Datenschutz im Umbruch -
Auswirkungen der EU-Datenschutz-Grundverordnung auf nationales Recht

B a c h e l o r - A r b e i t
an der Hochschule für öffentliche Verwaltung und Rechtspflege (FH),
Fortbildungszentrum des Freistaates Sachsen
zum Erwerb des Hochschulgrades
Bachelor of Laws (LL.B.)

vorgelegt von
Jolene Kunze
aus Drebach

Meißen, 26.03.2018

Inhaltsverzeichnis

Abkürzungsverzeichnis IV
1 Einleitung 1
2 Ausgangslage 4
2.1 Abgrenzung zu anderen Bereichen 4
2.2 Entwicklung und Zweck des Datenschutzes 5
2.3 Das Volkszählungsurteil 6
2.4 Neue Anforderungen 7
2.5 Systematik des geltenden Rechts bis zum 25.05.2018 8
3 Die DSGVO 10
3.1 Rechtsetzung 10
3.2 Aufbau der Verordnung 12
3.3 Allgemeine Bestimmungen 12
3.3.1 Gegenstand und Ziele 12
3.3.2 Anwendungsbereich 13
3.4 Fortschreibung der Grundsätze des Datenschutzes 15
3.4.1 Verbotsprinzip 15
3.4.2 Zweckbindung 16
3.4.3 Datenminimierung 16
3.4.4 Datensicherheit 17
3.5 Neuerungen/ Präzisierungen 17
3.5.1 Zum Verbotsprinzip: Die Zustimmung 17
3.5.2 Marktortprinzip und territoriale Neuerungen 19
3.5.3 Technisch-organisatorische Neuerungen 21
3.5.4 Betroffenenrechte 25
3.5.5 Aufsicht und Durchsetzung 27
3.6 Regelungsräume 28
4 Novelle des BDSG 31
4.1 Aufbau und Anwendungsbereich 32
4.2 Analyse 33
4.2.1 Die Betroffenenrechte 33
4.2.2 Der betriebliche Datenschutzbeauftragte 36
4.2.3 Der Beschäftigtendatenschutz 37
5 Ergebnisse 41
Thesen V
Anhang VI
Literatur- und Quellenverzeichnis X
Rechtsprechungsverzeichnis XV
Rechtsquellenverzeichnis XVI
Eidesstattliche Versicherung XVII

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BDSG	Bundesdatenschutzgesetz (gültig bis 25.05.2018)
BDSG-E	Entwurf zum BDSG vom
BDSG-neu	Bundesdatenschutzgesetz (Art. 1 des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU – DSAnpUG-EU vom 30. Juni 2017)
BfDI	Die Bundesbeauftrate für den Datenschutz und die Informationsfreiheit
BIU	Bundesverband Interaktive Unterhaltungssoftware e.V.
DGB	Deutscher Gewerkschaftsbund
DSB	Datenschutzbeauftragter
DSF	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSRL	Europäische Datenschutzrichtlinie
ErwGr	Erwägungsgrund (Erwägungsgründe der Datenschutz-Grundverordung)
GRCh	Die Charta der Grundrechte der Europäischen Union (Grundrechtscharta)
Rn.	Randnummer
SächsDSDG-E	Entwurf des Sächsischen Datenschutzdurchführungsgesetz
SMI SN	Sächsisches Staatsministerium des Innern

1 Einleitung

Die Verarbeitung von Informationen über Personen spielt im täglichen Leben der heutigen Informationsgesellschaft eine ständige Rolle. Einige Beispiele sollen den Blick auf die Thematik richten.

Bei einem Bezahlvorgang mit der Kreditkarte, ob im Geschäft oder beim Online-Shopping, werden Daten zur Kreditkarte des Zahlenden und Bankdaten des Zahlungsempfängers übertragen. Ergänzend zum Bezahlen wird hierzu häufig noch die Sammelpunktekarte vorgezeigt. Geräte wie Fitness-Armbänder übertragen Daten zum Gesundheitszustand, um diese zu speichern, auszuwerten und dem Nutzer zur Verfügung zu stellen. Möchte man sich vom Smartphone navigieren lassen, so werden Standortdaten übermittelt. Vor einigen Jahren noch futuristisch klingende Konzepte, wie das Smart Home (engl. für intelligentes Zuhause), werden heut rege beworben. Hierbei kommunizieren vernetzte Haushalts- und Multimediageräte, um dem Nutzer das Leben zu erleichtern.

Mit der Frage, was mit diesen Daten nach der Übertragung geschieht, beschäftigen sich hingegen die wenigsten Nutzer. Die zu den Diensten gehörigen Datenschutzbelehrungen werden meist ungelesen akzeptiert und Auswirkungen werden nicht bemerkt. Für den Nutzer sichtbar wird ein solcher Effekt beispielsweise bei dem Konzept des Search Engine Advertising (engl. für Suchmaschinenmarketing). Nicht nur Google nutzt dieses Geschäftsmodell. Informiert man sich beim Surfen mit einer Suchmaschine über bestimmte Produkte, werden einem in der darauffolgenden Zeit ähnliche Produkte durch Werbung auf Webseiten gezeigt. Die IP-Adresse, die beim Surfen im Netz übertragen wird und mit der das genutzte Endgerät identifizierbar ist, lässt Rückschlüsse auf das Interesse des Nutzers an Produkten zu.[1] „Der Vorwurf der Geschäftemacherei mit Daten ist ebenso zutreffend wie naiv. Die Nutzung von Plattformen und Internetdiensten ist die Leistung, die Google anbietet. Die Daten, die der Nutzer bei Google hinterlässt, sind die Gegenleistung“[2]. Es wäre also gutgläubig, davon auszugehen, dass alle anderen von Google angebotenen Dienste wie Cloud-Speicher oder E-Mail kostenlos seien. Der Preis, den man zahlen muss, sind personenbezogene Daten.

Man erkennt demnach an diesem Beispiel, dass es Geschäftsmodelle gibt, die mit Daten als zentrale Ressource arbeiten. Hinzu kommt eine gesamte Datenindustrie mit entsprechender Lobby. Um lukrativ zu sein, kommt es nun auf die Menge der Daten an. An dieser Stelle kommt Big Data zum Einsatz. Aufgrund der großen,

[1] Vgl. Janzik: Suchmaschinen-Advertising (SEA) Definition, (Abgerufen am 08.02.2018)
[2] Härting/Schneider: Das Dilemma der Netzpolitik, ZRP 2011, S. 233.

komplexen und schnelllebigen Datenmengen, die übermittelt werden, kommen Technologien zum Einsatz, die es ermöglichen, Daten automatisiert zu verarbeiten. Nur so ist es möglich, die große Datenmasse, die nicht mehr manuell verarbeitet werden kann, zudem intelligent zu verknüpfen (Smart-Konzepte). Das meiste Potential für Erfolg haben dabei in vielen Fällen Daten, die Personen zuzuordnen sind. Hier bildet sich also die Verknüpfung zur Problematik, die in der vorliegenden Arbeit betrachtet wird. Persönliche Daten sind ein schützenswertes Gut. Werden solche missbraucht, können Persönlichkeitsrechte verletzt werden. Es bilden sich an dieser Stelle Widersprüche zwischen den aktuellen gesellschaftlichen bzw. wirtschaftlichen Entwicklungen und dem Datenschutz heraus. Der technologische Fortschritt ermöglicht einerseits den Einsatz von Big Data. Andererseits beschränkt der Grundsatz der Datensparsamkeit die Entfaltung der Technologie rechtlich. Weiterhin entsteht ein Spannungsverhältnis zwischen verantwortungsvollem Umgang mit Daten und Automatisierung von Datenverarbeitung[3]. Zudem entwickelt sich eine digitalisierte Informationsgesellschaft, in der ein freier Datenverkehr nicht unterbunden werden sollte, vor allem nicht in einem europäischen Binnenmarkt.

Die europäische Datenschutzrichtlinie (DSRL) aus dem Jahr 1995 kann aufgrund der Entwicklung der letzten 25 Jahre und den heutigen Anforderungen, die sich daraus ergeben haben, nicht genügen. Es musste also einen neuen rechtlichen Datenschutzrahmen geben. Man könnte nun den Europäischen Datenschutztag am 28.Januar, zum Anlass nehmen, um für das Thema zu sensibilisieren. Es gibt jedoch noch weitere Gründe und ein zentrales Datum im Jahr 2018, warum es sich lohnt, sich mit dem Thema auseinanderzusetzen. Die Datenschutz-Grundverordnung (DSGVO) vom 27.04.2016 wurde im Amtsblatt der Europäischen Union verkündet und gilt verbindlich in allen Mitgliedstaaten ab dem 25.05.2018. Die Verkündung der Verordnung zwingt alle Mitgliedstaaten bestehende nationale Regelungen EU-rechtskonform anzupassen. Diese Dringlichkeit hat die Bundesrepublik Deutschland erkannt. Deshalb wird am 25.05.2018 gleichzeitig mit der Europäischen Regelung ein neues Bundesdatenschutzgesetz in Kraft treten. Daraus folgt, dass die sich aktuell verändernde Rechtslage ein grundlegendes Thema in Wirtschaft und Politik ist.

Der datenschutzrechtliche Umbruch soll in der vorliegenden Arbeit systematisiert werden. Es sollen die Auswirkungen der Datenschutz-Grundverordnung der Europäischen Union auf nationales Datenschutzrecht in Deutschland untersucht

[3] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 137, Rn. 566.

werden. Hierzu ist es notwendig die DSGVO auf Neuerungen hin zu analysieren. In diesem Zusammenhang wird das bisher geltende Bundesdatenschutzgesetz (BDSG) anhand ausgewählter Themenbereiche mit der Novelle verglichen. Analysiert wird, welche Forderungen und Einwände während des Gesetzgebungsvorgangs des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) maßgeblich waren. Dabei wird ausschließlich Artikel 1 des DSAnpUG-EU, nämlich die Neufassung des Bundesdatenschutzgesetzes (BDSG-neu), und deren Diskussion betrachtet. Abschließend soll der rechtliche Schutz nach Inkrafttreten der DSGVO und des BDSG-neu ansatzweise bewertet werden. Die Frage, ob man von einem wirklichen Umbruch im Datenschutzrecht sprechen kann, soll beantwortet werden.

Methodisch wird der Thematik mit einer Literaturanalyse begegnet. Es wird bereits bestehende Literatur über die DSGVO gesammelt und mithilfe neuer Fragestellungen untersucht. Primärdaten in Form von Plenarprotokollen werden hinzugezogen um die relevanten Themen im Gesetzgebungsvorgang mit einzubinden. Weiterhin wird, anhand ausgewählter Themen, ein Vergleich des alten BDSG mit der Neufassung vorgenommen. Es soll die grundlegende Struktur dargestellt werden und die wesentlichen Veränderungen aufzeigen.

Die vorliegende Arbeit wurde auf dem Stand der Literatur von Februar 2018 verfasst.

2 Ausgangslage

In diesem Kapitel soll eine Einordnung des Themas Datenschutz sowie dessen historische Entwicklung Gegenstand sein. Auf diese Ausgangslage wirken neue Anforderungen, die sich aus der technologischen Entwicklung ergeben haben ein und werden unter 2.4 aufgezeigt.

2.1 Abgrenzung zu anderen Bereichen

Um eine thematische Abgrenzung vorzunehmen, werden zunächst die Begriffe Datenschutz, Datensicherheit und Geheimschutz bzw. Verschwiegenheitspflichten aus der Wirtschaft, z.B. bei Banken oder Anwälten, erklärt.

Häufig werden die Begriffe Datenschutz und Datensicherheit im gleichen Atemzug verwendet. Unter Datenschutz versteht man den Schutz personenbezogener Daten vor missbräuchlicher Verwendung, im engeren Sinne der Erhebung, Verarbeitung und Nutzung dieser[4]. Für die Verarbeitung personenbezogener Daten gibt es gewisse Regeln zum Schutz vor Missbrauch. Mit diesem rechtlichen Rahmen wird sich auch die vorliegende Arbeit beschäftigen.

Zentraler Bestandteil des Datenschutzes sind personenbezogene Daten. Solche Daten sind gemäß Art. 4 Nr.1 der Datenschutz-Grundverordnung (DSGVO) „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen.“. Weiterhin ist eine Person identifizierbar, in § 3 Abs.1 des Bundesdatenschutzgesetz (BDSG) als „bestimmbar“ bezeichnet, wenn Sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;“ Gemäß Erwägungsgrund (ErwGr) 30 zur DSGVO können „natürlichen Personen […] unter Umständen [durch] Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen [identifiziert werden]“. Man erkennt hier eine sehr weite Auslegung der Bezeichnung der identifizierbaren Person. Anonyme Daten können nach dieser Definition nicht dazu zählen.

Datensicherheit bildet die Voraussetzung für effektiven Datenschutz aus technischer Sicht. Unter Datensicherheit versteh man das technische Ziel, Daten

[4] Vgl. § 1 BDSG.

jeglicher Art, also nicht nur personenbezogene, in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern.[5] Daten, wie z.B. Konstruktions- oder Projektpläne auf Servern von Unternehmen, sollten beispielsweise weder manipulierbar sein, noch verloren gehen können. Als zentrales Prinzip des Datenschutzes wurde auch die Gewährleistung von Datensicherheit in Art. 5 Abs. 1 lit. f und Art. 32 der DSGVO verankert[6].

Eine weitere Abgrenzung kann man zu der Verpflichtung zur Geheimhaltung von Daten ziehen. Es handelt sich dabei nicht um Datenschutz. In der Wirtschaft sind zum Beispiel Verschwiegenheitsverpflichtungen vor Vertragsschluss üblich. Im Arbeitsvertrag gibt es häufig eine Verschwiegenheitsklausel, in der geregelt ist, dass Firmengeheimnisse keinen unbefugten Dritten mitgeteilt werden dürfen. Allgemein bekannte Begriffe sind das Bankgeheimnis, das Anwaltsgeheimnis und die Verschwiegenheitspflicht von Ärzten. Gemäß § 203 Strafgesetzbuch wird der Verstoß gegen die Verschwiegenheitspflicht, auch in Ausübung vieler weiterer Berufe, unter Strafe gestellt.

2.2 Entwicklung und Zweck des Datenschutzes

Relevant wurde das Thema Datenschutz in der BRD mit der zunehmend automatisierten Datenverarbeitung und Datensammlung. Unter anderem nutzten Behörden im Sozial- und Steuerwesen seit den 1950er Jahren neue Technologien zur Datenverarbeitung für eine bessere Planung von zukünftigen Entwicklungen.[7] Dadurch sorgte sich die Bevölkerung vor der zunehmenden Informationsmacht des Staates und es entstand der Wunsch nach mehr Privatsphäre des Einzelnen.[8] Man erkennt also, dass der Ursprung und die Forderung nach Datenschutz zum einen in der Automatisierung der Datenverarbeitung lagen. Zum anderen ging es darum, dass „Staat und später auch Unternehmen gegenüber dem Einzelnen ein informationelles Übergewicht gewannen (Datenmacht)“[9].

Wegen dieses “Unbehagen[s] über die staatliche Datenmacht“[10] und zum Schutz vor Missbrauch dieser, beschloss bereits im Oktober 1970 Hessen als erstes Bundesland das Hessische Landesdatenschutzgesetz, um dem öffentlichen Druck vorzubeugen. Ziel war dabei die Einführung einer unabhängigen Kontrollinstanz im Sinne eines Datenschutzbeauftragten und die Abwehr gegen die staatliche

[5] Lackes/Siepermann: Gabler Wirtschaftslexikon, Stichwort: Datensicherheit, (Abgerufen am 28.02.2018)
[6] Vgl. BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.11.
[7] von Lewinski: Zur Geschichte von Privatsphäre und Datenschutz, 2012, S.28.
[8] Vgl. BPB: 27. Januar 1977: Das Bundesdatenschutzgesetz wird verabschiedet, (Abgerufen am 08.02.2018)
[9] von Lewinski: Zur Geschichte von Privatsphäre und Datenschutz, 2012, S.23.
[10] Ebenda, S. 28.

Datensammlung. Der Begriff Datenschutz wurde erstmals in die Rechtssprache eingeführt. Es folgten alle weiteren Bundesländer sowie ein Bundesdatenschutzgesetz sieben Jahre später. Bereits in dieser ersten Fassung stand inhaltlich der Schutz vor Missbrauch personenbezogener Daten im Zentrum des Gesetzes, vor allem auch gerichtet auf Unternehmen, hinsichtlich des Adresshandels. Ebenso war das grundsätzliche Verbotsprinzip mit Einwilligungsvorbehalt bereits integriert (siehe 2.3).[11] Die Bezeichnung des Gesetzes und wesentliche Grundsätze blieben über Weiterentwicklungen hinweg bestehen.

Konkret ist der Zweck des Datenschutzes, der Schutz des Rechts auf informationelle Selbstbestimmung sowie der Schutz vor Missbrauch personenbezogener Daten und die rechtliche Sicherung dieser Ansprüche. Über den Schutz des Einzelnen hinaus hat der Datenschutz ein „strukturelles Ziel: die Begrenzung jener Machtungleichgewichte, die durch die Informationsballung bei einzelnen Akteuren bestehen.“[12] Die bereits angesprochene Datenmacht bezieht sich heute nicht mehr nur auf den Staat, sondern vielmehr auf Datensammler aus der Privatwirtschaft.

Zur verfassungsrechtlichen Stellung dieses Rechts gibt es mehrere Perspektiven. Das Recht auf informationelle Selbstbestimmung ist nicht ausdrücklich im Grundgesetz verankert, wurde jedoch durch Rechtsprechung des Bundesverfassungsgerichts als daraus ableitbar erklärt (Siehe 2.3). Weiterhin ist das Recht auf informationelle Selbstbestimmung in Art. 8 der EU-Grundrechtscharta (GRCh)verankert. In Art. 33 der Sächsischen Verfassung wurde das konkrete Selbstbestimmungsrecht über eigene Daten aufgenommen.

2.3 Das Volkszählungsurteil

Die eben angesprochene Rechtsprechung auf Bundesebene wird nun näher erläutert, da sich daraus ein wesentlicher Einschnitt in die Entwicklung des Datenschutzrechts ergab. Ausgangslage war eine Verfassungsbeschwerde gegen das Volkszählungsgesetz von 1983. Es sollte eine Aktualisierung der veralteten Datenbestände in Form einer Volkszählung durchgeführt werden. Ziel der Erhebung war die maschinelle Weiterverarbeitung der erhobenen Daten durch öffentliche Hand.[13] Das Thema Datenschutz stand in diesem Zusammenhang erstmals in diesem Umfang in der Öffentlichkeit zur kontroversen, politischen Debatte und im Bewusstsein der Gesellschaft. Das Bundesverfassungsgericht erklärte und interpretierte am 15. Dezember 1983 aus dem verfassungsrechtlich gewährleisteten

[11] von Lewinski: Zur Geschichte von Privatsphäre und Datenschutz, 2012, S.23.
[12] Ebenda, S.32.
[13] Bieber: Datenschutz als politisches Thema, 2012, S.36.

Persönlichkeitsrecht (Artikel 2 Absatz 1 Grundgesetz) und der Menschenwürde (Artikel 1 Absatz 1 Grundgesetz) das Recht auf informationelle Selbstbestimmung. Dieses ist ein Recht des Einzelnen selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Die Zulässigkeit der staatlichen Einschränkung dieses neuen Grundrechts bestimmt sich weiterhin nur auf Grundlage einer verfassungsgemäßen Norm.[14]

Man erkennt hieran, dass es „kein absolutes Herrschaftsrecht des Einzelnen über ‚seine' Daten gibt"[15], da es nur einer Norm bedarf, die dieses Recht einschränken kann. Daraufhin entwickelte sich in Deutschland eine zersplitterte Rechtslandschaft hinsichtlich rechtlicher Einschränkungen des Rechts auf informationelle Selbstbestimmung. Eine „modifizierte Volkszählung" unter Beachtung der festgestellten Grundsätze fand dann erst 1987 statt.

2.4 Neue Anforderungen

In der bisher erörterten Ausgangslage spielte vorrangig die Datenmacht des Staats eine Rolle, da Anlagen zur elektronischen Datenverarbeitung in der Anfangszeit seiner Entwicklung für Unternehmen noch recht teuer waren. Mit dem Angebot für die breite Masse wurde die Nutzung solcher Anlagen auch für wirtschaftliche Unternehmen bezahlbar. Dadurch rückten im Laufe der 1980er und 1990er Jahre auch private Datenverarbeiter, wie Versicherungen und Kreditinstitute, in problematische Felder des Datenschutzes.[16] In diesem Zusammenhang entstand die Frage nach dem „Verhältnis zwischen dem Recht der Daten- ‚Besitzer' und dem Anspruch auf 'informationelle Selbstbestimmung' der Betroffenen"[17].

Noch problematischer wurde die Lage mit der Entwicklung und Nutzung des Internets. Mittlerweile gibt es Unternehmen, die als Unternehmensziel hauptsächlich die Datenverarbeitung verfolgen. Es stellt sich die Frage, welches Recht für solche Unternehmen, die Ihre Dienste durch das Internet anbieten können, gilt. Eine internationale Regelung für Datenschutz im Internet gibt es nicht und welches nationale Recht einschlägig ist, ist unklar. Noch schwieriger ist demnach die Frage nach der Durchsetzung des jeweils geltenden Rechts. Das ursprüngliche BDSG war für einen wesentlich engeren Anwendungsbereich entwickelt worden[18]. Weiterhin stellte die Entwicklung des Web 2.0 mit seinen sozialen Netzwerken, neue Anforderungen an den Datenschutz. Web 2.0 funktioniert hauptsächlich durch die

[14] Vgl. BVerfG, 15.12.1983.
[15] Härting/Schneider: Das Dilemma der Netzpolitik, ZRP, 2011, S. 234.
[16] Vgl. von Lewinski: Zur Geschichte von Privatsphäre und Datenschutz, 2012, S.31.
[17] Ebenda.
[18] Vgl. Härting/Schneider: Warum wir ein neues BDSG brauchen- Kritischer Beitrag zum BDSG und dessen Defiziten, ZD, 2011, S. 64.

freiwillige Preisgabe von personenbezogenen Daten. Oftmals findet die Preisgabe im großen Umfang jedoch unbewusst statt. Fraglich ist dann auch hier die Vereinbarkeit mit Anonymität und Datensparsamkeit. Der einzige Schutz hiervor besteht darin, sich dieser Technologie zu entziehen, sofern es keine effektiven Datenschutzregeln gibt.[19]

Wie bereits in der Einleitung benannt, gibt es weitere Technologien, die sich durch alle Lebensbereiche ziehen und sich in den Alltag der Informationsgesellschaft eingefügt haben. So ist grundsätzlich die Verarbeitung von Daten bezüglich des eigenen Zuhauses, von Bewegungsprofilen, Gesundheitsdaten, Einkaufsverhalten und durch Surfverhalten möglich geworden. Durch die Vernetzung von Gegenständen mit dem Internet und deren automatisierter Kommunikation wurden solche Geräte zu Alltagshelfern (Internet der Dinge).[20] Gleichzeitig wurden sie so aber auch zu Übertragungsschnittstellen von personenbezogenen Daten. Um diese neuen Anforderungen für den Gesetzgeber einzuordnen, wird im folgenden Unterabschnitt zunächst eine Bestandsaufnahme zur bestehenden Systematik im Datenschutzrecht in der BRD gemacht.

2.5 Systematik des geltenden Rechts bis zum 25.05.2018

Der folgende Abschnitt bezieht sich auf die im Anhang 1 dargestellte Übersicht.

Die Systematik beruht auf dem Grundsatz der Gesetzmäßigkeit und dem Rang von Normen. Es besteht das Verbot gegen höherrangiges Recht zu verstoßen. Auf europäischer Ebene besteht bis zum Inkrafttreten der DSGVO im Mai 2018 die Datenschutzrichtlinie 95/46/EG (DSRL). Die zu dem Zeitpunkt noch bestehende Europäische Gemeinschaft legte Mindeststandards für den Datenschutz in den Mitgliedstaaten zur Übermittlung von personenbezogenen Daten an Mitglieds- und Drittstaaten fest. 2001 wurde die Richtlinie in nationales Recht in der BRD umgesetzt. Auf verfassungsrechtlicher Ebene besteht, wie im Punkt 2.3 bereits erörtert, das Recht auf informationelle Selbstbestimmung, das aus dem Grundgesetz abgeleitet werden kann. In der Sächsischen Verfassung besteht ferner ein expliziter Artikel zu diesem Recht, der den wichtigsten Inhalt des Volkszählungsurteils wiedergibt. Auf Bundesebene gibt es ein allgemeines Datenschutzgesetz (BDSG) und vielfältige bereichsspezifische Datenschutzgesetze (z.B. das Telekommunikationsgesetz). Die konkreten Veränderungen im Anwendungsbereich (öffentliche und nichtöffentliche Stellen) nach Inkrafttreten des BDSG-neu wird im Kapitel 4

[19] Vgl. von Lewinski: Zur Geschichte von Privatsphäre und Datenschutz, 2012, S.31.
[20] Lackes/Siepermann**:** Gabler Wirtschaftslexikon, Stichwort: Internet der Dinge (Abgerufen am 12.02.2018)

erörtert. Das Bundedatenschutzgesetz eröffnet die Möglichkeit Landesdatenschutzgesetze zu erlassen. Sachsen hat diese Möglichkeit wahrgenommen und regelt speziell für alle Landes- und Kommunalbehörden Grundsätze des Datenschutzes. Auf landesrechtlicher Ebene gibt es demnach keine einschlägigen Normen für private Datenverarbeiter.

3 Die DSGVO

Die neuen Anforderungen, die sich aus dem vorherigen Kapitel ergeben, wurden auch auf Europäischer Ebene erkannt. Daraufhin wurde nach einer Lösung gesucht, die den neuen Sachverhalten entspricht. Die DSGVO soll ein entscheidender Schritt im Entwicklungsprozess des Datenschutzes sein. Experten sind der Meinung, dass sich „das Gesicht des Datenschutzrechts nachhaltig verändern“[21] wird.

3.1 Rechtsetzung

Bereits im Jahr 2012 wurde durch die Europäische Kommission vorgeschlagen, das Datenschutzrecht zu reformieren. Es folgte ein langwieriges Rechtsetzungsverfahren, „vier Jahre lang mit viel Mühe, mit langem Atem und mit sehr unterschiedlichen Interessen zwischen allen möglichen Beteiligten“[22]. Verabschiedet wurde dann am 27. April 2016 neben der DSGVO, eine weitere Richtlinie. Sie wird umgangssprachlich auch Richtlinie für Polizei und Justiz genannt und enthält Grundregeln für die Mitgliedstaaten bei der Datenverarbeitung zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder deren Vollstreckung.[23] Diese Richtlinie bedarf der Umsetzung in nationale Rechts- und Verwaltungsvorschriften bis zum 6.5.2018, in Ausnahmefällen auch bis 2023 oder 2026[24].

Im Gegensatz dazu bedarf die DSGVO grundsätzlich keiner weiteren Rechtsetzung in den Mitgliedstaaten und wird deshalb auch schneller seine Wirkung entfalten. Bei der DSGVO handelt es sich um eine Verordnung gemäß Art. 288 Abs. 2 AEUV. Sie ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat, ab dem 25.05.2018.[25] Es besteht ein Anwendungsvorrang vor Regelungen der Mitgliedstaaten und bestehende Regelungen dürfen der Verordnung nicht widersprechen.

Primärrechtliche Grundlage und somit auch verfassungsrechtliche Basis der Europäischen Union für den Schutz personenbezogener Daten bildet ausdrücklich Art. 8 der Grundrechts-Charta. Aus dem Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) kann die Regelungskompetenz, sowie die Schutzpflicht hinsichtlich des Datenschutzes entnommen werden.[26]

---

[21] Kühling/Martini: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW, 2016, S. 448.
[22] Deutscher Bundestag: Plenarprotokoll 18/221, S. 22176(D)
[23] Vgl. SMI SN: Datenschutzrecht für öffentliche Stellen - Dokumentation zum Themenportal, S.9. (Abgerufen am 07.02.2018)
[24] Vgl. Art. 63, Art. 65 Richtlinie (EU) 2016/680.
[25] Vgl. Art. 99 Abs. 2 DSGVO.
[26] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Einleitung Eu-DatSchGrVO Rn. 12, S. 27.

Die gewählte Handlungsform unterscheidet sich von der Europäischen Regelung, die bis zur Geltung der DSGVO besteht. Die bestehende DSRL 95/46/EG (siehe Punkt 2.5) von 1995, die durch die DSGVO aufgehoben wird, stellte die Mitgliedstaaten der EU vor die Herausforderung eigene Datenschutznormen zu erlassen[27]. Das Ziel war die Erreichung eines einheitlichen Datenschutzniveaus innerhalb der EU. So schätzte der Europäische Gerichtshof im Jahr 2011 noch ein, dass dieses Ziel der „grundsätzlich umfassende[n] Harmonisierung“[28] erreicht wurde. Nach wie vor bestehende nationale Regelungen störten den Binnenmarkt der EU jedoch weiterhin[29]. Es wurde in ErwGr 9 der DSGVO darauf hingewiesen, dass Datenschutzrecht in den Mitgliedstaaten „unterschiedlich gehandhabt wird, Rechtsunsicherheit besteht oder in der Öffentlichkeit die Meinung weit verbreitet ist, dass erhebliche Risiken für den Schutz natürlicher Personen bestehen, insbesondere im Zusammenhang mit der Benutzung des Internets“.

Die bisherige Niederlassung großer Software-Konzerne in Irland, als Zentrale für den europäischen Markt, ist ein Beispiel für die bestehende Problematik. Neben günstigen Steuersätzen und der Sprache war besonderer Grund hierfür das vergleichsweise niedrige, irische Datenschutzniveau. Bei der Nutzung dieser Anbieter gelten deshalb auch irische Normen. Die Kontrolle der Datenschutzbelange europäischer Kunden von Apple, Google, oder WhatsApp lag so in der Verantwortung vergleichsweise schwacher, irischer Datenschutzbehörden. Mit der DSGVO sollen unter anderem solche datenschutzrechtlichen Rückzugsorte innerhalb Europas ausgeschlossen werden.[30]

Es stellt sich die Frage, ob die Wahl einer anderen Handlungsform, nämlich einer Verordnung, dieser Anforderung der Harmonisierung besser gerecht werden kann. Mit einer Menge an Öffnungsklauseln, wird der Wechsel der Handlungsform jedoch kritisch betrachtet. Durch viele nationale Spielräume bei der Ausgestaltung wird die DSGVO in Teilen kritisch auch als „Richtlinie im Verordnungsgewand“[31] oder als „Hybrid“[32] bezeichnet.

Die konkrete Gestaltung der Verordnung unterlag während der Verhandlungen einem Wandel. Ursprünglich sollte die Bezeichnung *Grund*verordnung darauf abzielen, dass es ein Normenwerk mit grundlegenden und zentralen Bestimmungen

[27] ErwGr 173 zur DSGVO.
[28] EuGH, Urt. v. 24.11.2011, Az.: C-468/10, Rn. 29.
[29] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Einleitung Eu-DatSchGrVO Rn. 8, S.25f.
[30] Vgl. Schöneberg: Democracy - Hintergrund -Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[31] Kühling/Martini: Die Datenschutz-Grundverordnung, EuZW, 2016, S. 448.
[32] Kühling/Martini: Die DSGVO und das nationale Recht, 2016, S.1.

werden sollte. Die konkretisierende Ausgestaltung sollte der Kommission vorbehalten bleiben. Aufgrund von Bedenken hinsichtlich der Kompetenzen und Befugnisse der Kommission wurde dieses zweistufige Verfahren bis auf wenige Konkretisierungsfragen nicht durchgeführt. Wegen der begrifflichen Offenheit einiger Vorschriften, wird die DSGVO in den kommenden Jahren durch den Europäischen Gerichtshof bzw. durch die Datenschutzaufsichtsbehörden ausgelegt werden müssen.[33] Deshalb könnte man, entgegen vieler Meinungen gegenüber der DSGVO, auch von „zaghafte[r] Evolution statt Revolution“ [34] sprechen.

3.2 Aufbau der Verordnung

Hinsichtlich der Anzahl der Artikel hat sich die Verordnung gegenüber der Richtlinie, von 34 auf 99 Artikeln deutlich vergrößert.[35] Die DSGVO beinhaltet elf Kapitel und 173 zugehörigen Erwägungsgründe, welche keinen Normcharakter haben, jedoch zur Auslegung und Erklärung dieser dienen. Dabei ist die große Anzahl dieser Erwägungsgründe beachtlich. „Der textliche Umfang der einzelnen Erwägungsgründe korreliert dabei oftmals mit der politischen Brisanz, welche die Regelung in der Diskussion der europäischen Union hatte: Je umstrittener sie im Gesetzgebungsprozess war, desto ausführlicher fällt auch der Erwägungsgrund tendenziell aus.“[36]

3.3 Allgemeine Bestimmungen

Um von den Formalitäten hin zu den Inhalten der DSGVO zu kommen, stehen im folgenden Abschnitt die Art. 1 und 2 der DSGVO im Zentrum der Betrachtung. Dort werden grundlegende Aussagen getroffen, die den Gegenstand, die Ziele und den Anwendungsbereich der Verordnung erläutern.

3.3.1 Gegenstand und Ziele

Art. 1 der DSGVO besteht aus 3 Absätzen, welche Auslegungsgrundsätze darstellen, aber keine direkte Normwirkung besitzen. Das bereits in Gliederungspunkt 2.4 aufgezeigte Spannungsverhältnis zwischen Recht auf informationelle Selbstbestimmung (Art. 1 Abs. 2 DSGVO) und dem Ziel eines digitalen wirtschaftlichen Binnenmarktes (Art.1 Abs. 3 DSGVO) kommt zum Ausdruck. Nach dem Prinzip der begrenzten Einzelermächtigung kann die EU nur Regelungen treffen, für die sie von ihren Mitgliedstaaten die Kompetenz übertragen bekommen hat.[37] Wie bereits beschrieben, findet sich die primärrechtliche Grundlage für die DSGVO im Art. 16

[33] Vgl. Kühling/Martini: Die Datenschutz-Grundverordnung, EuZW, 2016, S. 450.
[34] Ebenda.
[35] Vgl. ebenda, S. 448.
[36] Vgl. ebenda, S. 450.
[37] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Art. 1 DS-GVO, Rn.1-2, S.35.

AEUV, auch wenn diese Grundlage nicht explizit genannt wurde. Es stehen also mit dem **freien Verkehr** personenbezogener Daten und dem **Grundrecht** jeder natürlichen Person auf Schutz personenbezogenen Daten (Art. 8 GRCh) zwei große Ziele am Anfang des Verordnungstextes. Somit konkretisiert die DSGVO das Grundrecht, welches laut Grundrechtscharta sogar „Menschenrecht und nicht Bürgerrecht“[38] ist. Die DSGVO beinhaltet hierzu „zahlreiche Vorschriften mit Schutzgesetzcharakter“[39]. Der Schutz gilt sowohl gegen den Staat als auch private Datenverarbeiter[40].

Gleichzeitig kann dieses Recht nicht uneingeschränkt sein, wie ErwGr 4 der DSGVO verdeutlicht. Demnach soll Datenschutz im Dienste der Menschheit stehen und unter Wahrung des Verhältnismäßigkeitsprinzips bei der Abwägung mit anderen Grundrechten beachtet werden.[41]

Art. 1 Abs.3 DSGVO macht außerdem deutlich, dass Datenschutz nicht fälschlicherweise als Argument für den Aufbau von Grenzen im Europäischen Binnenmarkt genutzt werden darf[42]. Das Funktionieren des Binnenmarktes gemäß Art. 26 Abs. 2 AEUV soll stattdessen mithilfe eines einheitlichem Datenschutzrechts verwirklicht werden.

Das soeben beschriebene zweistufige Schutzziel der Verordnung bildet gleichzeitig die neue Ober- und Untergrenze des Datenschutzniveaus. Werden Standards der DSGVO unterschritten, so verletzt man das Grundrecht aus Art. 8 GRCh. Setzt man den Datenschutz strenger an, als in der DSGVO gefordert, so verhindert man möglicherweise den freien Verkehr von Informationen auf dem Binnenmarkt und schadet Unternehmen im freien Wettbewerb.[43]

3.3.2 Anwendungsbereich

Im Art. 2 Abs. 1 DSGVO wird der sachliche Anwendungsbereich beleuchtet. Dies erfolgt so technologieneutral, dass zunächst alle Arten von automatisierten Datenverarbeitungsanlagen beinhaltet sind, auch wenn sie nur teilweise zur Verarbeitung genutzt werden. An dieser Stelle bedarf es der Definition des Begriffs Verarbeitung. Die DSGVO bestimmt den Begriff nach Art. 4 Nr. 2 sinngemäß als Vorgang im Zusammenhang mit personenbezogenen Daten. Solche Vorgänge beginnen bei der Erhebung und enden bei der Löschung. Die Aufzählung aus Art. 4

[38] Ernst In: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 1 DS-GVO, Rn. 7, S.11.
[39] Vgl. Pötters In: Gola, DS-GVO, 2017, Art. 1 DS-GVO, Rn. 13, S.137.
[40] Vgl. Ernst In: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 1 DS-GVO, Rn. 7, S.11.
[41] Vgl. ErwGr 4 zur DSGVO.
[42] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Art.1 DS-GVO, Rn.8, S. 36.
[43] Vgl. Pötters In: Gola, DS-GVO, 2017, Art. 1 DS-GVO, Rn. 24, S. 140.

DSGV ist jedoch nicht abschließend, erkennbar an der Einleitung mit „wie“. Hier kann man einen Rückblick auf die Einleitung dieser Arbeit zulassen. Die dort angesprochenen Smart-Home-Geräte oder Wearables, wie Fitness-Tracker, würden somit in diesen Anwendungsbereich fallen[44]. Weiterhin wird auch die nichtautomatisierte Datenverarbeitung erfasst, sofern die Speicherung in einem Dateisystem erfolgt. Das Dateisystem ist definiert als eine “strukturierte Sammlung personenbezogener Daten […]“[45]. Diese Form der nichtautomatisierten, also manuellen, Verarbeitung personenbezogener Daten in einer strukturierten Sammlung könnte man in Papierakten wiederfinden. Ausgehend von der zum Großteil digitalisierten Gesellschaft, kann man sagen, dass der Anwendungsbereich aus Art. 2 Abs. 1 DSGVO sehr weit ist und somit alle Fälle von Verarbeitung personenbezogener Daten erfasst.[46] An dieser Stelle soll noch einmal darauf hingewiesen werden, dass die DSGVO für Daten mit Personenbezug gilt. Nicht umfasst sind anonyme Informationen, gem. ErwGr 25 zur DSGVO.

Im Art. 2 Abs. 2 DSGVO werden vier Ausnahmen bestimmt, für die die DSGVO nicht gilt. In Abs. 2 lit a) und b) werden grundsätzlich Fälle ausgeschlossen, in denen personenbezogene Daten im Zusammenhang mit Tätigkeiten verarbeitet werden, die nicht in den Anwendungsbereich von Unionsrecht fallen und die mit der gemeinsamen Außen- und Sicherheitspolitik im Zusammenhang stehen. In ErwGr 16 wird als Beispiel für lit a) die nationale Sicherheit betreffende Tätigkeiten genannt.

Des Weiteren nimmt Abs. 2 lit c) die Fälle aus, in denen personenbezogenen Daten im persönlichen oder familiären Bereich verarbeitet werden. Dies kann ausdrücklich nur durch natürliche Personen erfolgen und es darf sich in keiner Weise um geschäftliche Nutzung handeln. Beispielsweise könnte diese sogenannte Haushaltsausnahme Adress- oder Geburtstagslisten betreffen. Die in Abs. 2 lit. d) benannten Verarbeitungen zur Verfolgung von Straftaten und zur Strafvollstreckung sind von der Anwendung der DSGVO ausgeschlossen, weil diese in den Anwendungsbereich der Richtlinie für Polizei und Justiz (3.1) einzuordnen sind. Die Mitgliedstaaten sollen in diesem Bereich eigene Regelungen treffen.[47]

Zusammenfassend kann man erkennen, dass im sachlichen Anwendungsbereich keine Unterscheidung zwischen öffentlichem und nichtöffentlichem Bereich, wie

[44] Vgl. Ernst In: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art 2 DS-GVO, Rn. 5, S.15.
[45] Art. 4 Nr.6 DSGVO.
[46] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Art.2 DS-GVO, Rn.5, S.40.
[47] Vgl. Ernst In: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art 2 DS-GVO, Rn. 11-23, S.17-19.

zuvor im deutschen Recht unterschieden wurde, gemacht wird.[48] An dieser Stelle ist eine erste Auswirkung auf nationales Recht erkennbar, welches es zu überarbeitenden gilt.

3.4 Fortschreibung der Grundsätze des Datenschutzes

„[…] Die Konzeption und weitgehend auch die Detailregelungen des geltenden Datenschutzrechts [werden durch die DSGVO] nicht grundlegend [verändert]. Vielmehr werden vielfach Bestimmungen der EG-Datenschutzrichtlinie 95/46 übernommen.“[49] Da sich das BDSG bereits auf die DSRL bezogen hat, sind die Regelungen der DSGVO auch im nationalen Recht zum Großteil bekannt gewesen.

In Art. 5 DSGVO werden verbindliche Grundsätze für die Verarbeitung personenbezogener Daten aufgezeigt. Diese acht Grundsätze heißen

- *Rechtmäßigkeit,*
- *Verarbeitung nach Treu und Glauben*
- *Transparenz*
- *Zweckbindung*
- *Datenminimierung*
- *Richtigkeit*
- *Speicherbegrenzung*
- *Integrität und Vertraulichkeit*

Durch den neunten Grundsatz aus Artikel 5 Abs. 2 DSGVO entsteht die Pflicht zur Rechenschaftslegung über die vorher genannten Bestimmungen. Diese Grundsätze der Datenverarbeitung finden sich in den weiteren Artikeln der DSGVO wieder und sind zum Teil aus der DSRL entwickelt worden oder hatten schon im BDSG bestand. Um Wiederholungen zu vermeiden, werden sie an der jeweils passenden Stelle erklärt. Weiterhin bereits inhaltlich bekannt ist der Begriff der personenbezogenen Daten (siehe 2.1).

3.4.1 Verbotsprinzip

Das grundlegende Verbotsprinzip mit Erlaubnisvorbehalt, also Einwilligung oder Erlaubnistatbestand, bleibt grundsätzlich beibehalten. Hierbei geht es um die Rechtmäßigkeit und den ersten Grundsatz aus Art. 5 DSGVO. Dieser wird konkretisiert in Art. 6 DSGVO. Dieses Prinzip meint, dass die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, die betroffene Person

[48] Vgl. von Lewinski In: Auernhammer: DS-GVO BDSG, 2017, Art.2 DS-GVO, Rn.40, S.47.
[49] Gola/Jaspers/Müthlein/Schwartmann: Datenschutz-Grundverordnung im Überblick, 2017, S.22.

hat die Zustimmung (oder auch Einwilligung) hierzu erteilt. Die Anforderungen an die Zustimmung haben sich hingegen verändert (siehe Punkt 3.5.1.). Weitere Ausnahmen von dem Verbotsprinzip gelten, wenn die Fallgruppen des Art. 6 DSGVO einschlägig sind. Beispielsweise dann, wenn die Verarbeitung zur Vertragserfüllung mit dem Betroffenen notwendig ist oder der Verantwortliche rechtlich dazu verpflichtet ist. Nur dann ist die Verarbeitung von personenbezogenen Daten auch rechtmäßig. Die Rechtmäßigkeit entbindet jedoch nicht davon, die Regeln der DSGVO zu beachten.[50]

Art. 9 DSGVO schreibt sensitiven, personenbezogenen Daten besonderen Schutz zu. Hierzu zählen Daten zur rassischen und ethnischen Herkunft, zu politischen Meinungen, religiösen Überzeugungen, Gesundheit und weitere. Die Verarbeitung solcher sensitiven Daten ist genauso grundsätzlich verboten, wenn nicht explizit eingewilligt wurde oder Ausnahmen nach Art. 9 Abs. 2 DSGVO bestehen. Durch die nationalen Konkretisierungsmöglichkeiten können Regelungen aus dem deutschen Sozial- und Gesundheitsrecht, wo es eben häufig um solche sensitiven Daten geht, weitgehend erhalten bleiben.[51]

3.4.2 Zweckbindung

Die Zweckbindung ergibt sich aus Grundsatz Art. 5 Abs. 1 lit. b) DSGVO und Art. 6 Abs. 4 DS-GVO. Personenbezogene Daten dürfen nach diesem Grundsatz nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Bei der Veränderung des Verarbeitungszwecks muss durch den Verarbeiter geprüft werden, ob der neue mit dem ursprünglichen Erhebungszweck vereinbar ist. Die hierfür nicht abschließenden Kriterien sind im Art. 6 Abs. 4 lit. a bis e DSGVO aufgezählt. Unter anderem müssen gemäß Art. 6 Abs. 4 lit. d DSGVO die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen beachtet werden.

3.4.3 Datenminimierung

Das Prinzip der Datensparsamkeit aus dem BDSG findet sich im Art. 5 Abs. 1 lit. c) DSGVO in Form der Datenminimierung wieder. Dem Prinzip nach „muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein“[52]. Hierzu werden Neuerungen im Punkt 3.5.3 erfasst.

[50] Vgl. BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.9f.
[51] Vgl. Gola/Jaspers/Müthlein/Schwartmann: Datenschutz-Grundverordnung im Überblick, 2017, S.40.
[52] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.10.

3.4.4 Datensicherheit

Weiterhin wurde die Gewährleistung der Datensicherheit in die DSGVO aufgenommen. Insbesondere Art. 25 DSGVO beschäftigt sich mit der technischen Gestaltung der Datensicherheit. Konkretisiert wird dieser Grundsatz durch eine Neuerung, die im Punkt 3.5.3 erläutert wird.

3.5 Neuerungen/ Präzisierungen

In dem folgenden Abschnitt werden Neuerungen betrachtet, die im Zusammenhang mit dem Inkrafttreten der DSGVO stehen. In manchen Teilen gibt es auch nur Präzisierungen aus bereits beaknnten Grundsätzen.

3.5.1 Zum Verbotsprinzip: Die Zustimmung

Bisher musste man der Datenverarbeitung aktiv widersprechen, z.B. in Form von Häkchen, die aus sogenannten Kontrollkästchen bzw. Checkboxen von elektronischen Formularen entfernt werden mussten. Es wurde also die Einwilligung vermutet. Das wird durch die DSGVO nicht mehr zulässig sein. Eine weitere Neuerung besteht darin, dass künftig einer Datenverarbeitung durch Unternehmen oder Institutionen durch eine klare Handlung zugestimmt werden muss. Das heißt, ein Häkchen müsste immerhin aktiv und freiwillig gesetzt werden und – bezogen auf die konkrete Datenverarbeitung – informiert abgegeben werden[53]. Daraus folgt auch, dass anders als im BDSG, die Schriftform nicht mehr erforderlich ist. Weiterhin muss die datenverarbeitende Stelle einen Nachweis zur Einwilligung vorweisen können. Das ergibt sich aus dem Grundsatz der Rechenschaftspflicht und aus ErwGr 42 zur DSGVO. Online sollte dies „durch die Dokumentation des ‚Einwilligungs-Klickverhaltens' der betroffenen Person ausreichen"[54].

Um die Problematik der freiwilligen Zustimmung plastisch zu beschreiben, kann man erklären, was bisher bei dem Download von Apps im Android-System aufgefallen ist. Beispielsweise forderten Apps die Zustimmung zum Zugriff auf Daten aus dem Adressbuch oder den Fotos, obwohl die App diese Informationen zum Erbringen der Leistung oder des Dienstes nicht verarbeiten müsste. Wird der Zugriff aber abgelehnt, konnte der Download nicht erfolgen. Es bestand also ein Zusammenhang zwischen Zustimmung und Vertrag. Es ist künftig nicht mehr möglich, die Zustimmung zu solchen dienstunabhängigen Verarbeitungen vorauszusetzen, damit der Vertrag zustande kommt. Weiterhin mussten vor der Nutzung

[53] Vgl. BayLDA: IX Einwilligung nach der DS-GVO, 2016 (Abgerufen am 12.03.2018)
[54] Ebenda.

der Dienste bisher häufig persönliche Daten angegeben werden. Die Neuerung besteht darin, dass es möglich sein muss, diese auch pseudonymisiert zu nutzen.[55]

„Wirtschaftsverbände kritisieren, dass auch die anonymisierte Verwendung persönlicher Daten einer gesonderten Zustimmung bedarf."[56] Die Frage nach dem Grade der Anonymität wird häufig diskutiert und wird unterschiedlich empfunden.
Ein weiterer Anspruch an die Einwilligung, der sich aus ErwGr 42 ergibt, ist, dass eine „vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden" soll. Dadurch sind sowohl ein Mindestgehalt für den Inhalt vorgeschrieben als auch Verklausulierungen verboten worden. Folge einer fehlenden oder nicht nach den Vorgaben gegebenen Einwilligung wäre die Rechtswidrigkeit der Datenverarbeitung, da dann das Verbotsprinzip (siehe 3.4.1) greifen würde. Hierfür kann ein entsprechendes Bußgeld verhängt werden.[57] Ein Problem zeigt sich bei der praktischen Betrachtung der Zustimmung in der täglichen Nutzung. In einem Ausschnitt des Films "Democracy - Im Rausch der Daten"[58], wird erklärt, dass der Wert einer Zustimmung im täglichen Gebrauch im Internet relativ gering sei. Am Beispiel des Kaufs eines Flugtickets wird erklärt, dass ein Angebot mit einem sehr günstigen Preis, das zeitlich begrenzt ist, eine schnelle Reaktion erfordert. Die Zustimmung würde einfach gegeben werden, da der Nutzer selbst weder Zeit noch Interesse daran hat, sich erst über Datenschutzbelange zu informieren.[59] Ein solcher Druck kann auch beispielsweise bei Angeboten zu ausverkauften Konzerttickets, die auf Online-Plattformen angeboten werden, bestehen.

Bei einer weiteren Neuerung geht es um den Datenschutz bei Kindern. Das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung personenbezogener Daten wird auf 16 Jahre festgesetzt. Die Rechtmäßigkeit ist ansonsten nur mit Einwilligung der Eltern gegeben. Das sollte vor allem im Zusammenhang mit sozialen Netzwerken wie Facebook und Kommunikationsdiensten wie WhatsApp schwierig werden, da nach US-Vorschriften hierfür momentan das Mindestalter von 13 gilt.[60] Die Öffnungsklausel in Art. 8 Abs. 1 Satz 3 DS-GVO bietet weiterhin die Möglichkeit eine niedrigere Altersgrenze festzulegen. Gemäß Marktortprinzip (siehe 3.5.2) müsste sich der Dienstanbieter jeweils an die

[55] Vgl. Schöneberg: Democracy- Hintergrund -Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[56] Vgl. ebenda.
[57] BayLDA: IX Einwilligung nach der DS-GVO (Abgerufen am 12.03.2018)
[58] Vgl. Videoausschnit Unter: Schöneberg, Democracy - Hintergrund-Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[59] Vgl. ebenda.
[60] Schöneberg: Democracy - Hintergrund-Was steht in der DSGVO? (Abgerufen am 14.02.2018)

nationale Altersgrenze, des Mitgliedsstaates halten, in dem Daten des Minderjährigen erhoben werden, sofern sie grenzüberschreitend tätig werden. Dies bildet neue Herausforderungen für Unternehmen, sofern es gegebenenfalls zu unterschiedlichen Altersgrenzen in den Mitgliedstaaten kommt. Die Frage der Umsetzbarkeit der Regelung scheint auch weiterhin problematisch. Mit Ausblick auf die Zukunft würden sich wohl in vielen Fällen Kinder unter 16 Jahre ohne Zustimmung der Eltern – und damit rechtswidrig – in sozialen Netzwerken anmelden. Anhand der Statistik in Anlage 3 kann man erkennen, dass 1,6 Millionen Facebook-Nutzer im Januar 2018 zwischen 13 und 17 Jahren alt waren. Nicht erfasst werden kann jedoch, welche Jugendlichen ein falsches Alter angegeben haben. Unabhängig davon müssten Einwilligungen der Erziehungsberechtigten für deutsche Kinder zwischen 13 und 16 Jahren nachgefordert werden.

Die Möglichkeit der Absenkung der Altersgrenze im Datenschutzrecht besteht, um diese an bestehende Jugendschutzvorschriften anzugleichen. Die Regelungen über die Einwilligung sind dabei unabhängig von der Geschäftsfähigkeit des Kindes gem. Art. 8 Abs. 3 DSGVO. Innenminister Thomas de Maizière erklärt zur möglichen nationalen Absenkung der Grenze auf den Minimalwert von 13 Jahren, dass darauf verzichtet wurde. „Wir halten das nicht für vernünftig; deswegen machen wir es nicht“[61], erklärt er in der zweiten Beratung zum DSAnpUG-EU. Kritisiert wurde diese Entscheidung durch Unternehmen der Spieleindustrie. Sie sehen ihre Unternehmensziele dadurch gefährdet. Für sie gestaltet sich die Gegebenheit problematisch, wenn z.B. ein 14-Jähriger legal ein Spiel mit Jugendschutzfreigabe von 12 Jahren kauft. Wenn die Datenverarbeitung über den Vertragszweck hinaus geht, so ist dann die Einwilligung der Eltern notwendig.[62] Es würde also die Pflicht entstehen, unter angemessener Anstrengung, Kontakt mit den Eltern gem. Art. 8 Abs. 2 aufzunehmen. Hier würde Interpretationsspielraum entstehen wann die Anstrengungen angemessen sind. Solche Rechtsunsicherheit bzw. zusätzliche Anstrengungen sind von der Industrie nicht gewollt, sollten jedoch kein ausschließlicher Grund für Anpassung durch den Gesetzgeber sein.

3.5.2 Marktortprinzip und territoriale Neuerungen

Die DSGVO hat nicht nur die Auswirkungen dahingehend, dass datenschutzrechtliche Rückzugsorte innerhalb Europas, wie unter Punkt 3.1 am Beispiel erklärt, nicht mehr möglich sind. Das Marktortprinzip, welches im Art. 3 Abs. 2 DSGVO

[61] Deutscher Bundestag: Plenarprotokoll 18/231, S. 23300(A)
[62] BIU: Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechtes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Abgerufen am 12.03.2018)

geregelt ist, besitzt auch Ausstrahlungswirkung auf Wirtschaftsunternehmen aus Drittstaaten. Voraussetzung für die Anwendbarkeit der DSGVO ist, „dass sich ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient“[63]. Eine „physische […] Betriebs- und Organisationsstrukturen in Europa“[64] ist dafür nicht notwendig. Diese Neuerung wird Konzerne, mit weltweiter Markttätigkeit, vor Herausforderungen stellen. „Verbraucherschützer […] begrüßen jedoch, dass sich künftig jedes Unternehmen an die DSGVO halten muss, das im europäischen Markt agiert.“[65] Auch im Deutschen Bundestag heißt es zu diesem Fortschritt: „Schluss mit dem Rosinenpicken beim europäischen Datenschutz: Unser Markt, unsere Regeln gelten für alle, ausnahmslos – auch für Unternehmen, die etwa aus den USA ihre Dienste in Deutschland anbieten.“[66]

Für die nähere Betrachtung bedarf es der Definition der Begriffe Verantwortlicher und Auftragsverarbeiter nach Art. 4 Abs. 1 Nr. 7 und 8 DSGVO. „‚Verantwortlicher‘ ist dabei die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Auftragsverarbeiter ist in dem Zusammenhang derjenige, der daraufhin im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.

ErwGr 23 zur DSGVO erläutert das Prinzip genauer. Die Verordnung soll gelten für diejenigen „[…] nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Verarbeitung dazu dient, […] betroffenen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten.“ Ausreichend ist dabei beispielsweise aber nicht die bloße Erreichbarkeit der Website des Verantwortlichen. Er muss bewusst auf dem Markt agieren, was durch das Angebot und mögliche Bestellbarkeit von Waren oder Dienstleistungen deutlich wird. Die Datenverarbeitung zur Beobachtung des Verhaltens von Personen in Europa, kann zum Beispiel über Tracking-Cookies erfolgen. Cookies sind Datenpakete die auf der Festplatte des Nutzers gespeichert werden, um sie später wieder zu identifizieren. Auf dieser Grundlage können persönliche Profile zur zielgruppenspezifischen Werbung erstellt werden.[67]

Eine weitere Auswirkung ist die Pflicht zur Bestellung eines Vertreters, solcher in den Anwendungsbereich der DSGVO fallenden Verantwortlichen, in der EU gem.

[63] Vgl. BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.18.
[64] DSK: Kurzpapier Nr. 7 Marktortprinzip S.1.
[65] Schöneberg: Democracy - Hintergrund - Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[66] Deutscher Bundestag: Plenarprotokoll 18/231, S. 23299(D)
[67] Vgl. DSK: Kurzpapier Nr. 7, S.1f.

Artikel 27 DSGVO. Bei Nichteinhaltung dieser Pflicht kann bereits Bußgeld drohen.[68] Nur so kann eine Zuordnung zu einer Aufsichtsbehörde gewährleistet werden, wenn es schon keinen Datenschutzbeauftragten gibt.

Der sogenannte One-Stop-Shop-Mechanismus aus Art. 65ff. DSGVO bewirkt, dass Unternehmen, die Daten in mehreren EU-Mitgliedstaaten verarbeiten, sich nur mit der Aufsichtsbehörde des Mitgliedsstaates auseinandersetzen müssen, in der sich ihr Hauptsitz befindet. Dieser alleinige Ansprechpartner wird federführende Aufsichtsbehörde genannt. Das Konzept soll praktische Vereinfachung und mehr Rechtssicherheit für Unternehmen mit sich bringen. [69]

Die Übertragung von personenbezogenen Daten an Drittländer oder an internationale Organisationen ist grundsätzlich verboten und nur unter Bedingungen des Kapitels 5 der DSGVO zulässig.[70] Drittländer sind Länder die nicht EU-Mitgliedstaaten sind und werden in der Praxis Drittstaaten genannt. Die Zulässigkeitsvoraussetzungen werden in einer zweistufigen Prüfung ermittelt. Zum einen müssen die Daten nach allen Vorschriften der DSGVO rechtmäßig verarbeitet worden sein und zusätzlich mindestens eine Anforderung der Art. 44ff. DSGVO einhalten. Zu diesen Anforderungen gehört, dass entweder ein Angemessenheitsbeschluss vorliegt, geeignete Garantien vorliegen oder Ausnahmen für bestimmte Fälle gelten. Angemessenheitsbeschlüsse werden durch die Kommission erlassen und stellen ein angemessenes Datenschutzniveau im Drittland fest. Einen solchen Beschluss gibt es für die USA (EU-US Privacy Shield). Die Datenübermittlung vorbehaltlich geeigneter Garantien zur Gewährleistung eines angemessenen Schutzniveaus richten sich nach Art. 46 DSGVO. Zu den Ausnahmetatbeständen des Art. 49 DSGVO zählt beispielsweise die ausdrückliche Einwilligung der betroffenen Person oder wichtige Gründe des öffentlichen Interesses. Laut ErwGr 112 zur DSGVO umfasst das öffentliche Interesse insbesondere die internationale behördliche Zusammenarbeit von Wettbewerbs-, Steuer- oder Zollbehörden.[71]

3.5.3 Technisch-organisatorische Neuerungen

Artikel 32 DSGVO spricht von „geeignete[n] technische[n] und organisatorische[n} Maßnahmen“, die unter Abwägung mit anderen Gesichtspunkten zu mehr Sicherheit bei personenbezogenen Daten führen sollen.

[68] Vgl. ebenda.
[69] Vgl. Der Sächsische Datenschutzbeauftragte: Datenschutz-Grundverordnung (DS-GVO) kurz erläutert, S.1 und BayLDA: XIII Der One Stop Shop (Abgerufen am 12.03.2018)
[70] Vgl. Art. 44 DSGVO.
[71] Vgl. DSK, Kurzpapier Nr. 4, S.1.

Zwei eng miteinander verbundene neue Konzepte sind Privacy by Design und Privacy by Default. Die Konzepte sind in Art. 25 DSGVO verankert. Datenschutz soll durch Technik- oder Softwaregestaltung bereits in der Planung (Design) und durch datenschutzfreundliche Standardeinstellungen (Default) verbessert werden. So können elektronische Geräten verbraucher- und datenschutzfreundlich werden.[72] Beispielsweise könnte man hier ein Produkt, wie einen vernetzten Kühlschrank nennen, der selbstständig erkennt, wenn ein Lebensmittel aufgebraucht ist und auf einem Display die Neubestellung anbietet. In diesem Fall müsste durch Privacy by Design ermöglicht werden, den Kühlschrank auch offline, ohne personenbezogene Datenverarbeitung nutzen zu können. Die Grundfunktionen müssen trotzdem funktionieren. Privacy by Default bedeutet in dem Zusammenhang, dass die Grundeinstellung auf Offlinebetrieb liegt und nach der Anschaffung und Inbetriebnahme nicht erst in den Einstellungen darauf umgestellt werden muss.[73]

Das Prinzip der Datensparsamkeit**,** bekannt aus dem bisher geltenden Recht, wird durch den Begriff der Datenminimierung in Art. 5 DSGVO ersetzt. „Dieser ist jedoch nach Einschätzung von Datenschutzexperten wesentlich weiter gefasst und ermöglicht grundsätzlich auch größere Datensammlungen“[74]. In diesem Zusammenhang bedeutet dies eine Lockerung, gerade in Zeiten von Big Data. Hierbei ist jedoch auch jeder Nutzer selbst gefragt, sparsam mit der Preisgabe seiner Daten zu sein. Prof. Niko Härting betrachtet die Fortschreibung und Präzisierung des Begriffs kritisch. „Daten sind der Rohstoff der Kommunikation und Information. ‚Datenminimierung‘ heißt daher zugleich ‚Kommunikations- und Informationsminimierung‘. Dies ist sozialschädlich. Eine freie Gesellschaft braucht nicht weniger, sondern mehr Kommunikation“[75] Auch im Deutschen Bundestag wurde diese Entwicklung erkannt. „Das Verständnis eines Datenschutzes im Sinne möglichst großer Datensparsamkeit hat sich auch durch die technische Entwicklung überholt.“[76] Zu den technisch-organisatorischen Gegebenheiten aus der DSGVO gehört auch die Pseudonymisierung, definiert im Art. 4 Nr. 5 DSGVO. Pseudonymisierte personenbezogene Daten können demnach nur durch Hinzuziehung weiterer Informationen einer Person zugeordnet werden. Man könnte sagen, es handelt sich um ein Zwischenstück zwischen anonymen und personenbezogen Daten. Gemäß

[72] Vgl. Schöneberg: Democracy – Hintergrund-Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[73] Vgl. Brugugnone: Digitalisierung und Datenschutz: Neue Herausforderungen für Unternehmen (Abgerufen am 27.02.2018)
[74] Berufsverband der Rechtsjournalisten e.V.: Datensparsamkeit in BDSG & DSGVO | Datenschutz 2018, (Abgerufen am 01.03.2018)
[75] Härting: Warum “Datenminimierung” kommunikations- und innovationsfeindlich ist (Abgerufen am 17.02.2018)
[76] Deutscher Bundestag. Plenarprotokoll 18/221, S.22177(D)

Erwägungsgründe 28 und 29 zur DSGVO befreit die Pseudonymisierung aber nicht von der Anwendung anderer Datenschutzmaßnahmen. Solche Maßnahmen sind ausdrücklich gewünscht, da sie die Risiken für die betroffenen Personen senken können.

„Ausdrückliche Regelungen zu Big Data finden sich im Datenschutzrecht bisher nicht.“[77] Grundsätzlich muss man für die datenschutzrechtliche Betrachtung von Big Data unterscheiden zwischen der Verarbeitung personenbezogener und nichtpersonenbezogener Daten, wie bei Wettervorhersagen oder anonymen, kollektiven Wahlprognosen. Sind personenbezogene Daten im Spiel, werden diese im Big Data Konzept aus verschiedenen Quellen und Kontexten zusammengefügt und verarbeitet. Somit ist die DSGVO zu beachten. Das Konzept scheint dabei unvereinbar mit dem Grundsatz der Datenminimierung und dem Zweckbindungsprinzip zu sein. Problematischer wird es aber, wenn sich aus anonym erhobenen Daten durch die Verknüpfung miteinander, später persönliche Merkmale prognostizieren lassen. Bei der Betrachtungsweise besteht der Personenbezug nicht am Anfang der Verarbeitung, sondern am Ende. Eine Person gibt sozusagen keine personenbezogenen Daten ein, die schützenswert sind, sondern wird durch Big Data erst identifiziert.[78] Häufig im Zusammenhang mit Big Data stehen Wahrscheinlichkeitsprognosen und die Begriffe Profiling und Scoring. Profiling gem. Art. 4 Nr. 4 DSGVO beinhaltet die automatisierte Datenverarbeitung zur Profilbildung von (potentiellen) Kunden, um beispielsweise Vorhersagen zu treffen, für welche Produkte diese sich interessieren könnten. Eine spezielle Form derartiger Profilbildung ist das Scoring und wird häufig für die Prüfung der Kreditwürdigkeit von Personen eingesetzt. Es werden Daten aus verschiedenen Lebensbereichen nach mathematisch-statistischen Analyseverfahren ausgewertet. Es ergibt sich dann ein Wert, der eine „automatisierte Einzelentscheidung“ gem. Art 22 DSGVO zur Kreditausgabe trifft.[79] Solch eine Entscheidung, mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung für den Betroffenen, die ausschließlich aufgrund des Scorings erfolgt, ist nicht zulässig. „Strittig ist hier bislang die Auslegung der ‚rechtlichen Wirkung‘ und der ‚in ähnlicher Weise erheblichen Beeinträchtigung‘“[80]. Laut Verbraucherzentrale Bundesverband gebe es bei dem Verfahren einen rechtlichen Rückschritt durch die Verordnung. Streitthema ist hier der Einfluss von ungeklärten

[77] Roßnagel/Geminn/Jandt/Richter: Datenschutzrecht 2016 „Smart“ genug für die Zukunft?, 2016, S.79.
[78] Vgl. ebenda, S. 26-28.
[79] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 147 Rn. 598-599.
[80] Härting**:** Datenschutzbehörden und die DSGVO | HÄRTING Rechtsanwälte (Abgerufen am 17.02.2018)

Verbindlichkeiten in das Scoring, was in Deutschland verboten sei, in der Verordnung jedoch wieder zugelassen würde.[81]

Eine der wichtigsten Neuerungen der DSGVO gegenüber dem BDSG ist, dass Unternehmen ein Datenschutzkonzept besitzen müssen. Für den Fall, dass die Einführung einer neuen Technologie vielleicht den Datenschutz gefährden würde, müssen die Unternehmen eine Datenschutz-Folgenabschätzung (DSF) vornehmen.[82] Es stellt sich also die Frage, wann diese mögliche Gefährdung zutreffend ist. „Bisher gibt es noch keine Black-/White-Listen von Seiten der Aufsichtsbehörden, anhand derer man abgleichen kann, ob man verpflichtet ist eine [DSF] durchzuführen. Darüber hinaus ist es strittig, wann ein ‚hohes Risiko' für die Rechte und Freiheiten natürlicher Personen besteht […]"[83]. Die Datenschutzkonferenz ist der Meinung, dass „die Datenschutz-Folgenabschätzung […] ein sinnvolles Instrument zur systematischen Risikoeindämmung" darstellt und „rechtzeitig auf den Weg gebracht [helfe,] die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen [sowie] die Pflichten nach der Grundverordnung umzusetzen"[84].

Der Einsatz des betrieblichen Datenschutzbeauftragten (DSB) richtet sich nach Art. 37 Abs. 1 lit. b und c DSGVO. Die DSGVO sieht vor, dass nur in zwei Fällen betriebliche Datenschutzbeauftragte zu bestellen sind. Voraussetzung ist, dass die Kernaktivität des Unternehmens die „umfangreiche regelmäßige und systematische Überwachung" von Betroffenen erfordert oder die „umfangreiche Verarbeitung" sensitiver Daten nach Art. 9 DSGVO darstellt.[85] Betrachtet man dies in der Praxis wären nur die wenigsten Unternehmen demnach verpflichtet zur Bestellung eines betrieblichen DSB. Es liegt also an der Ausgestaltung durch den nationalen Gesetzgeber (siehe Punkt 4.2.2). Die Aufgaben des DSB gem. Art. 38 und 39 DSGVO liegen in der Sensibilisierung der Mitarbeiter hinsichtlich Datenschutzfragen und der Durchführung der eben genannten Folgenabschätzung. Der DSB ist weiterhin Ansprechpartner für Betroffene und ihre Rechte im Zusammenhang mit dem Unternehmen und für die Aufsichtsbehörden. Dies erfordert die Bekanntgabe des Namens des DSB.[86]

---

[81] Vgl. Schöneberg: Democracy - Hintergrund-Was steht in der DSGVO? (Abgerufen am 14.02.2018)
[82] Vgl. Schöneberg: Democracy - Hintergrund-Was steht in der DSGVO? (Abgerufen am 14.02.2018) und Vgl. DSK: Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.
[83] Härting**:** Datenschutzbehörden und die DSGVO | HÄRTING Rechtsanwälte (Abgerufen am 17.02.2018)
[84] Vgl. DSK: Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.
[85] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 2.
[86] Vgl. ebenda, S. 1-6.

3.5.4 Betroffenenrechte

Die Informationspflicht im Zuge der Transparenz beginnt bereits bei der Erhebung von Daten gemäß Art. 12ff. DSGVO. Je nachdem, ob die Daten direkt vom Betroffenen durch dessen Mitwirkung erhoben werden (Art. 13 DSGVO) oder nicht direkt erhoben werden (Art. 14), gelten unterschiedliche Anforderungen an die Information und Benachrichtigung.

Aus dem Grundsatz der Transparenz ergibt sich weiterhin für Betroffene das Recht auf Auskunft hinsichtlich der sie betreffenden Daten. Sie haben das Recht diese in einem „strukturierten, gängigen und maschinenlesbaren Format zu erhalten“, beispielsweise dem Portable Document Format (PDF). Art. 15 Abs. 1. DSGVO ist damit grundsätzlich keine Neuerung, nur die Anforderungen an die Auskunft sind durch die Bestimmungen der DSGVO gestiegen. Zunächst haben Betroffene das Recht zu erfahren, ob der Verantwortliche personenbezogene Daten über sie verarbeitet und wenn ja, auch welche. Eine konkrete Neuerung besteht darin, dass der Verantwortliche zusätzlich Auskunft geben muss über die im Katalog des 15 Abs. 1 lit a) bis h) DSGVO aufgezählten Umstände, wie den Verarbeitungszweck oder die geplante Speicherdauer. Während der Auskunftserteilung ist darauf zu achten, dass angemessene Sicherheitsanforderungen gewährleistet werden. Die Anfrage zur Auskunft ist unverzüglich zu beantworten, mindestens aber innerhalb eines Monats nach Eingang. Eine Kopie der verarbeiteten personenbezogenen Daten muss kostenlos zur Verfügung gestellt werden.[87] Laut Art. 12 Abs. 5 DSGVO kann bei „unbegründeten oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anträgen“ ein Entgelt erhoben werden oder die Bearbeitung mit Begründung verweigert werden. Kritisch betrachtet, könnte die Auskunft über Daten die z.B. Facebook von einem Betroffenen besitzt so umfangreich sein, dass der Betroffene durch die Auskunft zu seinem Persönlichkeitsprofil überfordert ist und diese am Ende wenig Informationsgehalt besitzt.[88]

Zu den Betroffenenrechten gehört auch Berichtigung und Löschung aus Art. 16ff. DSGVO. In vielen Fällen gelangen personenbezogene Daten ohne die Absicht des Betroffenen in das Internet und sind dann für jeden auffindbar. „Anders als das menschliche Gehirn, das den ganz überwiegenden Teil der Informationen, die wir mit unseren fünf Sinnen wahrnehmen, sofort wieder vergisst (‚löscht‘), ist

[87] Vgl. Intersoft Consulting: Diese Auskunftsrechte haben Betroffene nach der DSGVO, (Abgerufen am 19.02.2018)
[88] Vgl. Roßnagel/Geminn/Jandt/Richter: Datenschutzrecht 2016 „Smart“ genug für die Zukunft?, 2016, S. 101.

die Speicherung digitaler Informationen umfassend, ungefiltert und im Prinzip dauerhaft."[89]

Aus dem Grundsatz der Datenminimierung ergibt sich, dass die Datenspeicherung auf ein notwendiges Maß begrenzt werden soll. Das Recht auf Löschung, bzw. auf Vergessenwerden, in Art. 17 DSGVO gilt grundsätzlich bei rechtswidriger weiterer Speicherung und Nutzung.[90] Das heißt, wenn Daten nicht mehr benötigt werden oder wenn die Einwilligung widerrufen wird, ist der Verantwortliche zur Löschung verpflichtet. Es besteht also ein legitimes Interesse daran, Daten über sich aus dem Internet löschen zu wollen, unabhängig von der Qualität und Richtigkeit der Daten. Es soll dadurch ein Ausgleich zwischen Betroffenenrecht und Recht auf freien Informationsfluss geschaffen werden.

Verantwortliche sind aus diesem Recht heraus verpflichtet, die Originalquelle zu löschen und darüber hinaus, die Information über die beantragte Löschung weiterzugeben, sodass im Fall von öffentlich gemachten Daten auch alle weiteren entfernt werden. „Das „Recht auf Vergessenwerden" gem. Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung" verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, einer breiten Öffentlichkeit zugänglich sind."[91] Das heißt Betroffenen steht eine stärkere Unterstützung gegenüber Dritten bei der Durchsetzung des Anspruchs zu. Öffentliche Beiträge im Internet dürfen dann durch keine Suchmaschine mehr auffindbar sein. Was Löschung genau heißt, lässt die DSGVO jedoch offen. Technisch wird das Recht wahrscheinlich nicht durchsetzbar sein. „Ein Computer vergisst grundsätzlich nur das, was er auf ausdrücklichen Befehl vergessen – in seiner Sprache löschen – soll."[92] Wie soll es nun also technisch möglich werden sowohl die Ursprungsquelle des Uploads als auch jegliche Zwischenspeicherungen und Verlinkungen zu löschen. Screenshots, also Abbildungen des Inhaltes von Webseiten können weiterhin jederzeit durch kostenlose Software erstellt und gespeichert werden.

Die Berichtigungspflicht aus dem BDSG wird in der DSGVO umgewandelt in das Berichtigungsrecht des Betroffenen. Die unverzügliche Berichtigung falscher Angaben oder unvollständiger Daten ist nach Art. 16 DSGVO vorzunehmen.[93] Vom

[89] Nolte**:** Zum Recht auf Vergessen im Internet. ZRP, 2011, S. 236.
[90] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 171 Rn. 700.
[91] DSK: Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden".
[92] Nolte: Zum Recht auf Vergessen im Internet. ZRP, 2011, S. 236.
[93] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 168 Rn. 687-689.

Betroffenen als unrichtig bezeichnete Daten müssen bis zur Klärung gesperrt werden, ebenso wenn der Widerspruch geprüft wird.[94]

Das Widerspruchsrecht für Betroffene aus Art. 21 DSGVO besagt, dass jederzeit gegen die Verarbeitung, auch wenn vorher eingewilligt wurde, Widerspruch eingelegt werden kann. Insbesondere gegen Direktwerbung und Profiling greift dieses Recht. Unter Abwägung des Interesses der betroffenen Person mit nachgewiesenen, zwingend schutzwürdigen Gründen für die Verarbeitung durch den Verantwortlichen kann der Widerspruch im Ergebnis ausnahmsweise erfolglos sein. Auf diese Rechte muss bereits bei der ersten Kommunikation, gesondert von anderen Informationen, hingewiesen werden.[95]

3.5.5 Aufsicht und Durchsetzung

Wie in Anlage 2 dargestellt, baut sich das Aufsichtssystem aus mehreren Ebenen auf. Zunächst steht der Betroffene, mit seinen Eigenschaften als Bürger, Kreditnehmer usw. an der Basis. Er kontrolliert auf erster Ebene, welche Daten er von sich preisgibt. Bereits in der ersten Kommunikation mit Unternehmen muss er über seine Rechte im Datenschutz, die soeben unter Punkt 3.5.4 erläutert wurden, in Kenntnis gesetzt werden. Bei Datenschutzverstößen in Unternehmen können Verbraucherverbände, die Rechte von Betroffenen übertragen bekommen und auf Unterlassung und Beseitigung hinwirken. Unternehmen, welche nach DSGVO verpflichtet sind, einen DSB zu bestellen, haben diesen bei der zuständigen Aufsichtsbehörde zu melden. Der bestellte DSB wirkt auf die Umsetzung der DSGVO im Unternehmen hin, kontrolliert somit auf zweiter Ebene, ist direkter Ansprechpartner für die Aufsichtsbehörde und hat eine besondere Verschwiegenheitspflicht hinsichtlich der Daten der Betroffenen. Die Aufsichtsbehörden, die nach Landesrecht zuständig sind, überwachen, kontrollieren und beraten auf staatlicher Ebene diese Umsetzung im privatwirtschaftlichen Bereich. Beschwerden von Betroffenen ist durch diese nachzugehen und aufzuklären. Jeder Bürger kann sich an die staatlichen Aufsichtsbehörden wenden. Die Aufgaben und Befugnisse richten sich nach Art. 57 und 58 DSGVO.

Alle öffentlichen Stellen haben gleichwohl einen Datenschutzbeauftragten zu bestellen. Aufsichtsbehörde sind jeweils die Bundesdatenschutzbeauftragte für Bundesbehörden und die Landesdatenschutzbeauftragten für Landes- und Kommunalbehörden, sowie bereits beschrieben, alle privatwirtschaftlichen Stellen.

[94] Vgl Härting: Datenschutz-Grundverordnung, 2016, S. 168, Rn. 687-690, 710.
[95] Vgl. Gola/Jaspers/Müthlein/Schwartmann: Datenschutz-Grundverordnung im Überblick, 2017, S.54f.

Die Umsetzung des Beschwerderechts hat der Datenschutzbeauftragte in Baden-Württemberg bereits gut vorbereitet. Es wurde ein Online-Formular zur einfacheren Einreichung und schnelleren Bearbeitung eingerichtet.[96] In Sachsen hingegen müsste man zunächst nach den Kontaktdaten des Datenschutzbeauftragten suchen und daraufhin Kontakt aufnehmen.

Auf Europäischer Ebene gibt es den Europäischen Datenschutzausschuss. Er ist ein Gremium, bestehend aus je einer Aufsichtsbehörde jedes Mitgliedstaats der EU. Er dient zur einheitlichen Auslegung der DSGVO in den Aufsichtsbehörden und koordiniert das Kohärenzverfahren.[97] ErwGr 135 beschreibt hierzu, dass ein solches Kohärenzverfahren für die Zusammenarbeit zwischen den Aufsichtsbehörden eingeführt werden muss. Neben der Klärung von Einzelfragen sollen in diesem Verfahren auch „gemeinsame Positionen, Stellungnahmen und Richtlinien“[98] zu bestimmten Auslegungsfragen erstellt werden.

Die wichtigsten Errungenschaften sind, nach der Meinung von Jan Philipp Albrecht, Grünen-Politiker im EU-Parlament, die Sanktionen**.** Sie werden die Einhaltung der DSGVO veranlassen.[99] Der Bußgeldrahmen aus Art. 83 DSGVO für Datenschutzverstöße ist drastisch erhöht worden. Im BDSG war die Obergrenze bei 300.000€ für schwere Verstöße. Die DSGVO hingegen sieht beträchtlichere Bußgelder vor. Bei Verstößen gegen bestimmte Artikel werden 10 Millionen Euro oder bis zu zwei Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres des Unternehmens fällig. Verstöße gegen andere Artikel können bis zu 20 Millionen Euro oder bis zu 4 Prozent des erzielten Jahresumsatzes kosten, je nachdem was höher ist. Die Bußgelder sollen in jedem Fall „wirksam, verhältnismäßig und abschreckend“[100] sein.[101]

3.6 Regelungsräume

Neben den Grundsätzen und Neuerungen bietet die DSGVO an vielen Stellen sogenannte Regelungsräume für nationale Gesetzgeber. „Zumindest die EU-Kommission legt Wert darauf, dass der Begriff ‚Öffnungsklausel‘ nicht verwendet wird, da dieser implizieren würde, dass Regelungen erlassen werden könnten, die den Regelungen der DSGVO widersprechen, [was] nicht zulässig [wäre].“[102]

[96] Unter: https://www.baden-wuerttemberg.datenschutz.de/online-beschwerde/
[97] Vgl. Gola/Jaspers/Müthlein/Schwartmann: Datenschutz-Grundverordnung im Überblick, 2017, S.65.
[98] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S. 21.
[99] Schöneberg: Democracy – Hintergrund - Interview mit Jan Philipp Albrecht (Abgerufen am 22.02.2018)
[100] Art. 83 Abs. 1 DSGVO.
[101] Vgl. Gola/Jaspers/Müthlein/Schwartmann: Datenschutz-Grundverordnung im Überblick, 2017, S.62ff.
[102] Hülsmann: DSGVO – Expertenwissen für die Praxis (Abgerufen am 21.02.2018)

Stattdessen könnte man die Regelungsräume klassifizieren in die Kategorien: Konkretisierungsklauseln, Optionen, Ausnahmen und Regelungsaufträge[103].

Eine Konkretisierungsklausel findet man beispielsweise im Art. 6 Abs. 1 lit. e) und c) DSGVO. Der nationale Gesetzgeber der Mitgliedstaaten kann demnach die Rechtmäßigkeit der Verarbeitung bei gesetzlicher Verpflichtung und die Rechtmäßigkeit der Verarbeitung bei Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt konkretisieren. Kann heißt dabei, dass die Regelung auch ohne Konkretisierung Bestand hat. Im Bereich Beschäftigtendatenschutz könnten spezielle, konkretisierende Regelungen erlassen werden, die jedoch den Anforderungen des Art. 88 nicht widersprechen dürften. Somit gibt es bei der Konkretisierung weder eine Verschärfung noch eine Lockerung.
Optionen sind Öffnungen, die der Gesetzgeber wahrnehmen kann, um Regelungen zu treffen, es besteht jedoch keine Pflicht hierzu. ErwGr 27 sieht beispielsweise vor, dass Mitgliedstaaten Regelungen zu Daten von Verstorbenen festlegen oder nach Art. 8 DSGVO die Altersgrenze für die zulässige Einwilligung bis auf 13 Jahre herabsetzen können. Bei Optionen kann demnach entschieden werden, ob überhaupt zusätzlich in einem bestimmten Bereich etwas geregelt wird. Weitere solcher Optionen bestehen im Klagerecht für Vereine, bei Bußgeldern im öffentlichen Bereich oder der Verpflichtung zur Bestellung von betrieblichen Datenschutzbeauftragten.
Eine weitere Möglichkeit ist es, Ausnahmen von bestimmten Regelungen zuzulassen. Insbesondere die Verarbeitung zu Archivzwecken im öffentlichen Interesse, zu wissenschaftlichen, statistischen oder historischen Forschungszwecken gem. Art. 89, Abs. 2 und 3 DSGVO bilden solche Ausnahmen. Hierzu zählt auch die Möglichkeit der Beschränkung von Betroffenenrechten gem. Art. 23 DSGVO, sofern es zur „Wahrung bestimmter öffentlicher Interessen erforderlich ist. Dabei sind der Verhältnismäßigkeitsgrundsatz und der Wesensgehalt der Grundrechte zu beachten. Einschränkungen sind beispielsweise aus Gründen des Schutzes der nationalen und der öffentlichen Sicherheit, der Landesverteidigung, aber auch der Interessen der Steuerverwaltung oder zum Schutz der Unabhängigkeit der Gerichte möglich.“[104]
Die einzigen Öffnungen die zwingend ausgefüllt werden müssen, sind konkrete Regelungsaufträge, wie die aus Art. 84 und 85 DSGVO. Das sind Vorschriften zu Sanktionen, Bußgeldern und Strafen. Außerdem soll das Spannungsfeld zwischen Datenschutz und Meinungsfreiheit, sowie die Regelung eines Presseprivilegs und

[103] Vgl. Hülsmann: DSGVO – Expertenwissen für die Praxis (Abgerufen am 21.02.2018)
[104] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.15.

einem Privileg von Wissenschaft, Kunst und Literatur geklärt und in Einklang mit der DSGVO gebracht werden. Pflicht ist weiterhin die Errichtung von Aufsichtsbehörden aus Art. 51 DSGVO, die gesetzlich verankert sein müssen. Die Regelungsräume die in diesem Unterkapitel betrachtet werden, sind nicht abschließend. Es werden in unterschiedlichen Quellen bis zu 69 Öffnungsklauseln erkannt.[105]

[105] Vgl. Feiler: Präsentation – Die 69 Öffnungsklauseln der DS-GVO (Abgerufen am 21.02.2018)

4 Novelle des BDSG

Für die Bundesregierung bestand nach der Verkündung der DSGVO ein „spürbarer Handlungsdruck“[106] hinsichtlich des Zeitraums, bis zu dem das neue Recht gelten muss. Hätte man den Zeitpunkt verpasst, hätte ein „vollzugsunfähige[r] Regelungstorso“[107] mit der DSGVO bestanden. De Maizière kommentiert dazu, dass beispielsweise „wesentliche datenschutzrechtliche Kontroll- und Sanktionsmechanismen unvollkommen [bleiben würden]“[108], sofern es an einer nationalen Umsetzung fehlt. Hinsichtlich fakultativer Spielräume hätte Rechtsunsicherheit bestanden, weil die Anwendbarkeit der bisher bestehenden allgemeinen und spezialgesetzlichen Datenschutzregelungen in Teilen nicht mehr gegeben wäre. Dadurch, dass es in der BRD bereits viele Gesetze zum Datenschutz gibt, werden durch die DSGVO viele nationalen Regelungen verdrängt. Mit dem dringenden Erfordernis der „Festlegung der deutschen Vertretung im Europäischen Datenschutzausschuss“[109], ist gleichzeitig klar, dass dieser Ausschuss sonst ohne Deutschland stattfinden würde. Gerade eine solche Mitwirkung der nationalen Datenschutzbehörden ist im Prozess der aufsichtsbehördlichen Zusammenarbeit wichtig und sollte nicht verpasst werden.

Aufgrund der Dringlichkeit wurde vorerst mit der ersten Novelle im deutschen Recht nur die rechtliche Anpassung an die DSGVO vor der Bundestagswahl im September 2017 vorgenommen. Das Vorhaben wurde im Mai 2017 mit der Verabschiedung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) durchgeführt. In der neuen Legislaturperiode soll dann die Ausfüllung der Spielräume stattfinden.[110] Man könnte daraus annehmen, dass die Öffnungsklauseln aus der DSGVO noch nicht allzu weit ausgereizt wurden. Dieser Frage ist im Folgenden nachzugehen.

Das DSAnpUG-EU beinhaltet die Änderung von sieben Gesetzen und tritt am 25. Mai 2018 in Kraft. Den größten Anteil an diesem Anpassungsgesetz hat mit Art. 1 die Neufassung des Bundesdatenschutzgesetzes.

Bereits vor Anwendung des BDSG-neu gibt es kritische Stimmen zur Anwendbarkeit der Regelungen. „Es bestehen [beispielsweise] Zweifel, ob die in

[106] Kühling/Martini: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW, 2016, S. 449.
[107] Ebenda.
[108] Deutscher Bundestag: Plenarprotokoll 18/221, S.22177(B)
[109] Ebenda.
[110] Paal/Pauly: Datenschutz-Grundverordnung, 2017, Einleitung, Rn.3, S.2

§ 35 BDSG-neu vorgesehenen Beschränkungen des Rechts auf Löschung nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in § 35 BDSG-neu vorgesehene Beschränkung des Rechts auf Löschung aufgrund des Anwendungsvorrangs der DSGVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten“[111].

Noch vor Beginn der Ausarbeitung der DSGVO, bzw. der Neufassung des BDSG, gab es Forderungen nach Inhalten solcher Regelungswerke. „Die Aufgabe eines modernen Datenschutzrechts muss es sein, Persönlichkeitsrechte dadurch zu schützen, dass die Sammlung von Informationen nicht im Geheimen erfolgt und dem Nutzer die Möglichkeit gegeben wird, selbst zu entscheiden, ob und inwieweit er Dienste nutzt, die mit persönlichen Informationen bezahlt werden. Ein modernes Datenschutzrecht schafft Transparenz, ohne die freie Kommunikation zu behindern.“[112] Es stellt sich nun die Frage, ob dies mit der Novelle umgesetzt wurde.

4.1 Aufbau und Anwendungsbereich

Das neue Bundesdatenschutzgesetz besteht aus 4 Teilen, beginnend mit allgemeinen Bestimmungen. Teil 2, bis § 44 BDSG-neu, beinhaltet Durchführungsbestimmungen für Datenverarbeitungen die im sachlichen Anwendungsbereich der DSGVO liegen und ist somit relevant für die weiteren Betrachtungen dieses Kapitels. Teil 3 bezieht sich auf die Richtlinie (EU) 2016/680 (für Polizei und Justiz). Teil 4 beinhaltet Regelungen für nicht in den Anwendungsbereich der DSGVO und der Richtlinie für Polizei und Justiz fallende Datenverarbeitungen. An dieser Stelle soll diese Richtlinie ausdrücklich vom Inhalt der vorliegenden Arbeit abgegrenzt werden. Im Folgenden sind demnach nur Teil 1 und 2 des BDSG-neu relevant.

In § 1 des BDSG-neu wird der Anwendungsbereich des Gesetzes geklärt. Er wird an die DSGVO angelehnt und gilt gleichwohl für öffentliche, wie nichtöffentliche Stellen, sofern die Datenverarbeitung automatisiert erfolgt oder zumindest die Speicherung durch ein Dateisystem erfolgt. In §1 Abs. 5 BDSG-neu wird noch einmal ausdrücklich darauf hingewiesen, dass das BDSG-neu nicht anwendbar ist, sofern die DSGVO unmittelbar gilt. Mit dieser Kollisionsregelung geht der Gesetzgeber der Problematik der Rechtswidrigkeit des Gesetzes aus dem Weg. Für die praktische Anwendung des Gesetzes ist das jedoch eher ungünstig und erfordert Zusatzaufwand. Weiterhin bleibt es gem. §1 Abs. 2 BDSG-neu bei dem Vorrang

[111] DSK: Kurzpapier Nr. 11 Recht auf Löschung/ „Recht auf Vergessenwerden“.
[112] Härting/Schneider: Das Dilemma der Netzpolitik, ZRP 2011, S.234.

des Spezialgesetzes. Im folgenden Unterkapitel werden die bereits beispielhaft kategorisierten Regelungsräume betrachtet und analysiert, inwiefern der nationale Gesetzgeber diese genutzt hat. Dabei wurden drei Themen ausgewählt, die in der Recherche häufig aufgekommen sind, weil sie viel diskutiert wurden und öffentliche Brisanz hatten. Relevant sollen dabei die Diskussionen, Forderungen sowie kritischen Meinungen vor, während und nach dem Gesetzgebungsverfahren sein.

4.2 Analyse

Gewählt wurden für die Analyse hinsichtlich der Ausgestaltung im BDSG-neu die Regelungsräume, die durch die DSGVO bei Ausnahmen bei Betroffenenrechten, der betrieblichen Datenschutzbeauftragten und des Beschäftigtendatenschutzes eingeräumt wurden.

4.2.1 Die Betroffenenrechte

In Punkt 3.5.4 der vorliegenden Arbeit wurden die Neuerungen der Betroffenenrechte in der DSGVO betrachtet. Die hierzu zählende Transparenz, sowie die Rechte auf Benachrichtigung, Auskunft, Löschung, Widerspruch und Berichtigung werden in diesem Abschnitt in Zusammenhang mit der nationalen Umsetzung gebracht. Neben der Möglichkeit aus Art. 89 DSGVO Ausnahmen von Betroffenenrechten aufgrund von wissenschaftlichen, historischen, statistischen oder archivarischen Zwecke zu regeln, gibt es eine weitere Öffnungsklausel. Demnach können sämtliche Betroffenenrechte gemäß Art. 23 DSGVO durch nationale Gesetze beschränkt werden. Grund hierfür muss die Wahrung bestimmter öffentlicher Interessen sein. Hierzu zählen zum Beispiel der Schutz der nationalen und der öffentlichen Sicherheit oder die Landesverteidigung.[113] In den §§ 32 bis 37 des BDSG-neu sind solche Beschränkungen vorgesehen.

Der Verhältnismäßigkeitsgrundsatz und der Wesensgehalt der Grundrechte sind bei dem Erlass solcher einschränkenden Gesetze zu beachten. An dieser Stelle gab es bereits während des Gesetzgebungsverfahrens des DSAnpUG-EU und somit auch des BDSG-neu, deutliche und kritische Stimmen. Die Fraktion Die Linke war der Meinung, dass zahlreiche Ausnahmetatbestände unverhältnismäßig seien, und eben genau diesem Grundsatz der Verhältnismäßigkeit widersprechen[114]. Auch die Fraktion Bündnis 90/Die Grünen sehen „allenfalls geringfügige nationale Spielräume“ [115] bei der Einschränkung der Betroffenenrechte.

[113] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.15.
[114] Vgl. Deutscher Bundestag**:** Antrag, Drs.Drucksache 18/11401, S. 3.
[115] Deutscher Bundestag: Entschließungsantrag der Fraktion Bündnis 90/Die Grünen, Drs. 18/12132, S.5.

„Diese [Ausnahmen] sind im Lichte der DSGVO grundsätzlich eng auszulegen und am Maßstab des Art. 23 DSGVO zu messen. Ob und in welchem Umfang diese Regelungen aufgrund des Anwendungsvorrangs der DSGVO angewendet werden können, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten."[116] Diese kritische Aussage der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit deutet schon darauf hin, dass es erforderlich ist, immer im Einzelfall zu prüfen, welche Rechtsgrundlage einschlägig ist und ob Ausnahmen gelten. Dies kann zu Rechtsunsicherheit führen, was gerade im Bereich von Betroffenenrechten nicht passieren sollte.

Die Fraktion Bündnis 90/Die Grünen sah insbesondere bei den Betroffenenrechten eine Aufweichung der Vorgaben der DSGVO und forderte deshalb „bei den Rechten der Betroffenen europarechtskonforme Umsetzungen vorzunehmen und schutzverkürzende Anpassungen unbedingt zu vermeiden."[117] Ausdrücklich wird auf die Informationspflichten der verantwortlichen Stellen und die Auskunfts- und Löschungsrechte der Betroffenen hingewiesen. Auch die Linken kritisieren, dass es weitgehend „den Behörden überlassen [sei], wie weit sie Bürgerinnen und Bürger[n] über die über sie gespeicherten Informationen Auskunft erteilen."[118] Auch Unternehmen können die Auskunft über die Speicherung und Verarbeitung von Daten verweigern, wenn „die Information die Geschäftszwecke des Verantwortlichen erheblich gefährden würde"[119]. „Damit werden Geschäftsinteressen grundsätzlich über den Schutz persönlicher Daten gestellt, der durch die Auskunftsrechte erst durchgesetzt werden kann. Im Bereich der Patienten- und Sozialdaten soll es zukünftig keine Datenschutzkontrolle mehr geben, wenn davon Berufsgeheimnisträger betroffen wären. Derzeit ist dies ein Schwerpunkt der Datenschutzkontrolle durch die Aufsichtsbehörden in den Bundesländern."[120]

Deshalb wird ein „weitgehendes Auskunftsrecht über die eigenen Daten" gefordert[121].

Die Ausnahmen von Betroffenenrechten im BDSG-neu stellen weiterhin laut Fraktion die Linke eine „Arbeitserleichterung für die Daten verarbeitenden Stellen dar, widersprechen aber dem Recht auf informationelle Selbstbestimmung."[122] Beispielsweise schmälern Ausnahmen in der Informationspflicht aufgrund

[116] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.15.
[117] Deutscher Bundestag: Entschließungsantrag der Fraktion Bündnis 90/Die Grünen, Drs. 18/12132, S. 3.
[118] Deutscher Bundestag**:** Antrag, Drs.Drucksache 18/11401, S. 1.
[119] Bundesregierung: Art.1, § 33 Abs. 1 Nr. 2 Gesetzentwurf DSAnpUG-EU**,** Drs. 110/17.
[120] Deutscher Bundestag**:** Antrag, Drs.Drucksache 18/11401, S. 1.
[121] Ebenda.
[122] Ebenda, S. 3

‚unverhältnismäßigen Aufwands' den Schutzcharakter der Vorschriften zur Auskunft und Information von personenbezogenen Daten. In dem § 32 des Entwurfs des BDSG- neu entfielen Informationspflichten bei der Erhebung personenbezogener Daten schon, wenn ein „unverhältnismäßiger Aufwand" bei der Erfüllung besteht. Diese äußerst unbestimmte Norm würde es Verantwortlichen ermöglichen, ohne weiteren Rechtfertigungsbedarf keine Betroffeneninformationen bereitzustellen.[123] Die gleiche Kritik bringt Gerold Reichenbach von der SPD in der ersten Beratung zum BDSG-neu an. Es herrsche Unverständnis über den Sinn der Vorschrift, da es gerade den großen Datenverarbeitern die Pflicht zur Auskunft abnehme.[124]

Im Entschließungsantrag der Fraktion Bündnis 90/Die Grünen wird angemerkt, dass beispielsweise Informationsrechte sowie das Recht auf Löschen Mindestvoraussetzungen der Transparenz darstellen und für immer komplexer werdende Datenverarbeitungsvorgänge eine Einschränkung dieser Rechte nicht sachgerecht sei. Es entstehe dadurch die Benachteiligung deutscher Verbraucherinnen und Verbraucher gegenüber anderen europäischen Verbrauchern. Dies widerspricht dem eigentlichen Ziel, dem einheitliches Schutzniveau.[125] Diese Möglichkeit des Missbrauchs und der Fehlinterpretation der Norm aus dem Entwurf sollte aus dem Gesetz entfernt werden. Deshalb wurde in der endgültigen Fassung hinsichtlich der eingeschränkten Betroffenenrechte nur die Ausnahme belassen, die die analoge Datenverarbeitung von den Auskunftspflichten befreit. Es wurde der kritischen Debatte also nachgegeben. Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit äußert in einer Pressemitteilung, dass das nun vorliegende Gesetz gegenüber dem Entwurf der Bundesregierung verbessert wurde und nur noch sehr wenige Einschränkungen der Betroffenenrechte enthält. Kleine Unternehmen mit oftmals noch analoger Datenverarbeitung sollen so entlastet werden. Somit gelte für die Mehrzahl der Datenverarbeitungen ein hoher Standard.[126] Von dieser Verbesserung spricht auch der vorherige Kritiker Gerold Reichenbach von der SPD in der 2. Beratung im Bundestag.

In diesem Zusammenhang kritisiert die Fraktion die Linke ein weiteres brisantes Thema. Im nationalen Umsetzungsprozess, wie auch in der Entstehung der DSGVO spiele Lobbyarbeit eine große Rolle. In dem Gesetzentwurf werden keine

[123] Deutsche Vereinigung für Datenschutz e.V: Stellungnahme zum Gesetzesentwurf DSAnpUG-EU, 2017, S.13.
[124] Vgl. Deutscher Bundestag: Plenarprotokoll 18/221, S.22180 (B)
[125] Vgl. Deutscher Bundestag: Entschließungsantrag der Fraktion Bündnis 90/Die Günen, Drs. 18/12132, S. 5.
[126] Vgl. BfDI: Pressemitteilung, Licht und Schatten: Bundestag verabschiedet neues Datenschutzrecht (Abgerufen am 02.03.2018)

Begründungen angegeben, „warum Geschäftsinteressen von Auskunfteien schwerer wiegen als Datenschutzrechte betroffener Bürgerinnen und Bürger. Eine solche Fokussierung auf die wirtschaftlichen Interessen im Umgang mit den Betroffenenrechten geht zu Lasten des Persönlichkeitsschutzes und steht der Harmonisierung des Datenschutzes in der Europäischen Union entgegen.“[127]

In der abschließenden Beschlussempfehlung des Innenausschusses wird empfohlen den Antrag der Fraktion die Linke im Bundestag abzulehnen. Ebenso abgelehnt wurde der Entschließungsantrag der Fraktion Bündnis 90/Die Grünen. Diese enthielten neben der Kritik an den eingeschränkten Betroffenenrechten noch weitere Kritikpunkte, welche also zu einem großen Teil unbeachtet gelassen wurden. Eventuell ist dies auch dem zeitlichen Handlungsdruck vor der Neuwahl geschuldet gewesen.

4.2.2 Der betriebliche Datenschutzbeauftragte

Europa hat einen Europäischen Datenschutzbeauftragten. In Deutschland gibt es für die Bundesbehörden eine Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). In den einzelnen Bundesländern gibt es Datenschutzbeauftragte mit unterschiedlichen Bezeichnungen.

In diesem Unterkapitel soll der betriebliche Datenschutzbeauftragte im Mittelpunkt stehen. Wenn man die Hierachie der Datenschutzbeauftraten betrachtet, ist man bei dem betrieblichen DSB an der Basis. Wie bereits in Punkt 3.5.3 erklärt wurde, müssen laut DSGVO nur in zwei Fällen betriebliche DSB bestellt werden. Anders als im geltenden BDSG wäre dies unabhängig von der Anzahl der Mitarbeiter und nur die wenigsten Unternehmen würden den Fällen zugeordnet werden, da weder mittelständische Handwerksunternehmen noch durchschnittliche Online-Händler umfangreich, regelmäßig und systematisch Kundendaten überwachen. In den meisten Fällen werden personenbezogene Daten nur für das zuleiten einer Rechnung verwendet. Zu den Kernaktivitäten der Unternehmen würde dies bei weitem nicht zählen.[128] Der nationale Gesetzgeber hat deshalb die Öffnungsklausel des Art. 37 Abs. DSGVO genutzt und die Pflicht zur Bestellung auch nach anderen Kriterien bemessen. § 38 Abs. 1 BDSG-neu beinhaltet die Pflicht zur Benennung von DSB für nicht-öffentliche Stellen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Es werden weiterhin Fälle aufgezeigt in denen ein DSB benannt werden muss, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten

[127] Deutscher Bundestag: Antrag, Drs.Drucksache 18/11401, S. 3.
[128] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 2, Rn. 7-9.

beschäftigt sind. Solche liegen vor, wenn Verarbeitungen durchgeführt werden, die einer Datenschutz-Folgenabschätzung unterliegen. Auch bei der geschäftsmäßigen Verarbeitung personenbezogener Daten und zum Zweck der Übermittlung oder Markt- oder Meinungsforschung, muss unabhängig von der Anzahl der damit beschäftigten Personen ein DSB zu benannt werden.

In der Gesetzesbegründung wird erklärt, dass § 38 Abs. 1 Satz 1 BDSG-neu inhaltlich an den bisherigen § 4f BDSG angelehnt ist. Absatz 2 verweist für die betrieblichen DSB, sofern aufgrund der Verordnung oder BDSG-neu eine Pflicht zur Benennung besteht, auf den besonderen Kündigungsschutz des § 6 Absatz 4. Prof. Niko Härting vertritt die Meinung, dass der erweiterte Kündigungsschutz, der hier durch den Gesetzgeber fortgeführt wurde, unzulässig ist, da die Öffnungsklausel aus Art. 37 DSGVO nur für die Bestellung und nicht für die Abberufung von DSB gilt[129]. Fraglich wäre, ob die Stellung des DSB mit dem Ziel der Vollharmonisierung der EU vereinbar ist. Zumindest hätte es keine direkte Auswirkung auf die anderen Mitgliedstaaten und Art. 38 Abs. 3 Satz 2 DSGVO sieht vor, dass der DSB wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden darf. Die Aufgabe der Sicherung und Umsetzung der DSGVO sowie die Vermeidung von Sanktionen soll möglichst durchgängig gewährleistet werden, was den erweiterten Kündigungsschutz rechtfertigen würde.

Im Gesetzgebungsvorgang gab es hierzu von der Opposition keine Kritik. Außerdem begrüßt der Deutsche Gewerkschaftsbund und seine Mitgliedsgewerkschaften den Ansatz einer weitreichenden Regelung des §38 BDSG-neu in ihrer Stellungnahme zum Gesetzesentwurf[130]. Jedoch enthält die neue Regelung auch keine Neuerung, die hervorgehoben werden könnte.

4.2.3 Der Beschäftigtendatenschutz

Synonym zu dem Begriff Beschäftigtendatenschutz wird auch Arbeitnehmerdatenschutz häufig verwendet. „Die Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu.“[131] Da es sich um eine Konkretisierungsklausel handelt („spezifischere Vorschriften“[132]), hat die Bundesregierung nach dem Vorbild des geltenden § 32 BDSG den § 26 BDSG-neu als nationale konkretisierende Vorschrift zum Beschäftigtendatenschutz geschaffen.[133] Inhalt der Regelung ist, dass

[129] Vgl. Härting: Datenschutz-Grundverordnung, 2016, S. 4, Rn 16.
[130] Vgl. DGB: Stellungnahme vom 27.02.2017, S. 25.
[131] Bundesregierung**:** Gesetzentwurf DSAnpUG-EU**,** Drs. 110/17 S. 96.
[132] Art. 88 Abs. 1 DSGVO.
[133] BfDI: Infobroschüre Datenschutz-Grundverordnung, 2017, S.30.

personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, sofern dies für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist (§ 26 Abs. 1 BDSG-neu). Sofern eine Einwilligung die Rechtmäßigkeit der Datenverarbeitung begründet, muss sie in Textform aufgrund der Rechenschaftslegung gegeben werden und die Freiwilligkeit muss nach § 26 Abs. 2 beurteilt werden. In der Gesetzesbegründung wird dargelegt, dass diese Regelung aus der besonderen Abhängigkeit zwischen Arbeitsgeber und Arbeitnehmer resultiert und deshalb die Freiwilligkeit der Einwilligung fraglich sein könnte. Es handelt sich hierbei konkret um eine Spezifizierung. Weiterhin kann die Rechtmäßigkeit durch eine Kollektivvereinbarung begründet werden, wie es Art. 88 Abs. 1 DSGVO vorsieht. ErwGr 155 zur DSGVO nennt konkret Betriebsvereinbarungen als eine solche Kollektivvereinbarung. Die Bundesregierung schließt außerdem den Tarifvertrag und Dienstvereinbarung ein. § 26 Abs. 3 BDSG-neu nimmt die Ausnahme aus Art. 9 Abs. 2 lit. b) DSGVO auf. Es geht dabei um die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten in bestimmten Fällen, wie der Ausübung von Pflichten aus dem Arbeitsrecht.

Die Mindestanforderungen der DSGVO müssen aber zwingend und trotz nationaler Regelungen eingehalten werden (Art. 88 Abs. 2 DSGVO). Keinesfalls dürfen diese lockerer sein. Diese Forderung kann man konkret in §26 Abs. 5 erkennen, da der nationale Gesetzgeber auf die Grundsätze aus Art. 5 DSGVO verweist. Bis auf diesen und wenige weitere konkrete Verweise wird es für den Gesetzesanwender schwierig zu erkennen, bis zu welchem Grad die nationale Regelung abschließend und an welcher Stelle die EU-Regelung einschlägig ist.

In Absatz 8 des §26 BDSG-neu werden Beschäftigte im Sinne des Datenschutzes definiert. Fraglich ist, ob die Definition EU-konform ist, da Art. 88 DSGVO zu Definitionen keine Öffnung enthält.[134] Es könnte dazu führen, dass unterschiedliche Definitionen von Beschäftigten innerhalb der EU bestehen würden. Dies wäre nicht im Einklang mit dem Ziel der Harmonisierung.

In der Gesetzesbegründung zu § 26 BDSG-neu wird erklärt, dass der Gesetzgeber sich vorbehält, „Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb [des BDSG-neu] oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln. Dies gilt insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von

[134] Selk: Beschäftigtendatenschutz nach DSGVO und DSAnpUG-EU (Abgerufen am 26.02.2018)

heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken.“[135] Genau dieses Vorhaben wurde bisher nicht umgesetzt, obwohl der geltenden § 32 BDSG als „ergänzungs- und überarbeitungsbedürftig“[136] kritisiert wird. Unter anderem die SPD fordert ein eigenes Beschäftigtendatenschutzgesetz zur ersten Beratung des DSAnpUG-EU in der Bundestagssitzung vom 09.03.2017[137].

Insbesondere der Bundesrat wies mit seiner Stellungnahme zum Entwurf deutlich auf die Überarbeitungsbedürftigkeit hin. „Der Gesetzentwurf sollte auch die Grundsätze aufgreifen, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind und in der Begründung zu § 26 BDSG-E in Bezug genommen werden.“[138] Die Bundesregierung wurde daraufhin aufgefordert „bereits einschlägige Gerichtsurteile“ in einen neuen Entwurf einzubinden und „im Interesse der Rechtsklarheit verbindliche allgemein geltende Regelungen schaffen.“[139]

Auch aus den Reihen der Opposition des Bundestages gab es Kritik an dem Entwurf. „[…] Den Beschäftigtendatenschutz gilt es an die digitalisierten Arbeitsprozesse anzupassen. Arbeitnehmerinnen und Arbeitnehmer müssen davor geschützt werden, zu Objekten vollständiger Überwachung und permanenter Leistungskontrolle degradiert zu werden. Die bisherigen Regelungen reichen dazu nicht aus.“[140]

Verabschiedet wurde trotz dieser massiven Kritik die ursprüngliche Fassung des § 26 BDSG-neu aus dem ersten Entwurf. „Die großen Problemfelder des Beschäftigtendatenschutzes bleiben damit weiterhin ungeregelt […].“[141] Deshalb sind „Arbeitgeber, Beschäftigte und Betriebsräte […] gut beraten, sich weiter an den Vorgaben der Rechtsprechung zu § 32 BDSG zu orientieren“[142]. Die Bundesregierung sieht in Legislaturperiode 18 keinen weiteren Handlungsbedarf. Weitere Regelungen, die sich aus dem Regelungsvorbehalt der Gesetzesbegründung ergeben, stehen in der neuen Legislaturperiode

[135] Bundesregierung**:** Gesetzentwurf DSAnpUG-EU**,** Drs. 110/17, S. 96.
[136] Ebenda.
[137] Deutscher Bundestag: Plenarprotokoll 18/221, S. 22180(A)
[138] Bundesregierung**:** Unterrichtung über Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, Drs**.** 18/11655, S.14.
[139] Ebenda.
[140] Deutscher Bundestag**:** Antrag, Drs. 18/11401, S.4.
[141] Rödl: § 26 BDSG-neu: Der neue Beschäftigtendatenschutz ist beschlossene Sache (Abgerufen am 24.02.2018)
[142] Wybitul: Der neue Beschäftigtendatenschutz nach § 26 BDSG – das Wichtigste auf einen Blick – Hogan Lovells Unternehmensblog (Abgerufen am 26.02.2018)

möglicherweise bevor.[143] Im Zusammenhang mit der Auswirkung der DSGVO wurde die Möglichkeit nicht ergriffen, das Beschäftigtendatenschutzrecht zu novellieren.

[143] Bundesregierung: Unterrichtung über Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, Drs**.** 18/11655, S. 30.

5 Ergebnisse

Hinsichtlich der eben analysierten Bereiche des BDSG-neu, kann man einige Ergebnisse festhalten. Die Betroffenenrechte wurden eingeschränkt gegenüber der DSGVO. Sie unterschreiten jedoch nicht das Datenschutzniveau des geltenden BDSG. Diese Option der Ausgestaltung bestand ausdrücklich. Inwieweit diese Einschränkungen tatsächlich europarechtskonform sind, wird die Auslegung durch zuständige Stellen zeigen. Im Ausblick auf das Sächsische Datenschutzdurchführungsgesetzt (SächsDSDG), wird es ähnliche Regelungen geben[144]. Zum Entwurf (SächsDSDG-E) fand am 19.01.2018 eine öffentliche Anhörung von Sachverständigen statt. Gerade zur Beschränkung von Betroffenenrechten, die auch in diesem Entwurf enthalten sind, wurden Stellungnahmen abgegeben. Für jegliche „Nachteile“ die dem „Wohle des Freistaates Sachsen, eines anderen Landes oder des Bundes“ entstehen, soll die Informationsplicht und das Auskunftsrecht, gem. §§ 8ff SächsDSDG-E, bereits nicht mehr bestehen. Diese wage Formulierung könnte dazu führen, dass Behörden gar keine Auskunft mehr geben müssten. Prof. Dr. Wedde kommentiert als Sachverständiger hierzu, dass der „Transparenzanspruch, den die Datenschutz-Grundverordnung den betroffenen Personen und Bürgern gibt“ auf diese Weise zu stark eingeschränkt werde.[145] Man erkennt also, dass die Auslegung dieser Frage in der Gesetzgebung auf Landesebene weiter anhält, da sich an dem BDSG-neu orientiert wurde. Es steht außer Frage, dass durch solche nationalen Abweichungen von der DSGVO, „der auch von der Wirtschaft gewünschten europaeinheitlichen Regelung entgegengewirkt wird“[146].

Auch bei dem betrieblichen Datenschutzbeauftragten wurde sich an die Vorlage des geltenden BDSG gehalten. In diesem Fall werden die Anforderungen zur Bestellung von DSB so gestrafft, dass der Fall häufiger einschlägig ist, als es die DSGVO gefordert hat. Dies ist grundsätzlich für den Datenschutz positiv zu werten, wenn mehr Unternehmen einen DSB haben, die als Ansprechpartner für Betroffene fungieren können. „Bis jetzt haben sich viele Firmen überhaupt nicht um Datenschutz gekümmert. Nun müssen sie möglicherweise sogar einen Datenschutzbeauftragten einstellen.“[147]

Bei dem Beschäftigtendatenschutz gab es auf nationaler Ebene keine Neuerungen, da die bestehenden Regelungen hierzu übernommen wurden. Die Chance,

[144] Sächsische Staatsregierung: Gesetzesentwurf, Drs 6/10918, Artikel 1 Sächsisches Datenschutzdurchführungsgesetz–SächsDSDG.
[145] Sächsischer Landtag: Wortprotokoll zur Anhörung vom 19.01.2018, APr 6/60410.
[146] Haag: Peter Gola im Interview zur DSG-VO und seinem Kommentar (Abgerufen am 02.03.2018)
[147] Schöneberg: Democracy – Hintergrund - Interview mit Viviane Reding (Abgerufen am 22.02.2018)

im Zuge der Auswirkungen der DSGVO, eine Überarbeitung dieser stark kritisierten Regelungsinhalte anzustreben, wurde in der vergangenen Legislaturperiode verpasst.

Wenn man ein Gesamturteil hierüber abgeben will, könnte man sagen, dass die Regelungsräume zum Teil weit ausgefüllt wurden. Das liegt daran, dass versucht wurde, bereits bestehende Regelungen in das neue Datenschutzrecht einzufügen und das Datenschutzniveau in Deutschland bereits recht hoch war. Von einer tiefgründigen Überarbeitung des nationalen Datenschutzrechts kann man jedoch nicht sprechen.

Trotzdem wird das Datenschutzrecht ab Mai 2018 einen Umbruch erfahren, nicht durch das BDSG-neu, sondern durch die DSGVO mit ihrer Direktwirkung und ihren Neuerungen. Beispielsweise soll die Transparenz gestärkt werden und „wie bei Verkehrsschildern [angezeigt werden]: ‚Achtung, hier passiert mit Deinen Daten [dieses] und jenes!' […] Verhindern soll die neue Grundverordnung, dass Daten aus jemandem herausgepresst werden, die für die eigentliche Dienstleistung nicht notwendig sind".[148] Die DSGVO soll außerdem ein Appell an die Eigenverantwortung der Unternehmen sein. Die drohenden Bußgelder sollen ein Mittel sein, dem Apell Nachdruck zu verleihen.[149] Ob die beabsichtigten Ziele erreicht werden, bleibt abzuwarten. Dem entsprechend ist auch das neue Marktortprinzip eine grundsätzlich gute Idee. Jedoch zeigen -metaphorisch gesehen- Bits und Bytes an der Grenze des europäischen Binnenmarktes keinen Ausweis vor. Solche Kontrollen gibt es technisch nicht. Die Aufsichtsbehörden müssen durch Betroffene darauf hingewiesen oder selbst auf die Verstöße aufmerksam werden.

Den Konflikt zwischen Privatsphäre und Big Data hebt die DSGVO nicht auf. Die Datenschutzgrundverordnung schützt Betroffene nicht davor, dass sie immer mehr Daten preisgegeben sollen „um immer neue Online-Innovationen in Anspruch nehmen zu können"[150]. Deshalb sollte jeder Nutzer selbst darauf achten, wie viele Daten Unternehmen gegeben werden, um nicht gläsern zu werden. Außerdem könnten für Big Data Analysen strengere Regeln gelten, z.B. „sollte man [für selbstfahrende Autos] eher Sensoren statt Kameras nutzen, um die Persönlichkeitsrechte besser zu wahren"[151].So brauche man für die Vervollständigung des digitalen Binnenmarktes „dutzende weitere neue Regelungen"[152]. Unabhängig vom Thema

[148] Schöneberg: Democracy – Hintergrund - Interview mit Jan Philipp Albrecht (Abgerufen am 22.02.2018)
[149] Vgl. ebenda.
[150] Ebenda.
[151] Ebenda.
[152] Schöneberg: Democracy -Hintergrund-Interview mit Viviane Reding (Abgerufen am 22.02.2018)

Datenschutz, aber zum europäischen Binnenmarkt, gibt es Beispiele hierfür. So sind die Abschaffung der EU-Roaming-Gebühren oder des sogenannten Geoblocking Schritte auf diesem Weg. Seit Juni 2017 werden keine zusätzlichen Roaming-Gebühren bei der Nutzung des Mobilfunknetzes im EU-Ausland erhoben.[153]

Noch nicht in Kraft, aber bereits vom Rat der Europäischen Union verabschiedet, wurde im Februar 2018 eine Verordnung die Geoblocking im Binnenmarkt verbietet. Kunden sollen Waren oder Dienstleistungen über eine Website auch erwerben können, wenn der Standort des Anbieters in einem anderen Mitgliedstaat ist. Das zeigt sich beim Online-Shopping oder bei der Nutzung von bezahlten Streaming-Diensten.[154]

Abschließend kann man hierzu die Aussage von Viviane Reding, ehemalige Vizepräsidentin der Europäischen Kommission, stehen lassen: „Die digitale Entwicklung ist zehn Mal schneller als die Gesetzgebung“[155].

[153] Vgl. Bundesnetzagentur: EU-Roaming (Abgerufen am 07.03.2018)
[154] Vgl. Rat der Europäischen Union: Pressemitteilung: Geoblocking: Rat verabschiedet Verordnung, die Hindernisse für den elektronischen Handel beseitigt (Abgerufen am 07.03.2018)
[155] Ebenda.

Thesen

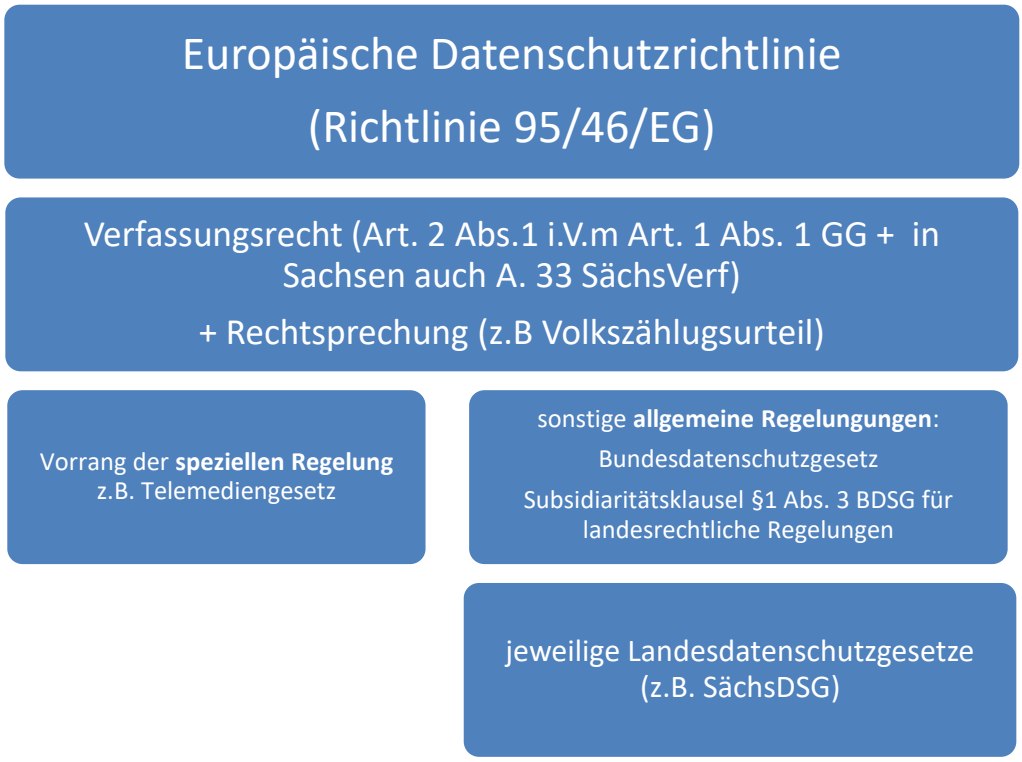
1. Die DSGVO hat durch ihre Direktwirkung eine große Auswirkung auf nationales Datenschutzrecht, da das BDSG sowie Spezialgesetze geändert werden mussten.
2. Bei der Anpassung des Bundesdatenschutzgesetzes wurde, zumindest bei den analysierten Themen, an den bekannten Regelungen festgehalten.
3. Während der Gesetzgebung wurde die Einschränkung von Betroffenenrechten kritisiert, da Regelungsräume im Entwurf stark ausgereizt wurden.
4. Das neue einheitliche Datenschutzrecht bringt grundsätzlich einen starken Schutz für Betroffenen und hohe, zum Teil schwer erfüllbare Anforderungen an Datenverarbeiter.
5. Ob Kontroll- und Aufsichtsmechanismen sowie Sanktionen zur gewünschten Durchsetzung der Rechte führen, wird sich nach Inkrafttreten zeigen.

Anhang

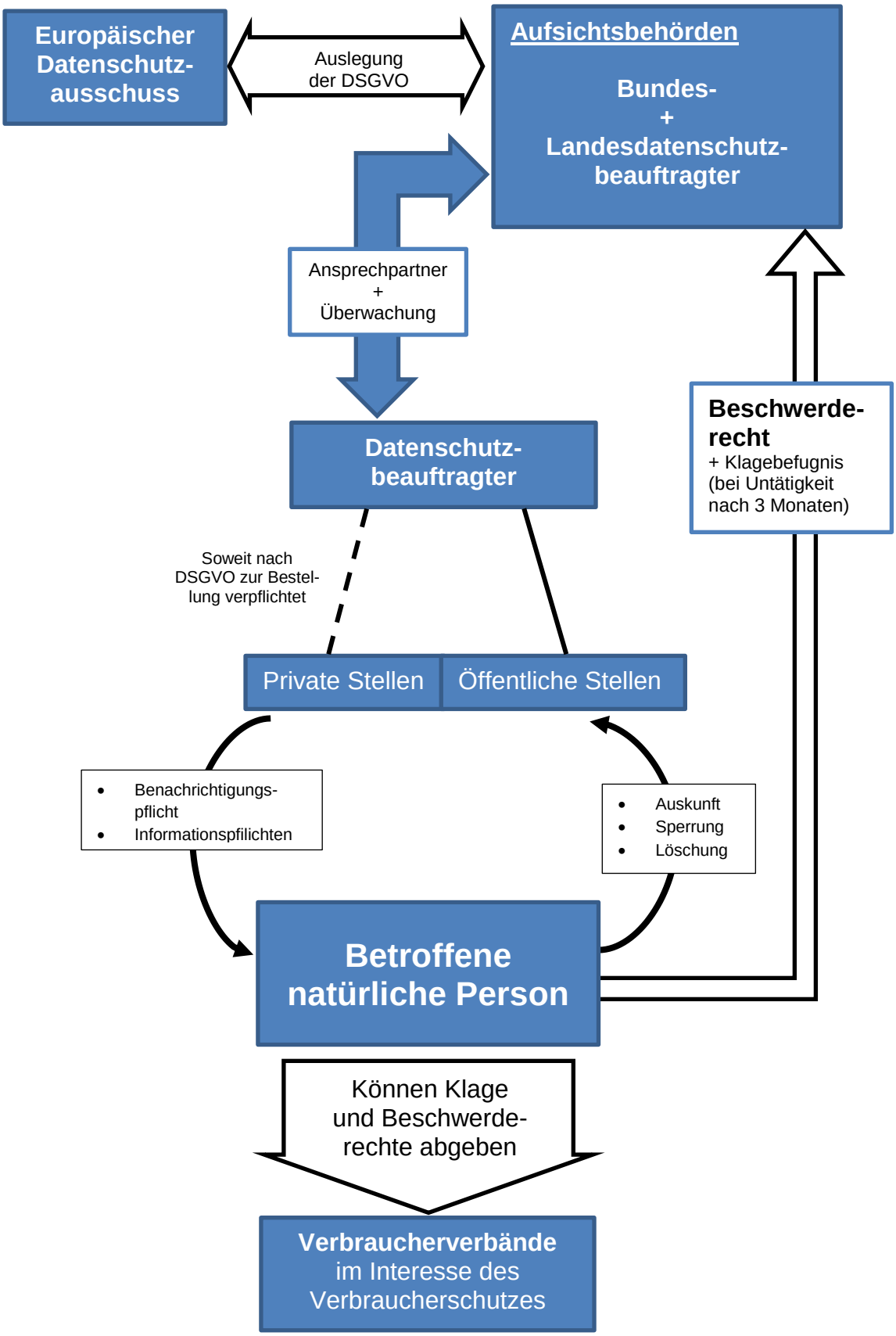
Anhangsverzeichnis

Anhang 1: Systematik des geltenden Rechts bis 25.05.2018 VII
Anhang 2: Kontroll- und Aufsichtssystem VIII
Anhang 3: Statistik VIII

Anhang 1: Systematik des geltenden Rechts bis 25.05.2018

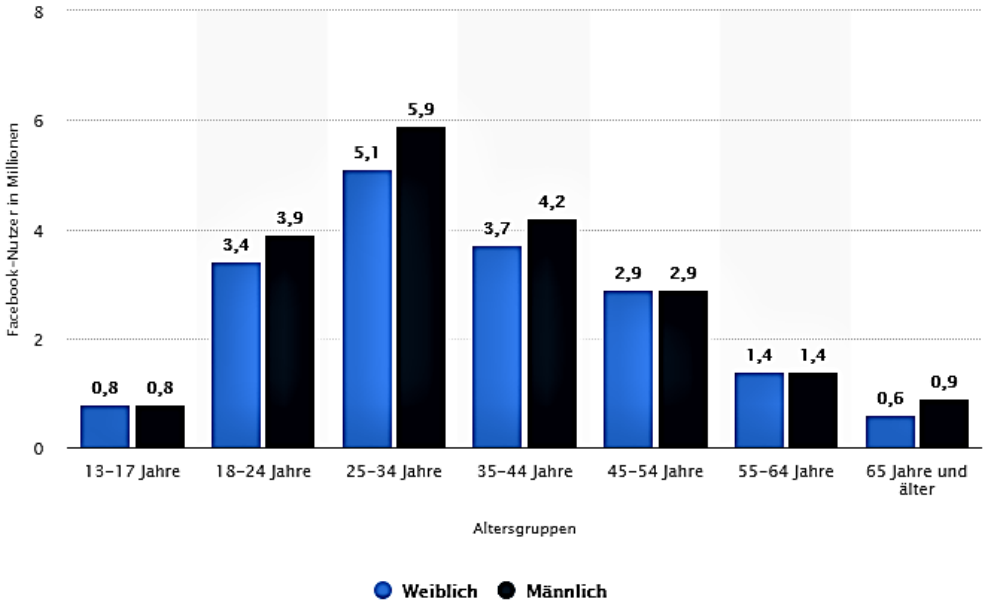


Anhang 2: Kontroll- und Aufsichtssystem



Anhang 3: Statistik

Anzahl der Facebook-Nutzer nach Altersgruppen und Geschlecht in Deutschland im Januar 2018 (in Millionen)



Quelle: Statista GmbH, Facebook - Nutzer nach Altersgruppen und Geschlecht in Deutschland 2018 | Statistik (Abgerufen am 28.02.2018)

Literatur- und Quellenverzeichnis

Auernhammer, Herbert (Hrsg): DSGVO BDSG Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar, Carl Heymanns Verlag, 2017, 5. Auflage

Bayrisches Landesamt für Datenschutzaufsicht (BayLDA): BayLDA-Kurzpapiere zur DS-GVO:, IX Einwilligung nach der DS-GVO, 2016, URL: https://www.lda.bayern.de/media/baylda_ds-gvo_9_consent.pdf (Abgerufen am 12.03.2018)

Bayrisches Landesamt für Datenschutzaufsicht (BayLDA): BayLDA-Kurzpapiere zur DS-GVO:, XII I Der One Stop Shop, 2017, URL: https://www.lda.bayern.de/media/baylda_ds-vo_13_one_stop_shop.pdf (Abgerufen am 12.03.2018)

Berufsverband der Rechtsjournalisten e.V: Datensparsamkeit in BDSG & DSGVO Datenschutz 2018, URL: https://www.datenschutz.org/datensparsamkeit (Abgerufen am 01.03.2018)

Bieber, Christoph: Datenschutz als politisches Thema –von der Volkszählung zur Piratenpartei In: In: Schmidt, Jan-Hinrik/ Weichert,Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen. Schriftenreihe (Bd. 1190), Bundeszentrale für politische Bildung, Bonn, 2012

Brugugnone, Giovanni: Interview, Digitalisierung und Datenschutz: Neue Herausforderungen für Unternehmen, URL: https://www.der-betrieb.de/interview/digitalisierung-und-datenschutz-neue-herausforderungen-fuer-unternehmen/ (Abgerufen am 27.02.2018)

Bundesnetzagentur: EU-Roaming, URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/WeitereThemen/InternRoaming/EURoaming/EURoaming-node.html (Abgerufen am 07.03.2018)

Bundesrat: Empfehlung der Ausschüsse zu Punkt 36 der 954. Sitzung des Bundesrates am 10. März 2017, Drucksache 110/1/17, 01.03.2017

Bundesregierung: Gesetzentwurf DSAnpUG-EU**,** Drs. 110/17, 02.02.2017

Bundesregierung: Unterrichtung über Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung Drs**.** 18/11655, 23.03.2017

Bundesverband Interaktive Unterhaltungssoftware e.V.(BIU): Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechtes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/datenschutz-anpassungs-und-umsetzungsgesetz-eu-dsanpug-eu/bundesverband-interaktive-unterhaltungssoftware-biu_stn.pdf?__blob=publicationFile&v=2 (Abgerufen am 12.03.2018)

Datenschutzkonferenz (DSK) unabhängigen Datenschutzbehörden des Bundes und der Länder: Kurzpapier Nr. 7 Marktortprinzip: Regelungen für außereuropäische Unternehmen, 2017

Datenschutzkonferenz (DSK) unabhängigen Datenschutzbehörden des Bundes und der Länder**:** Kurzpapier Nr. 4 Kurzpapier Nr. 4 Datenübermittlung in Drittländer, 2017

Datenschutzkonferenz (DSK) unabhängigen Datenschutzbehörden des Bundes und der Länder**:** Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, 2017

Datenschutzkonferenz (DSK) unabhängigen Datenschutzbehörden des Bundes und der Länder**:** Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“, 2017

Der Sächsische Datenschutzbeauftragte: Datenschutz-Grundverordnung (DS-GVO) kurz erläutert, S.1. URL: https://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/DS-GVO%20kurz%20erlaeutert%20271017.pdf (Abgerufen am 12.03.2018)

Deutsche Vereinigung für Datenschutz e.V: Stellungnahme zum Gesetzesentwurf DSAnpUG-EU, Bonn, 2017

Deutscher Bundestag: Antrag der Abgeordneten Jan Korte, Frank Tempel, Dr. André Hahn, Katrin Kunert,Petra Pau, Martina Renner, Dr. Petra Sitte und der Fraktion DIE LINKE.,Datenschutzrechte der Bürgerinnen und Bürger stärken, Drs. 18/11401, 07.03.2017

Deutscher Bundestag: Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drs. 18/12132 vom 26.04.2017

Deutscher Bundestag: Plenarprotokoll 18/221. Stenographischer Bericht der 221. Sitzung der 18. Wahlperiode (09.03.2017), S. 22176B - 22183D

Deutscher Bundestag: Plenarprotokoll 18/231. Stenographischer Bericht der 231. Sitzung der 18. Wahlperiode (27.04.2017), S. 23299A - 23307A

Deutscher Gewerkschaftsbund (DGB): Stellungnahme des Deutschen Gewerkschaftsbundes zum Gesetzentwurf der Bundesregierung vom 27.02.2017 URL: http://www.dgb.de/themen/++co++bee27cc0-1460-11e7-869c-525400e5a74a
(Abgerufen am 12.03.2018)

Die Bundesbeauftragte für den Datenschutzund die Informationsfreiheit (BfDI): Infobroschüre Datenschutz-Grundverordnung BfDI, 5. Auflage, Bonn, 2017

Die Bundesbeauftragte für den Datenschutzund die Informationsfreiheit (BfDI): Pressemitteilung, Licht und Schatten: Bundestag verabschiedet neues Datenschutzrecht, URL: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2017/10_BDSG_neu_April.html;jsessionid=DE0EB99EACD75CCC3BABCB87F44BD3B3.1_cid344?nn=5217154, (abgerufen am 02.03.2018)

Feiler, Lukas: Präsentation – Die 69 Öffnungsklauseln der DS-GVO, URL: http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf
(Abgerufen am 21.02.2018)

Gola, Peter/Jaspers, Andreas/ Müthlein, Thomas/ Schwartmann, Rolf: Datenschutz-Grundverordnung im Überblick. Datakontext, 2017, 2. Auflage

Gola, Peter: DS-GVO Kommentar, Verlag C.H. Beck, München, 2017

Haag, Nils: Peter Gola im Interview zur DSG-VO und seinem Kommentar, URL: https://www.datenschutzbeauftragter-info.de/peter-gola-im-interview-zur-ds-gvo-und-seinem-kommentar
(abgerufen am 02.03.2018)

Härting, Niko: Datenschutzbehörden und die DSGVO | HÄRTING Rechtsanwälte Stand: 19.01.2018 URL: https://www.haerting.de/neuigkeit/datenschutzbehoerden-und-die-dsgvo#AutomatisierteEntscheidung iling
(Abgerufen am 17.02.2018)

Härting, Niko: Datenschutz-Grundverordnung. Das neue Datenschutzrecht in der betrieblichen Praxis. Verlag Dr. Otto-Schmidt KG, Köln, 2016

Härting, Niko: Warum "Datenminimierung" kommunikations- und innovationsfeindlich ist – CR-online.de, Blogeintrag 12.2.2013, URL: https://www.cr-online.de/blog/2013/02/12/warum-datenminimierung-kommunikations-und-innovationsfeindlich-ist
(Abgerufen am 17.02.2018)

Härting, Niko/ Schneider, Jochen: Warum wir ein neues BDSG brauchen - Kritischer Beitrag zum BDSG und dessen Defiziten. In: ZD Zeitschrift für Datenschutz, 2011, S.63-68

Härting, Niko/ Schneider, Jochen: Das Dilemma der Netzpolitik. In: ZRP Zeitschrift für Rechtspolitik, 2011, 44. Jahrg., Heft 8, S. 233-236.

Hülsmann, Werner: DSGVO – Expertenwissen für die Praxis | Informationen zur Europäischen Datenschutzgrundverordnung, URL: https://dsgvo.expert/regelungsräume
(Abgerufen am 21.02.2018)

Intersoft Consulting services AG: Diese Auskunftsrechte haben Betroffene nach der DSGVO,URL: https://www.datenschutzbeauftragter-info.de/diese-auskunftsrechte-haben-betroffene-nach-der-dsgvo/
(Abgerufen am 19.02.2018)

Janzik, Lars: Suchmaschinen-Advertising (SEA) Definition | Gründerszene. URL: https://www.gruenderszene.de/lexikon/begriffe/suchmaschinen-advertising-sea.
(Abgerufen am: 08.02.2018)

Kühling, Jürgen/Martini, Mario et.al.: Die Datenschutz-Grundverordnung und das nationale Recht, Erste Überlegungen zum innerstaatlichen Regelungsbedarf**,** MV-Verlag, 2016

Kühling, Jürgen/Martini, Mario**:** Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? In**:** EuZW Europäische Zeitschrift für Wirtschaftsrecht, 2016, S. 448-454

Lackes, Richard/ Siepermann, Markus: Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Datensicherheit, URL: http://wirtschaftslexikon.gabler.de/Archiv/74976/datensicherheit-v9.html
(Abgerufen am 28.02.2018)

Lackes, Richard/Siepermann, Markus: Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Internet der Dinge, URL: http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v5.html
(Abgerufen am 12.02.2018)

Nolte, Norbert: Zum Recht auf Vergessen im Internet In: ZRP Zeitschrift für Rechtspolitik 2011, 44. Jahrg., Heft 8, 236-239

Paal, Boris/ Pauly, Daniel, Datenschutz-Grundverordnung, Beck'sche Kompakt-Kommentare, Verlag C.H.Beck, München, 2017

Rat der Europäischen Union: Pressemitteilung: Geoblocking: Rat verabschiedet Verordnung, die Hindernisse für den elektronischen Handel beseitigt, URL: www.consilium.europa.eu/de/press/press-releases/2018/02/27/geo-blocking-council-adopts-regulation-to-remove-barriers-to-e-commerce/ (Abgerufen am 07.03.2018)

Rödl, Christian: § 26 BDSG-neu: Der neue Beschäftigtendatenschutz ist beschlossene Sache | URL: http://www.roedl.de/themen/beschaeftigtendaten-schutz-eu-dsgvo-26-bdsg-neu (Abgerufen am 24.02.2018)

Roßnagel, Alexander /Geminn, Christian L./ Jandt, Silke/ Richter, Philipp: Datenschutzrecht 2016 - "smart" genug für die Zukunft? : Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts Hrsg.: ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung an der Universität Kassel, 2016

Sächsische Staatsregierung: Artikel 1 des Gesetzesentwurfs (Sächsisches Datenschutzdurchführungsgesetz), Drs. 6/10918, 29.09.2017

Sächsischer Landtag: Wortprotokoll zur Anhörung vom 19.01.2018, APr 6/60410

Sächsisches Staatsministerium des Innern (SMI SN): Datenschutzrecht für öffentliche Stellen - Dokumentation zum Themenportal, URL: http://www.datenschutzrecht.sachsen.de/download/Dokumentation_Themenportal_Datenschutz_30_11_2017.pdf (Abgerufen am 07.02.2018)

Schöneberg, Kai, Democracy – Hintergrund -Interview mit Jan Philipp Albrecht, für Bundeszentrale für Politische Bildung, 2017, URL: http://www.bpb.de/gesellschaft/digitales/democracy/254242/interview-mit-jan-philipp-albrecht (Abgerufen am 22.02.2018).

Schöneberg, Kai: Democracy - Hintergrund -Interview mit Viviane Reding, für Bundeszentrale für Politische Bildung, 2017, URL: http://www.bpb.de/internationales/europa/democracy/254242/interview-mit-jan-philipp-albrecht (Abgerufen am 22.02.2018)

Schöneberg, Kai: Democracy - Hintergrund -Was steht in der DSGVO?, URL: http://www.bpb.de/gesellschaft/digitales/democracy/255875/was-steht-in-der-dsgvo (Abgerufen am 14.02.2018)

Selk, Robert: Beschäftigtendatenschutz nach DSGVO und DSAnpUG-EU, URL: https://www.datenschutz-praxis.de/fachartikel/beschaeftigtendatenschutz-dsgvo-dsanpug-eu/ (Abgerufen am 26.02.2018)

Statista GmbH: Facebook - Nutzer nach Altersgruppen und Geschlecht in Deutschland 2018 | Statistik, URL: https://de.statista.com/statistik/daten/studie/512316/umfrage/anzahl-der-facebook-nutzer-in-deutschland-nach-alter-und-geschlecht/ (Abgerufen am 28.02.2018)

von Lewinski, Kai: Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: Schmidt, Jan-Hinrik/ Weichert,Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen. Schriftenreihe (Bd. 1190), Bundeszentrale für politische Bildung, Bonn, 2012

Wybitul, Tim: Der neue Beschäftigtendatenschutz nach § 26 BDSG – das Wichtigste auf einen Blick – Hogan Lovells Unternehmensblog, Eintrag vom 05.02.2017, URL: http://hoganlovells-blog.de/2017/02/05/der-neue-beschaeftigtendaten-schutz-nach-§-26-bdsg-das-wichtigste-auf-einen-blick/
(Abgerufen am 26.02.2018)

Rechtsprechungsverzeichnis

Bundesverfassungsgericht, Urteil vom 15.12.1983, Az.: 1 BvR 209/83 u.a

Europäischer Gerichtshof, Urteil vom 24.11.2011, Az.: C-468/10

Rechtsquellenverzeichnis

Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist

Charta der Grundrechte der Europäischen Union vom 26.10.2012 bekanntgemacht im ABl. EU C326/391

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU / DSAnpUG-EU) in der Fassung der Bekanntmachung vom 30. Juni 2017 (BGBl. I S. 2097)

Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347) geändert worden ist

Richtlinie (EU) 2016/680 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung bekanntgemacht im ABl. EU L 119/89 vom 04.05.2016

Strafgesetzbuch (StGB) in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist

Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), die durch das Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502) geändert worden ist

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) bekanntgemacht im ABl. EU L 119/1 vom 04.05.2016

Vertrag über die Arbeitsweise der Europäischen Union Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 9.5.2008, S. 47) zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m.W.v. 1.7.2013

Eidesstattliche Versicherung

Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorgelegte Bachelor-Arbeit selbstständig verfasst, nur die angegebenen Quellen und Hilfsmittel benutzt sowie alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht habe und die Bachelor-Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt worden ist.

Die gedruckte und digitalisierte Version der Bachelor-Arbeit sind identisch.

Meißen, 26.03.2018 *Jolene Kunze*