beispiel betroffene Personen als Muster sozusagen befragen, wie die das jetzt verstehen.“ (ID1, Z. 76-82).	müssen, ob eine Einwilligung wirklich verständlich ist. Hierbei könnten sie auch Betroffene befragen.		
ID1: „Die praktische Sicht ist natürlich die, dass selbstverständlich auch Betroffene ihre eigenen Daten unter Anführungszeichen verantwortlich sind. Aber ich muss natürlich auch selber auf gewisse Dinge schauen. Und das beginnt zum Beispiel damit, dass ich nicht überall dasselbe Passwort verwende, also dass ich zum Beispiel nicht dasselbe Passwort auf Facebook habe, wie für mein Online banking. Das heißt, ein gewisses Maß an Selbstverantwortung hat einfach jeder. Aber das ist, glaube ich, in allen Lebensbereichen so und nicht unbedingt im Datenschutz. (ID1, Z. 98-108)	Betroffene sind für ihre eigenen Daten verantwortlich und müssen zum Beispiel schauen, dass sie nicht für OnlineBanking das Passwort von Social Media verwenden. Ein Maß an Selbstverantwortung gilt in allen Lebensbereichen.	Betroffene haben ein gewisses Maß an Selbstverantwortung und sind für den Schutz ihrer Daten verantwortlich.	Verantwortung von Betroffenen/ Konsument-*innen
ID1: „Das wäre wahrscheinlich falsch, aber es hat einfach nicht diese Aufmerksamkeit bekommen, sage ich einmal. Das hat sich eben mit der DSGVO geändert, allein schon aufgrund der medialen Berichterstattung.“ (ID1, Z. 120-123)	Die DSGVO hat die mediale Aufmerksamkeit bekommen, welche der Datenschutz vorher nicht bekommen hat	Die DSGVO hat für Aufmerksamkeit gegenüber Datenschutz gesorgt.	Vorteile/ Stärken der DSGVO
ID1: „Ja, aber was die DSGVO auf jeden Fall gebracht hat, ist, dass die Leute, ob sie wollen oder nicht, über Datenschutz nachdenken und über Datenschutz sprechen. Das heißt, die awareness auch bei jemandem, der jetzt vielleicht nicht mit dieser Materie zu tun hat, ist einfach gestiegen. Und auch die Medien in Österreich, aber auch international, berichten immer mehr über datenschutzrechtliche Dinge. Und ich glaube, das ist auch gut so! (ID1, Z. 125-131)	Die Leute beschäftigen sich durch die DSGVO mit Datenschutz, ob sie wollen oder nicht. Die Aufmerksamkeit ist dadurch sowohl individuell, medial als auch international gestiegen.	Die DSGVO hat individuell, medial und international für Aufmerksamkeit gegenüber Datenschutz gesorgt.	Vorteile/ Stärken der DSGVO

ID1: „Das heißt, es gibt viele Dinge, die ich wahrscheinlich ändern würde. Damit beginnen, dass viele Dinge einfach unpräzise sind und unklar sind. Um ein Beispiel zu nennen was zumindest eine lange Zeit unklar war, ist, was überhaupt eine Datenkopie ist und in welchem Umfang eine Datenkopie zur Verfügung zu stellen ist. Das hat natürlich schon unmittelbare Auswirkungen auf die Betroffenen, weil je nachdem, wie ich das interpretiere, bekomme ich einmal mehr oder einmal weniger Daten. Und wenn ich einen Antrag auf Auskunft stelle. Also das heißt ja, manche Bestimmungen haben aufgrund ihrer Unschärfe sicherlich Auswirkungen (ID1, Z. 141-147)	Viele Dinge sind in der DSGVO unpräzise und unklar formuliert, wie zum Beispiel, was eine Datenkopie ist und in welchem Umfang sie zur Verfügung gestellt wird. Dies hat Auswirkungen auf Betroffene, weil sie je nach Interpretation mehr oder weniger Datenauskunft bekommen.	Viele Dinge sind in der DSGVO unklar formuliert, was im Falle der Datenkopie Auswirkungen auf Betroffene haben kann.	Nachteile/ Schwächen der DSGVO
ID1: „Und natürlich ist das auch eine Rechtsunsicherheit für Unternehmen oder Behörden, weil wenn etwas nicht klar geregelt ist und ich dann vielleicht doch eine Geldbuße bekomme, wenn ich dagegen verstoße, ist es natürlich ein Problem (ID1, Z. 151-155)	Wenn etwas nicht klar geregelt ist, dann sorgt das auch für Rechtsunsicherheit bei Behörden und Unternehmen, da sie sonst eine Geldbuße bekommen.	Wenn Recht nicht klar geregelt ist, sorgt dies für Rechtsunsicherheit und Nachteile.	Verantwortung Union / Staat
ID1: „Ja, es gibt sogenannte Öffnungsklauseln, wie Sie richtig gesagt haben. Ja, ich denke, je besser man die Lücken schließt, die die DSGVO eröffnet, umso besser. Also das heißt, daran sieht man schon auch der nationale Gesetzgeber in jedem Mitgliedstaat sollte sich am besten Gedanken machen, wie man die DSGVO idealerweise ergänzt, mit nationalen Gesetzgebungen, also dort, wo ein entsprechender Spielraum ist. (ID1, Z. 166-168)	Je besser Mitgliedsstaaten ihre Verantwortung wahrnehmen, die Öffnungsklauseln in der nationalen Gesetzgebung zu schließen, desto besser werden die Lücken in der DSGVO geschlossen.	Je besser Mitgliedsstaaten die Öffnungsklauseln im nationalen Gesetz regeln, desto weniger Lücken in der DSGVO.	Harmonisierungs -erfolg der DSGVO
ID1: „Allerdings indirekt ist es natürlich schon eine Verbesserung des Datenschutzniveaus auch. Es geht nicht nur um Datenschutz. Aber wenn ich zum Beispiel viele Verpflichtungen habe, was	Indirekt hebt der DSA das Datenschutzniveau an,weil Unternehmen durch den DSA viele Transparenzpflichten einhalten müssen und dies auch ein großer Punkt im Datenschutz ist.	Der DSA wird mit den Transparenzpflichten und den Plattformregulierungen das Grundrecht auf Datenschutz stärken.	Einfluss des DSA auf Schutz personen-bezogener Daten

gerade für große Plattformen, ja, dann profitieren natürlich indirekt auch die betroffenen Personen für ihr Grundrecht auf Datenschutz. Weil als große Plattform muss ich mir da ganz viele Gedanken machen, wie ich entsprechende Pflichten umsetze und diese Pflichten hängen sehr viel mit Transparenz zusammen. Und Transparenz ist natürlich auch ein großes Thema im Datenschutzrecht. Also kurz gesagt, es gibt natürlich sehr viele, ich nenne sie mal Synergieeffekte. Also das heißt, selbstverständlich wird auch dadurch das Grundrecht auf Datenschutz gestärkt, auch wenn es jetzt nicht primär um Datenschutz geht, sondern sozusagen allgemein um Plattformregulierung (ID1, Z. 193-204)	Durch Synergieeffekte mit Plattformregulierungen wird das Grundrecht auf Datenschutz gestärkt.		
ID1: „Das gibt es ja auch schon einige Jahrzehnte. Aber nichtsdestotrotz würde ich trotzdem sagen AI. So die massenhafte Datenverarbeitung innerhalb eines kurzen Zeitraums mit sehr sehr viel Rechenleistung. Ich glaube in kurzer Zeit, vielleicht zu 10, 15 Jahren, werden wir Fake von Realität nicht mehr unterscheiden können. Und eine der größten Herausforderungen wird eben sein, auf diese neuen Technologien zu reagieren. Sei es auf gesetzlicher Ebene, was mit dem AI Act probiert wird in der EU, oder sei es auch mit einem technologischen Ansatz, wie zum Beispiel Technologien, die wiederum selber auf AI basieren. Das ich überprüfe, ob etwas Fake ist oder nicht (ID1, Z. 216-227).	Künstliche Intelligenz, die enorme Datenverarbeitung in kurzer Zeit und der Unterschied zwischen Real und Fake: Das wird eine enorme Herausforderung, darauf zu reagieren, sowohl auf rechtlicher als auch auf technischer Ebene.	Künstliche Intelligenz und deren enorme Datenverarbeitung wird eine technologische und rechtliche Herausforderung.	Heraus-forderungen in Zukunft Datenschutz
ID2: „Nachhaltiger Datenschutz ist, wenn ich es auch aus dem Beratungskontext, dass man sich schon möglichst früh Gedanken macht, wie man das System, das Geschäftsmodell so aufzieht, dass man den Schutz der personenbezogenen Daten im Vordergrund sieht. Also eben dieses Privacy by Design, das heißt eben.	Nachhaltiger Datenschutz ist, dass man sich möglichst früh Datenschutz ins Geschäftsmodell integriert und, dass der Schutz personenbezogener Daten von Privacy by Design bis hin zu Speicherungsprozessen, Zweckgebundenheit und Minimalisierung und Information der	Nachhaltiger Datenschutz ist die möglichst frühe Integration von Datenschutz in jegliche Prozesse eines Geschäftsmodells.	Nachhaltiger Datenschutz

sich konstruktiv schon am Anfang Gedanken zu machen: Wie werde ich meine Daten abspeichern? Was sind Methoden, wie ich diese Daten dann in Verbindung, wie werde ich sie in Verbindung setzen? Und da muss ich wirklich sagen, ganz ehrlich, man muss eben wirklich jedes Datum für sich und im Zusammenhang sehen. Ohne dass ich jetzt über über konkrete Beispiele philosophiere. Ja, es muss immer Zweckgebunden sein und diese Minimalisierung im Hintergrund sein. Wie bringe ich, wie halte ich die Daten in einer zum Beispiel nicht Cloud basierten Datenbank, so dass ich, wenn ich zum Beispiel Neue User, die dazukommen, dass ich sie informier was passiert mit meinen Daten?“ (ID2, Z. 327-342, durchgeführt am 24.07.2023)	Betroffenen integriert und mitgedacht wird.		
ID2: „Dass ich Ihnen in dieser Datenschutzerklärung erkläre wie stehen meine Prozesse aus? Also auch da ist es sehr unterschiedlich wie weit die Unternehmen sind. Also ich sehe immer wieder, je besser man sich das überlegt und je genauer ich meine Prozesse beschreibe, was ich mit den Daten mache, desto umfangreicher wird natürlich auch die Datenschutzerklärung. Aber desto eher bin ich dann selber, wenn ich es mir durchgedacht habe, auch auf der sicheren Seite weil ich einfach meinem Anwender oder meinem Kundenstamm das genau beschrieben habe.“ (ID2, Z.345-352)	Als Unternehmen muss ich mir überlegen, wie ich meine Prozesse beschreibe. Je besser Unternehmen diese beschreiben, desto umfangreicher wird die Datenschutzerklärung, jedoch sind sie dann auch rechtlich abgesichert.	Wenn Unternehmen ihre Prozesse ausführlich in Datenschutz-erklärungen beschreiben, sind sie rechtlich abgesichert, jedoch werden sie sehr lang.	Verständnis Einwilligungs-erklärung
ID2: „Ja, also die Verantwortlichkeit würde ich schon bei den Unternehmern sehen, allerdings im Sinne, dass man natürlich die Auflagen hat, also die Verantwortlichkeit der Umsetzung, ist definitiv für den Unternehmen. In der Umsetzung die Verantwortung da gibt es unterschiedliche Schritte.“ (ID2, Z. 364-367)	Die Verantwortung liegt definitiv bei den Unternehmen, sich an die Auflagen zu halten und die Umsetzung dieser Verantwortung einzuhalten.	Die Verantwortung, die Auflagen einzuhalten und umzusetzen, liegt definitiv bei den Unternehmen.	Verantwortung Unternehmen
ID2: „Also nachdem ich aus dem Gesetzesbereich komme, die Verantwortung dass ich eine Vorlage habe, an die ich	Die Verantwortung, eine Vorlage zu liefern und die Regulierung liegen auf europäischer Ebene und	Die Verantwortung eine Vorlage zu definieren und somit eine Regulierung zu schaffen	Verantwortung Union / Staat

mich halten kann, liegt es natürlich an der Regulierung. Und nachdem die DSGVO auf europäischer Ebene ja beschlossen worden ist und in Kraft getreten ist, ist es dann immer noch auf nationaler Eben so eine Sache, dass ich da nachdrücke und nach definiere.“ (ID2, Z. 367-371).	auf nationaler Ebene. Besonders, wenn ich weiter formulieren und definieren muss.	liegt bei der EU und den Mitgliedsstaaten.	
ID2: „Und dann davor waren alle Unternehmen. Na ja, die kommt jetzt irgendwann einmal und dann war sie, was sie dann doch da. Und das war dann relativ überraschend für viele große Unternehmen Also Verantwortung in dem Sinne liegt bei Unternehmen, würde ich sagen, die sich frühzeitig auch auf das vorbereiten. Aber ich kann sagen aus Erfahrung, dass das die wenigsten tun. Also frühzeitig sich in Kenntnis setzen, wie und welche Regulatoren. Gerade kleinere, haben diese Kenntnisse, die Regulatoren haben sie vielleicht, aber haben keine Kapazität, größere haben die haben die Kenntnis und und müssen es dann umsetzen.“ (ID2, Z. 375-382)	Die DSGVO ist für viele Unternehmen sehr plötzlich in Kraft getreten. Sich als Unternehmen frühzeitig mit Regulatoren zu beschäftigen und sich vorzubereiten, liegt in der Verantwortung von Unternehmen. Gerade kleinere Unternehmen haben von der Kapazität her einen Nachteil.	Unternehmen haben die Verantwortung sich auf neue Regulatoren frühzeitig vorzubereiten, wobei kleinere Unternehmen dadurch oft wegen geringerer Kapazitäten einen Nachteil haben.	Verantwortung Unternehmen
ID2: „Ein Vorteil ist es natürlich, dass eher die natürlichen Personen also ganz stark definiert worden sind, also die Betroffenenrechte. Das ist ein klarer Vorteil, dass die für die Betroffenen ausgelegt sind und das sehr klar und strukturiert gemacht worden ist.“ (ID2, Z. 399-402)	Ein Vorteil der DSGVO ist, dass die Betroffenenrechte alle klar formuliert worden sind,und zwar sehr genau und strukturiert.	Die Betroffenenrechte wurden in der DSGVO klar und strukturiert formuliert.	Vorteile/Stärken der DSGVO
ID2: „Was eher weniger gut gelungen ist, ist diese Sache mit dem regionalen, also die räumliche Anwendung. Ich habe immer wieder Fragestellungen, wenn es denn ein Unternehmen ist, das in Amerika sitzt und Daten von EU Bürgern hat, also aufnimmt und analysiert. (ID2, Z. 402-405)	Ein Nachteil ist die räumliche Anwendung, dass immer wieder Unternehmen fragen, wie denn nun die Verarbeitung ist, wenn der Sitz des Unternehmens außerhalb der EU ist.	Ein Nachteil ist die räumliche Anwendung, da dies für Unternehmen außerhalb der EU nicht klar ist.	Nachteile/ Schwächen der DSGVO
ID2: „Aber was ich schon kriege, sind Anfragen, wo Sie fragen. Mein Unternehmen ist in Europa. Aber ich verarbeite Daten von englischen ist von Leuten, die in England sind. Da gilt es Übergangsregelungen. Also Bürger aus Großbritannien	Besonders kompliziert ist die räumliche Anwendung für Unternehmen in der EU, wenn es um personenbezogene Daten in Großbritannien geht.	Der Umgang mit der räumlichen Anwendungs-bereich ist komplex, wie zum Beispiel für EU Unternehmen mit Daten aus Großbritannien	Nachteile/ Schwächen der DSGVO

diese Sachen sind auch extrem tricky und noch nicht so klar.“ (ID2, Z. 421-428)			
ID2: „Also Forschungszwecke das ist noch nicht so angekommen im weitesten Sinne ja, aber ich glaube, das liegt daran, dass es in der DSGVO, da müsse man schon sehr große juristische Kenntnisse haben. Ja, die wenigstens suchen die DSGVO nach Forschungszwecken. Also da müsste man schon viel Kenntnis haben.“ (ID2, Z. 437-441)	Wie die Verarbeitung im Rahmen von Forschungszwecken ist, ist für viele noch unklar, und man benötigt große juristische Kenntnisse.	Für die Verarbeitung von personen-bezogenen Daten benötigt man große juristische Kenntnisse.	Nachteile/ Schwächen der DSGVO
ID2: „Im Großen und Ganzen glaube ich, dass diese Regel eigentlich ganz gut vielleicht einen Techniker beschreibt, was man zu machen hat, dass man eben bei Default, keine Sachen anpackt im Vorhinein, dass man eben dann explizit den User darauf hinweist. Ich glaube, was man machen kann, um das Ganze noch zu verdeutlichen bei Privacy by Design, das ist eben geschriebener Text, dass man Beispiele dazu gibt. Aber das ist eben die Regulierung mit Text, aber die EU hat ja immer wieder die haben wir immer wieder Seiten, wo sie dann darauf verweisen mit einem FAQ oder einem Guide, dass man dabei praktische Anwendungsbeispiele erbringt.“ (ID2, Z. 459-468)	Allgemein ist die Privacy by Design-Regelung ganz gut, da sie Techniker*innen beschreibt, was zu tun ist. Was man jedoch besser machen kann neben dem Gesetzestext, ist Beispiele zu erbringen. Auf solche verweist die EU aber in FAQs oder einem Guide.	Die Privacy by Design Regelung beschreibt Techniker*innen ganz gut, was zu tun ist. Trotzdem verbessern Beispiele, wie auf jene auf die die EU hinweist die Umsetzung.	Privacy by Design.
ID2: „Wenn etwas eher vage formuliert ist, zum Beispiel Artikel 20, glaube ich, die Datenübertragbarkeit, das ist vielleicht ein ganz gutes Beispiel. Da ist die Auswirkung, dass in einigen Domänen haben wir ganz gute Standards was diese Datenübertragbarkeit angeht. (...) Dann kann ich mir eigentlich nie sicher sein was wird alles rübergezogen. Ich meine, was sicher nicht rübergezogen wird, sind Geschäftsgeheimnisse von der einen App in die andere. Es stehen zwar Fristen zur Verfügung. Wie lange, das ist eindeutig definiert, aber es gibt keine einheitliche Standards über den Austausch der Daten: In welchem Format ist das? Was	Nachteile in der DSGVO sind vage Formulierungen wie die Datenübertragbarkeit. Dabei gibt es keine klaren Standards beim Austausch der Daten, wo man sich nie sicher sein kann, was übertragen wird.	Ein Nachteil in der DSGVO sind die vagen Formulierungen wie zum Beispiel die Datenübertragbar-keit, wo es keine Standards gibt.	Nachteile/ Schwächen der DSGVO

sollen da tatsächlich für Objekte dranhängen? Wenn ich da Bilder gemacht habe, beispielsweise wenn ich da fotografiert habe, sind das eigentlich meine Bilder, auf die ich ein Recht drauf habe, wenn ich dir nicht schon abgegeben habe in dem Moment, wo ich es hochgeladen habe.“(ID2, Z. 481-484 und Z. 493-500)			
ID2: „Wo man aber was machen kann natürlich in der Kommunikation zum Anwender. Das ist eben der Unterschied zwischen juristischer Sprache und einfacher Sprache, dass ich da den Übergang noch einmal finde, weil wenn ich dem das hinknallt, es ist auch so im Forschungskontext. Immer wieder, dass man ellenlange Erklärungen bekommt und zwei oder drei oder vier Seiten. Aber wer liest sich das wirklich durch? Die Leute schauen dann einmal auf den ersten Satz oben und hinten aufs Datum und sind eh schon überfordert. ? Wir fassen noch einmal zusammen, was eigentlich ein Paragraph oder was ein Abschnitt eigentlich, das heißt, für denjenigen der einwilligt.“ (ID2, Z. 538-547).	Einwilligungserklärungen sind ellenlang und niemand liest sie sich durch, was man jedoch machen kann: die Paragraphen und Absätze noch einmal zusammenfassen.	Da Einwilligungs-erklärungen derart lang sind und sie keiner liest, sollten Paragraphen und Absätze zusammengefasst werden.	Verständnis von Einwilligungs -erklärungen
ID2: „Ich meine, das geht auch immer ganz stark von in die Richtung: Wie groß ist das Unternehmen, weil ein großes Unternehmen kann sich ausgeklügelte Prozesse eher leisten, also und Forschungsunternehmen, die oder oder Universitäten, die kleineren. Da ist es eine Frage der Zeit und natürlich der Effektivität. Aber da habe ich bei zehn Mitarbeitern ja, ich weiß nicht, wo das so die Grenze ist. Die ganz Kleinen werden auch nicht anfangen mit Flow Charts sich überlegen wie sind seine Prozesse? Das ist einfach völlig irrelevant. Aber ein bewusst sein muss es im öffentlichen Dienst der Forschungsunternehmen und bei Großunternehmen definitiv geben.“ (ID2, Z. 555-562)	Auch wenn kleinere Unternehmen nicht die Ressourcen von großen Unternehmen haben, um ihre Prozesse ausgeklügelt darzustellen, muss trotzdem ein Bewusstsein auch im öffentlichen Dienst, in Forschungsunternehmen und bei Großunternehmen dafür da sein.	Auch wenn in kleineren Unternehmen die Ressourcen für genaue Prozessdarstellung nicht da sind, muss es ein Bewusstsein dafür in allen Unternehmen geben.	Verantwortung Unternehmen
ID2: „Es kann jetzt nicht dazu nicht nur so kommen, dass die Exfrau anruft. Mittlerweile	Wenn Daten nach draußen gelangen, weil das Unternehmen keine	Unternehmen haben die Verantwortung Prozesse zu haben, dass Daten	Verantwortung Unternehmen

kommt, dass KI gesteuerte Auskunft ersuchen und wenn die Firma keine Prozesse hat, dann gehen in dem Fall die Daten nach draußen. Und da muss man immer sagen, gilt dann die Regel, Ja, wie schnell habe ich dann die Personen benachrichtigt, Wie viele Daten sind betroffen? Ja, habe ich auch alles getan, um dann die Personen zu benachrichtigen. Und das minimiert natürlich dann auch wieder meine Rechenschaft und die Strafe.“ (ID2, Z. 608-614)	Prozesse dagegen hat, dann kommt es bei der Strafe auf die Schnelligkeit der Benachrichtigung der Betroffenen an.	nicht nach draußen gelangen, wenn sie das doch tun, kommt es bei der Strafe auf die Schnelligkeit der Benachrichtigung an.	
ID2: „Die Technikneutralität eigentlich würde ich sagen. Also von der DSGVO gegenüber in dem Sinne. Äh, ja. Ähm. Dass man eigentlich technikneutral demgegenüber stehen sollte. Aber also sprich zum Schutz personenbezogener Daten. Ähm. Um das mal kurz zu beschreiben, noch ein Beispiel zu bringen. Ja, eine große Herausforderung wird in der Zukunft eben diese ganzen Machine Learning Modelle, Softwaresysteme, die die Möglichkeit haben, ich gebe Ihnen was vor und sie lernen dann aufgrund von dem, was ich für Eingaben mache. Also da muss man dann sicherlich eine Schicht dazwischen ziehen.“ (ID2, Z. 718-726)	Eine der größten Herausforderungen zum Schutz personenbezogener Daten in der Zukunft ist die Technikneutralität, Machine learning-Modelle und Softwaresysteme, die selbstlernend sind.	Herausforderungen in der Zukunft werden Technikneutralität und selbstlernende Machine Learning-Modelle sein.	Heraus-forderungen in Zukunft.
ID2: „Es besteht genau die Verantwortung, die eigentlich überhaupt auf das System über, das ist ja ähnlich. Aber das ist ja auch so beim autonomen Fahren geht es ja auch in die Richtung. Ähm. Es würde beim autonomen Fahren insofern auch ganz gut sein, wenn es das System wäre. Nur das ist leider nicht die Lösung weil am System sind meistens 10 oder 15 Leute beteiligt in der Programmierung. Wahrscheinlich wissen wir es selber… Also man hat beim autonomen Fahren halt 55 zum Beispiel für ein Steuergerät 55 Funktionen und das sind 120 Entwickler. Wie hol ich den raus, wenn etwas passiert, ist das der unterste oder ist das der	Die Verantwortung wird sich auf Systeme verschieben, aber dann ist die Frage: Welcher der Programmierer*innen und Entwickler*innen ist dann verantwortlich? Die Repräsentant*innen-haftung wird also eine Herausforderung in der Zukunft sein.	Die Repräsentant*innen-haftung wird eine Herausforderung, weil sich die Verantwortung auf das System verschiebt.	Heraus-forderungen in Zukunft.

oberste? Also Repräsentantenhaftung.“ (ID2, Z. 734-742)			
ID2: „Also das wird sicherlich noch einmal mehr von Bedeutung, dass man in Novellierungen. Ja einen Rückverweis auf die DSGVO macht, dass man weiß, wie man umgeht mit personenbezogenen Daten. Genau. Je ausgeklügelter dieser… Je technisch reifer und je höher der Reifegrad von KI wird. Genau desto schwieriger wird das auch mit Personendaten.“ (ID2. Z. 765-769)	Je technisch reifer und ausgeklügelter und größer der Reifegrad von KI wird, desto schwieriger wird in Zukunft der Umgang mit Personendaten werden.	Je größer der Reifegrad von KI wird, desto schwieriger wird das in Zukunft mit Personendaten werden.	Heraus-forderungen in Zukunft
ID3: „Für mich ist nachhaltiger Datenschutz das Niveau des Schutzes personenbezogener Daten in einer datengesteuerten Welt, einem datengesteuerten Leben, einer datengesteuerten Gesellschaft, das mehr oder weniger allen zugutekommt, aber lassen Sie uns versuchen, dass es mehr oder weniger allen zugutekommt und nicht nur ein paar anderen. Das wäre meine Definition eines nachhaltigen Datenschutzes. Die Tendenz, der Privatsphäre einen Preis zu geben, macht mir große Sorgen. Ich würde also sagen, dass ich schon lange über dieses Thema nachdenke. Der Schutz personenbezogener Daten wird immer wichtiger, aber die Gewährleistung eines mehr oder weniger gleichen Schutzes für alle Teile unserer Gesellschaft, von den Schwächsten bis hin zu den wohlhabenderen, fast privilegierten Mitgliedern unserer Gesellschaft, wäre meiner Meinung nach ein sehr vernünftiger und nachhaltiger Schutz personenbezogener Daten. (ID3, Z. 859-870, durchgeführt am 25.07. 2023)	Nachhaltiger Datenschutz ist in einer datengesteuerten Welt das Niveau, das allen zugutekommt und nicht nur wenigen, welche der Privatsphäre einen Preis geben.	Nachhaltiger Datenschutz ist das Niveau, welches allen zugutekommt und nicht nur denjenigen die an Privatsphäre einen Preis hängen	Nachhaltiger Datenschutz
ID3: „(…) Ich denke, ich kann Ihnen sehr konkrete Beispiele aus meiner Tätigkeit in europäischen Institutionen nennen, die mit Unternehmen zu tun haben, deren Namen ich nicht nennen möchte, die aber nicht einmal in der Lage sind, den Aufsichtsbehörden klar und deutlich zu erklären,	Wir haben schon mit einigen Unternehmen zu tun gehabt, die Aufsichtsbehörden nicht einmal klar und deutlich sagen können, was sie mit personenbezogenen Daten machen und welche sie verarbeiten,	Es gibt einige Unternehmen, die nicht einmal Aufsichtsbehörden deutlich sagen können in welchem Umfang sie personenbezogene Daten verarbeiten, was nicht sehr glaubwürdig wirkt.	Verantwortung Unternehmen

was sie manchmal mit personenbezogenen Daten machen, ob sie personenbezogene Daten oder nicht personenbezogene Daten verarbeiten, in welchem Umfang usw., das zeugt von einem sehr geringen Maß an Glaubwürdigkeit.“ (ID3, Z. 892-898)	was nicht sehr glaubwürdig ist.		
ID3: „Ich denke, es hängt sehr davon ab, wie ernst die Unternehmen den Schutz der Privatsphäre und den Datenschutz nehmen, was sehr stark vom Geschäftsmodell des Unternehmens und seinen eigenen wirtschaftlichen Interessen abhängt.“ (ID3, Z. 904-907)	Es hängt sehr davon ab, wie ernst Unternehmen den Schutz der Privatsphäre und den Datenschutz nehmen und wie groß ihr wirtschaftliches Interesse an Daten ist.	Es hängt davon ab wie groß das wirtschaftliche Interesse von Unternehmen an Daten ist, wie ernst sie Datenschutz nehmen	Verantwortung Unternehmen
ID3: „Ich glaube nicht wirklich an die individuelle Autonomie und die Macht der Zustimmung und Verantwortlichkeit des Einzelnen in der digitalen Welt. Ich verstehe, dass das ein sehr bewusster, notwendiger Standpunkt ist. Ich denke, die Betonung der Zustimmung liegt wahrscheinlich direkt auf der Wahl des Einzelnen und seiner Autonomie und seiner Fähigkeit, selbst Entscheidungen zu treffen, usw., die der Zustimmungspflicht zugrunde liegen. Und die Rechenschaftspflicht der Nutzer oder Verbraucher, die vermeintliche Rechenschaftspflicht, ist meiner Meinung nach ein sehr schwieriger Teil. Ich glaube nicht, dass der Einzelne sich bewusst sein kann, hinreichend bewusst sein kann, gut bewusst sein kann, was bei der Verarbeitung der personenbezogenen Daten auf dem Spiel steht.“ (ID3, Z. 924-934).	Die individuelle Autonomie und die Zustimmung zur Verarbeitung personenbezogener Daten müssten voraussetzen, dass die Einzelnen wissen, was auf dem Spiel steht.d Das Bewusstseindafür fehlt, weshalb bei den Einzelnen keine Rechenschaftspflicht zu sehen ist.	Für die individuelle Autonomie der Einzelne, müssen ein Bewusstsein da sein, was auf dem Spiel steht und da dies nicht der Fall ist, ist die Zustimmung nicht das beste Instrument.	Verständnis Einwilligungs-erklärungen.
ID3: „Die Tatsache, dass die Datenschutz-Grundverordnung aus technologischer Sicht neutral ist, beruht auf allgemeinen Konzepten und Grundsätzen, die einer Auslegung bedürfen und offensichtlich auf konkrete Technologien, Fälle und sehr komplexe Verarbeitungsvorgänge anzuwenden sind. Aber dieses	Die DSGVO ist technikneutral, was wiederum bedeutet, dass sie Auslegung benötigt, da sie nicht auf spezielle Technologien anzuwenden ist. Dafür hat diese neutrale Sprache eine längere Gültigkeitsdauer.	Die DSGVO ist durch ihre allgemeine Formulierung Technikneutral und deswegen langwierig.	Vorteile/ Stärken der DSGVO

neutrale Sprachkonzept, die hochrangigen Konzepte der Verarbeitung personenbezogener Daten, die Grundsätze der begrenzten Datenaufbewahrung, die Datenqualität, all die allgemeinen Grundsätze, die die Datenschutz-Grundverordnung manchmal aufstellt und auf denen sie aufbaut, haben meiner Meinung nach eine gewisse Dauer.(…) Dies ist also eine der Stärken.“ (ID3, Z. 943-954).			
ID3: „Die Schwächen liegen darin, dass sie, da es sich um eine technologisch natürliche Verordnung handelt, die auf jede Art der Verarbeitung von Daten, jede neue Technologie, die aus dem Innovationssektor kommt, angewendet werden soll, ständig angepasst, neu angepasst und neu interpretiert werden muss. Ich erinnere mich an die Biometrie, und innerhalb der Biometrie muss man sie auf Fingerabdrücke oder jede Art von neuen Technologien anwenden, die auftauchen werden, was es zu einem Instrument macht, das besonders schwierig durchzusetzen ist, weil es schwer zu stabilisieren ist. Es braucht Zeit, um die Auslegung der Datenschutz-Grundverordnung zu einer zukunftssicheren Verordnung zu stabilisieren. Aber ich denke, dass die allgemeinen Grundsätze und Bestandteile, die rechtlichen Kosten, für deren Entwicklung, Erfassung und gesetzliche Verankerung wir so viel Zeit gebraucht haben, mit der Zeit ihr volles Potenzial entfalten werden. Aber in der Tat ist es auch schwierig, sie an so viele verschiedene Situationen bei der Verarbeitung personenbezogener Daten anzupassen.“ (ID3, Z. 954-969)	Die Technikneutralität ist auch eine Schwäche, da die DSGVO ständig neu angepasst und interpretiert werden muss, und um die DSGVO zukunftssicher zu stabilisieren, braucht es Zeit, damit sie ihr ganzes Potential entfalten kann.	Die Technikneutralität ist auch eine Schwäche, da es Zeit braucht, die DSGVO ständig neu zu interpretieren, um ihr ganzes Potential auszuschöpfen.	Nachteile/ Schwächen der DSGVO
ID3: „Wir befinden uns hier in den Anfängen des digitalen Rechts, und der Datenschutz befindet sich ohnehin noch in einem recht frühen Lebensstadium. Ich glaube,	Datenschutz und digitales Recht sind sehr junge Disziplinen, da in den 90ern und 2000ern die Euphorie gegenüber sozialen Medien und den	Die Euphorie der 90er und 2000er hat dazu geführt, dass die Auswirkungen von Sozialen Medien und Datenschutz nicht	Verantwortung Union / Staat

wir verlieren manchmal ein wenig den Abstand und denken, dass all dies existieren und völlig effizient sein und alle Probleme der Welt, die durch Technologie und digitales Recht entstehen, erfassen sollte. Aber das war einfach nicht möglich und machbar, weil es auch keinen politischen Konsens gab, die negativen Auswirkungen der Technologie zu erkennen. Es gab eine volle Begeisterung in den 90ern und 2000ern, alle waren von den sozialen Medien begeistert. Es hat ein bisschen gedauert, bis die Wissenschaftler das erkannt haben, dass das nicht nur die Menschen zusammenbringt, sondern dass das auch eine Polarisierung ist, dass das auch eine Spaltung der Gesellschaft ist, dass das auch eine Nebenwirkung ist.“ (ID3, Z. 987-997)	Technologien so hoch war, dass die negativen Auswirkungen nicht so schnell absehbar waren und die Politik erst später reagiert hat.	absehbar waren, weswegen die Politik auch nicht sofort reagieren konnte.	
ID3: „Das ist nicht nur gut und besser für die Welt, sondern bringt auch Probleme mit sich. Und das hat ein bisschen gedauert, und ich weiß das, weil ich zu der Gruppe von Leuten gehörte, die vor den Risiken gewarnt haben, die diese Technologien mit sich bringen. Aber man braucht politische Unterstützung, man braucht einen Gesetzgeber, der das versteht, oder man muss in der Lage sein, die Legitimation zu übernehmen. Man muss eine Menge Leute mit ins Boot holen, bevor man diese Probleme tatsächlich angehen kann. Glücklicherweise hat der Datenschutz eine etwas längere Geschichte, denn unser eigenes Trauma, das Trauma des 20. Jahrhunderts mit dem Krieg und all dem, sagen wir mal, hat dazu geführt, dass die Europäer sich gewisser Risiken vielleicht etwas bewusster sind als andere Teile der Welt und dass sie aufgeklärter und vorsichtiger sind, würde ich sagen. Vorsichtig genug, um als erste in der Welt Rechtsvorschriften in diesem Bereich zu erlassen und ein Interesse an der Regulierung der Verarbeitung	Die Probleme, die das Internet bringen wird und diese zu erkennen, hat gedauert und für Maßnahmen benötigt man viel politische Unterstützung und Gesetzgeber, welche die Problematik verstehen.	Die Probleme des Internets zu erkennen hat gedauert und für Maßnahmen hat es viel Überzeugung in der Politik und in der Gesetzgebung gebraucht.	Verantwortung Union / Staat

personenbezogener Daten zu erkennen, ohne jedoch genau zu wissen, wohin uns das alles führen würde. Denn wir konnten nicht wissen, Isabel, wir konnten nicht wissen, dass das Internet in die Knie gehen würde, obwohl all diese Grundsätze schon vor dem Internet festgelegt wurden, das sich dramatisch verändert hat.“ (ID3, Z. 1000-1016)			
ID3: „Ja, das stimmt. Ich denke also, die Grundlage ist gut, die Prinzipien sind gut, aber es gibt tatsächlich eine Reihe von Anpassungen des Verständnisses der Technologie, die jeder vornehmen muss. Regulierungsbehörden, Gesetzgeber und Durchsetzungsbehörden. Und das ist eine echte Herausforderung, denn wir müssen das richtige Gleichgewicht zwischen Innovation und dem Potenzial, das hinter der Verarbeitung personenbezogener Daten steckt, finden und finden, gleichzeitig aber auch einen angemessenen Schutz gewährleisten und für soziale Güter sorgen (…)“ (ID3, Z. 1019-1026)	Es gibt eine Reihe von Verständnisanpassungen bezüglich Technologie Regulierungsbehörde, Gesetzgeber und Datenschutzbehörden. Dabei müssen sie ein Gleichgewicht zwischen Schutzniveau, Innovation und Potential finden.	Es müssen noch einige Verständnis-Anpassungen geschehen, die ein Gleichgewicht zwischen Innovation, Schutzniveau und Potential schaffen müssen.	Verantwortung Union / Staat
ID3: „Und dieses Recht, und das führt mich zu einem weiteren Punkt, mein erster Punkt ist, dass dieses Recht meiner Meinung nach wirklich an der Kreuzung zwischen einem rein individuellen Recht und einem kollektiven Recht liegt. Es ist etwas, das allein nicht wirklich Sinn macht. Mein eigener, sehr begrenzter Schutz persönlicher Daten, der von Claire Gairel, ist vielleicht nicht so individuell wichtig, sondern weil wir Menschen insgesamt fast wie digitale Wesen behandelt werden. Die Verarbeitung unserer persönlichen Daten insgesamt macht uns aber viel anfälliger für die Macht einer Handvoll von Unternehmen oder Regierungen. Und das ist immer das Tückische an der Privatsphäre und den persönlichen Daten, dass es nicht unbedingt um mich geht. Das ist keine Gefahr für die Regierung,	Das Schwierige am Datenschutzrecht ist, dass es zwischen individuellem und kollektivem Recht liegt. Der Schutz von einzelnen Daten ist vielleicht nicht so wichtig, die Verarbeitung von persönlichen Daten macht jeden jedoch angreifbar. Die Verarbeitung von vielen personenbezogenen Daten ist vielmehr eine kollektive Bedrohung.	Die Schwierigkeit im Datenschutzrecht liegt in der Kreuzung zwischen individuellem und kollektivem Recht, denn die Bedrohung liegt eigentlich in der kollektiven Verarbeitung personenbezogener Daten.	Nachteile/ Schwäche der DSGVO

vielleicht nicht für mich. Aber insgesamt ist die Fähigkeit, personenbezogene Daten jedes Einzelnen mit einer so großen Rechenleistung zu verarbeiten, eine kollektive Bedrohung für die Art und Weise, wie wir leben. Und das ist der Grund, warum es so interessant ist. Der Schutz personenbezogener Daten ist eine Art Stellvertreter, aber auch ein Dienst an allen Rechten, am Schutz des kollektiven Interesses. Und nicht auf individuelle Interessen.“ (ID3, Z. 1027-1042).			
ID3: „Ja, auch auf individueller Ebene würde ich persönlich nicht so viel Wert darauf legen. Wir brauchen, in gewisser Weise, denn wir brauchen Bildung, digitale Bildung. (…) Wir sollten meiner Meinung nach nicht den Schwerpunkt der Verantwortung auf die Endnutzer und Verbraucher legen. Das ist nicht mein Standpunkt.“ (ID3, Z. 1055-1060)	Wir brauchen zwar auf individueller Ebene digitale Bildung, jedoch liegt der Schwerpunkt der Verantwortung nicht bei den individuellen Verbraucher*innen.	Die große Verantwortung liegt nicht bei den Verbraucher*innen, dennoch brauchen sie digitale Bildung.	Verantwortung Betroffene/ Konsument*innen
ID3: „Ich denke, der Schwerpunkt liegt bei der Gesetzgebung, bei den Regierungen, die die Verantwortung übernehmen müssen, um die Probleme und Herausforderungen anzugehen, die durch die massive Verarbeitung von Daten entstehen, (…)“ (ID3, Z. 1060-1063).	Große Verantwortung liegt bei der Regierung, welche sich den Herausforderungen stellen und die Datenverarbeitung weiter regulieren muss.	Große Verantwortung haben Regierungen, welche Datenverarbeitung weiter regulieren müssen.	Verantwortung Union / Staat
ID3: „(…)und bei den Unternehmen, die rechenschaftspflichtig sind und tatsächlich überwacht werden müssen. Und dann ist da noch die strenge Überwachung. Und das ist eher eine Frage des Schwerpunkts.“ (ID3, Z. 1063-1065)	Große Verantwortung liegt bei Unternehmen, die ihre Rechenschafts-pflichten einhalten müssen und überwacht werden sollten.	Große Verantwortung haben Unternehmen bezüglich Rechenschaftspflichten und sie sollten deswegen überwacht werden.	Verantwortung Unternehmen
ID3: „Ja, das ist eine große Frage, denn wir haben jetzt eine Einwilligung in der Datenschutz-Grundverordnung, die unter den sechs Rechtsgrundlagen recht ausgewogen war, weil der Europäische Datenschutzausschuss und die Arbeitsgruppe 29 immer gesagt haben, dass die Einwilligung nicht die beste	Unter Datenschutzexpert*innen ist die Einwilligungserklärung schon seit vielen Jahren bekannt, aber als die den Verbraucher/die Verbraucherin nicht am besten schützende Form. Dennoch wird ihr und der individuellen Kontrolle vor	Unter Datenschutz-expert*innen ist die Einwilligungserklärung nicht die am besten schützende Form, dennoch gewichten sie Gerichte sehr stark.	Verständnis Einwilligungs-erklärung

oder schützenste Rechtsgrundlage für Datenschutzexperten ist. Die Einwilligung ist nicht unbedingt die schützenste Rechtsgrundlage.(…) Interessanterweise legt das Gericht, die europäischen Institutionen und der Gesetzgeber in der Tat das Gewicht auf individuelle Kontrolle, mehr individuelle Kontrollen, mehr Verantwortung für die Endnutzer und die Wahl der Verbraucher usw. drängen und dem Konzept mehr Bedeutung beimessen. Mein persönlicher Standpunkt ist, dass ich dem etwas skeptisch gegenüberstehe.“ (ID3, Z. 1086-1091 und 1096-1099)	Gericht ein sehr hoher Wert beigemessen.		
ID3: „Und meiner Meinung nach ist es genau das, was ich mit dem EU-Recht gerne vermieden hätte, nämlich die Monetarisierung und die Bepreisung der Privatsphäre, denn was bedeutet das dann? Es bedeutet, dass ich, weil ich reich bin, mir ein sehr teures iPhone leisten kann, das ein sehr hohes Maß an Schutz für persönliche Daten und Sicherheit bietet. Aber wenn man das Geld nicht hat, kann man nur ein billiges und schlechtes Sicherheitsprodukt benutzen, oder wenn man Facebook ohne personalisierte Werbung benutzen will, muss man dafür bezahlen. Ich finde nicht, dass es das ist, warum ich meinen Punkt auf die nachhaltige Daten für die Generation begonnen, weil dies ist genau das Gegenteil von dem, was jetzt passiert. Ja, ich hätte mir die Fähigkeit bewahrt, einen Weg zu finden, die Privatsphäre des Einzelnen mit der unternehmerischen Freiheit der Unternehmen in Einklang zu bringen, und sie müssen ein gewisses Interesse an der Monetarisierung haben, um diese Dienste weiterhin kostenlos anbieten zu können, ein offenes Internet, die freie Verbreitung von Informationen. Ich hätte einen ausgewogenen Ansatz in Bezug auf all diese Interessen und Rechte, die miteinander in	Zunehmend wird die Privatsphäre monetarisiert in dem Sinne, dass es darum geht, ob man ein sicheres Gerät hat, das teurer ist oder ein weniger sicheres, das billiger ist, oder für Dienste wie Facebook personalisierte Werbung durch ein Abo abbestellen zu können. Das bedeutet, dass sich reichere Menschen besseren Schutz ihrer Privatsphäre und ihrer Personendaten leisten können.	Wenn Privatsphäre weiter monetarisiert wird, dann können sich reichere mehr Privatsphäre und Datenschutz leisten als ärmere.	Heraus-forderungen in Zukunft

Konflikt stehen, viel lieber gesehen, als zu sagen, ihr könnt euch ein sehr hohes Maß an Privatsphäre leisten, und wenn ihr das nicht könnt, tut mir leid. Ich hasse das wirklich.“ (ID3, Z. 1107-1123)			
ID3: „Ja, ich denke, das ist nur eine Folge der DSGVO, die meiner Meinung nach keine solche Ungleichheit geschaffen hat. Dies ist in der Tat eine Folge der Interpretation des Missbrauchs durch einige Unternehmen, die Daten insbesondere für einiges missbraucht haben, und jetzt haben wir es mit etwas zu tun, das leider nicht wirklich unter Kontrolle war. Die Tatsache, dass wir jetzt riskieren, diese Ungleichheit in der Privatsphäre in Europa zu haben, war meiner Meinung nach nicht beabsichtigt, und das ist der Grund, warum ich denke, dass das so schade ist, weil es nicht beabsichtigt war.“ (ID3, Z. 1131-1138)	Die DSGVO hat nicht Ungleichheiten geschaffen, aber die offenen Formulierungen und deren Missbrauch seitens der Unternehmen führen zu Ungleichheiten, auch wenn diese nicht beabsichtigt waren.	Die offenen Formulierungen der DSGVO und der Missbrauch von Unternehmen, hat zu unbeabsichtigten Ungleichheiten geführt.	Nachteile/ Schwächen der DSGVO
ID3: „Meta wird sich nicht weiterhin kostenlos anbieten, wenn es nicht zu Geld gemacht werden kann. Wir müssen also auch das Interesse an diesen Unternehmen verstehen. Sie haben missbraucht, das ist richtig. Aber gleichzeitig begeben wir uns auf einen, wie ich finde, sehr riskanten Weg, der darin besteht, dass diese Dienste in Zukunft in Europa billig sein könnten, und ich denke, das bedeutet eine größere digitale Kluft. Und die Menschen, die keinen Zugang zu diesen Diensten haben, die Menschen, die es können. Und das finde ich schade, denn Internet, soziale Medien, Suchmaschinenverbindungen, all diese Dienste sind entscheidend für die Informationsfreiheit und den Zugang zu Informationen. Sie sind auch sehr wichtig, um andere Grundrechte zu genießen.“ (ID3, Z. 1149-1158)	Die sozialen Medien und digitalen Dienste sind entscheidend für Informationsfreiheit und den Zugang zu Information. Deswegen ist es entscheidend, dass dieser Zugang nicht nur denjenigen gewährt wird, die es sich leisten können.	Die Sozialen Medien und digitale Dienste sind entscheidend für Informationsfreiheiten und Zugang zu Information, weswegen der Zugang allen ermöglicht werden muss.	Heraus-forderungen in Zukunft
ID3: „Vielleicht nicht mehr aber ich hätte mir ein ausgewogeneres Verhältnis zwischen all diesen Interessen und Rechten gewünscht. Die	Der Staat muss dafür sorgen, dass alle Freiheiten, Rechte und Interessen in einem ausgewogenen Verhältnis	Der Staat muss ein ausgewogenen Verhältnis aus Freiheiten, Rechte und berechtigen Interessen	Verantwortung Union / Staat

Unternehmensfreiheit ist auch eine Freiheit in der Charta. Informationsfreiheit ist auch ein Zugang zum Internet. Der Zugang zu diesen Diensten ist heute von entscheidender Bedeutung, wenn man irgendetwas tun will, ich meine, wenn man miteinander kommunizieren will, braucht man soziale Medien, man braucht all diese Dienste. Sie sind auch ungeheuer wichtig. Sie sind nicht nur problematisch, sie sind offensichtlich auch sehr gut, und ich denke, wir müssen das beibehalten, um davon zu profitieren.“(ID3, Z. 1172-1179)	stehen. Dafür ist der Zugang zu digitalen Dienstleistungen erforderlich, die nicht nur problematisch sind.	finden und den Zugang zu digitalen Dienstleistungen gewähren.	
ID3: „Ich denke, dass das Verbot der gezielten Werbung von Kindern auf Social Media, ist sehr klar und sehr notwendig. Ich denke, dass Kinder nicht gezielter Werbung und gezielten Inhalten ausgesetzt werden sollten. Es handelt sich also um eine sehr wichtige und klar umrissene Regelung, die meiner Meinung nach sehr zu begrüßen ist und die die Datenschutz-Grundverordnung wirklich versucht hat, ohne dass es zu Problemen kommt. Das Gleiche gilt für das Verbot der gezielten Werbung auf der Grundlage sensibler Daten. Ich denke, dass die Möglichkeit zu sagen, nein, Werbung darf nicht auf sensiblen Daten basieren, eine sehr bedeutende Klassifizierung der DSA über die DSGVO ist, die eine natürliche, sagen wir, natürliche Fortsetzung ist, und die Verbesserung des Schutzes, den die DSGVO bietet. Dies sind die beiden Aspekte, die meiner Meinung nach sehr wichtig sind.“ (ID3, Z. 1205-1216)	Der DSA wird die DSGVO um zwei wichtige Aspekte ergänzen, erstens das Verbot für digitale Dienstleister, gezielte Werbung und Inhalte Kindern zu zeigen und das Verbot von gezielter Werbung basierend auf sensiblen Daten, wie zum Beispiel der religiösen Zugehörigkeit. Hierbei gibt es auch nichts zu interpretieren, was wichtig ist.	Der DSA wird die DSGVO mit zwei Verboten ergänzen, einerseits das Verbot, Kinder gezielter Werbung und Inhalten auszusetzen und andererseits das Verbot, Werbung basierend auf sensiblen Daten auszustrahlen.	Einfluss DSA auf Schutz personen-bezogener Daten
ID3: “Ja weil es wird die treffen, die am problematischsten sind. Und die Ausrichtung von Inhalten und Werbung auf der Grundlage sensibler Daten ist der Punkt, an dem man die meisten Probleme verursacht, weil man Menschen wirklich nach ihrer sexuellen	Der DSA trifft diejenigen am härtesten, die am problematischsten sind, und Werbung basierend auf sensiblen Daten war extrem problematisch, weswegen hier entschieden wurde, keine Balance zu finden, sondern diese Art von	Der DSA trifft die, die am problematischsten sind und, da Werbung basierend auf sensiblen Daten als sehr gefährlich eingestuft wurde, wurde sie jetzt verboten.	Einfluss DSA auf Schutz personen-bezogener Daten

Orientierung oder ihrer Gesundheit identifiziert. Und ich denke, dass dies eine enorme und sehr bedeutende Einschränkung für Plattformen ist, da sie auf der Grundlage ihrer politischen Orientierung arbeitet. Das ist also sehr wichtig. Wir haben festgestellt, dass es hier Probleme gab und jetzt haben wird das auf eine ganz klare Art und Weise angesprochen, die nicht so viel Raum für Interpretationen oder Diskussionen lässt. Und ich denke, das ist gut so, denn jetzt haben wir ein klares Prinzip, das einfach Grenzen setzt und es verbietet. Es geht hier nicht darum, die richtige Balance zu finden.“ (ID3, Z. 1222-1232)	Werbung einfach zu verbieten.		
ID4: „ (…)die schrittweise Hoheit über die eigenen Daten, wenn Sie seine Daten haben wollen oder die Herrschaft über die eigenen Daten. Also ja, ich würde das im Prinzip auch, ich würde Ihre Definition da schon auch mitgehen. Die Frage ist, wie ich es mit Nachhaltigkeit in Verbindung bringen kann. Also es gab mal von dem, ich glaube es sind die Macher von Mozilla den Ansatz, dass sie gesagt haben, personenbezogene Daten sind für sich genommen ein Gut, über das man verfügt, das auch einen gewissen Wert hat, was man ja sieht, wenn man jetzt also die Entwicklung im Internet verfolgt, werden ja Auswertungen, Profilbildung vorgenommen, dann zum Beispiel Targeting, Werbung zu machen, Analysen zu machen und so weiter. Die haben gesagt, wieso nicht einfach den Browser so vorkonzipieren, dass man seine personenbezogenen Daten hinterlegen kann? Und dann kann man gegenüber Anbietern entscheiden, ob man seine personenbezogenen Daten herausgeben möchte oder nicht, wird dann aber dafür auch vergütet. Also das heißt, man hat einen eigenen Auswertungsanspruch auf seinen Daten, wenn man diesen Browser benutzt, ist	Nachhaltiger Datenschutz ist die schrittweise Hoheit über die eigenen Daten. Dabei gibt es ein Konzept, bei dem Betroffene ihre Daten hinterlegt haben und sich pro Anbieter entscheiden, ob sie ihre Daten gegen Vergütung zur Verfügung stellen. Dies wäre Autonomie über seine Daten, bei der man auch einen eigenen Auswertungsanspruch hätte.	Nachhaltiger Datenschutz ist die schrittweise Hoheit, über die eigenen Daten.	Nachhaltiger Datenschutz

leider glaube ich auch wieder gestorben irgendwann in diesem Projekt.“(ID4, Z. 1902-1917, durchgeführt am 25. Juli 2023).			
ID4: „Das Problem bei, also wenn man von vorne anfängt, also bei Betroffenen quasi ist ja eine gewisse, dass eine gewisse Informiertheit vorausgesetzt würde, wenn man eine Eigenverantwortlichkeit unterstellen würde. Also ich sehe schon eine große Verantwortung für den einzelnen Bürger, kann aber natürlich auch verstehen, wenn für viele dieses Thema nicht, äh, wenn sie keine Sensibilität dafür haben, wenn bei ihnen noch nie irgendwie ein Schaden gewesen ist oder irgendein Schaden, eine Schadenssituation gewesen ist, also man immer sorglos mit den Personen, also nicht sorglos, sag ich mal, mit den Personen bezogen und Daten umgegangen ist und es ist einfach auch nie was passiert. Dann ist das in der Regel so, dass das der Betroffene das sicherlich auch so weiter vollziehen wird. Deswegen ist es ein bisschen schwierig, da eine große Verantwortlichkeit draufzulegen.“ (ID4, Z. 1933-1943)	Das Problem ist, dass Betroffene, um eigenverantwortlich zu sein, informiert sein müssen. Da dies nicht der Fall ist, haben die Betroffenen für Datenschutz wenig Sensibilität und sind, bis ein Schaden passiert, sehr sorglos, weswegen sie nicht so stark in der Verantwortung gesehen werden können.	Betroffene können nicht so stark in der Verantwortung stehen, da Eigen-verantwortung Informiertheit voraussetzt.	Verantwortung Betroffene/ Konsument*innen
ID4: „Also ich sehe die Verantwortung da schon eher in den Verarbeitern und im Staat selber, weil man ja auch in anderen Teilbereichen so ein bisschen die Verantwortung vom Betroffenen runter nimmt oder vom Bürger runter nimmt und sagt, wir regeln das jetzt als Staat für dich, weil wir uns eben mit diesem Thema für dich beschäftigt haben. Und wir haben im Konsens entschieden, aus der Masse an Fällen, die bei uns jetzt aufgetaucht ist, legen wir da jetzt den Fokus drauf und nehmen dir ein bisschen die Verantwortung ab und regulieren das für dich jetzt mit.“(ID4, Z. 1943-1950)	Die Verantwortung liegt eher beim Staat, da er die Bürger*innen durch die Regelungen zum Teil von ihrer Verantwortung entbindet und dort reguliert wo Handlungsbedarf gesehen wird.	Die Verantwortung liegt zu großen Teilen beim Staat, da er Bürger*innen schützt und dort reguliert wo es notwendig ist.	Verantwortung Union / Staat
ID4: „Also da sehe ich jetzt tatsächlich beim Datenschutz so ein bisschen wie in der Medizin, beim Impfen, bei verschiedenen anderen	Eine gewisse Verantwortung haben Bürger*innen wie in der Medizin schon.	Ein gewisses Maß an Verantwortung liegt auch bei den Betroffenen.	Verantwortung Betroffene/ Konsument*innen

Kategorien, so, da sehe ich die Verantwortung natürlich schon aus meiner aufgeklärten Sicht beim Bürger.“ (ID4, Z. 1953-1955)			
ID4: „Aber ich halte es für gut und sinnvoll, wenn der Staat eben für den Bürger reguliert, weil er eben diese Sachen nicht so im Blick haben kann. Und beim Verantwortlichen sehe ich sie natürlich am meisten, weil dort das Know how in der Regel sitzt, diese Daten entsprechend zu verwenden.“ (ID4, Z. 1955-1959)	Der Staat hat zwar eine Verantwortung zu regeln, jedoch ist die Verantwortung von Unternehmen größer, da dort das Wissen sitzt, wie mit Daten umgegangen werden muss.	Die Verantwortung ist bei Unternehmen größer als beim Staat, da dort das Wissen zur Verarbeitung von Daten sitzt.	Verantwortung Unternehmen
ID4: „Wie bin ich compliant mit den gesetzlichen Regelungen. Ich sage meinen Kunden immer, wir wollen nicht als erst durchs Ziel gehen, wenn es Compliance geht, sondern wir wollen halt nur hauptsächlich über das Ziel kommen, weil es auch immer so einen gewissen Verhältnismäßigkeitsgrundsatz in der DSGVO gibt. Manche Dinge sind auch, ich glaube das kommt später in ihrem Katalog auch noch ein bisschen schwierig zumutbar oder teilweise einfach über die Angemessenheit abzuwürgen, weil das einfach nicht geht.“ (ID4, Z. 1964-1970)	Das Ziel ist es, so konformwie möglich zu arbeiten, auch wenn dies manchmal eine Herausforderung ist, aber deswegen gibt es den Verhältnismäßigkeits-grundsatz in der DSGVO.	Ziel ist es als Unternehmen nach dem Verhältnismäßigkeits-grundsatz der DSGVO so rechtskonform wie möglich zu arbeiten.	Verantwortung Unternehmen
ID4: „Also die DSGVO hat überschießende Tendenzen drinnen, die ganz offensichtlich größere Unternehmens sind, die tatsächlich Datenverarbeiter im Hauptgeschäft sind, quasi als Target haben. Und das hat mittelständische und kleinere Unternehmen mitgetroffen, wo das Risiko eine ganz andere ist.“ (ID4, Z. 1971-1974)	Die DSGVO hat überschießende Tendenzen, welche große Unternehmen als Ziel hat, trotzdem trifft sie mittlere und kleine mit.	Die DSGVO hat überschießende Tendenzen, die nicht nur große Unternehmen, sondern auch kleinere und mittlere trifft.	Nachteile/ Schwächen der DSGVO
ID4: „Unterschiedlich, je nachdem, wen man da als Kunden oder Ansprechpartner im Unternehmen hat. Also das variiert sehr stark. Ich habe ja gerade schon mal gesagt, wir wollen nicht als erstes durchs Ziel gehen, aber wir wollen halt irgendwie durchs Ziel gehen. Manche wollen noch nicht mal wirklich das, also die bestellen sich einen externen Datenschutzbeauftragten oder einen Datenschutzbeauftragten, weil	Wie ernst Unternehmen die Verantwortung sehen, variiert. Manche Unternehmen nehmen die Verantwortung des Datenschutzes nicht ernst und haben nicht einmal das Ziel, konform zu arbeiten.	Manche Unternehmen verfolgen nicht einmal das Ziel konform zu arbeiten.	Verantwortung Unternehmen

sie es halt irgendwie müssen.“ (ID4, Z. 1986-1991)			
ID4: „Und dann kommen wir halt irgendwie zu dem Punkt, müssen wir zum Beispiel bei der Datenschutzfolgenabschätzung für irgendeinen Prozess machen und dann bügeln wir das im Idealfall schon bei der Schwellenanalyse irgendwie ab, weil wir davon gegebenenfalls den Prozess vielleicht ein bisschen simplifiziert darstellen und da schon dann irgendwie rausfliegen und dann gar keine DSFA oder sowas machen müssen. In anderen Unternehmen wird es natürlich seriöser gemacht. Da ist natürlich schon ein sehr großer Spielraum für, der jetzt nicht missbrauch, aber man kann da schon über die eigene Dokumentation sich ein bisschen so hinstellen, als hätte man sich mit dem Thema beschäftigt, hat man aber nicht so wirklich, hat aber dann halt irgendwas, was man halt hinhalten kann und kann halt irgendwie sagen, wir haben ja mal eine Datenschutzfolgenabschätzung bei der Schwellenanalyse gemacht, wir sind halt damals zu dem Ergebnis gekommen, dass wir das nicht brauchen. Und der Hintergedanke ist natürlich ganz alleine, heißt, wenn irgendwann mal eine Beschwerde kommt oder eine Aufsichtsbehörde daher kommt, dass man halt irgendwas hat.“ (ID4, Z. 1991-2006)	In manchen Unternehmen wird keine DSFA gemacht, da der Prozess schon bei der Schwellenanalyse so simplifiziert dargestellt wird, dass es dazu nicht kommt. Andere Unternehmen machen dies seriöser, dennoch geht es häufig darum, dass im Beschwerdefall die Unternehmen etwas der Aufsichtsbehörde vorweisen können.	Wie seriös eine DSFA gemacht wird variiert stark, wenn es überhaupt zu einer kommt, Unternehmen ist es wichtig einer Aufsichtsbehörde etwas vorweisen zu können.	Datenschutz-folgen-abschätzung
ID4: „Ähm, also ein Vorteil ist natürlich schon, dass durch die Transparenzpflichten, diese Verantwortung, die wir vorher nicht so sehr beim Bürger gesehen haben, ausgeübt werden könnte durch den Bürger, weil er viel mehr gewahrt werden kann, was überhaupt passiert, was seine Datenverarbeitung ist, wo seine Daten über Land und so weiter, dass er Instrumentarien hat, sich zu beschweren, berichtigen zu lassen, löschen zu lassen, einschränken zu lassen etc. Pp. Und dass das auch einfach europäisch geregelt ist	Vorteile sind die Transparenzpflichten und dass Bürger*innen stärker geschützt werden. Sie s können sich beschweren und etwas berichtigen lassen und das auf EU-Ebene! Der Sanktionsgedanke zieht sich von kleinen Unternehmen bis zu den ganz großen.	Vorteile sind die EU-weiten Transparenz-pflichten, das Bürger*innen geschützt werden und sich wehren können und der Sanktionsgedanke in Unternehmen jeder Größe.	Vorteile/ Stärken der DSGVO

und dass es dazu eine Kommentarliteratur gibt, eine weit überwiegend durch den EuGH geprägte Rechtsprechung und so weiter. Das ist natürlich schon ein sehr, sehr großer Vorteil. Insgesamt auch das Datenschutzniveau, das angeglichene war ja sehr, sehr stark unterschiedlich in den europäischen Ländern. Und, also das ist natürlich schon ein sehr großer Vorteil. Dann noch zusätzlich ist noch mal ein großer Vorteil, dass man eben doch am Ende des Tages dieses Instrumentarium hat der hohen Bußgelder, die natürlich nie so verhängt werden, außer jetzt mal gegen Facebook in Frankreich oder in Irland oder so, aber in der Regel nicht für die kleineren oder mittelständischen Unternehmen. Aber das ist eben schon ein Punkt, bei dem zumindest mal über den Sanktionsgedanken auch in einem kleineren und mittelständischen Unternehmen reingetragen wird.“ (ID4, Z. 2019-2035)			
ID4: „Nachteil ist dann wiederum, es ist sehr viel bürokratischer Aufwand. Also teilweise haben sie natürlich unglaublich viel Dokumentationsaufwand, haben unglaublich oft Datenschutzerklärungen, Informationstexte, die weit überwiegend die gleichen Prozesse beschreiben. Sie werden immer wieder darüber informiert, werden auf Webseiten immer wieder auf Cookies auf sonstige Drittanbieter Tools hingewiesen. Sie werden immer wieder damit konfrontiert und es schafft halt unglaublich viel Arbeit vonseiten der Verantwortlichen, aber auch in gewisser Weise einen Bot und eine Genervtheit beim Betroffenen selber (ID4, Z. 2040-2047)	Zu den Nachteilen gehört der bürokratische Aufwand, der Dokumentationsaufwand seitens Verantwortlicher, welcher oft die gleichen Prozesse beschreibt und die Genervtheit über die Informations-overloads seitens der Betroffenen.	Nachteile sind der Bürokratische Aufwand seitens der Verantwortlichen und der Informations-overload seitens Betroffener.	Nachteile/ Schwächen DSGVO
ID4: „Hey, da gibt es was, worum wir uns dann doch irgendwie kümmern müssen. Wir müssen doch irgendwie informieren, wir müssen doch irgendwie schauen, dass wir	Durch die DSGVO nehmen es Unternehmen ernster und versuchen, Datenschutz seriöser zu gestalten.	Durch die DSGVO nehmen Unternehmen Datenschutz ernster.	Vorteile/ Stärken der DSGVO

das halbwegs seriös machen und das ist eben schon ein Punkt, der mit der DSGVO von Vorteil ist.“ (ID4, Z. 2041-2048)			
ID4:“ Ich habe teilweise gar keine andere Wahl als kleiner Betreiber irgendwie eines Onlineshops mir als mir so einen Baukasten zu nehmen, weil es mich sonst 30.000 € kosten würde, mir eine seriöse Seite machen zu lassen. Dann bin ich aber an so einem Content Delivery Network mit dran, weil da werden dann Sachen rausgeladen. Und ich würde jetzt als Datenschutzbeauftragter oder als Anwalt sagen, streng genommen sind sogar solche Content Delivery Networks nicht technisch, rein technisch notwendig ohne weiteres einsetzen unter diesem Gesichtspunkt, sondern sie müssten vielleicht sogar Einbindung bitten und darüber und teilweise wissen sie dann nicht mal, was mit dem IP Adressen passiert. Also ein absoluter Datenschutz und Verwaltungsnightmare. Und ja, das ist dann auch ein bisschen zu weit. Das ist wiederum eher so ein Nachteil und das ist an der technischen Realität vorbei. Weil auch generell diese Rechtsprechung, dass eine IP Adresse eine dynamisch generierte IP Adresse an ein personenbezogenes Datum ist eigentlich so ein bisschen an der Realität vorbei.“ (ID4, Z. 2081-2093)	Kleinen Anbietern bleibt teilweise gar nichts anderes über, als nicht ganz konformzu arbeiten, weil der Datenschutz sonst zu einem Verwaltungsalbtraum wird, da die DSGVO manchmal an der technischen Machbarkeit vorbeiläuft.	Kleine Anbieter können manchmal nicht 100% konform arbeiten, da hier die DSGVO an der technischen Realität vorbeigeht und es sonst zu einem Verwaltungs-albtraum wird.	Nachteile/ Schwächen DSGVO
ID4: „Also ein Nachteil ist definitiv, denke ich, dass es Innovationen schon bremst, also zumindest in der Form, wie es jetzt gerade ist. Wir hatten jetzt vorher schon nicht die riesige Anzahl an Cloud Anbietern oder an Technik Anbietern in Deutschland oder Europa, aber jetzt sicherlich noch unattraktiver als es vorher schon war. Die sitzen halt alle einfach in den USA oder in anderen Ländern. Ist jetzt hier nicht leichter geworden, irgendwelche technischen Innovationen anzubieten, wo sie gegebenenfalls irgendwie personenbezogene Daten	Ein Nachteil ist, dass die DSGVO Innovationen aufhält und manche Innovationen nicht angeboten werden können, und Europa als Markt unattraktiver gemacht wird.	Ein Nachteil ist, dass die DSGVO Innovationen aufhält und Europa als Markt unattraktiver macht.	Nachteile/ Schwächen der DSGVO

brauchen.“ (ID4, Z. 2137-2143)			
ID4: „Und auch dieser Privacy by Design Grundsatz halte ich für absolut sinnvoll. Aber das können andere Unternehmen im internationalen Vergleich halt dann einfach nicht so krass berücksichtigen und haben dadurch vielleicht schneller ein Produkt, das dann doch so überzeugend ist für den Endkunden, dass er sagt okay, das ist mir jetzt relativ egal, ob ich da eine gewisse Anzahl an Daten preisgeben muss oder ob das jetzt optimiert ist auf Privacy by Design oder bei Default.“ (ID4, Z. 2143-2148)	Privacy by Design ist sinnvoll, dennoch berücksichtigen einige Unternehmen dieses Werkzeug zum Schutz von Daten nicht, um schneller am Markt zu sein. Es ist ihnen egal, ob ein Gerät auf Privacy by Design ausgerichtet ist oder nicht.	Privacy by Design ist wichtig, aber das berücksichtigen nicht alle wenn es darum geht wer schneller am Markt ist.	Privacy by Design
ID4: „Ja, aber weit überwiegend muss ich sagen, dass ich, wenn ich mit Datenschutzbeauftragten in anderen EU Ländern meiner Kunden spreche, also beispielsweise jetzt habe ich ja mit deiner Frau Brottochter einen Kunden, der quasi in knapp 80 Ländern tätig ist und natürlich haben die fast jedem europäischen Land einen eigenen Datenschutzbeauftragten. Da sprechen wir weit überwiegend schon auf einem Niveau miteinander und tauschen auch untereinander Templates aus und tauschen untereinander Best Practices aus. Also das ist schon ein erheblicher Vorteil trotz individueller Kleinigkeiten, die in anderen Ländern gegebenenfalls anders sein könnten. Aber letzten Endes muss ich sagen, ist das schon mal ein sehr, sehr großer Schritt in die richtige Richtung. Natürlich wäre eine Vollharmonisierung noch besser gewesen.“ (ID4, Z. 2160-2170)	Eine Vollharmonisierung wäre natürlich besser gewesen, trotzdem sprechen wir in fast jedem europäischen Land großteils auf dem gleichen Niveau und tauschen sogar Templates aus.	Eine Vollharmonisierung wäre besser gewesen, trotzdem sprechen wir in jedem EU-Staat Großteils auf dem gleiche Niveau.	Harmonisierungs-erfolg der DSGVO
ID4: „Halte ich natürlich für sehr sinnvoll, darüber noch mal ein Instrumentarium zu schaffen, über das man von vornherein klare Spielregeln festlegt. Was darf ich als Provider, was darf ich nicht, zu welchem, zu welchem Handlungen bin ich verpflichtet? Spätestens ab dem Zeitpunkt, ab dem mir eine Rechtsverletzung klar wird. Wobei ich in Europa	Es ist gut, dass Provider jetzt Spielregeln bekommen. Gerade wenn es um den Schutz von Kindern oder Verleumdungsinhalte geht, sieht man oft bei einer IP Adressenabfrage, dass diese gar nicht in der EU ist.	Es ist gut, dass Provider nun Regeln bekommen, die zum Schutz von Kindern dienen und, dass es auch die trifft, die nicht in der EU sind.	Einfluss DSA auf Schutz personen-bezogener Daten

sowieso, wenn ich, was solche Rechtsverletzungen angeht, weniger das Problem sehe. Also es geht ja zum Beispiel auch den Schutz von Kindern, beispielsweise bei kinderpornografischen Inhalten oder sowas. Oder Verleumdungsinhalte und so weiter. Jedes Mal, wenn ich so ein Verfahren habe und dann machen wir irgendwie eine IP Abfrage und machen irgendwie eine Domain Abfrage, wo sitzen die denn eigentlich und wieso auch immer, ist das eigentlich nie in Europa sind." (ID4, Z. 2195-2204)			
ID4: „Die Datenschutzgrundverordnung und der Digital Service Act sind ja so ein bisschen anmaßend, weil wir regeln ja einfach was für Europa, was Unternehmen mit Sitzen in komplett anderen Ländern, die dort völlig komplett arbeiten, bitte befolgen sollen. Facebook hat angekündigt vor einem Jahr circa prüfen zu wollen, ob sie überhaupt ihr Angebot in Deutschland so weiter fortsetzen wollen oder in Europa weiter fortsetzen wollen, weil sie eben keine Lust haben, sich der DSGVO vollständig zu unterwerfen und ständig Bußgelder zahlen zu müssen, weil an ihrem Geschäftssitz arbeiten sie vollkommen compliant. Und was soll das eigentlich, dass jetzt die Europäer sich herausnehmen, ihnen einen Spielregeln aufgeben zu wollen, wo sie doch in den USA sitzen? Was auch ein bisschen verständlich ist. Im Endeffekt, wer jetzt am Ende des Tages bei Facebook noch sein will, muss eben mit den sauren Apfel beißen und muss sich auf der Plattform halt anmelden nach amerikanischem Recht. (…)Die anderen sind ja schon lange auf andere Portale abgewandert. Aber das gleiche gilt natürlich auch für TikTok und China. Also ein riesen riesen Provider, ein riesen Content Provider, den wir über die DSGVO oder über den Digital Service Act kontrollieren wollen, der aber	Hoffentlich ziehen sich durch die DSGVO und den DSA nicht große internationale Player aus dem Markt zurück, da die beiden Rechtsakte auch anmaßend sind, da Dienstleister oft in ihren eigenen Ländern konformabeiten.	Es kann sein, dass sich große Internationale Dienstanbieter aus dem EU-Markt zurückzeihen, da sie in ihren Ländern an und für sich rechtkonform arbeiten.	Heraus-forderungen in Zukunft

seinen Schlüssel in China hat und dort komplett arbeitet. Also ich habe teilweise Schriftstücke von Chinesen, die sind der Ansicht, dass die meisten Daten, die wir in Europa als personenbezogen ansehen würden, gar keine personenbezogenen Daten sind. Und damit hat sich das Problem erledigt.“ (ID4, Z. 2214-2226 und 2230-2236)			
ID4: „Ich denke doch schon, dass es so eine Harmonisierung der Providerhaftung ist. Also das natürlich schon, aber vom europäischen Markt an sich für europäische Unternehmen wird das natürlich eine Rolle spielen für europäische Provider, Access Provider, Host Provider, bla bla bla. Aber es könnte natürlich auch eine gegenläufige, gegenläufige Geschichte werden.“ (ID4, Z. 2258-2262)	Hoffentlich hat die Providerhaftung nicht die gegenläufige Wirkung, nämlich die eines Rückzugs, auch wenn dies für europäische Provider ganz gut wäre.	Auch wenn es für europäische Provider nicht so schlecht wäre, kann es sein, dass der DSA eine gegenläufige Wirkung für Provider hat.	Heraus-forderungen in Zukunft
ID4: „Also die größte Herausforderung für den Datenschutz wäre wahrscheinlich überhaupt erst mal mündige Bürger zu schaffen, die das noch als großen Punkt sehen, aus Eigenverantwortlichkeit heraus und nicht. Die Tendenz weiter zu verstärken, sein komplettes Leben in die Öffentlichkeit zu schieben.“(ID4, Z. 2281-2284)	Die größte Herausforderung ist es, mündige eigenverantwortliche Bürger*innen zu schaffen, die gleichzeitig große Teile ihres Lebens veröffentlichen.	Neben der Tendenz, sein Leben zu veröffentlichen wird es eine Herausforderung, mündige Bürger*innen zu schaffen.	Heraus-forderungen in Zukunft
ID4: „Und das ist für mich ein ganz, ganz großes Problem, wenn man dazu Studien sieht und wenn man dazu sieht, dass dieser Datenflut sowieso die Ermittlungsbehörden für ein unlösbares Problem sind, wo sie es niemals auswerten könnten und dazu halt eben noch eine gigantische Anzahl von Likes geben würde, dann habe ich bei sowas ziemlich starke Bauchschmerzen. Ich hatte vorhin auch schon mal gesagt, das ist so als Herausforderung, je schärfer Datenschutzgesetze werden, je höher die Strafen werden, je konkreter die Rechte des Einzelnen betroffen werden, birgt das natürlich auch Missbrauchsmöglichkeiten auch durch, durch Betroffene an der Datenverarbeitung. Also das sind eben dann das, was ich vorhin auch meinte.	Je stärker die Betroffenenrechte werden und die Höhe der Strafen, und je höher die Datenfluten ansteigen, desto größer werden auch die Herausforderungen, was den Missbrauch dieser Rechte betrifft.	Je stärker Rechte von Betroffenen und Sanktionen angehoben werden und die Datenflut steigt, desto mehr Missbrauchsfälle dieser Rechte wird es auch geben.	Heraus-forderungen in Zukunft

Da kam dann die Beschwerden ein Jahr später (…) Mit einer Datenauskunft in Verzug zu setzen, sofort eine Abmahnung auszusprechen, rechtsame Kosten geltend zu machen, Schadensersatz aufgrund eines Unwohlseins und so weiter zu fordern und solche Sachen. Das kann wirklich sehr unangenehm werden.“ (ID4, Z. 2387- 2402)			
ID4: „Tatsächlich ist das Datenschutzrecht ein Magnet für, ich will jetzt nicht sagen Querköpfe, aber für Leute mit starker Meinung und als Geltungsbedürfnis. Also ich habe das tatsächlich sehr, sehr oft. Ich lehne auch private Datenschutzmandate mittlerweile auch sehr oft ab, weil oft irgendwas noch mal nachgelagert rauskommt, was dann die Ursache für den eigentlichen datenschutzrechtlichen Anspruch ist. Und das kann dann teilweise sehr, sehr unangenehme Züge annehmen und es macht dann auch keinen Spaß, mit diesen Daten selber zu arbeiten.“ (ID4, Z. 2433-2439)	Gerade das Datenschutzrecht ist anziehend für Menschen mit starkem Geltungsbedürfnis, bei denen sich später herausstellt, dass sie eine Agenda damit haben.	Gerade Datenschutzrecht ist auch anziehend für Betroffene die eine missbräuchliche Agenda haben.	Heraus-forderungen in Zukunft
ID5: „Nachhaltig wäre, was wir leider in Österreich nicht haben und in ganz Europa, dass tatsächlich die Daten geschützt werden und dass nicht Geld geht oder dass es darum geht, dass ich kalkuliere, wie viel Strafe ich bekomme, wenn ich es nicht mich daran halte, sondern mich einfach daran halte, weil es sinnvoll ist. Und nachhaltig wäre auch für mich, wenn die Leute nicht zu zweigleisig fahren würden die ganze Zeit, weil ich sehe sehr oft, dass die Leute, wenn irgendein Problem ist, super haglich sind und sofort die DSGVO als einfach ein riesen Compliance Thema nehmen.(…) Für mich wäre nachhaltig, wenn die Leute manchmal ein bisschen drüber mehr nachdenken, auch umgekehrt, wenn die Leute drüber nachdenken.“ (ID5, Z. 2509-2515 und 2519-2521, durchgeführt am 31.07.2023)	Nachhaltig wäre einerseits, wenn Daten wirklich geschützt werden und Unternehmen nicht kalkulieren, wieviel Strafe sie zahlen und sich an die Regelungen halten. Nachhaltig wäre andererseits auch, wenn Individuen mehr über den Schutz ihrer Daten nachdenken würden.	Nachhaltig wäre es wenn Unternehmen nicht nach Grauzonen in der DSGVO suchen und Individuen mehr über den Schutz ihrer Daten nachdenken.	Nachhaltiger Datenschutz
ID5: „Also ich sage, ich sollte drüber nachdenken, welche	Alle wollen wie Erwachsene behandelt	Betroffene sollten mehr über den Schutz ihrer	Verantwortung Betroffene/

Daten ich von mir preisgebe, weil manches habe ich einfach in der Hand dazu. Und ob ich wirklich bei jedem Gewinnspiel mitmachen will oder was eigentlich die Kosten dafür sind, dass man die ganzen Sachen geschenkt bekommt oder nicht(…)Wir wollen alle als erwachsene Menschen behandelt werden. Und diesen Satz gehe ich da rein, weil einerseits wollen wir darüber aufgeklärt werden über jeden Blödsinn, aber alle Vorteile wollen wir auch haben dazu. Und da ist für mich so die Grenze. Also ich sage immer mit Hausverstand arbeiten ist sinnvoll.“ (ID5, Z. 2535-2538 und 2541-2544)	werden, dann müssen sie auch mehr über den Schutz ihrer Daten nachdenken und nicht alles preisgeben.	Daten nachdenken, nicht überall mitmachen und alles preisgeben.	Konsument*innen
ID5: „Ich finde es verdammt schwierig vom Staat das zu regulieren. Also ich bin immer ein Jurist, der dann denkt, wie schreibe ich so etwas rein, dass es wirklich alles abdeckt? (…)Wie schreibe ich ein Gesetz, was alle Dinge, die schützen soll, schützt, aber nicht gleichzeitig das, was es helfen soll, nicht irgendwie blockiert.“ (ID5, Z. 2560-2561 und 2565-2566)	Es ist für einen Staat sehr schwierig, ein Gesetz so zu schreiben, dass alles, was es zu schützen gilt, geschützt wird, ohne andere Dinge einzuschränken.	Es ist als Staat schwer Gesetze zu schreiben, die alles schützen und nichts einschränken.	Verantwortung Union/ Staat
ID5: „Und ich habe das Gefühl, unser heutiges Gesetz ist teilweise auch die DSGVO, dass wirklich große Unternehmen wie jetzt, ich spreche da von Meta oder Google, die natürlich einer der größten Datenverarbeiter sind, nur kalkulieren, wo setze ich mich hin, wo dauert das Verfahren am längsten und was kostet mir das Ganze und was soll mir schon passieren? Weil die Leute haben eh keine andere Option, weil ohne Google alles zu finden. Also das denke ich mir dann immer.“ (ID5, Z. 2566-2571)	Große Unternehmen kalkulieren nur, wie hoch die Strafen sind und wie lange Verfahren dauern und kümmern sich nicht um die DSGVO.	Große Unternehmen kalkulieren, wie groß die Strafe und wie lange das Verfahren ist und nicht die compliance.	Nachteile/ Schwächen der DSGVO
ID5: „Ich finde, die Stärke ist dahinter, dass wir in Europa ein ziemlich gleiches Rechtssystem haben unter Anführungszeichen, weil wenn man sich dann näher damit beschäftigt ist eh wieder. Aber das finde ich grundsätzlich eine Stärke. (…)Eine juristische Ausführung ist immer nur auf ein Land ausgelegt und nicht auf ganz viele Länder. Das ist die Stärke.(…) Der Vorteil ist, wir	Ein einheitliches Rechtssystem in der EU ist die Stärke im Gegensatz zu anderen Ländern.	Ein einheitliches Rechtssystem in der EU ist die Stärke.	Vorteile/ Stärken der DSGVO

haben in der EU ein komplett gleiches System, wenn man sich ein bisschen weiter anschaut, auch in Kalifornien oder so etwas.“ (ID5, Z. 2579-2581, 2584-2585 und 2596-2598)			
ID5: „Die Schwäche finde ich extremst dahinter ist, dass es teilweise von Juristen geschrieben ist, die keinerlei technisches Verständnis haben. Das merkt man extremst. Das merkt man jetzt auch beim neuen Artificial Intelligence Act oder so etwas. Also wenn man da jemanden in der KI Forschung fragt, dem dreht es alles weil der sagt, das ist sowas von hinterwäldlerisch, dem geht es nicht mehr. Das befürchte ich auch mit dieser Digital Service Act werden. (…)Man sollte viel mehr Techniker einbinden. Weil es gibt eine riesen Bandbreite, wenn wir jetzt über Anonymität, Pseudonymität zum Beispiel von Technischen reden, über technische Sicherheitsmaßnahmen. Und das wird einfach nicht gedacht von den Juristen(…)“ (ID5, Z. 2585-2590 und 2593-2596)	Zu den Schwächen gehören die Formulierungen, die Jurist*innen ohne technisches Verständnis gewählt haben, vor allem bei technischen Sicherheitsmaßnahmen sollten mehr Techniker*innen einbezogen werden.	Zu den Schwächen gehören unklare Formulierungen, bei denen keine Techniker*innen hinzugezogen wurden.	Nachteile/ Schwächen der DSGVO
ID5: „Es ist nicht so gut geglückt. Also ich sehe das nur gerade in Österreich im Forschungsbereich. Da merke ich es am ärgsten. Wir haben teilweise wirklich gute Öffnungsklauseln rein bekommen in die DSGVO und wir haben das komplett versaut in Österreich.(…) Ich sage, ich finde es grundsätzlich gut. Die Grundsätze sind zumindest überall gleich. Und man versteht eigentlich die meisten Entscheidungen, die EU weitergeben. Es kommen aber dann teilweise Entscheidungen, wo ich sage, da hat man überhaupt keinen Überblick. Also ich würde jetzt nicht sagen, es ist alles gut geglückt oder es ist alles überhaupt gut geglückt, sondern je nachdem welchen Teilbereich man sich rausnimmt, kann es super funktionieren und kann es katastrophal sein einfach.“ (ID5, Z. 2608-2611 und 2613-2618)	Die Harmonisierung ist nicht so geglückt, obwohl wir gute Öffnungsklauseln haben, aber Österreich hat das nicht gut geregelt, denn grundsätzlich sind Öffnungsklauseln nicht so schlecht. Wie gut sie geregelt wurden, kommt jedoch auf den Bereich an, und im Forschungsbereich sind sie schlecht.	Die Harmonisierung ist nicht so gut geglückt, da Österreich die Öffnungsklauseln nicht gut geregelt hat wie zum Beispiel den Forschungsbereich.	Harmonisierungs-erfolg der DSGVO

ID5: „Ich finde, da muss ich wieder sagen, da möchte ich lieber nicht in der Hand eines Gesetzeschreiber stehen, weil diese natürlich wäre eine Komplettharmonisierung das Idealste gewesen. Nur mich sich mit so vielen Parteien zu einigen, ich denke mal von meiner Studienzeit aus, wo eine Gruppenarbeit mit vier Personen einen Termin schon finden ist eine Katastrophe. Darum finde ich die Öffnungsklauseln gut. Wir in Österreich haben einfach ein Talent, solche Dinge zu versauen, das muss man ehrlich sagen vom Gesetzgeber her. (…)“ (ID5, Z. 2625-2632)	Eine komplette Harmonisierung wäre das Beste gewesen, aber dies kann kompliziert sein bei vielen Ländern. Darum sind die Öffnungsklauseln nicht schlecht, nur Österreich hat sie nicht gut gemacht.	Eine Komplett Harmonisierung wäre am besten gewesen, dennoch sind Öffnungsklauseln nicht schlecht wenn sie gut geregelt werden.	Harmonisierungs-erfolg der DSGVO
ID5: „Es kommt immer darauf an, in welchem Gebiet wir sind. Ich finde zum Beispiel, je schneller sich das Gebiet entwickelt, desto schwieriger ist das genau zu regeln, weil sonst müsste ich jedes halbe Jahr die Gesetze novellieren. Also ich kenne das jetzt nur von der Forschung und eben gerade im Digitalisierungsbereich haben wir halt jetzt Zeiten von Neuerfindungen zwischen einem halben Jahr und Jahr, wenn überhaupt. Da kommst du als Gesetzgeber gar nicht hinterher, das neu zu regeln, zu regeln, zu regeln. Soll es lieber offen sein.“ (ID5, Z. 2645-2651)	Je schneller ein Gebiet sich entwickelt, desto schwerer ist es, das zu regeln. Manches sollte vielleicht offener gestaltet werden, wie zum Beispiel im Forschungs- und Digitalisierungs-bereich.	Je schneller sich etwas entwickelt desto offener sollte es geregelt sein, da sonst Gesetze nicht mehr hinterherkommen.	Harmonisierungs-erfolg der DSGVO
ID5: „Das Problem ist, es ist so offen gestaltet, was ist Privacy by Design überhaupt? Das finde ich schon mal die Definition. Und es ist nur, weil es vielleicht für mich als Juristen total verständlich ist und logisch ist, wie ich das anklicke. Kannst einerseits, ich finde zum Beispiel dieser Cookie Banner ist ja auch eine gewisse Art des Privacy by Design Umsetzung, auch wenn es eigentlich, aber auch den Datenschutz betreffen. Und ich weiß von allen Freunden, die sind nur mal genervt und klicken nur mal auf alles akzeptieren, weil niemand sich mehr durchklicken will oder sowas. Jeder ist genervt.“ (ID5, Z. 2667-2673)	Privacy by Design ist zu offen gestaltet, es gibt keine Definition, was es überhaupt ist, und nur weil etwas für Juristen logisch ist, ist es das nicht auch für andere.	Privacy by Design ist zu offen gestaltet und es gibt wenig Klarheit was mit Privacy by Design genau gemeint ist.	Privacy by Design

ID5: „Was ist Privacy by Design? schnellst mögliche Anonymisierung überhaupt? Anonym arbeiten? Was ist Anonym arbeiten? Da wissen Sie, wenn Sie zehn ITler fragen, kriegen Sie zwölf Antworten, was Anonymisierung ist dahinter. Und das ist, was einfach fehlt, weil nur weil es für uns vielleicht logisch ist. Also wenn ich meinem Vorstand sage, ich kann es immer nur an der FH Seite besprechen, anonymisiert die Daten, da bekomme ich fünf verschiedene anonymisierte Datensätze. Heißt aber noch lange nicht, dass das irgendwie gleich anonymisiert ist. (…) Aber das finde ich, sind diese schwierigen technischen Dinge auch beim Privacy by Design. Bei welchen IT Ansatz muss ich ansetzen, dass das so sicher ist laut Privacy by Design.“ (ID5, Z. 2689-2695 und 2702-2704)	Unklarheiten, was mit Privacy by Design und anonymem Arbeiten gemeint ist, allein was Anonymisierung bedeutet, da bekommt man viele verschiedene Antworten aus der IT. Es ist unklar, bei welchem IT-Ansatz man bei Privacy by Design ansetzen muss.	Es ist unklar bei welchem IT Ansatz man bei Privacy by Design ansetzt, denn es gibt allein Unklarheit was Anonymisierung bedeutet.	Privacy by Design
ID5: „Ich finde das extrem schwierig, weil erstens mal festzustellen, brauche ich eine oder nicht? Und dann habe ich das Gefühl, Papier ist extremst geduldig. Ich habe selber welche im Bereich jetzt schon geschrieben. Ich habe sie mit unseren Datenschutzbeauftragten auch noch mal abgeglichen und bekam die Antwort, Naja, sie bemühen sich wieder und machen das i -Tüpfelchen, was nicht notwendig ist bei manchen Dingen. Weil ich kann erst nimm Papier ist wirklich geduldig. Ich kann so viel reinschreiben, wie ich da jetzt schütze und warum das zum Vorteil ist und nicht und so etwas. Aber ich würde wirklich gern wissen, wie viel dann technisch im Hintergrund dann wirklich umgesetzt wird und nicht nur hingeschrieben wird. Ich halt persönlich auch nicht viel davon. Ich wäre dafür, dass die Unternehmen regelmäßig kontrolliert werden, ob es tatsächlich passiert. Als diese Selbstevaluierungen.“ (ID5, Z. 2720-2730)	Es ist schwer festzustellen wann es eine DSFA ist, und dann heißt es noch lange nicht bei einer DSFA, was wirklich technisch umgesetzt wird, darum sollten Unternehmen strenger kontrolliert werden.	Wann genau eine DSFA gebraucht wird, ist unklar und was technisch wirklich umgesetzt wird auch, weswegen strenger kontrolliert werden müsste.	Datenschutz-folgen-abschätzung

ID5: „Extremst schwierig, extremst wirklich schwierig. Weil ich schon mal finde, die Frage ist, was kann man ansetzen, was Leute verstehen oder nicht? Ich tu mir immer schwer, sie sollen immer einfacher geschrieben werden, die Einwilligung, also Klärungen, Stichwort einfache Sprache, kurzer Sätze und alles. Dann mich juckt es dann immer zu hinterfragen, sind diese Menschen überhaupt einwilligungsfähig, wenn sie nicht einmal mehr als drei Wörter lesen können? Ganz schlecht, immer solche Fragen zu stellen. Ich weiß, dass es dann immer in der Praxis ist. Andererseits erkläre ich, eigentlich müsste man ja jede KI im Hintergrund erklären, was da passiert und wie die verarbeitet. Ich habe jetzt schon einen relativ technischen Hintergrund und wenn mir mein Mann seine KI's erklärt, denke ich mir, ja, was will er von mir eigentlich? Ich weiß schon ein bisschen mehr als jemand, der das normal macht oder so etwas. (…)“ (ID5, Z. 2744-2754)	Es ist schwer einzuschätzen, was Menschen verstehen und ob Menschen einwilligungsfähig sind. Noch schwerer wird es zu erklären, wie eine KI zum Beispiel funktioniert, weil das schon für einen technikaffinen Menschen schwer nachzuvollziehen ist.	Es ist schwer einzuschätzen wann Menschen einwilligungsfähig sind und das Ganze wird noch schwerer wenn erklärt werden muss wie eine KI funktioniert.	Verständnis Einwilligungs-erklärungen
ID5: „Und da sehe ich auch, es gibt Leute, die einfach Experten sind im Datenschutz, in den ganzen Technik Sachen. Warum nicht die einfach entscheiden lassen in diesem Bereich, dass wir hier vielleicht so einen Datenschutzrat haben? Ich kenne das eben so wie es den Ethikrat gibt bei Studien, gerade im Gesundheits- oder Sozialbereich, warum nicht auch im Datenschutz so eine Kommission ansetzen? Wo ich solche Dinge regelt? Ich würde das jetzt nicht schlecht finden, weil da haben wir halt Leute, die sich tagtäglich mit nichts anderem beschäftigen drinnen und nicht den Otto Normalverbraucher, der von den drei Lampen im Auto schon überfordert ist und dann soll er entscheiden, ob die KI seine Daten verarbeitet oder nicht.“ (ID5, Z. 2777-2786)	Eigentlich sollte vielleicht ein Datenschutzrat solche Entscheidungen treffen und nicht die Einzelnen, ob in Zukunft eine KI ihre Daten verarbeitet oder nicht.	Eigentlich sollte nicht von einzelnen Entschieden werden ob ihre Daten verarbeitet werden oder nicht, sondern eher ein Expert*innenpool wie zB. ein Datenschutzrat.	Verantwortung Union / Staat
ID5: „Ich bin zum Beispiel sehr gespannt, ob Geschäftsmodelle zusammenbrechen, immer wieder, wenn irgendwas	Wenn weiter Dinge verboten werden wie zum Beispiel schon mit der DSGVO, kann es sein, dass Geschäftsmodelle	Wenn Dinge wie durch die DSGVO stark eingeschränkt werden können Geschäftsmodelle	Nachteile/ Schwächen der DSGVO

Neues verboten wird oder dazukommen, auch ob neue Geschäftsmodelle kommen. (…)Und es ist teilweise wirklich unnötiger Mehraufwand, den keiner versteht und keinem was bringt. Weil wie gesagt vorher, die, die das wirklich kleinlich machen und sehr genau machen, reißen sich an Haxen aus und es bringt einem genau Nüsse als die, die es trotzdem machen.“ (ID5, Z. 2854-2856 und 2865-2868)	zusammenbrechen, da sich kleinere Unternehmen bemühen, alles korrekt zu machen.	zusammenbrechen, vor allem kleinere Unternehmen.	
ID5: „Nämlich eigentlich, also für mich ist die DSGVO und das sage ich jetzt als Datenschützer selber, nervig, arbeitsaufwendig und die, die wirklich betroffen sein sollten, was ändern sollen kalkulieren nur mit den Strafen und nicht mit der Umsetzung.“ (ID5, Z. 2898-2901)	Sogar für einen Datenschützer/eine Datenschützerin ist die DSGVO nur arbeitsaufwändig, da diejenigen, die etwas ändern sollten, nur mit Strafen kalkulieren.	Ich als Datenschützerin finde die DSGVO nervig, da diejenigen, die etwas ändern sollten, sie nicht ernst nehmen.	Nachteile/ Schwächen der DSGVO
ID5: „Aber was ich dabei, ich habe mitbekommen, es sollen ja wirklich auch die in den USA sitzenden Unternehmen und sowas. Nur da frage ich mich wieder, wie ist dieser Übergriff möglich, jetzt vom rein rechtlichen her, auf ein anderes Gesetz zuzugreifen, auf ein anderes, weil wir haben ja ein Territorialitätsprinzip in den einzelnen Gesetzen. Und jetzt umgekehrt keiner von uns würde wollen, dass die USA Gesetze beschließt, die uns Österreicher in Österreich einschränken. Also warum soll das umgekehrt gehen oder so? Das stelle ich mir halt auch dann immer sehr problematisch vor. Und was ich mir auch immer wieder die andere Schwierigkeit denke, ist die Grundfreiheiten dahinter. Weil wie stelle ich fest, was soll erlaubt sein oder nicht? Ich finde, das ist ja sowieso immer so eine Schwierigkeit bei jedem Gesetz. Und welche Plattformen, wie schränke ich die dann ein? Thema Meinungsfreiheit und so oder geht man komplett in ein Darknet über, wo dann schon zwei Schubladen.“ (ID5, Z. 2923-2934)	Was ich fragwürdig finde, ist, dass die EU einfach die USA und so beschränkt, das würden wir umgekehrt auch nicht so toll finden, und schwierig stelle ich mir die Vereinbarkeit der Grundfreiheiten, speziell die Meinungsfreiheit mit dem DSA vor.	Fragwürdig bleibt, ob der DSA aus der EU die USA stark einschränkt, und die Vereinbarkeit des DSA mit den Grundfreiheiten, speziell mit der Meinungsfreiheit, ist fraglich.	Einfluss des DSA auf Schutz personen-bezogener Daten
ID5: „Ja, da muss ich aber ganz ehrlich dann wieder an den Menschen denken, weil	Unternehmen nehmen die Verantwortung nicht so ernst, da jeder Mensch	Jeder Mensch nutzt die größten Vorteile für sich, das machen auch	Verantwortung Unternehmen

jeder von uns wird natürlich seine größten Vorteile nutzen wollen und nicht, wenn ich am meisten Geld verdienen kann mit etwas, was vielleicht, da gibt es ja diese tollen Studien mit entweder jemand bekommt 100 € oder ich bekomme nur 50 €, für was entscheiden sich die Menschen lieber? Und das glaube ich auch bei den Unternehmen, dass das leider öfters passieren wird. Also wie gesagt, Unternehmen, die sich jetzt ganz strikt an die DSGVO halten, sind eigentlich die Verlierer in der ganzen Geschichte als die, die nur damit kalkulieren mit den Strafen. Das habe ich halt die Panik. Aber das ist sowieso bei jedem Gesetz. (…)“ (ID5, Z. 2962-2970)	die größten Vorteile nutzt und am Ende des Tages sind Unternehmen, die sich strikt an die DSGVO halten, oft die Verlierer dabei.	Unternehmen und diejenigen die sich an die DSGVO halten sind leider oft die Verlierer.	
ID5: „Die größte Herausforderung ist, dass Gesetze, Leute schreiben sie von der Technik keine Ahnung ab. Muss man ehrlich so sagen. Und die größte Herausforderung ist auch die Gradwanderung, die wir jetzt auch ganze Zeit besprochen haben zwischen wie viel sollen die Menschen selber entscheiden und wieviel ist, wenn vorab entschieden wird von anderen Leuten. Das finde ich, sind für mich die beiden größten Herausforderungen. Das ist auch die große Herausforderung jetzt im KI Bereich, was immer weiterentwickelt wird. Kommen wir irgendwann in eine Welt, ist es schön, dass alles mitdenkend ist und immer moderner und besser wird, was ein Mensch nicht schafft, aber können uns die Roboter dann irgendwann überholen oder nicht? Und das finde ich, sind die Schwierigkeiten dahinter.“ (ID5, Z. 2980-2989)	Gesetze, die von Juristen ohne Technikerfahrung geschrieben werden, sind eine große Herausforderung. Es ist auch eine Gradwanderung dazwischen, wieviel Leute selbst entscheiden können, gerade wenn wir uns in Richtung KI bewegen, und wie viel von höheren Instanzen entschieden werden soll.	Die KI und Gesetze von Jurist*innen ohne Technikerfahrung und der Grad wieviel Leute selbst entscheiden können, ist eine Herausforderung.	Heraus-forderungen in Zukunft
ID5: „Weil sich sehr viel schneller was entwickelt und weil die KI etwas kann, was wir Menschen nicht können. Wir haben nämlich auch wenn immer alle Leute sagen, sie entscheiden rein auf Fakten basierend, glaub ich, wird man trotzdem keinen Menschen finden, der das nur aus	Eine Herausforderung wird sein, dass eine KI im Gegensatz zum Menschen nur basierend auf Fakten entscheidet, gleichzeitig aber von Menschen und ihrem Weltbild angelernt sind.	KI entscheidet basierend auf Fakten, ist aber von Menschen und dessen Weltbild angelernt.	Heraus-forderungen in der Zukunft

diesem Grund macht oder so. Und eine KI entscheidet aber rein auf Fakten basierend. Andererseits ist eine KI von uns angelernt im Endeffekt. Und das ist die nächste, es gibt ja mittlerweile Forschungen, warum eigentlich ur viele KIs rassistisch sind, weil wir im Hintergrund genauso rassistisch sind. (…) Also die KI ist, sind die neuen Tiere. Es ist kein Tier von Grund auf böse oder so, ein Hund oder so etwas, sondern immer der, der die Leine führt dahinter. Und dasselbe auch die KI ist. Ki ist ja nicht von Grund auf böse oder schlecht oder positiv, sondern der, der sie anlernt oder programmiert kann das dahinter machen. Und das ist unsere Herausforderung dahinter. Wir haben KI's, wir sind weit weg von einer starken KI, wobei meine Forscher sagen, es kann jeden Tag passieren oder auch noch hundert Jahre dauern, irgendwo dazwischen liegt die Wahrheit.“(ID5, Z. 2997-3003 und 3005-3012)			
ID6: „Dieses Jahr zum Beispiel mit KI in dieser Weise, dass es irgendwie jetzt eine Welle werden würde, war glaube ich schon klar. Aber welche Welle wie und was das bedeutet, deswegen KI Regulierung, das war für uns alle ein bisschen überraschend. Aber wie geht man damit jetzt um? Oder wie kann man vermeiden, dass man da und deswegen das Oberthema zu unfairer Datenverarbeitung oder unfairer Gesellschaft kommt, besser gesagt. Und wieder heruntergebrochen auf Verarbeitung ist das Hauptthema Risikobeherrschung, also nicht Risiken schaffen, die man nicht beherrschen kann, sondern immer gleich schon mitdenken, also Folgenabschätzung denken. Und da ist der Datenschutzbereich ein wichtiger, auch ein mächtiger Teil, aber nicht der einzige und deswegen gucken wir auch auf die anderen Punkte der Regulierung oder eben der	Es stellt sich die Frage: Wie geht man mit Dingen um, die so plötzlich auftreten wie dieses Jahr die KI zum Beispiel? Wie schafft man sich da einen Überblick über das Risiko? Dabei spielt der Datenschutzbereich eine große Rolle, aber nicht die einzige.	Datenschutz spielt im schnellen Auftreten von Dingen mit der Risikobewertung immer eine große Rolle, vorallem wenn etwas plötzlich eintritt wie die KI dieses Jahr.	Heraus-forderungen in Zukunft

Systemgestaltung im Bereich der Praxis.“ (ID6, Z. 3092-3103, durchgeführt am 18.07.2023)			
ID6: „Da steht nichts über Prozessorlast oder Hitzegenerierung oder so, sondern Datenschutz auf eine Art und Weise, dass sie beständig ist, dass man also ständig hat eben Risikobeherrschung gesagt, das Risiko im Griff hat, auch dauerhaft das Ganze anlegt. Es gibt einen verwandten Begriff, den ich jetzt mitnehmen würde, die souveräne Datenschutz oder souveräne Sicherheit, abgeleitet aus der digitalen Souveränität. Und wir haben vor kurzem als Datenschutzkonferenz dazu was definiert und wenn Sie möchten, kann ich Ihnen noch ein paar neue Texte schicken. Also wir haben es definiert, auch mit drei Worten, die aber nicht aus unserem Kopf kommen, sondern aus dem Gesetz effektiv, überprüfbar und dauerhaft. Und für Datenschutz eben genau Schutz der personenbezogenen Daten in Bezug auf die Rechte und Freiheiten für die Menschen, also nicht die Daten an sich, sondern im Gesamtbereich Grundrechte. Aber effektiv, es muss wirken, sonst nicht. Und die Nebenwirkungen müssen wir im Blick haben.“ (ID6, Z.3114-3126)	Wir definieren nachhaltigen Datenschutz mit effektiv, dauerhaft und überprüfbar, was bedeutet, dass man das Risiko und die Nebenwirkungen dauerhaft im Griff hat, ohne den Gesamtbereich der Grundrechte einzuschränken.	Nachhaltiger Datenschutz ist wenn er effektiv, dauerhaft und überprüfbar passiert und das Risiko unter Kontrolle hat ohne Grundrechte einzuschränken.	Nachhaltiger Datenschutz
ID6: „Wie kriegen wir die Gesamtidee auch so hin, dass Datenschutz und die anderen Grundrechte gleichermaßen nachhaltig gewahrt sind? Sonst befürchte ich nämlich, dass vielleicht auch eine gute Lösung, die nicht den Weitblick hat, entweder gar nicht Bestand haben kann, was anderes kaputt macht, was beschränkt und vielleicht auch gerichtlich gar nicht mehr bestehen darf. Also nachhaltig heißt auch, die Folgen von solchen Lösungsvorschlägen mit zu bedenken. Und jetzt mal ein Beispiel, was vielleicht eher in Ihre Richtung auch geht.“ (ID6, Z. 3151-3157)	Nachhaltiger Datenschutz bedeutet, auch die Folgen von Lösungen mitzudenken und darauf zu achten, dass sie nicht andere Grundrechte einschränken.	Nachhaltiger Datenschutz bedeutet auch die Folgen von Lösungen einzuschätzen und im Gesamtkontext zu sehen.	Nachhaltiger Datenschutz

ID6: „Wir haben zum Beispiel die Möglichkeit für den Verantwortlichen, dass er die Daten anonymisiert oder pseudonymisiert und für sich dann hält und jetzt in Daten teilen, Paradigma, diese Daten vielleicht von ihm ja weitergegeben werden müssen. Er könnte es auf eine Art machen, dass er selbst mit den Daten ganz viel anfangen kann und alle anderen nichts mehr. Und damit hätte er aus Datenschutz Sicht auch sogar eine gute Lösung. Und wir könnten das sogar, ja vielleicht gibt es sogar Datenschutz Siegel, also Nachweis, dass das DSGVO auch verständlich erfüllt ist. Es hätte aber massive Auswirkungen auf den Markt.“ (ID6, Z. 3159-3166)	Unternehmen haben die Möglichkeit, Daten zu anonymisieren, sie könnten das auf eine Art machen, dass sie damit viel anfangen können und andere nichts. Das hätte große Auswirkungen auf den Markt.	Unternehmen hätten mit der Anonymisierung viel mit Daten anfangen können und andere nichts mehr, was aber Auswirkungen auf den Markt hätte.	Verantwortung Unternehmen
ID6: „Jeder, der die Daten verarbeitet, das sind Organisationen, die Personen, persönliche, so was ich mache, mein kleines Tagebuch oder Adressbuch, da habe ich natürlich auch als Privatperson meine Verantwortung, aber nicht nach dem Datenschutzrecht, weil ich das nur für mich tue. Aber da wünsche ich mir auch, dass viele verantwortungsvoll mit dem umgehen, was sie da tun. Aber eine rechtliche Verpflichtung haben sie ein Stück weit weniger. Die einzelnen, wie viel kann man auf die Last der Einzelnen packen? Also Eltern haben die Verantwortung für ihre Kinder und so, aber man darf es nicht abwälzen. Und soweit muss auch jeder selbst ein bisschen gucken.“ (ID6, Z. 3190-3195)	Alle, die Daten verarbeiten, haben eine Verantwortung, das sind auch Private, dennoch haben sie weniger rechtliche Verpflichtungen, und viel Last kann man nicht auf die Einzelnen abwälzen.	Alle, auch Privatpersonen, die Datenverarbeiten haben eine Verantwortung, aber weniger rechtliche Pflichten und viel Verantwortung kann man nicht bei den Einzelnen einordnen.	Verantwortung Betroffene/ Konsument*innen
ID6: „Außerdem haben wir aber Infrastrukturen und das ist etwas, was oft vergessen wird, darf man sich eben nicht blind machen, auch als Staat. Man hat, der Staat hat Infrastruktur Verantwortung und davon hängt eine Menge ab. Sagen wir mal, einige betrachten bestimmte Social Media als Infrastruktur und sagen Ich muss da unbedingt überall jetzt Accounts haben, auch als Behörde und weiß aber alles ist nicht rechtskonform. Also da,	Als Staat hat man auch eine Infrastruktur-verantwortung und muss darauf achten, dass diese Infrastrukturen wie Social Media weiter bestehen und gleichzeitig den Weitblick haben, was diese für Auswirkungen haben.	Der Staat hat eine Infrastruktur-verantwortung wie zb. social Media und muss darauf achten, dass diese rechtskonform bestehen bleiben ohne den Weitblick zu verlieren.	Verantwortung Union / Staat

obwohl ich ermutige sozusagen die Kommunikation über diese Infrastrukturen. Es gibt aber nicht die Garantien über Telefonie, Telekommunikationsgeheimnis oder Strafe gestellt, wenn da eine Telekom oder so was ausplaudern würde. Das haben wir ja nicht vergleichbar bei Social Media, sondern eher im Gegenteil schon ziemlich klar, dass da Verstöße bei mindestens großen Firmen stattfinden. Und deswegen, Infrastrukturverantwortung beim Staat. Aber der Blick, der Weitblick, der wird vom Staat gefordert.“(ID6, 3197-3211)			
ID6: „Ein großer Vorteil ist, dass es eigentlich was ist, und jetzt habe ich schon eigentlich gesagt, eine Sache ist, die für alle Mitgliedsstaaten gleichermaßen gilt (…).Das gilt für alle und es gilt auch für diejenigen, deswegen ist noch eine Export oder noch eine weitere Bindungswirkung für alle, die entweder auf den Markt in Europa nutzen, mit Daten die personenbezogen sind oder auch diese Daten beobachten. Also der Geltungsbereich, auch wenn man gar nicht in der EU eine Niederlassung hat, erstreckt sich darauf. Das ist also riesig, was damit erreicht wurde, wie viel man an vereinheitlichter Denke hat und natürlich auch nachher den Instanzen Weg bis zum EuGH, also eine Instanz, die das nach meiner Beobachtung auch weise oder einfach so wie es da steht, entscheidet.“ (ID6, Z. 3221-3222 und 3227-3235)	Dieer gleichen Bedingungen in allen Mitgliedsstaaten ist ein großer Vorteil und der Geltungsbereich für diejenigen, die keine Niederlassung in der EU haben. Diese Vereinheitlichung ist ein Riesenerfolg.	Die Vereinheitlichung in allen Mitgliedsstaaten und die Gültigkeit auch außerhalb der EU ist ein großer Erfolg.	Vorteile/ Stärken DSGVO
ID6: „Um gleich schon zu sagen, ja, jetzt gibt es natürlich Öffnungsklauseln, es wird eben doch unterschiedlich gelebt. Das heißt, ganz ist diese Einigkeit nicht erreicht worden. Das muss einem jetzt nicht missmutig stimmen. Es ist wahrscheinlich gar nicht anders möglich gewesen. Und ich glaube allein durch die weitere Annäherung auch durch den Europäischen Datenschutz Ausschuss gibt	Die komplette Harmonisierung wurde mit den Öffnungsklauseln nicht erreicht, aber vielleicht war dies das Einzige, was möglich war.	Die komplette Harmonisierung konnte mit den Öffnungsklauseln nicht erreicht werden.	Harmonisierungs-erfolg der DSGVO

es eine ganze Menge, wo man erst mal versteht, warum vielleicht unterschiedliche Mitgliedsstaaten kulturell das unterschiedlich auslegen und so, dass es also nicht jetzt zu schlecht ist, dass es Öffnungspausen gibt, sondern wahrscheinlich war das jetzt das Einzige, was ging.“ (ID6, Z. 3236-3244)			
ID6: „Was aber auch sehr schwierig ist, ist, dass es doch abstrakt ist. Also was für den EuGH vielleicht ganz offensichtlich ist, ist jetzt für denjenigen vor Ort gar nicht so klar, was das alles soll. Der allerdings in dieser Denke so ein bisschen drin ist, der wird wahrscheinlich doch immer zu Lösungen kommen. Das ist auch das, was wir hier in der Erfahrung haben. Wir haben am Anfang 2018, als die Geltung losging, vor allen Dingen Schulungen gemacht für Unternehmen. Wie kommt man von dem alten BDSG jetzt zu der neuen Welt und was sind zehn Punkte, die man schnell mal macht und dann merkt man schon, man hat ja schon eigentlich alles. Diese Annahme war leider falsch, weil nämlich gar nicht die vorherige Datenschutz, das Bewusstsein noch gar nicht da war, überhaupt von den alten Startpunkten in die neue Welt zu kommen.“ (ID6, Z. 3244-3254)	Die abstrakten Formulierungen in der DSGVO sind schwierig, da sie viel Interpretations-spielraum lassen. Auch bei Schulungen in Unternehmen ist zu Beginn der Einführung aufgefallen, dass Unternehmen dachten, schon alles korrekt zu machen, was offensichtlich falsch war.	Sowohl die abstrakten Formulierungen, als auch die anfängliche Umsetzung in den Unternehmen, hat sich als schwierig erwiesen.	Nachteile/ Schwächen der DSGVO
ID6: „Also maschinenlesbare Policies sind da im Prinzip angelegt, die gibt es in der Realität leider so gut wie gar nicht. Die würden eine ganze Menge lösen, die müssen auch standardisiert werden. Und dann sehe ich die Kommission noch am Zug. Also wir haben eine Sache, die noch gar nicht so viel Fleisch auf den Knochen hat, wie sie haben sollte. Ich bin ein ungeduldiger Mensch, wie sie eigentlich haben müsste. Die Zertifizierung nach fünf Jahren immer noch kein einziges Zertifikat und so. (…) (ID6, Z. 3267-3274)	Es gibt in der DSGVO noch einige Dinge, die noch nicht so stark ausformuliert wurden, wie zum Beispiel eine Zertifizierung für datenschutzkonformes Arbeiten.	Einige Dinge wurden noch nicht ausformuliert in der DSGVO wie zum Beispiel eine Zertifizierung.	Nachteile/ Schwächen der DSGVO
ID6: „Aber es ist ein Fundament drin und das ist sicher, wenn man sie jetzt, bin ich hin und her gesprungen zwischen gut und nicht so gut,	Trotzdem hat die DSGVO ein Fundament geschaffen, das auch für die Zukunft gut ist und für neue Techniken und	Die DSGVO ist ein Fundament, das auch gegen zukünftige Innovationen wie	Vorteile/ Stärken der DSGVO

die dann auch mit den Problemen, die jetzt wegen KI oder so neu kommen, mit neuen Techniken, die im Prinzip die Lösung bieten und die diesen Diskurs, die Wichtigkeit des Diskurses deutlich machen und auch vor allem glaube ich jetzt gelernt haben, das Ding geht nicht weg. Also man kann es nicht einfach so ignorieren, sondern man muss jetzt damit leben.“ (ID6, Z. 3275-3280)	Innovationen wie KI gewappnet ist.	künstliche Intelligenz gewappnet ist.	
ID6: „Vielleicht ein Punkt, der mich persönlich sehr ärgert, ist, dass die Großen, mächtigen Giganten die DSGVO persiflieren oder sabotiert haben, während die kleinen mittelständischen Unternehmen aus großer Angst vor den Aufsichtsbehörden vielleicht ganz genau ganz viel gemacht haben und sich zu bestimmten Innovationen gar nicht mehr getraut haben. Nicht weil sie, die wären vielleicht auch alle gegangen, aber sozusagen auf Nummer sicher zu sein. Das wäre natürlich eine Fehlentwicklung. Und es darf nicht sein, dass diejenigen auch im Markt benachteiligt sind, die sich an die Regeln halten, wie jetzt die ChatGPT oder was anderes, Marktanteile durch unreifere Produkte erobern.“ (ID6, Z. 3282-3290)	Eine Schwäche der DSGVO ist der mangelnde Unterschied zwischen großen und kleinen Unternehmen, sodass große sie sabotieren und Grauzonen suchen, und kleinere aus Angst vor Strafen sich nicht mehr trauen, Innovationen einzuführen, , was eine Fehlentwicklung ist.	Eine Schwäche der DSGVO ist die Fehlentwicklung, dass große Unternehmen sie sabotieren und kleine sich nicht an Innovationen herantrauen aus Angst vor Sanktionen.	Nachteile/ Schwächen der DSGVO
ID6: „Die ist noch unterentwickelt. Also bedeutet, man weiß noch nicht genau, was es alles bedeutet. Das war schon sehr umfangreich, wobei eine Aufsichtsbehörde gerichtliche Bescheide oder gerichtliche Verfahren und Aufsichtsbehördliche Bescheide nur dann erlassen kann, wenn eine ausreichende Klarheit besteht. Und hier ist jetzt der Vorwurf an Artikel 25, der ist so abstrakt. Der ist zwar supertoll, weil er sagt implementier doch einfach, was da schon an anderer Stelle steht, die Datenschutzgrundsätze. Aber auch wieder wie soll es genau gehen? Jede Annäherung muss man weiter schauen. Und wir haben einige konzeptionelle	Die Privacy by Design-Regelung ist noch unterentwickelt, und Bescheide können nur erlassen werden,wenn genug Klarheit besteht,. Denn viele Dinge, wie zum Beispiel eine Methode, wie Privacy by-Design gemacht werden soll, gibt es noch nicht.	Die Privacy by Design-Regelung ist noch unterentwickelt und es fehlt Klarheit wie zum Beispiel eine Methode zur Privacy by Design.	Privacy by Design

Schwierigkeiten, auch weil zum Beispiel eine Methode für Datenschutz bei Design und bei Default ist übrigens eine sehr starke Regel, die nicht oft so erfüllt wird, leider. Also Artikel 25 Absatz 2 ist eher, da läuft oft leer.“ (ID6, Z. 3306-3307 und 3313-3321)			
ID6: „Aber ich sehe, dass viele nicht wissen, was Best Practices sind, wie geht es wirklich? Woran kann man sich orientieren, damit es okay ist? Oder wie kann man Incentives dafür bringen, dass auch Innovationen noch leichter sind, dass man nicht denkt, ich habe jetzt Angst vom vom Bußen Geld und wie geht das vielleicht aber auch, dass bei den Großen das Enforcement schneller geht, weil die mit einem großen Juristenstab vielleicht alle Instanzen ausloten. (…)Das bedeutet nur, die kleinen würden vielleicht nicht kämpfen und wenn sie gar nichts machen, werden die Großen das aushalten und sagen nach zehn Jahren, Okay die eine Fanpage, die ist jetzt weg, aber wir haben alles geändert seitdem. Also diese Problematik, dasist aber Enforcement, was vielleicht durch irgendwelche Fast Tracks und eben noch stärkere Klarheits- oder Untersagungsmöglichkeiten auf dieser Basis besteht.“ (ID6, Z. 3371-3376 und 3384-3389)	Ein Problem der DSGVO ist, dass viele nicht wissen, was Best Practice Beispiele sind. Man müsste eigentlich mehr Anreize schaffen und die Angst vor Innovationen und Bußgeldern nehmen, und da müssten stärkere Klarheits- und Untersagungs-möglichkeiten her.	Viele wissen nicht, was Best Practice beim Datenschutz ist und das führt dazu, dass die Angst vor Innovationen und Bußgeldern groß ist und mehr Klarheit und Untersagungsarten kommen müssen.	Nachteile/ Schwächen der DSGVO
ID6: „Ich glaube, wir werden in eine Phase kommen, wo das scheinen wir jetzt in der ganzen Welt so zu sein, wo es immer nur noch es wird ausprobieren, es wird gemacht, also auch disruptiv. Man ist stolz darauf, dass man so die Dinge ein bisschen scheitern ist gut und so. Und wenn das mit Daten passiert, dann mit diesem mentalen Modell, dann kann es sein, dass Leute Identitätsdiebstahl erleiden, dass sie Leib und Leben Probleme haben und so. Im Bereich Sicherheit kann ich mir vorstellen oder jetzt auch Daten teilen, wenn da zu viel an Personenbezug herausgeht, dass wenn da	Wir werden in eine disruptiv geprägte Phase kommen, in der das Scheitern etwas Gutes ist. Wenn das aber mit Daten passiert, können Personen einen Identitätsdiebstahl erleiden und es geht in die Richtung Privacy by Desaster.	Wir kommen in eine disruptive Phase, des Probierens und Scheiterns und wenn das mit Daten passiert, dann kann Identitätsdiebstahl passieren und es geht in Richtung Privacy by Desaster.	Heraus-forderungen in der Zukunft

irgendwie falsche Entscheidungen sind, dann wird man lernen im Sinne von Privacy by Desaster.“ (ID6, Z. 3470-3478)			
ID6: „Jetzt geht es noch schlimmer los, weil die Bilder auch nicht mehr authentisch sein müssen. Und die Wirkung, das ist vielleicht jetzt bei KI, dass ist das Größte für mich, die Wirkung wird eintreten, selbst wenn man mental weiß, das ist ja gar nicht echt. Das sind nicht so die nur Datenschutz Themen. Aber das ist eben auch dieser Punkt. Wir können nicht mehr nur Datenschutz denken, das Gesamtbild, das wegen ihrer Arbeit super. Das ist... Um das Gesamtproblem in den Blick zu nehmen, man muss diese Interdependenzen mit einplanen und deswegen die Herausforderung ist, in dieser komplexen Welt schnell, jetzt mache ich noch einen Satz daraus, schnell genug zu agieren und zu reagieren und vorauszuschauen, dass die Probleme noch nicht so schlimm geworden sind.“ (ID6, Z. 3498-3508)	Eine Herausforderung wird einerseits die KI und der Unterschied zwischen real und falsch sein und andererseits die Herausforderung, auf eine immer komplexer und schneller werdende Welt reagieren zu können.	KI und die Wahrnehmung von real und falsch als auch die Reaktion auf eine immer komplexere und schnellere Welt werden eine Herausforderung.	Heraus-forderungen in Zukunft
ID6: „Und dann merkt man schon, dass unter dem Begriff personenbezogen was ganz anderes verstanden wurde, also schon die Grundlage, die Grundentscheidungen anders war. Oder dass eben was wie Netzwerkeffekte natürlich oder Login Effekte im Datenschutz auch eine riesen Rolle spielen, auch wenn das mit Portabilität nur so ein bisschen ungenügend adressiert ist. Aber dass das auch alles Auswirkungen haben wird.(…)“ (ID6, Z. 3523-3528)	Manche Auswirkungen waren nicht absehbar, personenbezogene Daten wurden, als die Grundentscheidungen getroffen wurden, anders verstanden und Login- und Netzwerkeffekte sind ungenügend definiert, da deren Rolle nicht absehbar war.	Personendaten wurden zur Zeit der Grundentscheidungen anders verstanden, und die Rolle von Login- und Netzwerkeffekten war nicht absehbar und ist unzureichend definiert.	Nachteile/ Schwächen der DSGVO
ID7: „(…) also ich sage es jetzt aus der Unternehmens Perspektive, wenn man eigentlich bei den Menschen, die mit Daten arbeiten, das wirklich verinnerlicht haben. Das heißt, die, das, wie soll ich sagen, unterbewusst mit leben und das in die Prozesse und Arbeitsabläufe einwirken kann. Und ich glaube, dass man das sehr stark dadurch sicherstellen kann, wenn ein Unternehmen das Thema Datenschutz in der DNA hat	Das Bewusstsein zum Thema Datenschutz in Unternehmen muss in jedem Prozess und Arbeitsablauf gelebt werden und am Ende des Tages Teil der Unternehmensstrategie sein.	Datenschutz muss Teil der Unternehmens-strategie sein und in allen Prozessen und Abläufen gelebt werden.	Nachhaltiger Datenschutz

oder als Teil der Strategie, also wenn das irgendwie so ein bisschen in die Unternehmensstrategie einfließt und die Leute können sich mit der Strategie identifizieren, dann geht es halt auch in die Köpfe der Menschen ein. Jeden Tag mit den Daten arbeiten, nämlich im Rahmen von Prozessen oder Arbeitsabläufen. Also wenn man es schafft, das in die DNA des Unternehmens zu bekommen und Mitarbeiter zu haben, die sich mit dem Unternehmen identifizieren können, dann glaube ich, kann man es schaffen. Oder dann kann man, glaube ich, von nachhaltigem Datenschutz sprechen, wenn das wirklich immer mitgelebt wird.“(ID7, Z. 3662-3674, durchgeführt am 07.08.2023)			
ID7: „Also ich glaube, dass durch die DSGVO, die hatte irgendwie dieses Prinzip ins Leben gerufen, dass die Unternehmen sehr viel selbst machen müssen und sich sehr viel selbst Sachen kümmern müssen und sich selbst überlegen müssen, ist das noch okay oder ist es nicht mehr okay? Also dieser Austausch und diese Kontaktmöglichkeit mit der Datenschutzbehörde, also eigentlich mit dem Regulator, mehr oder weniger, ist in der Form jetzt nicht mehr möglich. Also ich glaube, dass die DSGVO sehr stark diese Verantwortung an die Unternehmen abgegeben hat (…) (ID7, Z. 3698-3704)	Unternehmen müssen durch die DSGVO sich viel selbst überlegen und sich darum kümmern, ob ihre Prozesse ok sind, und der Staat hat somit die Verantwortung den Unternehmen übergeben.	Unternehmen wurde durch die DSGVO die Verantwortung übergeben und müssen sich überlegen, ob ihre Prozesse ok sind oder nicht.	Verantwortung Unternehmen
ID7: „(…)und dann eigentlich nur überwacht und überprüft und schaut, passt es oder passt es nicht? Und dann punktuell gibt es dann Rechtsprechungen und da kommt dann, wenn man so will, der Staat irgendwie seine Verantwortung vielleicht auch dann wieder wahr.(…)“ (ID7, Z. 3704-3707)	Die Rolle liegt hier in der Überwachung, Überprüfung und in der Rechtssprechung.	Überprüfung, Überwachung und Rechtsprechung liegt in ihrer Verantwortung.	Verantwortung Unternehmen
ID7: „(…) Und Unternehmen können sich wieder an einer Aussage oder einer Entscheidung orientieren. Aber im Grunde glaube ich, obliegt es den Unternehmen, also den Verantwortlichen, die	Die Hauptverantwortung liegt bei den Unternehmen, welche die Pflichten erfüllen müssen und ihre Verantwortung wahrnehmen müssen. Das Gute daran ist, dass	Die Haupt-verantwortung liegt bei Unternehmen.	Verantwortung Unternehmen

halt die Pflichten erfüllen müssen, diese Verantwortung auch wahrzunehmen. Was ja auch irgendwie ein bisschen einen Vorteil vielleicht hat, weil Unternehmen können halt interpretieren, haben vielleicht Spielräume, weil jetzt nicht alles so stark vorgegeben ist. Das heißt, sie müssen jetzt nicht, wenn sie eine Datenverarbeitung beabsichtigen, stets die Datenschutzbehörde vorher konsultieren und fragen, darf ich das? So wie das früher mit dem Datenverarbeitungsregister zum Beispiel der Fall war, sondern man kann da sehr viel machen und muss halt nur aufpassen, dass wenn es zu einer Überprüfung oder zu einem Verfahren kommt, dass das halt, wie soll ich sagen, hinreichend rechtskonform ist.“ (ID7, Z. 3707-3718)	es Spielräume gibt, rechtskonform zu arbeiten.		
ID7: „ Und der Konsument, ja ich meine was kann der Konsument machen? Der kann halt durch sein Verhalten kann der halt steuern. Also der kann halt sagen, ja, ich beanspruche dieses Service oder diese Dienstleistung nicht und beeinflusse sozusagen dadurch ein bisschen die Praxis oder das, wie der Datenschutz gelebt wird, wie die Unternehmen ihrer Verantwortung nachkommen, ob sie die Bestimmungen erfüllen oder einhalten. Aber da ist halt natürlich, das ist halt theoretisch. In der Praxis will dann niemand auf Facebook verzichten oder vielleicht niemand auf irgendwelche Microsoft Services verzichten. Also theoretisch wäre das schon möglich. In der Praxis, glaube ich, hat sich das jetzt bei mir, hat sich noch nicht wirklich gezeigt, dass das Verhalten vom Endkonsumenten da so stark wirkt.“ (ID7, Z. 3719-3729)	Konsument*innen können durch ihr Verhalten den Umgang mit ihren Daten steuern, indem sie Services und Dienstleistungen nutzen oder nicht, aber in der Praxis werden sie nicht auf diese Dienste von Meta oder Alphabet verzichten wollen.	Konsument*innen können steuern, ob sie gewisse Dienste und Services nutzen oder nicht aber das ist in der Praxis unwahrscheinlich.	Verantwortung Betroffene/ Konsument*innen
ID7: „Das heißt, ich kann jetzt als Unternehmen sagen, ich möchte jetzt... Ich verwende jetzt keine, wie soll ich sagen, keine Microsoft Cloud, weil das ist mir zu unsicher. Und ich bin dann eine Vielzahl Unternehmen abspringen,	Als Unternehmen gewisse Dienste und Services nicht zu nutzen, würde mehr awareness schaffen, aber das hat sich leider in der Praxis noch nicht so durchgesetzt.	Unternehmen könnten awareness schaffen, indem sie gewisse Dienste und Services nicht verwenden, dies hat sich aber noch nicht durchgesetzt.	Verantwortung Unternehmen

dass man dadurch dann dieses Verhalten von Microsoft, das ist jetzt nur ein Beispiel, beeinflusst und zu einem größeren Datenschutz awareness bringt. Aber ich glaube nicht, dass sich das in der Praxis schon jetzt nicht so stark durchgesetzt hat. Ein bisschen vielleicht, aber...“(ID7, Z. 3733-3738)			
ID7: „Ich meine, die Stärke ist schon, man muss schon sagen, das hat sich schon als Standard durchgesetzt weltweit. Also wenn sich Länder oder Kontinente anschauen, wie sie das Thema Datenschutz regulieren, dann schauen sie sich zuerst ganz stark auch mal die DSGVO an. Ich meine da kann man dann immer lernen und man muss nicht alles genauso umsetzen. Aber das ist auf jeden Fall schon ein weltweiter Standard, den man da gesetzt hat. (…)Aber im Großen und Ganzen ist es schon was, ist es schon was tolles gelungen. Und jetzt als Unternehmen, das in Europa ansässig ist und ich sage jetzt mal vor allem Daten in Europa verarbeitet, macht es das Leben halt auch leichter, weil man hat ja ein einheitliches Gesetz oder einen einheitlichen Standard im europäischen Raum. Eigentlich auch internationale Unternehmen müssen sich ja unter bestimmten Umständen halt an die DSGVO halten. Das macht schon einfacher. Man spricht dann halt oder man ja, es gibt da Datenschutzvorgaben und alle wissen Bescheid, weil es halt ein Set an Regelung ist. Ja, die Vorteile für ein Unternehmen, das ist natürlich, habe ich eh schon angesprochen, ja, Interpretationsmöglichkeiten. Ist halt auch, ist alles ein bisschen schwierig, aber ist ja auch ein bisschen dadurch bedingt, dass man natürlich in der DSGVO jetzt nicht so ganz so stark ins Detail geht oder ich glaube auch nicht gehen wollte, weil die DSGVO soll natürlich auch noch in fünf oder zehn Jahren als Gesetz	Die Stärke der DSGVO liegt darin, dass sie sich als Standard im europäischen Raum durchgesetzt hat, dass sich andere Länder an der DSGVO orientieren und, dass sie für alle gilt, die mit Daten von EU-Bürger*innen arbeiten. Vorteile für Unternehmen liegen in den Interpretations-möglichkeiten und, dass diese das Gesetz auch in ferner Zukunft noch anwendbar machen.	Die DSGVO hat sich als Standard im europäischen Raum und als Vorbild durchgesetzt und gilt für alle, die mit EU-Bürger*innen Daten arbeiten und ist so weit interpretierbar, dass dies einen Spielraum für Unternehmen bietet und auch in Zukunft anwendbar bleibt.	Vorteile/ Stärken der DSGVO

anwendbar bleiben. Also es soll jetzt nichts sein, wo dann durch Technologieentwicklungen das in zwei Jahren eigentlich obsolet ist oder die Regelungen keinen Sinn mehr machen.“ (ID7, Z. 3759-3765 und 3770-3785)			
ID7: „(…)Also es gibt Punkte, die sich halt dann in der Praxis, wo sich in der Praxis gezeigt hat, das ist für ein Unternehmen eigentlich schwierig oder vielleicht nicht machbar. Also ich denke da vor allem an diese Auskunftsrechte und Informationspflichten, an wen übermittel ich alles, an wen übermittel ich Daten (…)“ (ID7, Z. 3766-3770)	Es gibt Sachen, die für Unternehmen in der Praxis nur schwer machbar sind, wie zum Beispiel das Auskunftsrecht oder Informationspflichten.	In der Praxis sind das Auskunftsrecht und die Informations-pflichten für Unternehmen nur schwer machbar.	Nachteile/ Schwächen DSGVO
ID7: „Ja, also das, was halt jetzt immer stark erwartet wird oder was halt dadurch, dass die DSGVO noch jung ist und noch nicht so viel Rechtsprechung zu den einzelnen Themen da ist, werden halt eben auch diese EuGH Entscheidungen dann sehr erwartet, weil jeder halt hofft, dass da ein bisschen eine Sicherheit dann auch gebracht wird. Wie ist das zu interpretieren eigentlich die Bestimmung? Und da ein bisschen mehr Rechtssicherheit zu haben. (…)“ (ID7, Z. 3794-3799)	Die DSGVO ist noch sehr jung, und es wird immer auf neue Rechtssprechungen seitens des EUGH gehofft, um Interpretationen zu klären.	Da die DSGVO noch jung ist, gibt es noch nicht viele Rechts-sprechungen, die Interpretationen klären.	Nachteile/ Schwächen DSGVO
ID7: (…) Also da gab es am Anfang viele Unsicherheiten, die sich halt nach und nach auflösen mit der Rechtsprechung. Vielleicht setzt sich irgendeine Linie in der Praxis durch, aber die DSGVO wird einfach immer auch interpretationsfähig bleiben und soll halt auch so bleiben, weil die Technik entwickelt sich weiter oder die Anwendungsfälle entwickeln sich, aber das Gesetz soll halt auf dem Angebot bleiben oder so stehen. (ID7. Z. 3805-3810)	Die DSGVO wird immer interpretationsfähig sein, das wird die Rechtssprechung nicht auflösen und das macht sie auch zukunftstauglich.	Die Interpretations-fähigkeit der DSGVO macht sie auch zukunftstauglich.	Vorteile/ Stärken der DSGVO
ID7: Ich meine in der EU, wenn man zum Datenschutz spricht, spricht man halt dann von der DSGVO. Also es ist ein Regelungset, das für alle halt einmal, also es ist die gleiche Grundlage da. Das ist	Wenn man in der EU von Datenschutz spricht, dann spricht man von der DSGVO, auch wenn viele Dinge erst interpretiert werden müssen. Es ist auch nicht unbedingt	Das Gute ist, wenn man von Datenschutz spricht, dann ist es die DSGVO, trotz all ihrer Interpretationen und auch guter Spielräume	Vorteile/ Stärken der DSGVO

schon mal, glaube ich, ein ganz wichtiger Schritt. Jetzt natürlich muss sich irgendwie noch nach und nach, muss sich halt dann auch die Interpretation von den Bestimmungen vielleicht noch angleichen. Aber ich glaube, das ist ein Prozess, den kann man auch gar nicht beschleunigen. (…)Und natürlich jetzt gibt es halt auch noch Spielräume im nationalen Bereich, die wird man halt auch nicht ganz wegbekommen können oder wollen. Weil natürlich in jedem Land gibt es auch bestimmte Eigenheiten. Also ich glaube, es ist vielleicht gar nicht anstrebenswert, dass man diese Spielräume ganz beseitigt. Aber ich glaube, das ist halt, also man hat ja die Grundstände gesetzt für einen Harmonisierungsprozess und das dauert halt einfach, bis sich das halt nach und nach auch in der Anwendung einfach eingreift (ID7, Z. 3816-3821 und 3323-3229)	anstrebenswert, alle Spielräume zu entfernen, es ist ein Harmonisierungsprozess, und der dauert.	ist sie ein guter Standard.	
ID7: „Ich meine, was ist gut, wenn es halt, wenn es bestimmte kritische, also nach Sicht von der DSGVO kritische Datenverarbeitung gibt, ist halt einmal sichergestellt, dass man sich systematisch damit auseinandersetzt. Wenn man das halt nicht macht, dann kann es halt manchmal sein, dass man was vergisst, dass man was vielleicht nicht aus allen Perspektiven beleuchtet oder irgendwie, was sich jetzt unbewusst auch ein bisschen kleinredet und das als nicht so wichtig erachtet. Also Datenschutz-Folgenabschätzung, das hilft einmal, sich systematisch mit einem Thema auseinanderzusetzen, also mit einer kritischen Datenverarbeitung. Ja, ich meine, es ist natürlich eine weitere Bestimmung, die natürlich den Arbeitsaufwand erhöht (…)Aber im Großen und Ganzen finde ich es schon eine gute Sache, weil ich jetzt auch aus Erfahrung schon kenne, dass wenn man sich halt strukturiert, dass man sich mit einer	Die DSFA ist eine gute Sache, um einmal einen kritischen Blick auf Datenverarbeitung zu werfen und aus allen Perspektiven zu beleuchten, was vielleicht übersehen wurde. Sie beinhaltet dennoch einen erhöhten Arbeitsaufwand.	Die DSFA ist trotz des großen Aufwands eine gute Sache, um Datenverarbeitungsprozesse systematisch aus allen Blickwinkeln zu prüfen.	Datenschutz-folgen-Abschätzung

Datenverarbeitung auseinandersetzen muss, dass das sicherstellt, dass man alle Aspekte irgendwie berücksichtigt hat. Also grundsätzlich sehe ich es als gute Sache.“ (ID7, Z. 3837-3846 und 3849-3853)			
ID7: „Das ist halt das Thema, die Verantwortung liegt beim Unternehmen. Ja, da kann man jetzt wirklich philosophieren. Es ordnet sich, es ist zumindest im Einklang mit der grundsätzlichen Systematik, dass die Verantwortung bei den Unternehmen liegt. Wir haben auch schon viel diskutiert. Das ist natürlich auch ein Ressourcenthema, weil man gibt halt die Verantwortung ab und auch den zeitlichen Aufwand an die Unternehmen bringt das halt weg von Behörden oder Aufsichtsorganen.“ (ID7, Z. 3864-3870)	Die Verantwortung liegt beim Unternehmen, und das muss im Einklang mit der Systematik sein. Das Problem ist, dass die DSFA abhängig von Ressourcen und Zeit ist.	Die Verantwortung liegt bei den Unternehmen das zu machen und nicht bei Aufsichtsbehörden und ist außerdem ressourcen-abhängig.	Datenschutz-folgen-abschätzung
ID7: „Ich meine auch wenn man im Rahmen bleibt, kann man unterschiedlich, kann man Sachen unterschiedlich interpretieren. Also man muss nicht immer den vorsichtigen Weg gehen, aber man kann ja trotzdem im Rahmen bleiben. Ja, ich sehe, ich sehe, also ich stimme schon zu. Problematisch ist es natürlich, wenn ich mich selber eigentlich überwache. Und man könnte natürlich sagen, ja, bei allen Themen, die halt eine Datenschutzfolgenabschätzung bedürfen, also dort, wo es kritisch wird, wäre es sinnvoll, wenn irgendwie eine externe Stelle eingebunden wäre oder eine staatliche Stelle, ist ja dann auch im letzten Schritt vorgesehen.“ (ID7, Z. 3886-3893)	Man muss nicht immer den vorsichtigen Weg gehen, nur im Rahmen bleiben, aber es ist problematisch, sich selbst bei der DSFA zu überwachen. Da, wo es kritisch ist, sollten externe oder staatliche Stellen überprüfen.	Es ist problematisch sich bei einer DSFA selbst zu überwachen und es wäre besser wenn dies externe oder staatliche Stellen machen würden.	Datenschutz-folgen-abschätzung
ID7: „Ja, da sehe ich halt, dass also grundsätzlich die Einwilligung ist, also als generell als Rechtsgrundlage und so wie es eingesetzt werden soll. Also das Prinzip davon finde ich eigentlich super. Weil ich... Und dann ist halt die Schwierigkeit, was will man eigentlich damit erreichen? Man will eigentlich erreichen, dass für den Betroffenen im Vorhinein	Das Prinzip der Einwilligung ist eigentlich gut, da es Prozesse, was mit Daten passiert, transparent macht und man zustimmen kann oder nicht. Dennoch sind viele Prozesse so komplex, dass die Einwilligung noch verwirrender ist. Das Problem ist die	Einwilligungen und das Prinzip der Transparenz und der Zustimmung sind gut, doch sind Prozesse manchmal so komplex, dass die Ausgestaltung der derzeitigen Einwilligung nicht das beste Mittel ist.	Verständnis von Einwilligungs-erklärungen

transparent klar wird, was passiert da jetzt oder was wollen die machen? Und ich habe jetzt die Möglichkeit zu sagen, ja oder nein. Jetzt sind natürlich Datenverarbeitungsprozesse teilweise so komplex, dass das nicht transparent wird mit der Einwilligung vielleicht, sondern noch verwirrender. Also da, da dieses, dieses Mittel oder diesen richtigen Weg zu finden, das ist glaube ich dann manchmal schwierig. Also Einwilligung grundsätzlich ein gutes Instrument. Aber wie ist das jetzt aufgebaut, wie ist das ausgestaltet? Oder muss es sein, damit es wirklich transparent oder verständlich wird oder bleibt? Ich glaube, dasselbe Thema haben wir auch mit den Datenschutzinformationen (…)“ (ID7, Z. 3906-3918)	Ausgestaltung der Einwilligung		
ID7: „(...)Also das durfte nur eine A4 Seite sein und das musste bestimmte Informationen beinhalten. Und man hat eben geschaut, dass das dann dadurch nicht zu kompliziert wird. Also für den Kunden musste auf einen Blick erkennbar sein, was sage ich da jetzt ja? Was macht dieses Finanzinstrument? Das wäre natürlich auch irgendwie vielleicht eine nette Sache für einen, wie die Auserklärungen, dass man sagt, die muss auf eine bestimmte Art und Weise strukturiert sein oder muss bestimmte... Zu bestimmten Punkten eine Information geben. Und der Betroffene weiß, egal was eine Einwilligung gibt, also er kennt das Format, es schaut immer gleich aus und für ihn ist es dann einfacher, das zu verstehen. Also es wird dann viel transparenter. Ob das wirklich in der Praxis gehen wird, weiß ich nicht. (ID7, Z. 3924-3933)	Eine Einwilligung müsste eigentlich nur eine A4 Seite mit bestimmten Informationen sein, damit es für Betroffene klar ist, und dabei sollte sie auch eine bestimmte Struktur haben, also dass das Format immer gleich ist für ein besseres Verständnis.	Für ein besseres Verständnis sollte eine Einwilligung vielleicht nur eine A4 Seite mit bestimmten Informationen und mit einer Standardstruktur sein.	Verständnis von Einwilligungs-erklärungen
ID7: „(…) Du musst, du musst Sachen bereitstellen, aber du darfst nicht, es darf nicht zu kompliziert sein, aber schon allein durch die Länge wird es ja eigentlich kompliziert. Also auch wenn ich in einfacher	Es ist komplex weil die Information bereit gestellt werden muss, und die Einwilligung dadurch so lang wird.	Die Information muss bereitgestellt werden und dadurch wird die Einverständnis-erklärung so lang.	Verständnis von Einwilligungs-erklärungen

Sprache Unterzeilen schreibe, ist es für mich dann jetzt persönlich nicht mehr transparent, weil mich das auch niemanden zumuten kann.“ (ID7, Z. 3943-3947)			
ID7: „(…) Die Lücken, die werden halt immer, die... Die werden halt immer einerseits vom Unternehmen, werden die halt unternehmensfreundlich interpretiert und vom Konsumenten, der sich halt ärgert, werden sie halt konsumentenfreundlich ausgelegt. Also da gibt es halt dann immer ein Spannungsverhältnis, dass sich das, also das muss sich halt einfach in der Rechtsprechung dann zeigen, wie das dann wirklich zu interpretieren ist. Also das sind für mich halt dann die Fälle, die einfach ausgefochten, also jetzt gerade ausgefochten werden oder ausgefochten werden müssen.(..) Ja, das ist dann aber doch im Ernstfall oder in Fall der Fällen so, dass ein Unternehmen noch immer sagen kann, das ist jetzt nicht Rechtsprechung und das ist jetzt nicht Gesetz. Das sind Empfehlungen und das sind irgendwie Leitfäden. Also die Lücken, die sind halt da und die bleiben halt so lange, bis das halt dann beim Höchstgericht war.“ (ID7, Z. 3955-3962 und 3963-3967).	Das Problem ist, dass Stellen mit großem Interpretationsspielraum von Unternehmen zu ihren Gunsten und von Betroffenen wiederum zu ihren Gunsten ausgelegt werden, was zu einem Spannungsverhältnis führt, und das bleibt solange, bis ein Höchstgericht entscheidet.	Stellen mit viel Interpretations-spielraum werden von Unternehmen und Betroffenen zu ihren Gunsten ausgelegt, woraus solange eine Spannung entsteht, bis ein Höchstgericht entscheidet.	Nachteile/ Schwächen der DSGVO
ID7: „(…)Ich meine, bestimmte, also in dem Fall sind es dann Lücken, aber Interpretationsspielräume oder allgemeine Formulierungen sollen ja glaube ich einfach auch sein. Ich meine, es ist jetzt nicht beabsichtigt, dass das für Rechtsunsicherheit schafft, aber praktisch schafft es halt auch Rechtsunsicherheit, weil allgemeine Formulierungen, das ist halt immer, da kann man halt dann interpretieren. (…)“ (ID7, Z. 3976-3981)	Allgemeine Formulierungen sorgen nun einmal für Interpretationsspiel-räume und Rechtsunsicherheit und das ganz unbeabsichtigt.	Allgemeine Formulierungen sorgen nun einmal für Interpretationsspiel-räume und Rechtsunsicherheit.	Nachteile/ Schwächen der DSGVO
ID7: „Das Problem, also ich meine, die praktische Erfahrung ist da jetzt auch nicht so groß bei mir, aber doch jetzt bezogen auf	In der Praxis hat die Offenheit der DSGVO für sehr viel Rechtsunsicherheit gesorgt, da viele nicht	Die Offenheit der DSGVO hat in der Praxis für viel Rechtsunsicherheit gesorgt, dennoch sind	Harmonisierungs -erfolg der DSGVO

einzelne Bestimmungen, das Problem, das ich dann eher sehe, ist, dass schon mal niemand gewusst hat, wie soll er mit der DSGVO umgehen oder wie wird sich das dann in der Praxis einzelne Bestimmungen wirklich herausstellen? Aber in dem Zeitpunkt musste man dann gleichzeitig dann vielleicht schon von diesen Öffnungsklauseln Gebrauch machen und auch die nationalen Gesetze anpassen. Das heißt 2017/2018. Und das hat dann eher ein bisschen zu einem Wirrwarr geführt, weil man hat dann manchmal vielleicht nationale Bestimmungen, die jetzt nicht zu hundert Prozentig im Eingang sind mit der DSGVO. Hat man damals aber vielleicht noch nicht gewusst, wenn man noch nicht genau gewusst hat, wie muss man einzelne Bestimmungen in der DSGVO auslegen? Das heißt, ich glaube die Öffnungsklauseln, die braucht man schon. Aber ich glaube, das Ganze ist nicht so optimal dann umgesetzt worden von den einzelnen Nationalstaaten.“ (ID7. Z. 3996-4009)	wussten, wie sie mit der DSGVO umgehen sollen, auch wenn die Öffnungsklauseln national schlecht umgesetzt wurden, sind sie gut.	Öffnungsklauseln, wenn sie gut umgesetzt werden.	
ID7: „Ja, also ich habe noch nicht so, also es ist jetzt nicht so auf meinem Schreibtisch, der DSA, aber was ich halt glaube ist, bezogen auf was kannst du DSGVO bringen oder dem Level an Datenschutz. Ich glaube halt, wenn man halt noch ein Gesetz hat, das wiederum bestimmte Aspekte thematisiert und auch Bußgelder vorsieht, dann fällt es für Unternehmen dann vielleicht doch schon schwerer zu sagen, ich lege jetzt zwei Gesetze risikofreundlich aus. Also ich glaube halt mit der zusätzlichen Regulatorik muss man sich dann zweimal überlegen, gehe ich einen risikobasierten Weg oder gehe ich doch den sicheren Weg? Das heißt, ich glaube, es kann unterstützend wirken, dass man die DSGVO vielleicht dann noch mehr beachtet oder sich in manchen Aspekten dann doch denkt, da	Unternehmen werden durch den DSA auch die DSGVO mehr beachten, da es einen Unterschied machen wird, gleich zwei Gesetze risikofreundlich auszulegen.	Der DSA wird auch für mehr Beachtung gegenüber der DSGVO sorgen, da das Compliance Risiko steigt.	Einfluss DSA auf Schutz personen-bezogener Daten

nehme ich den sicheren Weg. Also ich würde es so ein bisschen als Unterstützung sehen und jetzt indirekt, dass es indirekt dazu führt, dass Unternehmen dann auch sich vielleicht noch stärker an die DSGVO halten.“ (ID7, Z. 4018-4029)			
ID7: „Also wenn ich jetzt, wenn ich jetzt, ich sehe es jetzt aus Unternehmenssicht und ich sage jetzt, ich bin in irgendeinem datenschutzrechtlichen Drittland und ich möchte in Europa Geld verdienen, dann kann ich mir überlegen, ob ich gegen ein Gesetz verstoße. Aber wenn es dann schon darum geht, dass ich gegen zwei oder drei Gesetze verstoße, dann würde ich mir das doch eher mal anschauen und mir anschauen, was kann ich es grundsätzlich aufsetzen, dass das dann rechtskonform ist und dann vielleicht auch mit allen dreien im Einklang steht. Also, dass das Compliance Risiko oder das Risiko steigt. Und ich glaube auch, dass Unternehmen nur einen gewissen Risikoappetit haben und das halt dann irgendwann überwiegt das. Und dann muss man sich doch irgendwann vielleicht damit auseinandersetzen, wie kann ich es rechtskonform aufsetzen, wenn ich es bisher halt nicht gemacht habe?(…)“ (ID7, Z. 4043-4054)	Das Compliance Risiko wird irgendwann steigen für die Unternehmen, da es ein Unterschied ist, ob man gegen ein Gesetz verstößt und Strafe zahlt oder dann schon gegen zwei oder drei. Irgendwann ist das Risiko zu hoch.	Irgendwann ist das Risiko auch für große Unternehmen zu hoch, wenn sie gegen mehr als ein Gesetz verstoßen.	Einfluss DSA auf Schutz personen-bezogener Daten
ID7: „Und wenn sie sich so einer nicht dran gehalten hat, dann wird sie sich wahrscheinlich in nicht Zukunft dran halten. Aber das wird man halt dann auch sehen, ob dann wirklich von den, von den, ja, von diesen Höhen Gebrauch gemacht wird. Also wenn man sich anschaut mit den DSGVO Strafen, und zwar gegenüber jetzt den US Konzernen, da muss ich halt schon fragen, ob es nicht höher sein könnte, nämlich als ob es wirklich weh tut. Aber das ist halt, ist halt auch eine politische Frage. Vergraulen will man die wahrscheinlich auch nicht. Schwierig.“ (ID7, Z. 4067-4073)	Es ist schwer, Unternehmen dazu zu bringen, sich an Regeln wie die DSGVO zu halten, ohne sie irgendwann aus dem Markt zu vergraulen.	Die Komplexität ist es zu schaffen, Unternehmen dazu zu veranlassen, sich an Regeln wie die DSGVO zu halten ohne, dass sie den Markt verlassen.	Heraus-forderungen in Zukunft

ID7: „(…) Und was sich halt schon meiner Meinung nach gezeigt hat, ist, dass durch die, durch die Entwicklungen, die es halt gibt und die Möglichkeiten auf Basis von Daten auch wirtschaftlich erfolgreicher zu sein, das heißt Dienstleistungen besser anbieten zu können, Services besser anbieten zu können, das heißt das Verhalten steuern zu können. Das heißt mit den Entwicklungen... Mit den Entwicklungen wird das Thema Daten halt interessanter und damit wird halt auch die DSGVO relevanter. Und ich glaube halt, dass in Zukunft, ich glaube halt, dass die technologische Entwicklung nicht abnehmen wird und zu einem gewissen Grad die Daten natürlich noch interessanter werden. Das heißt der Datenschutz wird wichtiger für den Konsumenten und wird auch für den Regulator wichtiger, dass der eingehalten wird, weil natürlich Beeinflussungsmöglichkeiten da sind, Missbrauchsmöglichkeiten da sind. Das heißt, ich glaube, das Thema an sich wird von der Wichtigkeit eher noch ein bisschen zunehmen.“ (ID7, Z. 4082-4094)	Da Daten ein großes wirtschaftliches Thema sind, das auch immer größer wird, wird der Datenschutz wichtiger, da es zu mehr Beeinflussungsmöglichkeiten und Missbrauch kommen kann.	Mehr technologische Entwicklung bedeutet mehr Daten, mehr Datenschutz, da es auch zu mehr Missbrauch kommt.	Heraus-forderungen in Zukunft
ID7: „Ja, ich meine KI ist halt so, KI ist halt was anderes. Also eigentlich die Komplexität, die zunehmende Komplexität von technischen Systemen. Weil es wird halt für den Menschen immer undurchschaubarer. Für mich als Konsumenten wird es undurchschaubarer, aber eventuell auch als Unternehmen, weil ich, weil ich was kaufe halt dann Leistungen an, ich lasse halt bestimmte Dateninformationen verarbeiten. Aber ich kann sie irgendwann nicht mehr wirklich nachvollziehen. Also ich kann es ungefähr einschätzen, was da passiert. Aber wenn es einen gewissen Komplexitätsgrad übersteigt, kann ich es als Mensch nicht mehr fassen oder ich kann es	Die zunehmende Komplexität von technischen Systemen macht sie immer undurchschaubarer und zwar sowohl für Konsument*innen als auch für Unternehmen. Denn ab einer gewissen Komplexität kann man nur darauf vertrauen, dass das Richtige passiert, und es ist nur schwer nachprüfbar.	Die zunehmende Komplexität technischer Systeme macht sie für Unternehmen und Betroffene undurchsichtiger. Ab einem gewissen Punkt kann man nur darauf vertrauen, dass alles richtig läuft.	Heraus-forderungen in Zukunft

nicht mehr wirklich im Detail nachprüfen. Ich muss mich zu einem gewissen Grad darauf verlassen, dass da was richtig passiert oder so wie ich das beabsichtige. Und da kann es halt dann schon auch sein, dass Sachen passieren, die Auswirkungen haben, negative Auswirkungen auf den Betroffenen, auf den Endkunden, die ich aber vielleicht gar nicht so sehe oder auch nicht beabsichtigt habe. Das heißt, mit der technologischen Entwicklung steigt halt einfach das Risiko auch. (…)“ (ID7, Z. 4101-4114)			
ID7: „(…)Wir haben jetzt bei der DSGVO das Thema Profiling zum Beispiel als Regelung drinnen. Da gibt es halt dann die Pflicht, du musst halt den, wenn du das halt machst als Unternehmen, dann musst du darüber informieren und du musst halt bestimmte Informationen bereitstellen, dass du das halt auch vollziehen kannst. Aber, also das Unternehmen versuchen oft halt sich sehr allgemeine Formulierungen, auch allgemeine Formulierungen durchzuziehen. Und vielleicht ist es sogar schon schwierig für Unternehmen selber das so darzustellen, dass es in einem kurzen Absatz wirklich verständlich ist, was da passiert, weil es dann doch auch schon komplex ist. (...)“ (ID7, Z. 4115-4123)	Als Unternehmen hast du die Pflicht, bestimmte Informationen bereitzustellen, wenn du Daten verarbeitest. Es ist auch sicher schwierig, Informationen immer genau, kurz und einfach zu formulieren.	Als Unternehmen musst du Informationen über Datenverarbeitung zur Verfügung stellen und das kann kompliziert sein, das einfach und kurz zu formulieren.	Verantwortung Unternehmen
ID8: „Ja, sehr oft und die Frage nachhaltig ist eigentlich dann, wenn in einer Organisation die Beteiligten wirklich verstanden haben, was es geht. Das heißt, den Wert und die Rechtsaspekte der Informationen verstehen und entsprechend sorgfältig mit der Information umgehen.“ (ID8, Z. 4191-4194, durchgeführt am 10.08.2023)	Von nachhaltigem Datenschutz kann gesprochen werden, wenn in einer Organisation alle Beteiligten den Wert und die Rechtsaspekte der Informationen verstehen und sorgfältig damit umgehen.	Nachhaltiger Datenschutz ist, wenn Organisationen nach dem Recht sorgfältig mit Informationen umgehen.	Nachhaltiger Datenschutz
ID8: „Also die privaten Unternehmer, die haben einfach die Verantwortung, dass sie verstehen, dass sie nicht die Informationen über Personen einfach nehmen können, sondern dass sie da irgendeine Form der Berechtigung haben und auch	Unternehmen haben die Verantwortung, dass sie Informationen über Personen nicht einfach nehmen können, sondern eine Berechtigung dafür brauchen und eine Rechenschaftspflicht für	Unternehmen dürfen Personendaten nicht nehmen ohne eine Berechtigung und haben eine Rechenschaftspflicht.	Verantwortung von Unternehmen

einen adäquaten Umgang mit diesen Informationen an den Tag legen müssen und verantwortlich sind dafür, also auch dies irgendwie in einer Rechenschaft darlegen müssen, dass sie gemacht werden.“ (ID8, Z. 4204-4209)	einen passenden Umgang damit haben.		
ID8: „Das wäre eigentlich beim Staat. Das denke ich auch. Es ist wichtig, dass der Staat auch weiß, es geht, wenn ich Informationen von Personen nehme, ist das, wie wenn ich die Person selber nehme und das darf ich nicht.“ (ID8, Z. 4209-4212)	Der Staat muss wissen, dass Personendaten sind wie die Person selbst, nämlich sehr privat, und ich muss wissen, was erlaubt und was nicht erlaubt ist.	Der Staat muss Personendaten wie die Person selbst sehen.	Verantwortung Union / Staat
ID8: „Und die Personen halt, die sollten viel sensibilisierter umgehen mit ihren Informationen. Und da sehe ich schon noch einen sehr großen Handlungsbedarf. Die einzelne Person. Die kann sich wehren, die müsste sich wehren.“ (ID8, Z. 4212-2020)	Personen sollten viel sensibler mit ihren Daten umgehen und haben die größte Verantwortung, da sie sich mehr wehren müssten, und da ist auch großer Handlungsbedarf.	Es liegt Verantwortung beim Einzelnen, da sie sensibler mit ihren Daten umgehen und sich auch wehren müssen, da ist großer Handlungsbedarf.	Verantwortung von Betroffene/Konsument*innen
ID8: „Die Vorteile sind, dass der Datenschutz sehr prominent thematisiert wurde und auch zum Teil gut umgesetzt, sowohl in der EU als auch aus der Grund für die Schweiz, als auch generell Auswirkungen hat, weltweit im Umgang mit Personendaten. Und dieser Versuch der Vereinheitlichung des Umgangs in ganzen EU-Rahmen, also irgendeinen generellen Standard zu setzen. Das finde ich ein sehr großer Vorteil.“ (ID8, Z. 4234-4238)	Vorteile der DSGVO sind der prominente Umgang, die teilweise gute Umsetzung der EU, als auch die Auswirkungen auf die restliche Welt auf den Umgang mit personenbezogenen Daten, und es wäre wichtig, einen Standard zu finden.	Vorteile der DSGVO sind teils die gute Umsetzung in der EU, als auch die globalen Auswirkungen, die Prominenz von Datenschutz und einen Standard zu finden.	Vorteile/Stärken der DSGVO
ID8: „Die Schwächen sind sicher einmal, dass dies die Standardisierung etwas zu wenig mit diesen Öffnungsklauseln und mit diesen doch unterschiedlichen Kulturen der einzelnen Länder, dass die doch wieder weniger ausgeprägt ist, dass das geplant war. Und eine weitere, doch das finde ich ist halt die größte Schwäche. Ja und eine weitere Schwäche, denke ich, dass gewisse Zielsetzungen nicht greifen. Zum Beispiel diese Cookie Richtlinien, die man, ja, alle klicken einfach an. Vieles wird einfach wie durchgeklickt und dann wird das eigentliche Grundziel des Gesetzes nicht erreicht.“ (ID8, Z. 4224-4250)	Die Standardisierung wurde durch die Öffnungsklauseln geschwächt und ist deswegen weniger ausgeprägt. Außerdem greifen manche Zielsetzungen nicht, wie zum Beispiel die Cookie-Richtlinie.	Die Standardisierung der DSGVO wurde durch die Öffnungsklauseln geschwächt und manche Zielsetzungen der DSGVO greifen nicht.	Nachteile/ Schwächen der DSGVO

ID8: „Im Großen und Ganzen finde ich die nicht gut formuliert, also zu wenig verständlich für den Adressaten oder die Adressatin zu sehr auch von einander abgeschrieben, zu generisch. Insbesondere auf Webseiten könnte man die Benutzerführung viel netter gestalten und die Dinge vielleicht auch noch zeichnerisch oder mit einem kleinen Film oder so den Leuten begreifbar macht.“ (ID8, Z. 4258-4262)	Einwilligungserklärungen sind allgemein oft nicht gut formuliert und nicht verständlich. Gerade bei Websites könnte die Benutzer*inneneinführung zum Beispiel mit Videos, Einwilligungserklärungen greifbarer machen.	Einwilligungs-erklärungen sind nicht gut formuliert und unverständlich, Online könnte die Benutzer*innenführung durch Videos verbessert werden.	Verständnis Einwilligungs-erklärungen.
ID8: „Also ich finde grundsätzlich der Ansatz einfach Privacy by Design und Privacy by Default, ja nicht nur technisch, es ist auch organisatorisch. Das ist, finde ich sehr gut. Aber in der Praxis, sind da große Hürden noch zu nehmen. Häufig sind irgendwelche, zum Beispiel, Zugriffsmöglichkeiten zu weit, weil man sie gar nicht enger einschränken kann von der Technik her. Oder weil die Unternehmen organisatorische Probleme haben, diese Privacy by Default-Themen gut umzusetzen und genügend spezifische Rollen definieren können, damit nicht wieder zu viel auf zu viel Zugriff hat.“ (ID8, Z. 4278-4285)	Grundsätzlich ist Privacy by Design sehr gut, dennoch gibt es in der Praxis oft Hürden, was Einschränkungen von technischer Seite betrifft, wie zum Beispiel Zugriffsrechte und was die organisatorische Seite betrifft, wie zum Beispiel Rollen zu definieren.	Grundsätzlich ist Privacy by Design sehr gut, dennoch gibt es in der Praxis oft Hürden was Einschränkungen von technischer Seite und organisatorischer Seite betrifft.	Privacy by Design
ID8: „Also eigentlich eine Datenschutzfolgenabschätzung erwarte ich immer bei jedem Start eines Projektes. Irgendwie in einer Form. Also es muss ja nicht so ein großes Formular sein, sondern dass man sich einfach überlegt, geht es datenschutzmäßig überhaupt? Und welche Risiken hätten wir? Das ist selbstverständlich und es ist übrigens auch selbstverständlich, dass wenn man zu große Risiken hat, dass man das nicht macht oder anders macht. Und eigentlich, wenn man in einer Unternehmung, Privacy by Design umgesetzt hätte, dann müsste man für die bestehenden Prozesse ja gar keine Datenschutzfolgenabschätzung machen. Es dürfte ja gar nicht zu großem Risiko unterwegs sein. Und da sehe	Eine DSFA muss vor jedem Projekt gemacht werden, um die Risiken einzuschätzen, und wenn das Risiko zu groß ist, das Projekt nicht zu machen. Wenn Privacy by Design in einer Unternehmung gemacht werden würde, dann müsste es keine DSFA geben, da korrekt gearbeitet wurde.	Eine DSFA muss vor jedem Projekt sein um das Risiko einzuschätzen und wenn Privacy by Design korrekt gelebt werden würde, dann würde es keine DSFA benötigen.	Datenschutz-folge-abschätzung

ich zum Teil einen Widerspruch, weil jetzt zum Teil für alles noch Datenschutzfolgenabschätzung gemacht werden. Und das ist vielleicht auch das Instrument nicht immer richtig verstanden oder eingesetzt.“ (ID8, Z. 4305-4310)			
ID8: „Ja, also wenn ich Privacy by Design lebe, dann gibt es keinen Raum für Datenschutzfolgeabschätzung, weil ich nur korrekt arbeite. Also gibt es nur noch Raum für neue Projekte.“ (ID8, Z. 4325-4327)	Wenn man Privacy by Design lebt, braucht es keine DSFA, weil nur korrekt gearbeitet wird.	Wenn man Privacy by Design lebt, dann braucht es keine DSFA.	Privacy by Design
ID8: „Ja, genau. Weil, also, weil diese großen Anbieter jetzt auch klare Vorgaben erhalten, wie sie auftreten am Markt, was sie und somit auch klar kommunizieren müssen. Und das hat einen Einfluss auf den Umgang mit personenbezogenen Daten. Und zum Teil müssen sie sich auch zertifizieren oder Rechenschaft abgeben dem Staat gegenüber. Und das hat eine ordnende Wirkung auf den Umgang mit Informationen und somit auch auf Personen bezogene Daten.“ (ID8, Z. 4371-4376)	Anbieter*innen müssen durch den DSA sich an klare Vorgaben halten und auch klar kommunizieren und haben eine Rechenschaftspflicht gegenüber dem Staat. Das hat einen Einfluss auf den Schutz personenbezogener Daten und eine ordnende Wirkung.	Der DSA hat durch die neuen Vorgaben einen Einfluss auf personenbezogene Daten, da die klare Kommunikation und die Rechenschafts-pflichten eine ordnende Wirkung haben.	Einfluss DSA auf Schutz personen-bezogener Daten
ID8: „Im Grunde genommen ist die Herausforderung, dass wir wirklich gut in der digitalen Welt ankommen und uns in der digitalen Welt so bewegen, organisieren, transparent und anständig sind, wie wir das von einander in der physischen Welt erwarten. Und so weit sind wir noch nicht. Das wird noch einige Verwerfungen geben, bis wir an diesen Punkt angelangt sind.“ (ID8, Z. 4406-4410)	Die Herausforderung liegt darin, in der digitalen Welt anzukommen und das dauert noch. Bis dahin wird es noch einige Verwerfungen geben.	Die Herausforderung liegt darin vollends in der digitalen Welt anzukommen.	Heraus-forderungen in Zukunft.
ID8: „Ja, es wird, es wird einfach komplexer, aber es wird vor allem alles digital. Das ist es, oder? Und dann ist die Frage wie organisieren wir uns, dass wir rechtssicher uns da bewegen mit den Identitäten, mit den Verträgen, mit Beweisen, nicht nur mit Persönlichkeitsschutz, auch mit Urheberrechtsschutz. Alles kommt jetzt auf die digitale Ebene und man kann nicht eins zu eins die Instrumente der physischen Welt	Die Welt wird zunehmend komplexer und jetzt stellt sich die Frage, wie wir uns organisieren, um in die digitale Ebene zu kommen. Da wird die Abstraktion eine Herausforderung, da die digitale Welt andere Mechanismen hat.	In einer zunehmend komplexen Welt die immer digitaler wird, stellt die Abstraktion von physisch zu digital eine Herausforderung dar.	Heraus-forderungen in Zukunft

digitalisieren, weil es ergibt sich wegen der Digitalisierung andere Mechanismen. Und das können viele auch nicht. Ich denke, die Abstraktion ist eine Herausforderung für viele. Das Abstrahieren von der physischen Welt.“ (ID8, Z. 4430-4437)			

Tab.15: Induktive Kategorienbildung (Eigendarstellung angelehnt an Mayring)

9.2 Interviewleitfaden:

1. **Einleitung**
   - Vorstellung der Interviewerin: Isabella Haag
   - Vorgangsweise des Interviews
   - Hinweis auf Anonymität
   - Hinweis zur Aufnahme (Transkription)

2. **Erhebung persönlicher Daten (Name, beruflicher Kontext)**
   - Was ist für Sie nachhaltiger Datenschutz?
   - Wie beurteilen Sie die Verantwortlichkeit zum Schutz personenbezogener Daten? (Staat, Unternehmen, Betroffene/ Konsument*innen)

3. **Probleme:**
   - Welche Vorteile / Nachteile hat für Sie die DSGVO? (Stärken/ Schwächen vom Schutz personenbezogener Daten)
   - Wie beurteilen Sie die Harmonisierung von Datenschutz in der EU?
   - Wie bewerten Sie die Privacy by Design-Regelungen in der DSGVO?
   - Wie beurteilen Sie die Selbstevaluierung der DSFA?
   - Wie beurteilen Sie das Verständnis der Einwilligungserklärungen?

4. **Auswirkungen von Problemen:**
   - Welche Auswirkungen haben die Lücken der DSGVO?
   - Wie bewerten Sie die Auswirkungen, wenn Verantwortlichkeiten zum Schutz personenbezogener Daten nicht eingehalten werden (Staat, Unternehmen, User*innen)?

5. **Lösungsansätze**
   - In welchen Aspekten könnte der DSA die DSGVO ergänzen oder zu besserem Datenschutz verhelfen? (Plattformregulierungen, Transparenzrechte)
   - Worin liegen die größten Herausforderungen zum Schutz personenbezogener Daten, wenn Sie an die Zukunft denken (technologischer Fortschritt)?

6. **Ende**
   - Danksagung
   - Empfehlung für weitere Interviewpartner*innen
   - Empfehlung für weitere Informationsquellen

9.3 Exposé:

Familienname, Vorname	**Haag Isabella**
eMail-Adresse	mm211804@fhstp.ac.at
Telefonnummer	0660 4210381
Datum der Abgabe	22.11.2022
Name Betreuer*in (wird von der Studiengangsleitung zugeteilt)	FH-Prof. Ing. Dr. Harald Wimmer
Arbeitstitel	**Die Stärken und Schwächen der DSGVO im Vergleich zum DSA**
Fragestellung der Master-These	**Problemstellung:** Im April 2016 wurde durch das Europäische Parlament und des Rates die Datenschutz Grundverordnung verabschiedet und gilt seit Mai 2018 als Grundlage des allgemeinen Datenschutzes in der EU. Die DSGVO dient zum Schutz personenbezogener Daten bei Verarbeitung dieser und zum freien Datenverkehr in der Europäischen Union. (vgl. DSGVO, Art. 1). Genauer gesagt wird geregelt, dass Unternehmen Verantwortung für die Verarbeitung von Daten übernehmen müssen. Es müssen Prozesse überprüft, Daten gelöscht, Vorgänge festgehalten und ab 250 Mitarbeiter*innen Datenbeauftragte eingestellt werden. Die DSGVO hat auf jeden Fall für eine notwendige Sensibilisierung des Datenumgangs in der EU gesorgt, doch lässt sie noch Lücken offen, wie zum Beispiel das Thema Auskunft über Empfänger, das besagt, dass Unternehmen über gespeicherte Daten Auskunft geben müssen. Hierbei ist nicht berücksichtigt, in welchem Ausmaß, da Empfänger oder die Kategorie dessen Zugehörigkeit ausreicht und keine Auflistung genauer Firmen notwendig ist (vgl. DSGVO, Art.15, Abs. 1c).

	Ein weiteres Problem der DSGVO ist die Annahme des informierten Verbrauchers, der selbst einwilligt. Verbraucher*innen kreuzen freiwillig an, wem sie ihre Daten geben. Friedrichsen und Wersig hinterfragen die Verbraucherschutzperspektive, da die informationenpflichtigen Texte nicht gelesen, nicht verstanden werden oder es bei nicht Zustimmen zu Einschränkung der Nutzung kommt und schlicht und ergreifend auf Eigenverantwortung gesetzt wird (vgl. Friedrichsen & Wersig, 2020, S. 149). Außerdem finden die Zustimmungen, insbesondere bei Cookie Bannern, oft automatisiert statt. Eines der größten Probleme, bei der die DSGVO hätte Abhilfe schaffen sollen, war es, eine Art Gatekeeper Funktion gegenüber US amerikanischen Unternehmen zu schaffen. Rein rechtlich wurden Unternehmen, welche Waren und Dienstleistungen in der EU anbieten, durch Art. 3 Abs. 2 (DSGVO) dem „Marktortprinzip“ erfasst, wodurch sie bei Verstoß belangt werden können, ohne einen Sitz in der EU zu haben (vgl. Klementschitz, 2019, S. 67). Grundproblem ist hier jedoch vielmehr die irische Datenschutzbehörde, die sich bei datenschutzrechtlichen Themen bei Verstößen zu wenig durchsetzt, wenn nicht sogar den Datenmissbrauch fördert. Das Europäisches Zentrum für digitale Rechte „noyb“ hat in der Hinsicht einen umfassenden Bericht veröffentlicht, in dem erfasst wurde, wie die irische Datenschutzbehörde Facebook dazu verhilft, die DSGVO zu umgehen (vgl. Noyb, 2021, o. S.). Lücken wie diese öffnen den IT- Unternehmen weiterhin Tür und Tor, den europäischen Markt nach ihren Regeln zu bespielen. Nun wurde im Oktober 2022 der Digital Services Act vorgestellt, der digitale Dienstleitungen und digitale Märkte regeln soll. Genauer gesagt soll der DSA viele rechtliche Lücken, welche die DSGVO nicht schließen konnte, ergänzen, wie zum Beispiel die Bestimmung, dass sich alle Online-Dienste daran halten müssen, egal ob sie ihren Sitz in der EU haben oder nicht (vgl. Klementschitz, 2019, S. 67). Hier geht es besonders um die Regelung von sehr großen Dienstanbietern. Auch die Offenlegung von digitalem Profiling soll darin geregelt werden, also die Offenlegungspflicht von Empfehlungssystemen sowie das Verbot von Werbung basierend auf personenbezogene

	Daten. Dabei soll die DSA die DSGVO nicht ersetzen, sondern ergänzen (vgl. Europäische Kommission, 2023c, o. S.). **Zielsetzung:** Diese Arbeit versucht, die Lücken der DSGVO herauszuarbeiten und prüft, inwieweit der DSA den Schutz personenbezogener Daten weiter vorantreibt- oder eventuell für weitere Gesetzeslücken oder Grauzonen sorgen wird. Ziel ist es, auf Basis theoretischer Ausarbeitung der DSGVO und der DSA Hypothesen zu bilden und anhand qualitativer Expert*innen-Interviews zu prüfen, ob Konsument*innen von Online-Dienstleister*innen durch die Ergänzung der DSGVO einen nachhaltigen Schutz ihrer Daten erwarten können. **Forschungsfrage/Leitfrage:** Inwieweit ergänzt der DSA die DSGVO in Bezug auf den Schutz personenbezogener Daten, aus Sicht der Konsument*innen, und ist dieser ausreichend, um von nachhaltigem Datenschutz zu sprechen?
Wissen-schaftliche und praktische Relevanz	**Wissenschaftliche Relevanz:** Aus wissenschaftlicher Perspektive ist es notwendig, neuen EU-Richtlinien kritisch gegenüberzustehen und zu hinterfragen, was sie bedeuten und welche Folgen sie mit sich tragen. Es gibt speziell im deutschsprachigen Raum einige Journale und Bücher von Jurist*innen, die sich mit den Auswirkungen der DSGVO, auf ihre Branche bezogen, beschäftigen. So schrieb Körner ein Buch über die Auswirkungen der DSGVO auf Betriebe, worauf bei personenbezogenen Daten darauf geachtet werden muss, wer bei Verstößen überhaupt zuständig ist (vgl. Körner, 2019). Ein Beispiel für die wissenschaftliche Relevanz des Themas wäre die Dissertation von Klementschitz, die sich mit den Auswirkungen des internationalen Datenverkehrs durch die DSGVO beschäftigt (vgl. Klementschitz, 2019). Klementschitz zieht den Vergleich zur Datenschutz-Richtlinie von 1995 und versucht in seiner Arbeit herauszufinden, an welchen Stellen die DSGVO die veraltete Richtlinie ergänzt und verbessert (vgl. Klementschitz, 2019, S.67). Diese Dissertation stellt für meine Arbeit einen wichtigen Anhaltspunkt dar, da sie der vorliegenden Forschungsfrage ähnelt.

	Ein Problem der DSGVO, mit dem sich diese Arbeit beschäftigen wird, ist zudem, dass die Sanktionierung bei Verstoß derzeit zu wenig Wirksamkeit zeigt. Dies beschäftigt auch Martini, Wagner und Wenzel in „Das neue Sanktionsregime der DSGVO ein scharfes Schwert ohne legislativen Feinschliff“ (vgl. Martini, Wagner& Wenzel, 2018). **Praktische Relevanz:** In der Praxis haben wir jeden Tag mit Online-Diensten zu tun, sei es aus Unternehmensperspektive, aus der heraus es wichtig ist, zu wissen, wie man mit Kund*innendaten umgeht oder aus der Konsument*innenperspektive, aus der man keinen Überblick mehr hat, was man von sich aus preis gibt. Auch hier bietet das Buch von Körner über die Auswirkungen der DSGVO auf Betriebe Aufschluss, da es sehr praxisbezogen geschrieben ist und sich damit befasst, wie Betriebe die DSGVO am besten einhalten können (vgl. Körner, 2019). Gerade in der Praxis gibt es viele Belege über die Auswertungen der DSGVO und was sich auch technisch umsetzen lässt. Es gibt aus beinahe jeder Perspektive Artikel und Journale über Herausforderungen in der Praxis, sei es die Umsetzung, als auch über Social Media oder die IT. Je nachdem stehen verschiedene Unternehmen vor unterschiedlichen Herausforderungen in der Umsetzung. Speziell die Dissertation von Ivchenkov gibt Aufschluss darüber, wie sich die DSGVO auf datengetriebene Unternehmen auswirkt (vgl. Ivchenkov, 2019). Ein Beispiel für praktische Relevanz ist aus Sicht der Autorin auch die Einführung der DSA an sich, da sie derzeitige Datenschutzlücken schließen soll. **Relevanz für Digital Media Management:** Das Thema Datenschutz kommt speziell in den Lehrveranstaltungen Unternehmens- und Arbeitsrecht, als auch in Digital Commerce und Medien- und Internetökonomie vor. Dennoch ist das Thema eines, das unseren gesamten Studiengang betrifft, da wir als Digitale Medienmanager*innen uns in einem Umfeld der digitalen Dienste bewegen und dort auch zukünftig arbeiten werden. Es ist daher wichtig für unseren Studiengang, uns mit den Problematiken und Lücken der Rechtsprechung auseinanderzusetzen, um als Manager*innen ethisch und über Vorgaben hinaus agieren zu können.

Aufbau und Gliederung	

Methodenwahl und Sampling	**Empirische Methode:** Die Forschungsfrage soll anhand von Expert*innen Interviews und darauf folgende qualitative Inhaltsanalyse nach Mayring durchgeführt werden. **Begründung Methodenwahl inkl. Limitationen:** Ziel ist es herauszufinden, in welchen Aspekten die DSA weitere Abhilfe leisten wird, personenbezogene Daten zu schützen und welche derzeitigen Lücken sie in der DSGVO füllen wird. Dadurch die DSA erst eingeführt und umgesetzt werden muss, werden Expert*inneninterviews mit Jurist*innen geführt, die derzeit an der DSA arbeiten. Die Expert*innen werden anhand gewisser Kriterien ausgewählt, damit sie den notwendigen Einblick in die Thematik haben. Es wird speziell die inhaltsanalytische Methode nach Mayring gewählt, da die induktive Kategorienbildung nach Mayring zu den zusammenfassenden Techniken gehört und viel Material auf die wichtigsten Aspekte zusammengefasst werden kann (vgl. Mayring, 2010, S. 83ff.). Ein Vorteil der qualitativen Inhaltsanalyse nach Mayring ist, dass die Auswertung spezifisch nach Forschungsfrage konzipiert wird. Die Methode ist also in dem Sinne nicht fix, sondern wird mit der Erhebungs- und Auswertungsmethode der Forschungsfrage angepasst (vgl. Kuckartz, 2012, S. 24). Das bedeutet, dass die Forschungsfrage gezielt gestellt werden muss. Außerdem müssen die Daten, die bei den Expert*inneninterviews entstehen eine gewisse Qualität besitzen, damit sie ausreichend codiert werden können. Dementsprechend sollte, zum Beispiel, bei einer schriftlichen Durchführung der Interviews darauf geachtet werden, dass sie nicht in Stichworten beantwortet werden (vgl. Ramsenthaler, 2013, S. 37). Ein Nachteil der induktiven Kategorienbildung, ist, dass eine Kategorie innerhalb einer Passage öfter vorkommen und dies komplex werden kann bei der Auswertung (vgl. Mayring, 2020, S. 498) Die qualitative Inhaltsanalyse nach Mayring ist also von Vorteil, wenn das Ziel der Analyse eine Reduktion des Textes ist.

	Nach der Autorin ist eine quantitative Erhebung mittels Fragebogen ist in diesem Fall nicht möglich, da die Bevölkerung zu wenig über das Ausmaß von Datenschutz und das Recht auf den Schutz personenbezogener Daten weiß. Dies ist mitunter ein Grundproblem bei der Umsetzung der DSGVO, welches in dieser Arbeit mitunter erforscht wird. **Grundgesamtheit:** Die Grundgesamtheit wird aus ca. 7-10 Expert*innen bestehen. **Auswahlkriterien:** Expert*innen sollten einen beruflichen Bezug zur DSGVO bzw. DSA haben. Im besten Fall sollten sie an der DSA arbeiten. Ansonsten Personen die einen juristischen Hintergrund haben und entweder Datenschutzbeauftrage sind oder sich seit mindestens 5 Jahren aus juristischer Sichtweise mit dem Thema Datenschutz beschäftigen.
Literatur-hinweise	Quellenverzeichnis Kurzexposé: EU-Kommission (2023c), Ein Europa für das digitale Zeitalter – was sich für Nutzerinnen und Nutzer ändert. (o. J.). Abgerufen 27. Juli 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-users_de, abgerufen am 13.12.2023 Friedrichsen, M., & Wersig, W. (Hrsg.). (2020). *Digitale Kompetenz: Herausforderungen für Wissenschaft, Wirtschaft, Gesellschaft und Politik*. Wiesbaden: Springer Fachmedien Wiesbaden Ivchenkov, K. (2019). *Auswirkungen der EU-DSGVO auf das Online-Marketing–Eine Analyse am Beispiel von datengetriebenen Dienstleistungsunternehmen* (Doctoral dissertation, Universität Rostock). Klementschitz, R. (2019). *Auswirkungen der DSGVO auf den internationalen Datenverkehr,* Dissertation, Universität Linz.

Körner, M. (2019). *Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis*. Frankfurt am Main: Bund-Verlag.

Kuckartz, U. (2016). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (3., überarbeitete Auflage). Weinheim Basel: Beltz Juventa.

Martini, M., Wagner, D., & Wenzel, M. (2018). Das neue Sanktionsregime der DSGVO–ein scharfes Schwert ohne legislativen Feinschliff. *Verwaltungsarchiv*, *109*(2), S. 163-189.

Noyb, 2021, Irische Datenschutzbehörde gibt Facebooks „DSGVO-Umgehung“ grünes Licht. (o. J.). https://noyb.eu/de/irische-datenschutzbehoerde-gibt-facebooks-dsgvo-umgehung-gruenes-licht, abgerufen am 13.12.2023

Ramsenthaler, C. (2013). Was ist „Qualitative Inhaltsanalyse?“ In M. Schnell, C. Schulz, H. Kolbe, & C. Dunger (Hrsg.), *Der Patient am Lebensende* (S. 23–42). Wiesbaden: Springer Fachmedien Wiesbaden.

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), Fassung vom 27.04.2016

Weichert, T. (2020). Die DSGVO, ein – ganz guter – Anfang. *Datenschutz und Datensicherheit - DuD*, *44*, 293–296.

Kernquellen der Master These:

Cole, M. D., Etteldorf, C., & Ullrich, C. (2021). *Updating the rules for online content dissemination: Legislative options of the European Union and the Digital Services Act proposal* (1st edition). Baden-Baden: Nomos.

Friedrichsen, M., & Wersig, W. (Hrsg.). (2020). *Digitale Kompetenz: Herausforderungen für Wissenschaft, Wirtschaft, Gesellschaft und Politik*. Wiesbaden: Springer Fachmedien Wiesbaden

Kaiser, & Ratcliff, C. (2022). *Digital Services Act & Digital Markets Act*. European Parlament.

Klementschitz, R. (2019). *Auswirkungen der DSGVO auf den internationalen Datenverkehr,* Dissertation, Universität Linz.

Leistner, M. (2021). The Commission's vision for Europe's digital future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer. *Journal of Intellectual Property Law & Practice*, *16*, 778–784.

Mayring, P. (2010). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (11., aktual. und überarb. Aufl). Weinheim Basel: Beltz

Mayring, P. (2020). Qualitative Forschungsdesigns. In G. Mey & K. Mruck (Hrsg.), *Handbuch Qualitative Forschung in der Psychologie*. Wiesbaden: Springer Fachmedien Wiesbaden. S. 3-17

Schneider, R. (2021). *Gemeinsame Verantwortlichkeit: Entstehung, Ausgestaltung und Rechtsfolgen des Innenverhältnisses gemäß Art. 26 DSGVO*. Wiesbaden: Springer Fachmedien Wiesbaden.

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), Fassung vom 27.04.2016