HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

MASTERARBEIT

Herr/Frau
Katharina Schönner

Compliance unter Berücksichtigung der neuen DSGVO und national geltender Gesetze

2019

Fakultät: Angewandte Computer- und Biowissenschaften

MASTERARBEIT

Compliance unter Berücksichtigung der neuen DSGVO und national geltender Gesetze

Autor/in:
Frau Katharina Schönner

Studiengang:
Cybercrime/Cybersecurity

Seminargruppe:
CY17wC-M

Erstprüfer:
Frau Prof. Dr. rer. pol. Petra Schmidt

Zweitprüfer:
Herr Prof. Dr. jur. Frank Czerner

Einreichung:
Mittweida, den 29.11.2019

Faculty of Computer and Life Sciences

MASTER THESIS

Compliance regarding the new GDPR and national law

author:
Ms. Katharina Schönner

course of studies:
Cybercrime/Cybersecurity

seminar group:
CY17wC-M

first examiner:
Prof. Dr. rer. pol. Petra Schmidt

second examiner:
Prof. Dr. jur. Frank Czerner

submission:
Mittweida, 29.11.2019

Bibliografische Angaben

Nachname, Vorname: Schönner, Katharina

Thema der Masterarbeit: Compliance unter Berücksichtigung der neuen DSGVO und nationaler Gesetze

Topic of thesis: Compliance regarding the new GDPR and national law

77 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Computer- und Biowissenschaften, Masterarbeit, 2019

Abstract

Die vorliegende Arbeit befasst sich mit dem Datenschutz allgemein und der DSGVO im Konkreten als Herausforderung für Unternehmen. Die Einhaltung rechtlicher Vorschriften, vertraglicher Bestimmungen, externer sowie interner Regelwerke, im Begriff Compliance zusammengefasst, ist ein wichtiges Unternehmensziel. Die DSGVO, die am 25.05.2018 in Kraft trat, bringt für Betriebe einige zu beachtende Änderungen mit sich, so beispielsweise die Rechenschaftspflicht des Verantwortlichen und die verschärften Sanktionen bei Verstößen. Zusätzlich muss durch sie als Verordnung, aufgrund ihrer Vorrangstellung gegenüber nationalen Gesetzen, auch die Anwendbarkeit einiger bestehender Regelungen in Frage gestellt werden.

Abstract

This paper is about privacy and the concrete laws of GDPR, which is a big challenge for companies. Compliance means the correct behaviors regarding laws, contracts, external and internal guidelines, which are important corporate aims. GDPR came into effect the 25.05.2018 and brings some effective changes, for example in terms of accountability of the controller and sanctions. Due to the GDPRs primacy regarding national law the applicability of consisting regulations is questionable.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
AO	Abgabenordnung
BayDSG	Bayrisches Datenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz
BDSG_alt	Bundesdatenschutzgesetz in der alten Fassung vor 25.05.18
BMI	Bundesministerium des Inneren
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMS	Compliance Management System
DCGK	Deutscher Corporate Governance Kodex
DSGVO	Datenschutz-Grundverordnung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
HGB	Handelsgesetzbuch
ISO	International Organization for Standardization
IT-SiG	IT-Sicherheitsgesetz
OWiG	Ordnungswidrigkeitengesetz

TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
SächsDSG	Sächsisches Datenschutzgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
UWG	Gesetz gegen den unlauteren Wettbewerb

1 Bedeutung von Gesetzen und Compliance-Definition

“Recht ist die Einschränkung der Freiheit eines jeden auf die Bedingung ihrer Zusammenstimmung mit der Freiheit von jedermann, in so fern diese nach einem allgemeinen Gesetze möglich ist”[1].

Derartige Aussagen wie diese von Immanuel Kant betonen zwar eine Wichtigkeit von Gesetzen, die Freiheit eines jeden, heben allerdings ebenfalls die mögliche Freiheitseinschränkung des Individuums hervor. Auch heutige Gelehrte machen die Beobachtung, dass “Gesetze [...] im Alltag oft als Einschränkung von Freiheit empfunden”[2] werden. Hierfür gibt es verschiedene Situationen, in denen zum Teil auch deren Befolgen als kleinlich erachtet wird. So wird beispielsweise das Anhalten vor einer unbefahrenen Straße aufgrund einer roten Ampel oftmals als nutzlos und penibel gesehen. Derlei Gedanken führen zu einer der zentralsten Fragen der Rechtsphilosophie, nämlich zu der, wieso überhaupt ein Recht vonnöten ist und worauf sich damit dessen Verbindlichkeit stützt. Diese lässt sich mit verschiedenen Ansätzen und auf unterschiedliche Weise beantworten.

Schon Platon, einer der bedeutensten Philosophen der Antike, suchte den Nutzen der Gesetze, unter anderem in seinem dialogisch aufgebauten Werk ‚Nomoi’, zu erklären. In diesem kann man die Rolle des Atheners als den Vertreter von Platons Meinung erachten. Letzterer sieht den Frieden als Nutzen an. “Was den Endzweck der Gesetze betrifft, unterscheidet der Athener die göttlichen Güter Einsicht, Besonnenheit, Gerechtigkeit und Tapferkeit von den menschlichen Gütern Gesundheit, Schönheit, Kraft und Reichtum.”[3] Allerdings sind die Göttlichen als vernünftiger und somit erstrebenswerter zu erachten, weshalb diese zu erlangen die Zielvorstellung der Gesetze bestimmt. Demzufolge muss auch die Erziehung auf die richtige Art und Weise einwirken, um dieses Ziel zu erreichen.[4]

---

[1] Kant, Immanuel (1724 - 1804) : Über den Gemeinspruch: Das mag in der Theorie richtig sein, taugt aber nicht für die Praxis, http://www.zeno.org/Philosophie/M/Kant,+Immanuel/Über+den+Gemeinspruch%3A+Das+mag+in+der+Theorie+richtig+sein,+taugt+aber+nicht+für+die+Praxis/II.+Vom+Verhältnis+der+Theorie+zur+Praxis+im+Staatsrecht, 02.11.19

[2] Ladenthin, Volker: Eine Gesellschaft braucht Gesetze, netzwerk ethik heute, https://ethik-heute.org/eine-gesellschaft-braucht-gesetze/, 02.11.19

[3] URL: https://www.getabstract.com/de/zusammenfassung/nomoi/35632, 04.11.19

[4] vgl. ebd., weitere Einsicht: Platon: Nomoi, Die Gesetze, URL: http://www.opera-platonis.de/Nomoi.pdf, 04.11.19

Eine modernere Meinung diesbezüglich, die später noch häufig diskutiert oder abgewandelt aufgegriffen wurde, ist die von Thomas Hobbes. Thomas Hobbes war ein britischer Philosoph der von 1588 bis 1679 lebte.[5] Er nimmt für seine Argumentation einen Naturzustand an und leitet ausgehend von diesem neunzehn natürliche Gesetze her. Dieser Zustand beschreibt eine Situation ohne alle Gesetze, in der sich der Mensch ganz seiner Natur gemäß verhalten kann, jedoch liegt im Wesen eben dessen „da[ss] das Ziel menschlichen Verlangens nicht darin besteht, nur einmal und einen Augenblick zu genießen, sondern sich für immer den Weg zu seinem zukünftigen Verlangen zu sichern."[6]

Hieraus ergibt sich eine Konkurrenz zwischen Menschen um verschiedene Güter, aus welcher wiederum Unsicherheit resultiert.

Aus dieser unerwünschten Unsicherheit folgt eine allgemeine Regel der Vernunft, nämlich "suche Frieden, solange nur Hoffnung darauf besteht; verschwindet diese, so schaffe dir von allen Seiten Hilfe und nutze sie; dies steht dir frei."[7] Enthalten in dieser Regel ist das erste natürliche Gesetz, den Frieden als Idealzustand mit allen Mitteln erreichen zu wollen, aus welchem viele weitere abzuleiten sind. Hierunter, dass Verträge einzuhalten sind, dass alle Menschen von Natur aus untereinander gleich sind oder auch dass "niemand [...] durch Tat, Wort, Miene oder Gebärde Verachtung oder Haß gegen jemand zeigen"[8] darf. Ebenfalls ist Vergangenes zu vergeben, sofern die vorausgegangene Tat bereut wird, was nicht heißt, dass Verstöße nicht bestraft werden, allerdings stets lediglich mit der Absicht "den Sünder zu bessern oder andere zu warnen".[9] Des Weiteren beziehen sich manche der Gesetze auf Rechtssprüche, unter anderem indem es heißt, Friedensschlüsse müssen unparteiisch sein, niemand darf in seinem eigenen Fall Richter sein, eine Zeugenaussage ist im Sreitfall entscheidend. Durch derartige Gesetze, die aus dem natürlichen Wunsch des Menschen hervorgehen, sicher zu sein, soll der Frieden zwischen den Menschen gewahrt werden. Worin ebenfalls die Notwendigkeit eines Staats begründet ist, da Gesetze ohne Executive lediglich hohle Wörter sind.[10]

Ähnlich diesem Ansatz, sucht auch Hugo Grotius, ein niederländischer Aufklärer, der etwa zur gleichen Zeit lebte, einen Ursprung der Gesetze. Dieser liegt ihm zufolge in der

[5] vgl. Horster, Detlef: Texte zur Ethik, Zu den Autorinnen und Autoren, Reclam, Stuttgart 2012, S.403
[6] Hobbes, Thomas: Leviathan, Hamburg, Meiner, 1996, S. 4, URL: https://homepage.univie.ac.at/charlotte.annerl/texte/hobbes.pdf
[7] Hobbes, Thomas: Der Staatsvertrag, Von den beiden ersten natürlichen Gesetzen und den Verträgen, in: Horster, Detlef: Texte zur Ethik, Reclam, Stuttgart 2012, S. 312
[8] ebd. S. 317
[9] ebd. S.317
[10] vgl. ebd. S.313ff

Natur des Menschen, weshalb Grotius als ein Vertreter der Naturrechtstheorie angesehen wird. Es ist dem Menschen nun also der Drang der Selbsterhaltung sowie das Sehnen nach Soziabilität gegeben, welche sich im Wunsch nach einem friedlichen Zusammenleben vereinen. Aus diesem Begehren, in Verbindung mit den besonderen Fähigkeiten der Vernunft, über die der Mensch verfügt, resultiert das Gesetz.[11] In dem Willen nach einem Zusammenleben, welches erst durch Gesetze in einer wünschenswerten Form ermöglicht wird, sieht auch David Hume, ein schottischer Philosoph und Vertreter der Aufklärung, der im 18. Jahrhundert lebte,[12] die Notwendigkeit und die Entstehung der Gesetze zu suchen. Ausgehend von der These, dass sich "[n]ur in dem Menschen [...] die unnatürliche Verbindung von Schwäche und Bedürfnis in vollstem Maße ausgeprägt"[13] wiederfindet, schließt er, dass eine Kompensation eben dieses Nachteiles lediglich in einer Gesellschaft gefunden werden kann. Diese Gemeinschaft ist dann nicht nur im Stande, die Schwäche gegenüber anderen Arten auszugleichen, nein kann sogar dazu führen, dass der Mensch im Vergleich durch Überlegenheit glänzt. "Durch die Vermehrung von Kraft, Geschicklichkeit und Sicherheit wird die Gesellschaft nützlich."[14] Allerdings ist es in einem wilden, unkultivierten Zustand schwierig, wenn nicht unmöglich für den Menschen, diese Vorteile zu erkennen, weshalb zum einen durch die Natur gegeben ist, dass Menschen ein Bedürfnis nach Zusammenschlüssen haben und sie zum anderen Vorstellungen von Laster und Tugend haben, letzteres bemächtigt sie, über Verhalten zu urteilen. Aufgrund dieser Voraussetzungen wissen Menschen eine Gesellschaft zu schätzen, beziehungsweise können die Probleme besser beurteilen, die damit einhergehen können. So sind vor allem Güter Auslöser von Streitigkeiten, weshalb eine Besitzklärung derlei Auseinandersetzungen vorbeugen kann und hiermit nötig wird. Allerdings bezeichnet Eigentum "die Güter, deren Besitz uns durch die Gesetze der Gesellschaft gesichert ist"[15], womit Gesetze wichtig sind.[16] "Die Rechtsordnung hat nur in der Selbstsucht und der beschränkten Großmut der Menschen, im Verein mit der knappen Fürsorge, die die Natur für ihre Bedürfnisse getragen hat, ihren Ursprung"[17], fasst Hume abschließend zusammen.

[11] vgl. Aure, Andreas H., Der säkularisierte und subjektivierte Naturrechtsbegriff bei Hugo Grotius, https://forhistiur.de/2008-02-aure/, 05.11.19
[12] vgl. Horster, Detlef: Texte zur Ethik, Zu den Autorinnen und Autoren, Reclam, Stuttgart 2012, S.404
[13] Hume, David: Der Ursprung von Rechtsordnung und Eigentum, in in: Horster, Detlef: Texte zur Ethik, Reclam, Stuttgart 2012, S.321
[14] ebd. S.322
[15] ebd.S.326
[16] vgl. ebd S.321 ff
[17] ebd. S.329

Hervorzuheben ist hierbei, dass Hume den Menschen einen gewissen Grad an natürlichem moralischen Verhalten zugesteht oder zumindest die Fähigkeit, gut und böse zu unterscheiden, über Tugend zu verfügen. Ähnlich geht auch Rousseau, ein Schweizer Vertreter der Aufklärung, ebenfalls aus dem 18. Jahrhundert, bei der Entwicklung seines Gesellschaftsvertrages, der einen Versuch darstellt "eine staatliche Ordnung moralisch und institutionell zu begründen"[18], von ursprünglich moralischen Menschen aus. Im Gegensatz hierzu Hobbes, dessen bereits geschilderte Theorie von dieser Fähigkeit der Menschen befreit eine Erklärung für Gesetze sucht. Dieser Unterschied führt zu einer weiteren großen Frage der Rechtsphilosophie, nämlich nach dem Verhältnis zwischen Moral und Rechtsnormen, allerdings würde eine Erläuterung desselben an dieser Stelle zu weit führen.[19]

Zusammenfassend werden von den hier dargestellten Philosophen in den Gesetzen Vorteile für die Menschen gesehen, und durch diese die Möglichkeit eines Zusammenlebens in einer Gesellschaft überhaupt ermöglicht. Sei der positive Gewinn nun in der erlangten Sicherheit oder auch in der vermehrten Macht als Folge der Gemeinschaft zu suchen, immer geht ein klarer Nutzen für alle daraus hervor. Ein Nutzen, der so groß ist, dass er die ebenfalls notwendigen, freiheitseinschränkenden Folgen überschattet, schließlich ist Frieden das übergeordnete Gut, welches es durch diese zu erreichen gilt. "Die Gerechtigkeit ist die zweite große Aufgabe des Rechts, die erste aber ist die Rechtssicherheit, der Friede."[20]

Compliance ist ein im deutschen Recht vergleichsweise eher neuer Begriff, der im Deutschen Corporate Governance – Kodex erst seit der Fassung von 2007 Verwendung findet und ein wichtiges Unternehmensziel darstellt.[21] Er bedeutet im Prinzip die Einhaltung von Vorschriften, die in vier Bereiche eingeteilt werden können. Erstens rechtliche Vorgaben wie Gesetze oder Rechtsvorschriften, zweitens Verträge mit Kunden oder Partnern, drittens interne und viertens externe Regelwerke. Letztere sind beispielsweise Normen und Standards wie ISO 27 001, während interne Richtlinien beispielsweise das Rechte- oder das Risikomanagement regeln.

---

[18] Harrer, Julia: Jean-Jacques Rousseau: Der Gesellschaftsvertrag, studienarbeit, 2012, Grin, URL: https://www.grin.com/document/205970, 03.11.19

[19] Zu diesem Thema auch interessant: Die philosophische Strömung des Kontraktualismus oder Vertragstheorie, die die Moral als etwas vom Menschen Erzeugtes sieht und über welche der Vertrag abgeschlossen wird.

[20] Radbruch, Prof. Dr. Gustav (1878 - 1949), https://legalcareers.de/static_pages/Juristische_Zitate_02, 06.11.19

[21] vgl. URLs: https://www.dcgk.de/de/kodex/archiv.html, https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/170424_Kodex.pdf, Abschnitt 4.1.3, 03.10.19

Bedingt durch die fortlaufende rasante Weiterentwicklung technischer Möglichkeiten müssen beispielsweise auch die entsprechenden IT-Sicherheitsmaßnahmen ständig angepasst werden. Das spiegelt sich in regelmäßigem Überarbeiten bestehender oder Erlassen neuer gesetzlicher Vorgaben wieder. Zu nennen wären in diesem Zusammenhang das seit 2015 geltende Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) sowie die Anpassungen an der Strafprozessordnung von 2017, gegen die 2018 Verfassungsbeschwerde eingereicht wurde.[22] Für Unternehmen ergibt sich daraus die Schwierigkeit, den Überblick über alle für sie geltenden Regelungen und Gesetze zu behalten und diese möglichst effizient und effektiv umzusetzen.

Im Folgenden sollen einige compliancerelevante Gesetze und Regelungen, dabei auch mögliche Konfliktsituationen und Zusammenhänge zwischen denselben, insbesondere in Hinblick auf den Datenschutz und damit die Datenschutz-Grundverordnung der EU, dargelegt werden. Dabei wird zunächst auf die rechtlichen Grundlagen des Datenschutzes näher eingegangen und im Anschluss werden Compliance-Maßnahmen, die zum Teil ebenfalls gesetzlich vorgeschrieben sind, näher erläutert, zuletzt sollen einige bereits bestehende, auf der Grundlage der DSGVO gefällte Urteile vorgestellt werden. Da vertragliche Verpflichtungen für jedes Unternehmen spezifisch sein können, werden diese hier nicht behandelt, auch wenn sie für eine umfassende Compliance selbstverständlich ebenso einzuhalten sind.

2 Bedeutung Datenschutz

Mit der zunehmenden Bedeutung von technischen Systemen, insbesondere Mobiltelefonen, im Alltagsleben steigt auch die Menge der damit erhobenen und gespeicherten Daten. Anhand dieser Informationen sind zahlreiche Rückschlüsse auf den Nutzer des betreffenden Gerätes möglich, beispielsweise auf seine Identität, sein Geschlecht und seine Gewohnheiten, unter Umständen auch auf seinen Gesundheitszustand oder seine religiösen Ansichten.[23] Ein Smartphone kann so vielfältige persönliche Informationen enthalten, dass ihre Kenntnis nicht nur ein deutliches Bild des privaten Lebens des Nutzers, sondern auch seines Charakters ergeben kann, gerade durch

[22] vgl. URL : https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-staatstrojaner-fdp-anwalt-interview-online-durchsuchung/, 20.09.19

[23] vgl. Mylonas, Alexios: Security and Privacy in Ubiquitous Computing: The Smart Mobile Equipment Case, 2013, S.1ff

die zunehmende Verwendung solcher Geräte zur Kommunikation.[24] In Zeiten des Internets und damit einer vernetzten Welt, ist es technisch möglich, massenhaft Daten zu erheben, aus verschiedenen Quellen zusammenzuführen, zu speichern und flexibel auszuwerten. Dieses Vorgehen, unter dem Begriff Big Data bekannt, wird zum Beispiel schon länger für Scoring-Verfahren in der Kreditwirtschaft eingesetzt[25] oder für Ansätze im Bereich ‚Predictive Policing', also vorausschauende Polizeiarbeit, verwendet.[26] Und Daten werden heutzutage überall erhoben: bei Zahlungen mit EC-Karte[27] oder PayPal, beim Telefonieren mit Festnetz- oder Mobiltelefon werden bekanntermaßen Protokolle angefertigt, beim Aufrufen von Webseiten im Internet werden die IP-Adressen gespeichert, moderne Autos enthalten bis zu 100 Mikrochips, die die Klimaanlage steuern, bei Unfällen für das Auslösen des Airbags sorgen oder „Gesten des Fahrers erkennen und im Display entsprechende Funktionen anbieten."[28] Smarte TV-Geräte, die das Surfen im Internet und die Steuerung per Mikrofon ermöglichen, übermitteln Daten an die Hersteller.[29] Insgesamt werden im Bereich der künstlichen Intelligenz Unmengen an Daten verwendet.[30] Zusätzlich teilen sehr viele Menschen haufenweise auch persönliche Informationen auf Social Media Plattformen.

„Die zunehmende Vernetzung und Digitalisierung in allen Lebensbereichen, *ubiquitous computing* genannt, macht das soziale Verhalten eines Individuums immer zentraler zugänglich"[31], was zu einem Kontrollverlust über die eigenen persönlichen Daten führt.[32] Dabei ist „Privatsphäre als notwendiges Mittel zur autonomen Lebensführung in einer

[24] vgl. Mylonas et al.: Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition, 2011, S.254

[25] Mittels statistischer Verfahren werden hierzu Personen in Gruppen eingeteilt und bekommen einen Score, nach diesem wird dann über die Höhe der Kreditzinsen entschieden, beziehungsweise ob jemand überhaupt einen Kredit erhält oder nicht.

[26] vgl. Schaar, Peter : Datenschutz in Zeiten von Big Data, in: HMD Praxis der Wirtschaftsinformatik, 2014, S.840-852, S. 842f

[27] vgl. Lischka, Konrad : Zahlung per EC-Karte – Was die Datensammler wirklich wissen, Spiegel online, 2010, URL: https://www.spiegel.de/netzwelt/web/zahlung-per-ec-karte-was-die-datensammler-wirklich-wissen-a-719168.html, 12.10.19

[28] Deuse, Klaus : Intelligente Helfer – Halbleiter im Auto, 2014, URL: https://p.dw.com/p/1CgV1, 12.10.19

[29] vgl. URL : https://www.dirks-computerseite.de/smart-tv-vorteile/#:~:text=Vorteile%20und%20Nachteile%20der%20Smart%20TV%20Ger%C3%A4te&text=Daf%C3%BCr%20bekommt%20man%20mit%20den,das%20Budget%20im%20Auge%20beh%C3%A4lt., 12.10.19

[30] vgl. Kuhnigk, Nadine : Künstliche Intelligenz und Datenschutz: Passt nicht immer, in: Mainpost, 26.9.19, URL: https://www.mainpost.de/ueberregional/wirtschaft/mainpostwirtschaft/Kuenstliche-Intelligenz-und-Datenschutz-Passt-nicht-immer;art9485,10305975, 28.09.19

[31] Hotter, Maximilian : Privatsphäre – Der Wandel eines liberalen Rechts im Zeitalter des Internets, Campus Verlag GmbH, Frankfurt am Main, 2011, S.129

[32] vgl. Hotter, Maximilian : Privatsphäre – Der Wandel eines liberalen Rechts im Zeitalter des Internets, Campus Verlag GmbH, Frankfurt am Main, 2011, S.129f.

komplexen modernen Gesellschaft“[33] von zentraler Bedeutung. Wenn der Einzelne nun immer weniger selbst darüber entscheiden kann, wer wann was über ihn in Erfahrung bringen oder wissen darf, dann ist Kontrolle zum Schutz der Person, ihres privaten Lebens sowie ihrer Menschenwürde in anderer Instanz vonnöten.

Das weltweit erste Datenschutzgesetz wurde 1970 von Hessen verabschiedet, 1977 dann das Bundesdatenschutzgesetz (BDSG). Durch das Volkszählungsurteil des Bundesverfassungsgerichts 1983 wurde das Recht auf informationelle Selbstbestimmung aus dem Grundgesetz heraus abgeleitet und der Datenschutz damit unmissverständlich als Grundrecht etabliert.[34]

Dieses Recht ist im deutschen Grundgesetz (Art. 2 Abs. 1, Art. 1 Abs. 1 GG), der Europäischen Menschenrechtskonvention (Art. 8 EMRK) und der Charta der Grundrechte der Europäischen Union (Art. 8 EuGRCh) fest verankert.[35] Während sich dieses Grundrecht aus dem im seit 1949 gültigen[36] GG beschriebenen Recht auf freie Entfaltung der Persönlichkeit[37] sowie der in Artikel 1 Absatz 1 GG verankerten Unantastbarkeit der Würde des Menschen[38] noch eher indirekt ableiten lässt, da eine freie Entfaltung eine Überwachung ausschließt und damit die Privatssphäre schützt, ist in Artikel 8 Absatz 1 EMRK bereits vom „Recht auf Achtung [des] Privat- und Familienlebens“[39] die Rede, das ebenfalls in Artikel 7 EuGRCh aufgeführt ist. Artikel 8 EMRK besteht noch heute in seiner ursprünglichen Form von 1950[40] und erlaubt einen behördlichen Eingriff in dieses Persönlichkeitsrecht nur, „soweit [dieser] gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig“[41] für bestimmte Schutzziele ist, darunter auch die Moral und das wirtschaftliche Wohl des Landes.[42]

In Artikel 8 EuGRCh ist der Schutz personenbezogener Daten geregelt, hier wird bereits die Zweckbindung und die Einwilligung in die Verarbeitung sowie das Auskunftsrecht betroffener Personen und die Überwachung der Vorschriften durch eine unabhängige Stelle genannt.[43]

---

[33] Hotter, Maximilian : Privatsphäre – Der Wandel eines liberalen Rechts im Zeitalter des Internets, Campus Verlag GmbH, Frankfurt am Main, 2011, S.82
[34] vgl. URL : https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/, 13.07.19
[35] vgl. URL : https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/PDF-Dateien/Factsheets/factsheet_grundrecht_auf_datenschutz_07_05_2010.pdf, 15.07.19
[36] vgl. URL : https://www.gesetze-im-internet.de/gg/BJNR000010949.html, 15.07.19
[37] vgl. Art. 2, Abs. 1 GG, URL: https://dejure.org/gesetze/GG/2.html
[38] vgl. Art. 1, Abs. 1 GG, URL: https://dejure.org/gesetze/GG/1.html
[39] Art. 8, Abs. 1 EMRK, URL: https://dejure.org/gesetze/MRK/8.html
[40] vgl. URL : http://www.eugrz.info/PDF/EGMR1/Konvent.pdf, 03.07.19
[41] Art. 8 Abs. 2 EMRK, URL: https://dejure.org/gesetze/MRK/8.html
[42] vgl. Art. 8 Abs. 2 EMRK, URL: https://dejure.org/gesetze/MRK/8.html
[43] vgl. Art. 8 EuGRCh, URL: https://dejure.org/gesetze/GRCh/8.html

Ausführlicher wurde der Datenschutz von 1995 bis 2018 in der EU-Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr geregelt.[44] EU-Richtlinien legen gemeinsame Ziele der Mitgliedstaaten fest, die durch Erlassen nationaler Rechtsvorschriften umgesetzt werden sollen.[45] Hierfür ist in der Richtlinie 95/46/EG eine Frist von drei Jahren nach Annahme der Richtlinie, also bis 1998, festgelegt.[46] In Deutschland erfolgte eine entsprechende Anpassung des Bundesdatenschutzgesetzes (BDSG) erst ab 2001, also sechs Jahre später,[47] nachdem die Kommission gegen Deutschland und andere Länder beim Europäischen Gerichtshof Klage wegen „Nichteinhaltung der Pflicht zur Notifizierung aller zur Umsetzung der Richtlinie 95/46/EG erforderlichen Maßnahmen“[48] eingereicht hat.[49] Eine weitere Datenschutzrichtlinie von 2002 (RL 2002/58/EG) führte 2004, also zwei Jahre später, zu einer tatsächlichen Erneuerung des Telekommunikationsgesetzes (TKG) in Deutschland.[50] Die jeweiligen unterschiedlichen nationalen Umsetzungen der Richtlinien in den Mitgliedstaaten hinderten zusätzlich durch die verschieden strengen Datenschutzstandards den grenzüberschreitenden Datenverkehr, was sich mit der EU-Datenschutzgrundverordnung (DSGVO) ändern sollte. Diese stützt sich neben der EU-Grundrechtecharta besonders auch auf Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).[51] Nach diesem hat „[j]ede Person [...] das Recht auf Schutz der sie betreffenden personenbezogenen Daten“[52] und „[d]as Europäische Parlament und der Rat erlassen [...] Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr.“[53]

[44] vgl. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31995L0046, 03.09.19
[45] vgl. URL : https://europa.eu/european-union/eu-law/legal-acts_de, 17.09.19
[46] vgl. Art. 32 Abs. 1 RL 95/46/EG, URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31995L0046
[47] vgl. URL : https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/, 20.10.19
[48] Artikel 29-Datenschutzgruppe: Fünfter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Gemeinschaft und in Drittländern, 2002, S.13, URL: https://www.zaftda.de/tb-artikel-29-gruppe/143-05-ii-jahresbericht-art-29-gruppe-2000-06-03-2002/file, 18.09.19
[49] vgl. ebd.
[50] vgl. https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/, 20.10.19
[51] vgl. URL: https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html
[52] Art. 16 Abs. 1 AEUV, URL : https://dejure.org/gesetze/AEUV/16.html
[53] Art. 16 Abs. 2 AEUV, URL : https://dejure.org/gesetze/AEUV/16.html

Der Umgang mit EU-Verordnungen, -Richtlinien, -Beschlüssen, Empfehlungen und Stellungnahmen ist in Artikel 288 AEUV näher beschrieben.[54]

EU-Verordnungen wie die DSGVO sind im Gegensatz zu Richtlinien unmittelbar für alle Mitgliedstaaten verbindlich,[55] wodurch Aufschübe von mehreren Jahren, wie sie bereits dargestellt wurden, an dieser Stelle weniger problematisch sind, da Verordnungen nach dem Inkrafttreten direkt angewendet werden können und bis auf einige sogenannte Öffnungsklauseln, Kollisionsregeln oder Umsetzungsaufträge, die einen gewissen Spielraum für nationale Umsetzungen lassen, einheitlich geltendes Recht sind.[56] Grundsätzlich werden sowohl bei Richtlinien als auch Verordnungen Umsetzungsfristen festgelegt, im Falle der DSGVO waren dies zwei Jahre, von 2016 bis 2018. Die DSGVO gilt seit dem 25.05.2018,[57] sie löst die EU-Richtlinie 95/46/EG ab.[58] Eine Öffnungsklausel findet sich zum Beispiel in Artikel 6 Absatz 2 DSGVO, der den Mitgliedstaaten das Recht einräumt, „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung [...] bei[zu]behalten oder ein[zu]führen." Eine Öffnungsklausel dient also einer nationalen Umsetzung im Sinne von Konkretisierungen einzelner, hier datenschutzrechtlicher, Aspekte.[59] Eine Kollisionsregel findet sich in der DSGVO in Artikel 95 DSGVO, hier wird das Verhältnis der DSGVO zu einer EU-Richtlinie und damit ihren nationalen Umsetzungen geregelt.[60] Einen Umsetzungsauftrag stellt beispielsweise Artikel 85 DSGVO dar, in dem die Mitgliedstaaten ausdrücklich aufgefordert werden, entsprechende Rechtsvorschriften zu erlassen.[61]

---

[54] vgl. Art. 288 AEUV, URL : https://dejure.org/gesetze/AEUV/288.html
[55] vgl. URL : https://europa.eu/european-union/eu-law/legal-acts_de, 30.10.19
[56] vgl. Unterrichtung durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit, 27.Tätigkeitsbericht, Drucksache 19/9800, 08.05.2019, S. 99, URL: http://dip21.bundestag.de/dip21/btd/19/098/1909800.pdf
[57] vgl. URL : https://www.datenschutz-grundverordnung.eu/rechtsnormen-der-dsgvo/art-99-eu-dsgvo/, 27.09.19
[58] vgl. URL : https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html, 27.08.19
[59] vgl. URL: https://www.gabler-banklexikon.de/definition/europaeische-datenschutzgrundverordnung-eu-dsgvo-81652, 28.08.19
[60] vgl. DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 2, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, 30.08.19
[61] vgl. Art. 85 DSGVO, URL: https://dejure.org/gesetze/DSGVO/85.html und https://www.fachportal-steuerrecht.de/jportal/portal/page/fpsteuerrecht.psml?nid=jpr-NLBAADG000818&cmsuri=%2Ffachportal_steuerrecht%2Fde%2Fr17%2Fnachrichten_1%2Fzeige_nachricht.jsp, 02.09.19

3 DSGVO

Zur leichteren Verständlichkeit und für einen besseren Überblick werden nun vorerst kurz der Aufbau der DSGVO erklärt und einige Artikel, auf die im weiteren Verlauf häufig Bezug genommen wird, näher ausgeführt. Das erste Kapitel der DSGVO legt in allgemeinen Bestimmungen die Ziele der Verordnung, den räumlichen und sachlichen Anwendungsbereich, sowie im Folgenden verwendete Begriffe fest. So dient die DSGVO dem Schutz der Grundrechte natürlicher Personen, besonders in Hinsicht auf Datenschutz, aber gleichzeitig dem uneingeschränkten freien Datenverkehr innerhalb der EU.[62] Sie gilt, im Gegensatz zur Richtlinie 95/46/EG in Kombination mit den unterschiedlichen Umsetzungen, auch für Unternehmen mit Sitz außerhalb der EU, sofern diese personenbezogene Daten von EU-Bürgern verarbeiten (Art. 3 Abs. 2 DSGVO).[63] In Artikel 4 DSGVO finden sich die Begriffsbestimmungen. Im Folgenden sollen ein paar wenige ausgewählte Begriffe, die für diese Arbeit besonders grundlegend sind, genauer vorgestellt werden.

Personenbezogene Daten nach der DSGVO sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“,[64] darunter fallen beispielsweise Namen, Adressen, genetische Merkmale oder Kennnummern der darüber identifizierbaren Personen.[65] Auch IP-Adressen oder Cookie-Kennungen sind personenbezogene Daten.[66]

Eine Verarbeitung ist jeder Vorgang oder jede Abfolge von Vorgängen in Zusammenhang mit personenbezogenen Daten, die mit oder ohne Hilfe von automatischen Verfahren ausgeführt wird, beispielsweise das Erfassen, Erheben, die Organisation, die Speicherung oder die Verwendung dieser Daten.[67]

Der Verantwortliche ist eine „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“[68], diese also zum Beispiel zu

[62] vgl. Art. 1f. DSGVO, URLs: https://dejure.org/gesetze/DSGVO/1.html, https://dejure.org/gesetze/DSGVO/2.html
[63] vgl. Art. 3, Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/3.html
[64] Art. 4, Nr. 1. DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[65] vgl. Art. 4, Nr. 1. DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[66] vgl. URL : https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_de, 07.09.19
[67] vgl. Art. 4, Nr. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[68] Art.4, Nr 7 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html

Zwecken der Marktforschung erhebt oder aufgrund bestehender Aufbewahrungsfristen speichert.

Die Einwilligung ist im Sinne der DSGVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung“[69], die das Einverständnis in die Verarbeitung deutlich macht.[70]

Ein Unternehmen ist „eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform“.[71]

Kapitel 2 der DSGVO umfasst Artikel 5 bis 11 und erklärt die Grundsätze der Verordnung.

In Artikel 5 DSGVO werden Verarbeitungsgrundsätze für personenbezogene Daten aufgeführt, nämlich die Rechtmäßigkeit, die Transparenz, die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung sowie die Integrität und Vertraulichkeit der Datenverarbeitung. Rechtmäßig ist eine solche Verarbeitung laut Artikel 6 DSGVO beispielsweise, wenn die betroffene Person ihre Einwilligung dazu gegeben hat, wenn sie für eine Vertragserfüllung oder im Zuge vorvertraglicher Maßnahmen nötig ist, wenn die Erfüllung rechtlicher Verpflichtungen selbige erfordert oder damit lebenswichtige Interessen einer natürlichen Person geschützt werden.[72] Hierbei ist zu beachten, dass die für die Rechtmäßigkeit der Verarbeitung in vielen Fällen erforderliche Einwilligung der betroffenen Person in die Verarbeitung ihrer Daten durch die Begriffsbestimmungen in Artikel 4 DSGVO voraussetzt, dass die betroffene Person über den oder die jeweiligen Zwecke aufgeklärt und informiert wurde. In Artikel 7 und 8 DSGVO werden Bedingungen für die Einwilligung von Personen in die Verarbeitung sie betreffender Daten näher beschrieben.[73] Die Einwilligung muss vom Verantwortlichen nachgewiesen werden können und kann von der betroffenen Person jederzeit widerrufen werden, was auf die Rechtmäßigkeit der Verarbeitung bis zu diesem Zeitpunkt keine Auswirkung hat, diese also nicht rückwirkend betrifft. Bei Kindern und Jugendlichen unter sechzehn Jaheren ist nach Artikel 8 der DSGVO „bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird“,[74] zusätzlich die Einwilligung der „Träger der elterlichen Verantwortung“[75] nötig, der Verantwortliche hat

[69] Art. 4, Nr. 11 DSGVO, URL : https://dejure.org/gesetze/DSGVO/4.html
[70] vgl. Art. 4, Nr. 11 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[71] Art. 4, Nr. 18 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[72] vgl. Art. 6 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[73] vgl. Art. 7, 8 DSGVO, URL : https://dejure.org/gesetze/DSGVO/7.html, https://dejure.org/gesetze/DSGVO/8.html
[74] Art. 8 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/8.html
[75] Art. 8 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/8.html

„unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen“[76] zu unternehmen, um die Erfüllung dieser Bedingung sicherzustellen.[77] Die festgesetzte Altersgrenze von sechzehn Jahren kann von den Mitgliedstaaten bis zu einem erforderlichen Alter von dreizehn Jahren gesenkt werden, hiermit bietet die DSGVO eine Öffnungsklausel für eine Anpassung an national übliche Altersbestimmungen. Dienste der Informationsgesellschaft sind, wie in Artikel 4 Nummer 25 DSGVO erklärt, in Artikel 1 Nummer 1 Buchstabe b der EU-Richtlinie 2015/1535 definiert.[78] Demnach muss es sich um eine in der Regel gegen Entgelt und ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbrachte Dienstleistung, die durch die Übertragung von Daten mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten auf individuelle Anforderung erbracht wird, handeln, damit Artikel 8 DSGVO Anwendung finden kann. Im Anhang I der selben Richtlinie werden Beispiele von Dienstleistungen genannt, die nicht unter diese Kategorie fallen, so könnte man hierfür exemplarisch Sprachtelefondienste oder ärztliche Untersuchungen bei Anwesenheit des Patienten anführen.[79] Artikel 7 Absatz 4 DSGVO enthält ein Kopplungsverbot. So muss bei der Beurteilung der Freiwilligkeit einer Einwilligung besonders berücksichtigt werden, „ob [...] die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist.“[80] Eine Einwilligung kann also als nicht freiwillig und damit nicht mehr als Grundlage für die Rechtmäßigkeit einer Verarbeitung gesehen werden, wenn sie eine nicht für die Vertragserfüllung notwendige Datenverarbeitung betrifft, die dennoch vom Verantwortlichen im Zuge des Vertrags gefordert wurde. In Artikel 9 DSGVO wird die Verarbeitung besonderer Kategorien personenbezogener Daten thematisiert. Dabei geht es um Informationen, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit“[81] hervorgehen, aber auch um biometrische oder genetische Daten, die eine eindeutige Identifizierung einer Person erlauben, Gesundheitsdaten oder das Sexualleben einer natürlichen Person betreffende

[76] Art. 8 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/8.html
[77] vgl. Art. 7, 8 DSGVO, URL : https://dejure.org/gesetze/DSGVO/7.html, https://dejure.org/gesetze/DSGVO/8.html
[78] vgl. Art. 4 Nr. 25 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[79] vgl. Artikel 1 Nummer 1 Buchstabe b und Anhang I EU-Richtlinie 2015/1535, URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015L1535
[80] Art. 7 Abs. 4 DSGVO, URL: https://dejure.org/gesetze/DSGVO/7.html
[81] Art. 9 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html

Daten.[82] Hier handelt es sich um ein Verbot mit Erlaubnisvorbehalt, da eine Verarbeitung solcher Daten in Absatz 1 grundsätzlich für unzulässig erklärt wird und in Absatz 2 Ausnahmen für Absatz 1 genannt werden. In Artikel 9 Absatz 2 Buchstabe a wird festgelegt, dass eine Verarbeitung solcher Daten zulässig ist, wenn eine ausdrückliche Einwilligung des Betroffenen vorliegt, es sei denn, im jeweiligen Mitgliedstaat ist dies nicht ausreichend, um das Verbot aufzuheben. Zusätzlich dazu wird in Absatz 4 des selben Artikels ausdrücklich die Möglichkeit weiterer Beschränkungen oder Bedingungen der Mitgliedstaaten genannt.[83] Die neun weiteren Erlaubnistatbestände neben der ausdrücklichen Einwilligung beziehen sich beispielsweise auf aus dem Arbeitsrecht und dem Recht der sozielen Sicherheit und des Sozialschutzes erwachsende Rechte und Pflichten, den Schutz lebenswichtiger Interessen natürlicher Personen, öffentliches Interesse oder offensichtlich öffentlich gemachte Daten.[84] Artikel 10 DSGVO regelt die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen oder Straftaten, die nur unter behördlicher Aufsicht vorgenommen werden darf,[85] Artikel 11 befasst sich mit Verarbeitungen, für die eine Identifizierung der betroffenen Person nicht erforderlich ist.[86]

In Kapitel 3 sind die Rechte der betroffenen Person in fünf Abschnitten festgelegt. Es umfasst die Mitteilungs- und Informationspflichten des Verantwortlichen, das Auskunftsrecht der betroffenen Person, die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, das Widerspruchsrecht und Beschränkungen derselben.[87] Demnach ist der Verantwortliche verpflichtet, die betroffene Person zum Zeitpunkt der Datenerhebung über Namen und Kontaktdaten des oder der Verantwortlichen sowie des Datenschutzbeauftragten, den oder die Zwecke der Datenverarbeitung sowie ihre Rechtsgrundlage, die Kategorien der personenbezogenen Daten, unter Umständen die Empfänger der Daten, die Dauer der Speicherung oder die Kriterien zur Bestimmung derselben, das Bestehen verschiedener Betroffenenrechte, einschließlich des Beschwerderechts bei einer Aufsichtsbehörde, sowie gegebenenfalls die Quelle der personenbezogenen Daten, falls diese nicht beim Betroffenen erhoben wurden, zu informieren.[88] Auf Antrag ist der betroffenen Person eine Kopie der

[82] vgl. Art. 9 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[83] vgl. Art. 9 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[84] vgl. Art. 9 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[85] vgl. Art. 10 DSGVO, URL: https://dejure.org/gesetze/DSGVO/10.html
[86] vgl. Art. 11 DSGVO, URL: https://dejure.org/gesetze/DSGVO/11.html
[87] vgl. Art. 12-23 DSGVO
[88] vgl. Art. 13, 14 DSGVO

verarbeiteten personenbezogenen Daten zur Verfügung zu stellen.[89] Desweiteren kann der Betroffene eine unverzügliche Berichtigung unrichtiger personenbezogener Daten[90] oder die unverzügliche Löschung der ihn betreffenden Daten verlangen.[91]

Kapitel 4 legt die weiteren Pflichten des Verantwortlichen fest, regelt die Rolle des Datenschutzbeauftragten und von Zertifizierungen.[92] Hierunter fallen der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Artikel 25 DSGVO, wonach der Verantwortliche „[u]nter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen [...] sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen [ergreifen muss] [...], um den Anforderungen dieser Verordnung zu genügen und die Rechte der Betroffenen zu schützen.“[93] In Art. 25, Abs. 2 DSGVO werden zusätzlich datenschutzfreundliche Voreinstellungen gefordert.[94] Die zu ergreifenden Maßnahmen werden weder im Gesetzestext selbst noch im zugehörigen Erwägungsgrund 78 näher spezifiziert, es werden lediglich Beispiele genannt, wie die Pseudonymisierung oder die Möglichkeit, die Verarbeitung personenbezogener Daten so minimal wie nötig zu halten.[95] In Absatz 3 des selben Artikels wird ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 DSGVO als Möglichkeit zum Nachweis der Erfüllung der im Artikel festgelegten Anforderungen genannt.[96] Auch Artikel 32 DSGVO befasst sich mit der Pflicht des Verantwortlichen, die Sicherheit der Verarbeitung zu gewährleisten. Hier wird als mögliche Maßnahme auch die Verschlüsselung personenbezogener Daten genannt, außerdem die drei Hauptschutzziele der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität, die der Verantwortliche ebenfalls zu gewährleisten hat.[97] Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen, so ist der Verantwortliche verpflichtet, diese der zuständigen Aufsichtsbehörde binnen 72 Stunden zu melden, sofern diese voraussichtlich „zu einem Risiko für die

[89] vgl. Art. 15 Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/15.html
[90] vgl. Art. 16 DSGVO, URL: https://dejure.org/gesetze/DSGVO/16.html
[91] vgl. Art. 17 DSGVO, URL: https://dejure.org/gesetze/DSGVO/17.html
[92] vgl. Art.24-43 DSGVO
[93] Art. 25, Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/25.html
[94] vgl. Art. 25, Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/25.html
[95] vgl. Erwägungsgrund 78, URL : https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html
[96] vgl. Art. 25, Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/25.html
[97] vgl. Art. 32, Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/32.html

Rechte und Freiheiten natürlicher Personen führt“[98], bei einem hohen Risiko sind zusätzlich die Betroffenen unverzüglich zu benachrichtigen.[99] Bei Formen von Datenverarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben können, beispielsweise umfangreiche Verarbeitungen besonderer Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO oder eine „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen“[100] ist vorab eine Datenschutz-Folgenabschätzung vorzunehmen, die zumindest eine systematische Beschreibung mit den jeweiligen Zwecken der geplanten Verarbeitungsvorgänge, eine Bewertung ihrer Notwendigkeit und Verhältnismäßigkeit sowie ihrer Risiken und die Abhilfemaßnahmen zur Bewältigung dieser Risiken enthält.[101] Benennung, Stellung und Aufgaben des Datenschutzbeauftragten sind in den Artikeln 37 bis 39 DSGVO geregelt. Demnach sind öffentliche Stellen sowie jede Art von Unternehmen, deren Kerntätigkeit die Verarbeitung personenbezogener Daten oder die Verarbeitung von in Artikel 9 DSGVO beschriebenen sensiblen Daten darstellt, verpflichtet, einen Datenschutzbeauftragten zu bestellen.[102] Der Datenschutzbeauftragte berichtet direkt der höchsten Managementebene und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.[103]

Kapitel 5 befasst sich mit der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen,[104] in Kapitel 6 werden Aufsichtsbehörden näher definiert,[105] in Kapitel 7 wird dann deren Zusammenarbeit sowie der europäische Datenschutzausschuss beschrieben.[106]

Kapitel 8 legt Rechtsbehelfe, Sanktionen und Haftung fest. In Art. 77 DSGVO ist festgehalten, dass „[j]ede betroffene Person [...] das Recht auf Beschwerde bei einer Aufsichtsbehörde [hat] [...], wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.“[107] Laut Artikel 77 Absatz 2 und Artikel 78 Absatz 2 DSGVO ist die Aufsichtsbehörde verpflichtet, einer Beschwerde nachzugehen und die betroffene Person

[98] Art. 33, Abs. 1 DSGVO, URL : https://dejure.org/gesetze/DSGVO/33.html
[99] vgl. Art. 34, Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/34.html
[100] Art. 35 Abs. 3 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/35.html
[101] vgl. Art. 35 Abs. 1 und 7 DSGVO, URL: https://dejure.org/gesetze/DSGVO/35.html
[102] vgl. Art. 37, Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/37.html
[103] vgl. Art. 38 Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/38.html
[104] vgl. Art. 44-50 DSGVO
[105] vgl. Art. 51-59 DSGVO
[106] vgl. Art. 60-76 DSGVO
[107] Art. 77, Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/77.html

über die Ergebnisse der Beschwerde zu unterrichten.[108] Hier wird deutlich, dass die betroffene Person keinerlei Indizien oder stichhaltige Beweise für eine solche Ansicht benötigt und die Aufsichtsbehörde dem in jedem Fall nachgehen muss. In Artikel 82 DSGVO sind Haftung und Schadenersatz geregelt. Demnach haftet der Verantwortliche für den Schaden, der einer Person durch einen Verstoß gegen die DSGVO entstanden ist. Besonders hervorzuheben ist dabei die sich aus Art. 82 Abs. 3 DSGVO ergebende Beweislastumkehr. Anders als üblich muss hier der Verantwortliche nachweisen können, „dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“[109], um von der Haftung befreit zu werden.[110] Nach Art. 83 Abs. 1 DSGVO sollen Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“[111] sein, dabei dürfen diese Strafen bei Verstoß beispielsweise gegen „die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43“[112] bis zu einer Höhe von 10 Millionen Euro oder 2% des gesamten weltweiten Jahresumsatzes des vergangenen Geschäftsjahres betragen. Verstöße gegen die Artikel 5, 6, 7, 9, 12 bis 22, 44 bis 49 und 58 DSGVO, die sich auf die Rechtmäßigkeit der Verarbeitung, die Auskunftsrechte der Betroffenen und die Übermittlung personenbezogener Daten an Drittländer beziehen, können sogar mit bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes geahndet werden.[113]

In Kapitel 9 finden sich die Vorschriften für besondere Verarbeitungssituationen, Kapitel 10 beschreibt delegierte Rechtsakte und Durchführungsrechtsakte, in Kapitel 11 sind die Schlussbestimmungen wie das Verhältnis zu Richtlinien oder das Inkrafttreten festgelegt.[114]

Besonders bedeutend für Unternehmen ist wohl, dass nach der DSGVO die Beweislast bei ihnen als Verantwortlichen liegt.

[108] vgl. Art. 77f DSGVO, URL: https://dejure.org/gesetze/DSGVO/77.html, https://dejure.org/gesetze/DSGVO/78.html
[109] Art. 82, Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/82.html
[110] vgl. Art. 82 DSGVO, URL: https://dejure.org/gesetze/DSGVO/82.html
[111] Art. 83 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html
[112] Art. 83 Abs. 4 DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html
[113] vgl. Art. 83 DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html
[114] vgl. Art. 85-99 DSGVO

4 Mögliche aus der DSGVO resultierende Probleme für Unternehmen

Bereits durch den in Artikel 3 DSGVO festgelegten räumlichen Anwendungsbereich der EU Verordnung können sich Probleme ergeben. Demnach müssen auch Unternehmen mit Sitz außerhalb der EU die Regelungen der DSGVO befolgen, allerdings sind Drittländer streng genommen nicht befugt, Öffnungsklauseln durch nationales Recht zu nutzen. Besonders kritische Auswirkungen könnte das im Fall von Artikel 6 DSGVO haben. In Artikel 6 Absatz 1 Buchstabe c DSGVO ist die Erfüllung rechtlicher Verpflichtungen als Grundlage für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten genannt, hierfür wird in Absatz 3 des selben Artikels als zugehörige Rechtsgrundlage ausdrücklich das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, aufgeführt.[115] Diese Länder können also bestimmte Datenverarbeitungen durch das Erlassen von Rechtsvorschriften ohne Konflikt mit der DSGVO legalisieren, Drittländer haben diese Möglichkeit allerdings nicht.[116] Laut Artikel 6 Absatz 1 Buchstabe f DSGVO ist eine Verarbeitung rechtmäßig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“.[117] Da ein Verantwortlicher, der dem nationalen Recht eines Drittlandes unterliegt, ein berechtigtes Interesse an dessen Einhaltung hat, könnte diese Bedingung derartige Konfliktfälle abfangen.[118]

Für Unternehmen, die Dienste der Informationsgesellschaft anbieten, könnten sich aus Artikel 8 DSGVO zwei Probleme ergeben. Zum einen ist nicht genau definiert, in welchem Umfang die Anstrengungen zur Feststellung der Einwilligung des Trägers der elterlichen Verantwortung angemessen sind, zum anderen sind hier nationale Anpassungen möglich, so dass unter Umständen bei internationelen Unternehmen nach unterschiedlichen Altersgrenzen verfahren werden muss.[119]

Wie bereits genannt sind Verantwortliche angehalten, den natürlichen Personen auf Antrag Auskunft über die sie betreffenden Datenverarbeitungen, den Zweck derselben,

[115] vgl. Art. 6 Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[116] vgl. URL : https://www.telemedicus.info/article/3342-OEffnungsklauseln-und-Drittstaaten-Eine-uebersehene-Luecke.html, 19.08.19
[117] Art. 6 Abs. 1 Buchstabe f DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[118] vgl. URL : https://www.telemedicus.info/article/3342-OEffnungsklauseln-und-Drittstaaten-Eine-uebersehene-Luecke.html, 27.10.19
[119] vgl. URL : https://www.datenschutzbeauftragter-info.de/anforderungen-an-die-einwilligung-von-kindern-nach-der-dsgvo/, 23.07.19

die Dauer der Speicherung der Daten sowie die Rechtsgrundlage für diese in präziser, verständlicher und leicht zugänglicher Form zu erteilen.[120] Informationen zu hierfür ergriffenen Maßnahmen sind dem Betroffenen innerhalb eines Monats zu liefern.[121] Artikel 12 Absatz 1 weist für mündlich erteilte Informationen auf einen Identitätsnachweis hin,[122] ansonsten ist der Verantwortliche lediglich im Falle „begründeter Zweifel an der Identität der natürlichen Person, die den Antrag [...] stellt [befugt], [...] zusätzliche Informationen an[zu]fordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.“[123] Desweiteren besteht die Möglichkeit, einen Antrag auf Auskunft zu personenbezogenen Daten elektronisch zu stellen,[124] „die Informationen [sind dann] in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern [die betroffene Person] nichts anderes angibt.“[125] Gleichzeitig ist der Verantwortliche nach Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO verpflichtet, die Vertraulichkeit der personenbezogenen Daten in angemessenem Rahmen sicherzustellen.[126] Für Unternehmen dürfte sich daraus die Schwierigkeit ableiten, trotz der Verpflichtung zu zeitnaher Auskunft die Identität der betroffenen Person, häufig ohne das Anfordern weiterer Daten, festzustellen. Nicht für jede Datenverarbeitung beispielsweise muss dem Verantwortlichen die E-Mail Adresse der Betroffenen vorliegen, ein elektronischer Antrag könnte theoretisch von jedem gestellt werden und der Verantwortliche müsste abwägen, ob er daraufhin die Daten vorlegen darf. Selbst wenn dem Verantwortlichen die E-Mail Adressen vorliegen, bedeutet eine elektronische Nachricht, die als von der korrekten Adresse gesendet angezeigt wird, zum einen nicht, dass sie tatsächlich vom Betroffenen stammt,[127] und zum anderen nicht einmal, dass der Absender der E-Mail wirklich Zugang zu diesem Account hat.[128] Beispielsweise könnten die personenbezogenen Daten einer Person für einen Social Engineering Angriff nützlich sein, so dass ein Angreifer daran interessiert sein könnte, einen derartigen Antrag zu fälschen, um die enthaltenen Informationen abzufangen oder direkt zu erhalten, indem er im Zuge der Antragstellung mit Begründung um eine bestimmte Form der Antwort,

[120] vgl. Art. 12-15 DSGVO
[121] vgl. Art. 12 Abs. 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/12.html
[122] vgl. Art. 12 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/12.html
[123] Art. 12 Abs. 6 DSGVO, URL: https://dejure.org/gesetze/DSGVO/12.html
[124] vgl. Art. 15 Abs.3 DSGVO, URL : https://dejure.org/gesetze/DSGVO/15.html
[125] Art. 15 Abs. 3 DSGVO, URL : https://dejure.org/gesetze/DSGVO/15.html
[126] vgl. Art. 32, 5 Abs 1 Buchstabe f DSGVO, URLs: https://dejure.org/gesetze/DSGVO/5.html, https://dejure.org/gesetze/DSGVO/32.html
[127] Es ist nicht auszuschließen, dass, gewollt oder nicht, mehrere Personen Zugriff auf einen E-Mail-Account haben.
[128] Mit dem Programm Telnet zum Beispiel lassen sich E-Mails als von jeder beliebigen Adresse aus versendet ausgeben.

beispielsweise elektronisch zu einer aktuelleren E-Mail-Adresse oder postalisch zu einer möglicherweise abweichenden Adresse, bittet.

Besonders durch die verschiedenen Möglichkeiten der Übermittlung der Informationen und die nur bei begründeten Zweifeln an der Identität der natürlichen Person genannte Möglichkeit, mehr Informationen zur Identitätsfeststellung anzufordern, scheint sich dieses Vorgehen als Informationsquelle für Angreifer anzubieten. Ein Unternehmen, das personenbezogene Informationen zu leichtfertig einem Unbefugten preisgibt, wäre allerdings nach Artikel 82 DSGVO für jeden dadurch entstehenden Schaden für die betroffene Person haftbar.[129] Mit dieser bisher nicht ausreichend geklärten Problematik, die in der DSGVO nicht abschließend behandelt wird, hat sich der Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Ronald Petrlic, in einem Artikel in der DuD – Datenschutz und Datensicherheit, einer Fachzeitschrift mit rechtlichen, technischen und organisatorischen Aspekten des Datenschutzes und der Datensicherheit als inhaltlichen Schwerpunkten,[130] auseinandergesetzt. Er betont hier die strikte Zweckbindung an die Identifizierung und Authentifizierung der dafür bereitgestellten Daten der Betroffenen, die wegen Zweifeln daran manche Identifizierungsmöglichkeiten ablehnen, nennt verschiedene Verfahren zur Feststellung der Identität mit Vor- und Nachteilen[131] und hebt hervor, dass „Verantwortliche [...] selbst entscheiden [müssen], welche Identifizierungsmethode sie für Auskunftsersuchen von betroffenen Personen wählen; und zwar [...] unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen.“[132] Vorgegeben ist, dass sensible personenbezogene Daten nicht per einfacher E-Mail ohne Ende-zu-Ende-Verschlüsselung beauskunftet werden dürfen, bei anderen personenbezogenen Daten ist das nicht grundsätzlich verboten, wenn auch problematisch. Als sicherere Übermittlungswege nach der Identitätsbestätigung werden als einfachste Möglichkeit die Bereitstellung der Informationen über das HTTPS-gesicherte Nutzerkonto oder das Übermitteln eines verschlüsselten PDF-Dokuments genannt, wobei

[129] vgl. Art. 82 DSGVO, URL : https://dejure.org/gesetze/DSGVO/82.html
[130] vgl. URL : https://www.springerprofessional.de/datenschutz-und-datensicherheit-dud/7466274, 07.08.19
[131] vgl. Petrlic, Ronald: Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO – Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S. 71-75
[132] Petrlic, Ronald: Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO – Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S. 75

das Passwort auf gesondertem sicheren Weg bereitgestellt werden sollte.[133] In der selben Ausgabe der gleichen Zeitschrift wird eine Studie zu diesem Auskunftsersuchen nach Artikel 15 DSGVO vorgestellt. Hier wurden 14 Unternehmen aus den drei Kategorien Online-Unternehmen, klassisches Unternehmen mit Online-Geschäft und Dienstleister daraufhin untersucht, wie schwer es für ihre Nutzer ist, ihre Rechte nach Artikel 15 DSGVO wahrzunehmen. Dabei war die Umsetzung der Unternehmen hinsichtlich der Darstellung komplexer, auf langjährigen Kundenbeziehungen basierender Informationen besonders wichtig. Drei der 14 Unternehmen boten ein Online-Werkzeug an, mit dem ein Kunde alle ihn betreffenden personenbezogenen Daten herunterladen konnte.[134]

5 Zusammenspiel DSGVO & BDSG

Die neue Fassung des Bundesdatenschutzgesetzes (BDSG) trat gleichzeitig mit der DSGVO am 25.05.2018 in Kraft. Als nationale Umsetzung der EU Verordnung regelt sie insbesondere den Umgang mit den bereits erwähnten Öffnungsklauseln. Davon enthält die DSGVO einige, die nicht alle im Detail hier behandelt werden können. Genannt wurde in diesem Zusammenhang bereits Artikel 6 DSGVO, der das Recht der Mitgliedstaaten als Grundlage für die Rechtmäßigkeit von Datenverarbeitungen nennt. Weitere wichtige Öffnungsklauseln finden sich in Bezug auf Artikel 83 Absatz 7 DSGVO, der Mitgliedstaaten befugt, „Vorschriften dafür fest[zu]legen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können“,[135] auf die Verarbeitung besonders geschützter Kategorien von Daten, also sensible Daten nach Artikel 9 DSGVO, und die Betroffenenrechte.[136]

Im Allgemeinen sind die Grundsätze für die Verarbeitung personenbezogener Daten zumindest in Deutschland nicht neu und waren auch in der alten Fassung des

[133] vgl. Petrlic, Ronald: Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO – Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S. 75

[134] vgl. Buchmann, Erik, Eichhorn, Susanne: Auskunftsersuchen nach Art. 15 DSGVO – Wie leicht machen es Unternehmen ihren Kunden, ihre Rechte nach Art. 15 DSGVO auszuüben?, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S.65-70

[135] Art. 83 Abs. 7 DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html

[136] vgl. URLs :
http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DSGVO.pdf,
https://www.infolaw.at/downloads/mag_georg_fellner_ll_m-oeffnungsklauseln_der_dsgvo-2017-05-05.pdf,
10.08.19

Bundesdatenschutzgesetzes (BDSG_alt) vertreten.[137] Die in Artikel 5 Absatz 1 Buchstabe a DSGVO genannte und in Artikel 6 DSGVO näher spezifizierte Rechtmäßigkeit der Verarbeitung personenbezogener Daten zum Beispiel entspricht im Groben §§4 ff. BDSG_alt,[138] die geforderte Transparenz, die mit den Informationspflichten in Art. 12 ff. DSGVO konkretisiert ist, findet sich auch in den Auskunftspflichten in §§19 f. und §§33 f. BDSG_alt. Die Zweckbindung der erhobenen Daten ist aktuell durch Art. 5, Abs. 1 Buchstabe b DSGVO geregelt, ließ sich aber bereits vorher in §35 Absatz 2 Satz 2 Nummer 3 und §39 BDSG_alt finden,[139] die Integrität und Vertraulichkeit der Daten (Art. 5, Abs. 1 Buchstabe f, Art. 32 DSGVO) in §9 mit Anlage.[140] Neu ist allerdings die in Artikel 5 Absatz 2 DSGVO erklärte Rechenschaftspflicht der Verantwortlichen, durch die diese zum einen Maßnahmen zu ergreifen haben, die eine Verarbeitung der Daten gemäß der DSGVO gewährleisten, und zum anderen in der Lage sein müssen, selbige Einhaltung nachzuweisen.[141]

Als EU-Verordnung ist die DSGVO gegenüber nationalen Gesetzen mit Vorrang zu betrachten, ist diesen übergeordnet und in der Lage, sie bei gleichem Anwendungsbereich zu verdrängen. Sie enthält allerdings, wie bereits erwähnt, ein paar Öffnungsklauseln, die nationale Anpassungen beziehungsweise Erweiterungen anbieten.

In der neuen Fassung des Bundesdatenschutzgesetzes (BDSG) ist beispielsweise die Rolle des Datenschutzbeauftragten genauer festgelegt. Demnach müssen zusätzlich zu den Vorgaben in der DSGVO nach §38 BDSG auch diejenigen Unternehmen, also nichtöffentliche Stellen, einen Datenschutzbeauftragten bestellen, die „in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.“[142] Seine Aufgaben sind in Artikel 39 DSGVO und §7 BDSG beschrieben und bestehen aus der Unterrichtung und Beratung von mit der Verarbeitung personenbezogener Daten betrauten Beschäftigten sowie des Verantwortlichen[143] beziehungsweise der öffentlichen Stelle,[144] aus der Überwachung der Einhaltung der jeweiligen Gesetze, der Beratung in Hinsicht auf die Datenschutz-

[137] vgl. https://www.bits.gmbh/die-rechenschaftspflicht-nach-der-DSGVO/, 10.08.19
[138] vgl. Art. 6 DSGVO, URL : https://dejure.org/gesetze/DSGVO/6.html, §§4 f. BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./4.html
[139] vgl. §§39, 35 Abs. 2, Satz 2, Nr. 3, URL: https://dejure.org/gesetze/BDSG_a.F./35.html, https://dejure.org/gesetze/BDSG_a.F./39.html
[140] vgl. §9BDSG_alt, Anlage zu §9 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./9.html, https://dejure.org/gesetze/BDSG_a.F./Anlage.html
[141] vgl. URL : https://www.datenschutzbeauftragter-info.de/dsgvo-grundsaetze-fuer-die-verarbeitung-personenbezogener-daten/, 18.08.19
[142] §38 Abs. 1 Satz 1 BDSG, URL: https://dejure.org/gesetze/BDSG/38.html
[143] vgl. Art. 39 Abs. 1 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/39.html
[144] vgl. §7 Abs. 1 Nr. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/7.html

Folgenabschätzung und die Überwachung deren Durchführung und aus der Zusammenarbeit mit der Aufsichtsbehörde.[145] Die Stellung des Datenschutzbeauftragten ist in Artikel 38 DSGVO beschrieben. Hier heißt es, der nach der DSGVO für die Verarbeitung Verantwortliche hat eine ordnungsgemäße und frühzeitige Einbindung des Datenschutzbeauftragten in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen sicherzustellen[146] sowie selbigen bei der Erfüllung seiner Aufgaben durch Bereitstellen aller erforderlichen Ressourcen, Zugang zu den Daten und den Verarbeitungsvorgängen und der für das Erhalten seines Fachwissens nötigen Ressourcen zu unterstützen.[147] Zudem liegt es in seiner Verantwortung, mögliche Interessenskonflikte mit den sonstigen Aufgaben des internen Datenschutzbeauftragten sowie Anweisungen bezüglich der Ausübung seiner Aufgaben zu vermeiden.[148] In §6 BDSG ist ebenfalls die Stellung des Datenschutzbeauftragten geregelt. Dabei entsprechen die Absätze 1 – 3 des §6 BDSG inhaltlich den Absätzen 1 – 3 des Artikels 38 DSGVO, beziehen sich allerdings lediglich auf öffentliche Stellen als Verantwortliche. Nach §38 Absatz 2 BDSG gelten für den Datenschutzbeauftragten nichtöffentlicher Stellen ebenfalls die Bestimmungen von §6 Absatz 4, 5 Satz 2 und Absatz 6 BDSG.[149] Diese erklären eine Kündigung des Abeitsverhältnisses während der Ausübung der Tätigkeit als Datenschutzbeauftragter sowie innerhalb eines Jahres nach dem Ende dieser Tätigkeit für unzulässig, sofern kein wichtiger Grund für eine Kündigung ohne Kündigungsfrist nach §626 BGB vorliegt,[150] verpflichten den Datenschutzbeauftragten zur Verschwiegenheit[151] und regeln sein Zeugnisverweigerungsrecht.[152] Der Kündigungsschutz nach §6 Absatz 4 BDSG gilt allerdings nur, sofern die Benennung eines Datenschutzbeauftragten verpflichtend ist.[153] Aufgrund der Vorrangstellung der DSGVO, die sicherstellt, dass die dort enthaltenen Artikel grundsätzlich gelten und der nationalen Erweiterung im BDSG, das auch nichtöffentliche Stellen je nach Anzahl der mit der automatisierten Verarbeitung personenbezogener Daten betrauten Beschäftigten zur Benennung eines Datenschutzbeauftragten verpflichtet, gelten die in Artikel 38 DSGVO festgelegten Bestimmungen zur Stellung des Datenschutzbeauftragten ohnehin für jeden gesetzlich

[145] vgl. Art. 39 DSGVO, §7 BDSG, URL: https://dejure.org/gesetze/DSGVO/39.html, https://dejure.org/gesetze/BDSG/7.html
[146] vgl. Art 38 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/38.html
[147] vgl. Art. 38 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/38.html
[148] vgl. Art. 38 Abs. 6, 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/38.html
[149] vgl. §38 Abs. 2 BDSG, URL: https://dejure.org/gesetze/BDSG/38.html
[150] vgl. §6 Abs. 4 BDSG, URL: https://dejure.org/gesetze/BDSG/6.html
[151] vgl. §6 Abs. 5 Satz 2 BDSG, URL: https://dejure.org/gesetze/BDSG/6.html
[152] vgl. §6 Abs. 6 BDSG, URL: https://dejure.org/gesetze/BDSG/6.html
[153] vgl. §38 Abs 2 BDSG, URL: https://dejure.org/gesetze/BDSG/38.html

vorgeschriebenen Datenschutzbeauftragten, sodass für nichtöffentliche Stellen der Verweis auf die Absätze 1 – 3 des §6 BDSG, die mit den Vorgaben aus der DSGVO übereinstimmen, nicht nötig ist, deren Einhaltung aber dennoch gewährleistet sein muss.
Ein für Unternehmen ebenfalls besonders relevantes Thema dürfte der Beschäftigtendatenschutz sein. Hierzu stellt Artikel 88 DSGVO eine Öffnungsklausel, wonach die Mitgliedstaaten angehalten sind, spezifischere Rechtsvorschriften zu erlassen, die „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten [...] und die Überwachungssysteme am Arbeitsplatz“[154] umfassen. Umgesetzt wurde dies in §26 BDSG, der den in der alten Fassung zu dieser Thematik bestehenden §32 BDSG_alt[155] um eine Definition des Begriffs ‚Beschäftigter’, worunter zum Beispiel auch ehemalige Angestellte und Bewerber fallen, die Pflicht des Verantwortlichen, geeignete Maßnahmen für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 DSGVO zu ergreifen, und die Berücksichtigung der im Beschäftigungsverhältnis bestehenden Abhängigkeit für die Beurteilung der Freiwilligkeit der Einwilligung in die Datenverarbeitung, falls diese die Grundlage für die Rechtmäßigkeit derselben darstellt, erweitert.[156]

6 DSGVO und Datenschutz in Bezug auf andere Gesetze

6.1 Relevante strafrechtliche Begriffe

Zur besseren Verständlichkeit der nachfolgenden Thematik sollen an dieser Stelle ein paar wenige ausgewählte grundsätzliche Begriffe im Zusammenhang mit dem Strafrecht erläutert werden. Zunächst ist zwischen Straftaten und Ordnungswidrigkeiten zu unterscheiden. Während bei einer Straftat eine Freiheits- oder Geldstrafe verhängt wird, werden Ordnungswidrigkeiten mit Geldbußen belegt. Die zugehörigen Paragraphen sind ähnlich aufgebaut aus Tatbestand und Rechtsfolge.[157] Dies soll am Beispiel von §263 StGB näher beschrieben werden. In diesem heißt es: „Wer in der Absicht, sich oder einem

[154] Art. 88 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/88.html
[155] vgl. §32 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./32.html
[156] vgl. §26 BDSG, URL: https://dejure.org/gesetze/BDSG/26.html
[157] vgl. URLs : https://www.juraforum.de/lexikon/straftat-abgrenzung-zur-ordnungswidrigkeit, http://www.rechtslexikon.net/d/tatbestand/tatbestand.htm, 13.08.19

Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“[158] Hier handelt es sich beim ersten Teil, der Bereicherungsabsicht für sich oder einen Dritten, um den subjektiven Tatbestand, worunter Absichten und der Vorsatz fallen. Die Schädigung des Vermögens eines anderen durch das Hervorrufen oder das Unterhalten eines Irrtums durch Vorspiegelung falscher oder Entstellung beziehungsweise Unterdrückung wahrer Tatsachen stellt den objektiven Tatbestand dar. Die Rechtsfolge ist in diesem Fall eine Freiheitsstrafe bis zu fünf Jahren oder eine Geldstrafe.[159] In Absatz 3 des selben Paragraphen findet sich eine Regelung für besonders schwere Fälle von Betrug, zum Beispiel bei gewerbsmäßigem Handeln oder Mitgliedschaft in einer Bande des Täters.[160] Damit handelt es sich beim Betrug um eine qualifizierte Straftat, da die Erfüllung zusätzlicher Tatbestandsmerkmale zum Grundtatbestand, hier beispielsweise die Gewerbsmäßigkeit, zu einer höheren Strafe, im konkreten Fall zu Freiheitsstrafe von sechs Monaten bis zu zehn Jahren[161], führt.[162] Sollte der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Betrugs- oder Fälschungsdelikten verbunden hat, gewerbsmäßig handeln, liegt die Strafe bei einer Freiheitsstrafe von einem Jahr bis zu zehn Jahren[163], was die Erfüllung dieses Tatbestands zu einem Verbrechen macht. Bei einer Straftat, die als Rechtsfolge eine Mindeststrafe von einem Jahr Freiheitsstrafe nach sich zieht, handelt es sich um ein Verbrechen, bei geringeren Mindeststrafen oder Geldstrafen um ein Vergehen.[164]

6.2 BDSG & SächsDSG, BayDSG

Zusätzlich zur EU-weit gültigen DSGVO und dem deutschlandweit gültigen BDSG hat jedes Bundesland sein eigenes Datenschutzgesetz (DSG). Dieses gilt für öffentliche Stellen des jeweiligen Bundeslandes sowie nicht-öffentliche Stellen, die Aufgaben der

[158] §263 Abs. 1 StGB, URL: https://dejure.org/gesetze/StGB/263.html
[159] vgl. URL : http://www.rechtslexikon.net/d/tatbestand/tatbestand.htm, 13.08.19
[160] vgl. §263 Abs. 3 S. 2 Nr. 1 StGB, URL: https://dejure.org/gesetze/StGB/263.html
[161] vgl. §263 Abs. 3 StGB, URL: https://dejure.org/gesetze/StGB/263.html
[162] vgl. URL : http://rechtslexikon.net/d/qualifizierte-straftat/qualifizierte-straftat.htm, 13.08.19
[163] vgl. §263 Abs. 5 StGB, URL: https://dejure.org/gesetze/StGB/263.html
[164] vgl. URL : https://www.juraforum.de/lexikon/straftat-abgrenzung-zur-ordnungswidrigkeit, 13.08.19

öffentlichen Verwaltung wahrnehmen.[165] Aufgrund der daraus resultierenden vermutlich meist vergleichsweise untergeordneten Bedeutung dieses Gesetzes für Unternehmen und der 16 verschiedenen Bundesländer werden hier nur exemplarisch wenige ausgewählte Paragraphen des sächsischen und des bayrischen Datenschutzgesetzes sowohl miteinander als auch mit dem BDSG abgeglichen, von weiterführenden Betrachtungen wird abgesehen.

Im BDSG findet sich in §4 eine Regelung zur Videoüberwachung öffentlich zugänglicher Räume. Hier wird eine solche ausschließlich dann für zulässig erklärt, wenn sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke notwendig ist und schutzwürdige Interessen der Betroffenen nicht überwiegen.[166] Ähnlich ist die Regelung in Absatz 1 des §33 SächsDSG, hier wird insbesondere die Gewährleistung der öffentlichen Sicherheit und Ordnung als Aufgabe öffentlicher Stellen genannt.[167] Im Bayerischen Datenschutzgesetz ist eine engere Zweckbindung an den Schutz von Leben, Gesundheit, Freiheit oder Eigentum von Personen oder Schutz von Kulturgütern, öffentlichen Einrichtungen, baulichen Anlagen oder Dingen gegeben.[168] Sowohl das sächsische als auch das bayrische Datenschutzgesetz sieht die Möglichkeit der Datenverarbeitung zum Zweck der Verfolgung von Ordnungswidrigkeiten vor, das bayrische jedoch nur bei Ordnungswidrigkeiten von erheblicher Bedeutung.[169] Laut BDSG dagegen ist eine Weiterverarbeitung der Daten zu einem anderen Zweck als dem der Erhebung nur zulässig, „soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.“[170] Da Ordnungswidrigkeiten nicht grundsätzlich, sondern im Gegenteil vermutlich nur ausgesprochen selten eine Gefahr für die staatliche oder öffentliche Sicherheit darstellen, ist eine Zulässigkeit der Verarbeitung zum Zweck der Verfolgung von Ordnungswidrigkeiten eine Erweiterung im Vergleich zum BDSG. In Absatz 5 des selben Paragraphen ist eine mit durch Videoüberwachung gewonnenen Daten zusammenhängende Löschpflicht im BDSG geregelt. Demnach sind die Daten

[165] vgl. Art. 1 Abs. 1 und 2 BayDSG, §2 Abs. 1 SächsDSG, URLs: https://www.gesetze-bayern.de/Content/Document/BayDSG-1, https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p2

[166] vgl. §4 Abs. 1 S. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/4.html

[167] vgl. §33 Abs. 1 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p33

[168] vgl. Art. 24 Abs. 1 BayDSG, URL: https://www.gesetze-bayern.de/Content/Document/BayDSG-24

[169] vgl. §33 Abs. 2 SächsDSG, Art. 24 Abs. 3 BayDSG, URLs: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p33, https://www.gesetze-bayern.de/Content/Document/BayDSG-24

[170] §4 Abs. 3 S. 3 BDSG, URL: https://dejure.org/gesetze/BDSG/4.html

„unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.“[171] In den Gesetzen der Länder dagegen ist eine Aufbewahrungsfrist von zwei Monaten für die Daten, einschließlich daraus gewonnener Unterlagen, unabhängig vom Zweck der Erhebung gegeben, die nur aufgrund der Notwendigkeit der Daten beispielsweise zur Verfolgung von Straftaten oder der Geltendmachung von Rechtsansprüchen überzogen werden darf.[172] Hier wird das BDSG also eher verschärft.
Ordnungswidrigkeiten im Zusammenhang mit dem BDSG sind in §43 BDSG geregelt, dabei handelt es sich lediglich um Verstöße gegen oder mangelnde Umsetzung des §30 BDSG. Darin ist festgelegt, dass „[e]ine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, [...] Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union genauso zu behandeln [hat] wie Auskunftsverlangen inländischer Darlehensgeber.“[173] Der zweite Absatz des §30 BDSG verpflichtet dazu, einen Verbraucher, mit dem aufgrund einer Auskunft nach Absatz 1 kein Verbraucherdarlehensvertrag oder ein Vertrag über eine entgeltliche Finanzierungshilfe abgeschlossen wird, über diese Tatsache sowie die erteilte Auskunft zu unterrichten, sofern dadurch nicht die öffentliche Sicherheit oder Ordnung gefährdet würde.[174] Die Ordnungswidrigkeiten werden laut BDSG mit einer Geldbuße bis zu fünfzigtausend Euro geahndet. Zusätzlich enthält das BDSG in §42 Strafvorschriften, die im nachfolgenden Kapitel genauer beschrieben sind und gewerbsmäßiges Handeln gegen Entgelt oder eine Bereicherungs- bzw Schädigungsabsicht für eine Strafbarkeit von unberechtigter Datenverarbeitung voraussetzt.[175] Im ersten Absatz von Artikel 23 des bayrischen DSG wird das unbefugte Verarbeiten beziehungsweise Erschleichen von personenbezogenen Daten, die durch eine öffentliche Stelle verarbeitet werden, unabhängig von möglichem Entgelt oder der zugrundeliegenden Absicht mit einer Geldbuße von bis zu dreißigtausend Euro belegt.[176] Im sächsischen DSG werden in §38 SächsDSG weitaus mehr Ordnungswidrigkeiten genannt, darunter neben den bereits aus

[171] §4 Abs. 5 BDSG, URL: https://dejure.org/gesetze/BDSG/4.html
[172] vgl. §33 Abs. 4 SächsDSG, Art. 24 Abs. 4 BayDSG, URLs:
https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p33,
https://www.gesetze-bayern.de/Content/Document/BayDSG-24
[173] §30 Abs. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/30.html
[174] vgl. §30 Abs. 2 BDSG, URL: https://dejure.org/gesetze/BDSG/30.html
[175] vgl. §42 BDSG, URL: https://dejure.org/gesetze/BDSG/42.html
[176] vgl. Art. 23 Abs. 1 BayDSG, URL: https://www.gesetze-bayern.de/Content/Document/BayDSG-23

dem bayrischen DSG genannten[177] zum Beispiel auch die Benachteiligung des Datenschutzbeauftragten einer öffentlichen Stelle aufgrund der Erfüllung seiner Aufgaben[178] oder eine unvollständige oder unrichtige Auskunft an den Betroffenen nach §18 Absatz 1 SächsDSG.[179] Hiernach sind Ordnungswidrigkeiten mit einer Geldbuße von bis zu fünfundzwanzigtausend Euro belegt.[180] Die ersten acht der elf in §38 SächsDSG beschriebenen Ordnungswidrigkeiten sind nach §39 SächsDSG im Falle von Handeln gegen Entgelt oder in Bereicherungs- beziehungsweise Schädigungsabsicht mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe zu bestrafen,[181] die übrigen drei stellen unabhängig von der zugrundeliegenden Motivation keine Straftat, sondern weiterhin eine Ordnungswidrigkeit dar. Auch der Versuch, eine der genannten Straftaten zu begehen, ist demnach strafbar,[182] im BDSG und im bayrischen DSG findet sich dagegen keine Versuchsstrafbarkeit.

6.3 StGB, StPO

In Artikel 2 DSGVO, der ihren sachlichen Anwendungsbereich regelt, ist die Verarbeitung personenbezogener Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“[183] ausdrücklich aus dem Anwendungsbereich der DSGVO ausgeschlossen.[184]

Im Strafgesetzbuch (StGB) findet sich kein konkreter Paragraph für einen allgemein gültigen Datenschutz, das StGB wurde im Zuge des Inkrafttretens der DSGVO nicht angepasst.[185] Allerdings ist in §203 StGB die Verletzung von Privatgeheimnissen als mit

[177] vgl. §38 Abs. 1 Nr. 1 und 2 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p38
[178] vgl. §38 Abs. 1 Nr. 4 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p38
[179] vgl. §38 Abs. 1 Nr. 7 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p38
[180] vgl. §38 Abs. 2 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p38
[181] vgl. §39 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p39
[182] vgl. §39 SächsDSG, URL: https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz#p39
[183] Art. 2 Abs. 2 Buchstabe d DSGVO, URL: https://dejure.org/gesetze/DSGVO/2.html
[184] vgl Art. 2 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/2.html
[185] vgl. URL: https://www.buzer.de/gesetz/6165/l.htm, 23.09.19

einer Freiheitsstrafe bis zu einem Jahr oder Geldstrafe zu ahnden angegeben. Hierbei handelt es sich allerdings um beruflich erlangte Daten, also im Grunde eine Verletzung beruflicher Schweigepflichten, beispielsweise von Ärzten oder Anwälten, aber auch Suchtberatern oder Sozialpädagogen.[186] Selbiges gilt für Amtsträger, öffentlich bestellte Sachverständige oder Mitglieder eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses.[187] Ein Offenbaren solcher personenbezogener Daten gegenüber „Personen [...], die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist“,[188] ist dagegen nicht im Sinne dieser Vorschrift und damit nicht strafbar.[189] Sollte „der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, [handeln,] so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.“[190] Ähnlich wie die DSGVO selbst Sanktionen und Geldbußen für bestimmte Verstöße festlegt, enthält das BDSG strafrechtliche Vorschriften. In §42 BDSG ist geregelt, dass „[m]it Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe [bestraft wird], wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen“[191] einem Dritten gewerbsmäßig zugänglich macht.[192] Eine unberechtigte Verarbeitung solcher Daten oder ihr Erschleichen durch unrichtige Angaben kann bei Handeln gegen Entgelt, einer Bereicherungs- oder Schädigungsabsicht zu einer Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe führen.[193] Laut Absatz 3 des selben Paragraphen wird die Tat nur auf Antrag verfolgt, antragsberechtigt sind der Betroffene, der Verantwortliche, die oder der Bundesbeauftragte sowie die Aufsichtsbehörde.[194] Ordnungswidrigkeiten sind mit den Bußgeldvorschriften in §43 BDSG geregelt. Diese können mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden, wobei gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden.[195]

In der Strafprozessordnung (StPO), die ebenfalls nicht in Hinsicht auf die DSGVO geändert wurde,[196] sind datenschutzrechtliche Grundprinzipien im Vergleich zum StGB

[186] vgl. §203 Abs. 1 StGB, URL: https://dejure.org/gesetze/StGB/203.html
[187] vgl. §203 Abs. 2 StGB, URL: https://dejure.org/gesetze/StGB/203.html
[188] §203 Abs. 3 Satz 2 StGB, URL: https://dejure.org/gesetze/StGB/203.html
[189] vgl. §203 Abs. 3 StGB, URL: https://dejure.org/gesetze/StGB/203.html
[190] §203 Abs. 6 StGB, URL: https://dejure.org/gesetze/StGB/203.html
[191] §42 Abs. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/42.html
[192] vgl. §42 Abs. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/42.html
[193] vgl. §42 Abs. 2 BDSG, URL: https://dejure.org/gesetze/BDSG/42.html
[194] vgl. §42 Abs. 3 BDSG, URL: https://dejure.org/gesetze/BDSG/42.html
[195] vgl. §43 Abs. 2 und 3 BDSG, URL: https://dejure.org/gesetze/BDSG/43.html
[196] vgl. URL: https://www.buzer.de/gesetz/5815/l.htm, 23.09.19

fest verankert. Eine Zweckbindung findet sich beispielsweise in §477 StPO,[197] im Zuge der Datensparsamkeit oder Datenminimierung sind einige Löschpflichten in der StPO festgelegt[198] und in §496 der StPO wird direkt die Verwendung personenbezogener Daten in elektronischen Akten geregelt, wonach ausdrücklich „die organisatorischen und technischen Maßnahmen zu treffen [sind], um den besonderen Anforderungen des Datenschutzes und der Datensicherheit gerecht zu werden".[199] In den Paragraphen §§ 100a bis 100c StPO sind verschiedene Maßnahmen zur Überwachung von Personen beschrieben. In §100a StPO ist die Telekommunikationsüberwachung (TKÜ) geregelt. Dabei handelt es sich um das Mitschneiden von Telekommunikationsvorgängen und –inhalten, beispielsweise bei Telefongesprächen, Kurznachrichten oder E-Mails.[200] Betreiber von Telekommunikationsanlagen sind gesetzlich verpflichtet, „auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen."[201] Seit 2017 schließt §100a StPO durch das ‚Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens' auch das viel kritisierte Verfahren der Quellen-TKÜ als Eingriff in das vom Betroffenen verwendete informationstechnische System ein.[202] Bei einem solchen Vorgehen wird spezielle Software eingesetzt, um heutzutage oftmals Ende-zu-Ende verschlüsselte Kommunikation, wie sie ein Großteil der gängigen Messengerdienste verwendet[203], vor oder nach dem Verschlüsseln abzufangen, also direkt auf dem Sende- oder Zielgerät. Ähnlich verhält es sich mit der in §100b StPO geregelten ‚Online-Durchsuchung', bei der Informationssysteme vom Verdächtigen unbemerkt durchsucht werden, um Probleme wie beispielsweise verschlüsselte Festplattenbereiche zu vermeiden.[204] Während ein Nutzer selbst auf Dateien zugreift, sind diese schließlich nicht verschlüsselt, während zum Beispiel Programme verfügbar sind, die beim Herunterfahren das gesamte System verschlüsseln. In der Kritik stehen diese Maßnahmen besonders durch den hierfür nötigen

[197] vgl. §477 Abs. 2 S. 2 und 3 StPO, URL: https://dejure.org/gesetze/StPO/477.html
[198] vgl. Dr. Basar, Eren, Dr. Hiéramente, Mayeul: Datensparsamkeit in der StPO – Die Möglichkeit der Löschung, in: HRRS (Höchstrichterliche Rechtsprechung zum Strafrecht), Aug./Sept. 2018, S. 336 – 342, S. 336, URL: https://www.hrr-strafrecht.de/hrr/archiv/18-08/index.php?sz=8#336
[199] §496 Abs. 2 Nr. 1 StPO, URL: https://dejure.org/gesetze/StPO/496.html
[200] vgl. URL : https://www.juraforum.de/lexikon/telekommunikationsueberwachung, 21.08.19
[201] §110 Abs. 1 Nr. 1 TKG, URL: https://dejure.org/gesetze/TKG/110.html
[202] vgl. §100a Abs. 1 Satz 2 StPO, URL: https://dejure.org/gesetze/StPO/100a.html
[203] Darunter neben WhatsApp zum Beispiel Telegram, Threema, Signal, Viber und Wire, vgl. URL: https://www.heise.de/tipps-tricks/WhatsApp-Alternativen-Welche-Messenger-gibt-es-3976153.html, 21.08.19
[204] vgl. URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html, 03.09.19

Einsatz von sogenannten ‚Staatstrojanern', also staatlich genutzte Hacker-Programme. Diese werden durch Ausnutzen von Sicherheitslücken auf dem zu überwachenden IT-System platziert. Allerdings könnte das zur Folge haben, dass Behörden wie das Bundeskriminalamt (BKA) ihnen bekannte Sicherheitslücken den Herstellern nicht melden, um diese weiter nutzen zu können, so dass diese dann auch nicht geschlossen werden und ein allgemeines Risiko für die IT-Sicherheit darstellen könnten.[205] In diesem Zusammenhang wird sich häufig auf WannaCry von 2017 berufen, eine Erpresser-Software, die sich unter Ausnutzung einer der NSA lange bekannten Schwachstelle selbst von Gerät zu Gerät verbreiten konnte und die Systeme verschlüsselt hat. Die Entschlüsselung aller Daten wurde dann gegen Zahlung von Bitcoin[206] angeboten. Betroffen waren unter dem Microsoft-Betriebssystem Windows laufende Computer, auch 2019 haben noch nicht alle Nutzer die Sicherheits-Updates installiert, sodass diese Lücke, EternalBlue genannt, weiterhin ausgenutzt wird. Hätte die NSA sofort beim Auffinden der Schwachstelle Microsoft informiert, wäre Vermutungen zufolge kein so großer Schaden entstanden.[207] Laut Bundesverfassungsgericht umfasst „[d]as allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m.Art. 1 Abs. 1 GG) [...] das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme."[208] Demnach ist eine heimliche Infiltration eines IT-Systems nur bei Gefahr für ein überragend wichtiges Rechtsgut, genannt sind hier „Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt",[209] verfassungsrechtlich zulässig.[210] In den Paragraphen §§100a Absatz 2 und 100b Absatz 2 StPO sind schwere Straftaten aufgezählt, die ein heimliches Überwachen der IT-Systeme von Verdächtigen rechtfertigen, darunter zu Beispiel auch Bestechlichkeit und

[205] vgl. URL: https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-gff-staatstrojaner-ueberwachung-software-ermittlungen/, https://freiheitsrechte.org/trojaner/, 15.09.19
[206] Hierbei handelt es sich um eine digitale Kryptowährung, die allgemein für Anonymität bekannt und deswegen aufgrund der kaum möglichen Verfolgung für derartige Zahlungen geeignet ist. Dem Zahlenden ist zwar eine Bitcoin-Adresse bekannt, es kann aber kaum ein Personenbezug hergestellt werden. Weitere Informationen: URL: https://bitcoin.org/de/, 17.09.19
[207] vgl. URL: https://www.zeit.de/digital/datenschutz/2019-05/baltimore-nsa-tool-hackerangriff-ransomware-wannacry-usa, https://www.pandasecurity.com/de/security-info/wannacry/, 17.09.19
[208] BverG, Urteil des Ersten Senats vom 27. Februar 2008, -1 BvR 370/07-, Rn. (1-333), 1., URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html
[209] BverG, Urteil des Ersten Senats vom 27. Februar 2008, -1 BvR 370/07-, Rn. (1-333), 2., URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html
[210] vgl. BverG, Urteil des Ersten Senats vom 27. Februar 2008, -1 BvR 370/07-, Rn. (1-333), 2., URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

Bestechung nach den Paragraphen §§332, 334 StGB, unter Umständen Steuerhinterziehung, Betrug und Computerbetrug, in Fällen, in denen der Versuch der Tat strafbar ist, genügt ein Verdacht auf diesen bereits.[211] Viele Kritiker halten diese Straftaten für teilweise nicht ausreichend, um einen solchen Eingriff in das Persönlichkeitsrecht von Verdächtigen zu rechtfertigen.[212] Immerhin dürfte wohl eher nicht jeder Computerbetrug eine Gefahr für Leben oder Freiheit darstellen, gleichzeitig kann ein solcher auch schlecht grundsätzlich als eine Bedrohung des staatlichen Bestehens oder der menschlichen Existenzgrundlagen eingeordnet werden. Sowohl gegen Quellen-TKÜ als auch gegen Onlinedurchsuchungen wurde Verfassungsbeschwerde eingereicht.[213] Auch Andrea Voßhoff, die Bundesbeauftragte für Datenschutz und Informationsfreiheit, äußerte in ihrer Stellungnahme zur „Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung“[214] Kritik an zahlreichen Formulierungen, die genauso in die StPO übernommen wurden, und an der fehlenden Beteiligung ihrer Person an diesem Entwurf. Ihrer Einschätzung nach stellt besonders §100a StPO, der sich in der Formulierungshilfe unter Artikel 1 Nummer 2 findet, einen Verfassungsverstoß dar, da „[a]uf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation [...] überwacht und aufgezeichnet werden [dürfen], wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“,[215] was die Quellen-TKÜ in Einzelfällen zu einer Online-Durchsuchung ausweitet. Zudem merkt sie an, dass das Übertragen von Daten in oder aus der Cloud als Kommunikation mit sich selbst gewertet und ebenfalls überwacht werden könnte. Auch die erlaubte Dauer der Aufbewahrung von Protokolldaten zu einer

[211] vgl. §100a Abs.2 StPO, URL: https://dejure.org/gesetze/StPO/100a.html
[212] vgl. URL: https://freiheitsrechte.org/trojaner/, 15.09.19
[213] vgl. URLs: https://freiheitsrechte.org/trojaner/, https://www.zeit.de/politik/deutschland/2018-08/staatstrojaner-verfassungsbeschwerde-ueberwachungsinstrument-hajo-seppelt-can-duendar, 15.09.19
[214] vgl. Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 15.05.2017, URL : https://www.bundestag.de/resource/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf
[215] §100a Absatz 1 Satz 3 StPO, URL: https://dejure.org/gesetze/StPO/100a.html und Art. 1 Nr. 2 lit. a der Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 15.05.2017, URL: https://www.bundestag.de/resource/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf

Überwachung nach §100a StPO ist nicht geregelt. Desweiteren kritisiert sie den Straftatenkatalog des §100b StPO, also der Online-Durchsuchung, aufgrund der enthaltenen Qualifikationstatbestände, die das Risiko bergen, dass beispielsweise eine Hehlerei als gewerbsmäßige Hehlerei eingestuft werden könnte, die eine solche Maßnahme legitimiert, anders als der Grundtatbestand der Hehlerei. Auch §100b Absatz 3 StPO bemängelt sie, weil hier eine Ausweitung der Maßnahme auf andere Personen als den Beschuldigten unter Umständen ermöglicht wird. Die im Artikel 3 des ‚Gesetzesentwurfs zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze' BT-Drs. 18/11272[216] vorgeschlagene und so belassene Änderung des §81a StPO, der eine Blutentnahme ohne richterliche Anordnung in einigen Fällen erlaubt, sieht sie als datenschutzrechtlich problematisch, da es sich hierbei auch um sensible Daten nach Artikel 9 DSGVO handelt. Schließlich lassen sich aus Blutproben Rückschlüsse auf Gesundheitsdaten ziehen. Situationen die einen solchen Eingriff in die Privatsphäre rechtfertigen, lägen unter anderem bei einem Verdacht auf unterschiedliche Verkehrsdelikte, wie beispielsweise Alkohol am Steuer, vor.[217]

§100c StPO regelt die akustische Wohnraumüberwachung, die bei begründetem Verdacht einer schweren Straftat nach §100b Absatz 2 StPO bei im Einzelfall schwer wiegender Tat unter Umständen ohne Wissen des Betroffenen zulässig ist, wenn die Maßnahme vermutlich zur Erforschung des Sachverhalts oder der Bestimmung des Aufenthaltsortes von Mitbeschuldigten beiträgt, was ohne das Abhören unverhältnismäßig erschwert oder aussichtslos wäre.[218] Diese Überwachung lässt sich unter Umständen auf andere Personen ausweiten.[219]

Nach §100d Absatz 2 StPO dürfen im Zuge von den Überwachungsmaßnahmen in §§100a bis 100c StPO erhobene, den Kernbereich privater Lebensgestaltung betreffende, Daten nicht verwendet werden und Aufzeichnungen zu diesen Informationen sind unverzüglich zu löschen, wobei sowohl das Erheben als auch das Löschen der

[216] vgl. Gesetzesentwurf der Bundesregierung, Drucksache 18/11272, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 22.02.2017, URL: http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf

[217] vgl. Voßhoff, Andrea: Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272 und der Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334, 29.05.2017, Seite 11, URL: https://freiheitsrechte.org/home/wp-content/uploads/2017/05/186346_Stellungnahme_BfDI_zu_18-11272_und_186334.pdf

[218] vgl. §100c Abs. 1 StPO, URL: https://dejure.org/gesetze/StPO/100c.html

[219] vgl. §100c Abs. 2 S. 2 StPO, URL: https://dejure.org/gesetze/StPO/100c.html

betreffenden Daten zu protokollieren ist.[220] Diese Löschpflicht des §100d Absatz 2 StPO gilt auch für nach §53 StPO geschützte Kommunikationen, also solche mit Berufsgeheimnisträgern wie Geistlichen als Seelsorger oder Rechtsanwälten als Verteidiger. Interessant ist in diesem Zusammenhang, dass §100e Absatz 6 Nummer 2 Satz 1 StPO die Verwendung derartiger Daten zur Gefahrenabwehr erlaubt.[221] Für eine Einschätzung der Tauglichkeit solcher Informationen zu eben diesem Zweck dürfte eine regelmäßige Auswertung oder Speicherung nötig sein, was zu einem Aufschub der eigentlich sofortigen Löschung führen könnte. Zudem ist eine genaue Zurkenntnisnahme dieser Daten verbunden mit ihrer für eine Untersuchung und Bewertung wohl nötigen Speicherung genau das, was die Löschungsregelung vermeiden soll.[222]

2017 war die DSGVO noch nicht gültig, weswegen das späte bis nicht vorhandene Einbinden der Bundesbeauftragten für Datenschutz und Informationsfreiheit kein Verstoß gegen dieselbe darstellen kann. Allerdings war auch in der alten Fassung des BDSG in §26, der die Aufgaben dieses Postens beschrieb, geregelt, dass der oder die Bundesbeauftragte für Datenschutz und Informationsfreiheit unter anderem die Bundesregierung in Fragen des Datenschutzes beraten und gegebenenfalls Empfehlungen zur Verbesserung desselben geben kann.[223] In §24 Absatz 4 BDSG_alt heißt es zudem, „[d]ie öffentlichen Stellen des Bundes sind verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten und ihre oder seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen.“[224] Auch in der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) ist die frühzeitige Beteiligung von Bundesbeauftragten an allen Vorhaben, die ihre Aufgaben berühren, verlangt.[225] Diesen Vorgaben wurde damit bei genanntem Gesetzgebungsverfahren wohl nicht ausreichend Folge geleistet, indem Frau Voßhoff im Unwissen gelassen wurde.[226]

---

[220] vgl. §100d Abs. 2 StPO, URL: https://dejure.org/gesetze/StPO/100d.html
[221] vgl. §100e Abs. 6 Nr. 2 S.1 StPO, URL: https://dejure.org/gesetze/StPO/100e.html
[222] vgl. Dr. Basar, Eren, Dr. Hiéramente, Mayeul: Datensparsamkeit in der StPO – Die Möglichkeit der Löschung, in: HRRS (Höchstrichterliche Rechtsprechung zum Strafrecht), Aug./Sept. 2018, S. 336 – 342, S. 337f., URL: https://www.hrr-strafrecht.de/hrr/archiv/18-08/index.php?sz=8#337
[223] vgl. §26 Abs. 3 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./26.html
[224] §24 Abs. 4 S. 1 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./24.html
[225] vgl. §21 GGO, URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/AbteilungenReferate/IVA6_42GGO.pdf?__blob=publicationFile&v=4
[226] vgl. Voßhoff, Andrea: Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272 und der Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334, 29.05.2017, Seite 2, URL: https://freiheitsrechte.org/home/wp-content/uploads/2017/05/186346_Stellungnahme_BfDI_zu_18-11272_und_186334.pdf

Aus Unternehmenssicht ist in Hinsicht auf Strafverfahren auch zu beachten, dass Auskunftsersuchen durch Ermittlungsbehörden nicht unbedingt zulässig sind. Eine Übermittlung personenbezogener Daten ist nach Artikel 4 Nummer 2 DSGVO eine Verarbeitung[227] und damit nur unter Berücksichtigung der Verarbeitungsgrundsätze aus Artikel 5 DSGVO zu behandeln. Grob gesagt bedeutet das, dass für eine Weitergabe von Daten eine Rechtsgrundlage bestehen muss.[228] Dafür regelt Artikel 23 Absatz 1 DSGVO mögliche Beschränkungen der Rechte und Pflichten einiger Artikel, darunter Artikel 5 DSGVO, um die nationale oder die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zu gewährleisten.[229] Im BDSG wird dies in §24 genauer geregelt. Demnach ist eine Verarbeitung durch nicht-öffentliche Stellen zu anderen Zwecken als dem, zu dem die Daten erhoben wurden, zulässig, wenn sie zur Abwehr von Gefahren für staatliche oder öffentliche Sicherheit, zur Verfolgung von Straftaten oder zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche nötig ist, wobei die Interessen der betroffenen Person am Ausschluss der Verarbeitung mit dem der Verarbeitung zugrundeliegenden Interesse abzuwiegen sind.[230] Für Unternehmen hat das zur Folge, dass sie sich vor der Herausgabe angeforderter Informationen über den Tatvorwurf, den Zweck der Verarbeitung durch die Ermittlungsbehörde und die Rechtsgrundlage der Anfrage informieren und sicherstellen sollten, dass die Anfrage tatsächlich von der genannten Strafverfolgungsbehörde stammt.[231] Sollte es sich beim Betroffenen, dessen Daten von einer Ermittlungsbehörde erfragt werden, um einen Beschäftigten des Unternehmens handeln, ist zusätzlich §26 Absatz 1 Satz 2 BDSG zu beachten, wonach eine Weitergabe von Daten zur Aufdeckung von Straftaten nur bedingt zulässig ist.[232] Zu beachten ist hierbei auch die Trennung von Straftat und Ordnungswidrigkeit. Eine Ordnungswidrigkeit wie Falschparken wird vermutlich nur in eher seltenen Einzelfällen die Weitergabe personenbezogener Daten rechtfertigen.[233] Sollten die personenbezogenen Daten unzulässigerweise übermittelt werden, könnte dies zu Sanktionen nach Artikel 83 Absatz 5 Buchstabe a DSGVO führen. Sollten die Daten DSGVO konform übermittelt werden können, ist grundsätzlich nach

[227] vgl. Art. 4 Nr. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[228] vgl. URL : https://www.datenschutzbeauftragter-info.de/polizeianfragen-rechtskonforme-datenweitergabe-nach-der-dsgvo/, 17.09.19
[229] vgl. Art. 23 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/23.html
[230] vgl. §24 Abs. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/24.html
[231] vgl. URL : https://www.datenschutzbeauftragter-info.de/polizeianfragen-rechtskonforme-datenweitergabe-nach-der-dsgvo/, 17.09.19
[232] vgl. §26 Abs. 1 S. 2 BDSG, URL: https://dejure.org/gesetze/BDSG/26.html
[233] vgl. URL : https://datenschutzbeauftragter-hamburg.de/2016/03/weitergabe-personenbezogener-daten-an-ermittlungsbehoerden/, 17.09.19

Artikel 13 Absatz 3 DSGVO der Betroffene zu informieren. Sollte dies die Ermittlungsmaßnahmen gefährden, kann, wenn die Ermittlungsbehörde auch dafür eine bestehende Rechtsgrundlage nennt, davon abgesehen werden.[234]

6.4 TKG, TMG

Sowohl das Telekommunikationsgesetz (TKG, Teil 7, Abschnitt 2) als auch das Telemediengesetz (TMG, Abschnitt 4) enthalten Datenschutzbestimmungen. Eine Abgrenzung der Anwendungsbereiche der beiden Gesetze kann mitunter schwierig sein, da beispielsweise eine E-Mail-Kommunikation sowohl an sich ein Vorgang der Telekommunikation ist, also dem TKG unterliegt, als auch einen spezifischen Mail-Dienst erfordert, der unter das TMG fällt.[235] Internetanbieter können desweiteren unter Umständen als doppeltfunktionale Dienste eingestuft werden, wenn sowohl Signalübertragungen als auch inhaltliche Angebote wie Startportale geboten werden.[236] Ursprünglich sollte zeitgleich mit der DSGVO auch die Datenschutzrichtlinie für elektronische Kommunikation von 2002 **(**Richtlinie 2002/58/EG[237]) durch eine ePrivacy-Verordnung (Erster Entwurf vom Januar 2017, 2017/0003 (COD)) abgelöst werden, die die DSGVO präzisieren und ergänzen sollte.[238] Diese Verordnung ist bis dato noch nicht in Kraft getreten.

Daraus ergibt sich eine große Rechtsunsicherheit seitens Unternehmen, da aufgrund der Vorrangstellung der DSGVO unklar ist, inwieweit die Regelungen des TKG beziehungsweise des TMG anwendbar sind.

Die nationalen Regelungen des TMG entsprechen weder einer Umsetzung der aktuell noch gültigen ePrivacy Richtlinie 2002/58/EG,[239] noch wurden sie an die DSGVO angepasst.[240] Dadurch stellt sich die Frage nach der Anwendbarkeit dieses Gesetzes unter

---

[234] vgl. URL : https://www.datenschutzbeauftragter-info.de/polizeianfragen-rechtskonforme-datenweitergabe-nach-der-dsgvo/, 17.09.19

[235] vgl. URL: https://www.datenschutzexperte.de/telekommunikationsgesetz-tkg/, 22.09.19

[236] vgl. URLs: http://lexikon.jura-basic.de/aufruf.php?file=1&art=&find=Telemedien%20%3E%3EAbgrenzung%20zu%20Telekommunikation%20und%20Rundfunk, http://www.rechtzweinull.de/telemediengesetz, 22.09.19

[237] vgl. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058, 22.09.19

[238] vgl. Art. 1 Abs. 3 2017/0003 (COD), Vorschlag für die Verordnung über Privatsphäre und elektronische Kommunikation, 10.1.2017, von https://www.datenschutz-bayern.de/0/eprivacyVO.html

[239] vgl. DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 3, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

[240] vgl. URL: https://www.buzer.de/gesetz/7616/l.htm, 30.09.19

Berücksichtigung des Anwendungsvorrangs der DSGVO.[241] Zu dieser Problematik wurde im April 2018, also vor Inkrafttreten der DSGVO, eine Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) veröffentlicht.[242] Darin heißt es, Artikel 95 DSGVO, der besagt, dass „natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf[erlegt werden], soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen“[243], enthalte keine Aussage über die Gültigkeit der Regelungen im vierten Abschnitt des TMG, da dieser vorrangig eher einer Umsetzung der von der DSGVO abgelösten Datenschutzrichtlinie (95/46/EG) als einer der ePrivacy-Richtlinie entspricht und damit in den Anwendungsbereich der DSGVO fällt. Es wird der Schluss gezogen, dass die Paragraphen §§12, 13, 15 TMG nicht mehr angewendet werden können, um die Rechtmäßigkeit von Tracking-Maßnahmen, also dem Nachvollziehen des Verhaltens der Betroffenen im Internet, zu beurteilen.[244] §15 Absatz 3 TMG erlaubt „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen [zu] erstellen, sofern der Nutzer dem nicht widerspricht.“[245] Auch die ePrivacy-Richtlinie kann nicht unmittelbar angewendet werden, da es sich eben nicht um eine Verordnung handelt. Dadurch ist für die Verwendung von Tracking-Mechanismen und die Erstellung von Nutzerprofilen nach der Einschätzung der DSK in jedem Fall eine vorherige Einwilligung der Betroffenen im Sinne der DSGVO nötig. Eine solche Einwilligung erfordert eine freiwillige, informierte und unmissverständliche Entscheidung für die Verarbeitung,[246] ein schlichtes Nicht-Widersprechen wäre demnach dafür nicht ausreichend. Die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kann sich mangels

[241] vgl. URL: http://hoganlovells-blog.de/2018/06/11/dsgvo-oder-tmg-was-muessen-unternehmen-beim-einsatz-von-cookies-beachten/, 30.09.19
[242] vgl. DSK: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 26.04.2018, URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf
[243] Art. 95 DSGVO, URL: https://dejure.org/gesetze/DSGVO/95.html
[244] vgl. DSK: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 26.04.2018, S. 2, URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf
[245] §15 Abs. 3 S.1 TMG, URL: https://dejure.org/gesetze/TMG/15.html
[246] vgl. Art. 4 Nr. 11 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html

bestehender DSGVO- oder ePrivacy-Richtlinien-konformer Rechtsgrundlage nur auf Artikel 6 Absatz 1 Buchstabe a, b oder f DSGVO als Rechtsgrundlage stützen.[247] Artikel 6 DSGVO regelt, wie bereits beschrieben, die Rechtmäßigkeit von Verarbeitungen personenbezogener Daten. Unter Absatz 1 sind mögliche Bedingungen dafür genannt, von denen mindestens eine erfüllt sein muss. Bei den eben erwähnten Buchstaben dieses Absatzes handelt es sich um die Einwilligung der betroffenen Person, die Notwendigkeit der Verarbeitung zur Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen, sowie die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen, Grundrechte oder Grundfreiheiten des Betroffenen überwiegen.[248] In einer Stellungnahme zu dieser Positionsbestimmung der DSK führt der Verbraucherzentrale Bundesverband (vzbv) darüber hinaus die Frage an, inwieweit sich Tracking oder Profiling auf die Rechtsgrundlage der berechtigten Interessen des Verantwortlichen nach Artikel 6 Absatz 1 Buchstabe f DSGVO stützen kann, da Direktwerbung, zu deren Zweck Tracking- und Profiling-Maßnahmen dienen, durch Erwägungsgrund 47 DSGVO[249] nicht automatisch als berechtigtes Interesse anerkannt wird, sondern lediglich als solches verstanden werden kann.[250] Unabhängig von der diesbezüglichen Interpretation enthält Artikel 21 DSGVO ein Widerspruchsrecht betroffener Personen in Hinsicht auf Direktwerbung, ein solcher Widerspruch hat die Einstellung der Verarbeitung zu diesem Zweck zur Folge.[251] Im März 2019 hat die DSK eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht.[252] Darin wird der Schluss gezogen, dass Artikel 6 Absatz 1 Buchstab f DSGVO keine pauschale Begründung für die Rechtmäßigkeit einer Datenverarbeitung ist und dafür konkrete Einzelfallentscheidungen erforderlich sind, die nur nach einer substantiellen Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten möglich sind.[253] Für diese Interessensabwägung ist ein Schema bestehend aus drei Schritten vorgeschlagen, das auch in Hinsicht auf die

[247] vgl. DSK: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 26.04.2018, S. 2ff., URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf
[248] vgl. Art. 6 Abs. 1 Buchstaben a, b, f DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[249] vgl. https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html
[250] vgl. vzbv: Anwendbarkeit des Telemediengesetzes, 28.06.2018, S. 4ff., URL: https://www.vzbv.de/sites/default/files/downloads/2018/06/29/18-06-28_vzbv-stellungnahme_dsk_tmg-dsgvo.pdf
[251] vgl. Art. 21 Abs. 2 und 3 DSGVO, URL: https://dejure.org/gesetze/DSGVO/21.html
[252] vgl. DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
[253] vgl. DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 21, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Rechenschaftspflicht des Verantwortlichen sinnvoll scheint. Dabei sollen zunächst die berechtigten Interessen des Verantwortlichen oder eines Dritten ermittelt und festgehalten werden. Dann sind alle geplanten Datenverarbeitungen auf ihre Erforderlichkeit zur Wahrung dieser Interessen zu prüfen. Sollte es mildere, gleich geeignete Mittel für das Erreichen eines bestimmten Zwecks geben, so sind die geplanten Verarbeitungen nicht mehr erforderlich und damit auf dieser Rechtsgrundlage bereits unzulässig. Zuletzt sind die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person im konkreten Einzelfall gegen die bestehenden Interessen des Verantwortlichen abzuwägen. Möglich wären hier neben dem Recht auf Schutz personenbezogener Daten (Art. 8 GRCh[254]) beispielsweise das Recht auf Vertraulichkeit der Kommunikation (Art. 7 GRCh[255]) oder das Recht auf freie Meinungsäußerung und Informationsfreiheit (Art. 11 GRCh[256]). Für die zur Abwägung nötige Gewichtung der Interessen sind allgemeingültige Regeln schwer zu formulieren, allerdings gilt grundsätzlich, dass spezifisch verfassungsrechtliche Interessen, wie die in der GRCh genannten, gegenüber einfachgesetzlich anerkannten Interessen höher zu gewichten sind, und Interessen, die nicht ausschließlich dem Verantwortlichen sondern auch der Allgemeinheit dienen, ebenfalls gewichtiger sind. Hierbei sind die Informationspflichten oder eine Pseudonymisierung nicht zu Gunsten des Verantwortlichen auszulegen, sofern sie aus der DSGVO entstehende, gesetzlich tatsächlich vorgeschriebene Pflichten sind, zusätzliche Schutzmaßnahmen hingegen können die Beeinträchtigung durch die Verarbeitung reduzieren und das Ergebnis der Abwägung so beeinflussen.[257]

Das Positionspapier der DSK von April 2018 wurde inhaltlich in einer Stellungnahme des Bitkom[258] scharf kritisiert, da dieser die Ansicht vertritt, dass das TMG in der Tat die nationale Umsetzung der ePrivacy-Richtlinie darstellt und auch als solche der EU-Kommission übermittelt wurde, von der es keinen Widerspruch gab.[259] Tatsächlich entspricht dies der Argumentation des CDU/CSU-Politikers Andreas Lämmel als Reaktion auf einen Gesetzesentwurf zur Änderung des Telemediengesetzes seitens der SPD. Auch wenn letzteres in keinem Bezug zur DSGVO steht, da diese Sitzung bereits im

[254] URL: https://dejure.org/gesetze/GRCh/8.html
[255] URL: https://dejure.org/gesetze/GRCh/7.html
[256] URL: https://dejure.org/gesetze/GRCh/11.html
[257] vgl. DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 11-14, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
[258] Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.
[259] vgl. Bitkom: Stellungnahme zur Positionsbestimmung der Datenschutzkonferenz vom 26. April 2018 zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, 09.05.2018, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2018/Positionspapiere/180511-Positionsbestimmung-der-Datenschutzkonferenz-vom-26-April-2018/Bitkom-Stellungnahme-Position-DSK-DSGVO-TMG.pdf

Januar 2012 stattfand[260], wäre das TMG als Umsetzung der ePrivacy-Richtlinie weiterhin gültig. In seinem Tätigkeitsbericht 2017 und 2018 zum Datenschutz vom 08.05.2019 geht der Bundesbeauftragte für Datenschutz und Informationsfreiheit wiederum davon aus, dass die datenschutzrechtlichen Bestimmungen des TMG eben nicht der ePrivacy-Richtlinie entsprechen und deshalb neben der DSGVO nicht bestehen. Der Umgang mit personenbezogenen Daten im Zusammenhang mit Telemedien und die Beurteilung der Rechtmäßigkeit desselben muss deswegen rein von der DSGVO abgeleitet werden.[261]

Neben der bereits erwähnten Pflicht von Anbietern von Telekommunikationsdiensten zur Bereistellung geeigneter Schnittstellen zur Überwachung des Datenverkehrs nach §110 TKG sind in den Paragraphen §§113a bis 113g TKG die datenschutzrechtlich kritischen Pflichten von Anbietern öffentlich zugänglicher Telekommunikationsdienste für Endnutzer zur Vorratsdatenspeicherung geregelt. Demnach sind diese Anbieter verpflichtet, bei jeder Telekommunikation, darunter neben Telefonie auch SMS, MMS und ähnliches, anfallende Verkehrsdaten wie Rufnummern der an der Kommunikation Beteiligten, Datum und Uhrzeit von Beginn und Ende der Kommunikation unter Berücksichtigung der Zeitzone, bei mobilen Telefondiensten internationale Kennungen der Endgeräte, bei Internet-Telefondiensten die IP-Adressen sowie nach Möglichkeit Standortdaten für zehn beziehungsweise im Fall der Standortdaten für vier Wochen zu speichern.[262] Daneben ist bei der Speicherung die Möglichkeit einer unverzüglichen Beantwortung möglicher Auskunftsersuchen durch berechtigte Stellen zu berücksichtigen.[263] Die irreversible Löschung hat unverzüglich, spätestens jedoch innerhalb einer Woche nach Ablauf der Speicherfrist zu erfolgen.[264] Die auf dieser Grundlage erhobenen Daten dürfen „an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt.“[265] Der Anbieter des Telekommunikationsdienstes hat durch technische und organisatorische Maßnahmen nach dem Stand der Technik, darunter zum Beispiel der Einsatz eines Verschlüsselungsverfahrens, den Schutz der Daten gegen

[260] vgl. Deutscher Bundestag: Stenografischer Bericht, 155. Sitzung, Plenarprotokoll 17/155, 26.01.2012, S. 18700ff., URL: http://dipbt.bundestag.de/doc/btp/17/17155.pdf
[261] vgl. Unterrichtung durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit, 27.Tätigkeitsbericht, Drucksache 19/9800, 08.05.2019, S. 101, URL: http://dip21.bundestag.de/dip21/btd/19/098/1909800.pdf
[262] vgl. §113b Abs. 1 bis 4 TKG, URL: https://dejure.org/gesetze/TKG/113b.html
[263] vgl. §113b Abs. 7 TKG, URL: https://dejure.org/gesetze/TKG/113b.html
[264] vgl. §113b Abs. 8 TKG, URL: https://dejure.org/gesetze/TKG/113b.html
[265] §113c Abs. 1 Nr. 1 TKG, URL: https://dejure.org/gesetze/TKG/113c.html

unbefugte Kenntnissnahme und Verwendung zu gewährleisten.[266] In einem Vorabentscheidungsverfahren hat der Europäische Gerichtshof (EuGH) „entschieden, dass die Mitgliedstaaten den Betreibern elektronischer Kommunikationsdienste keine allgemeine Verpflichtung zur Vorratsdatenspeicherung auferlegen dürfen.“[267] Auch wenn es sich bei diesem Entscheid um englische und schwedische Regelungen handelt, enthält auch die deutsche Rechtslage eine „flächendeckende und anlasslose Vorratsdatenspeicherung, die alle Nutzer von elektronischer Kommunikation betrifft.“[268] Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hat 2017 „in einem Verfahren des einstweiligen Rechtsschutzes festgestellt, dass der klagende Internetzugangsdiensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens nicht verpflichtet ist, die in §113b Abs. 3 TKG genannten Telekommunikationsverkehrsdaten zu speichern.“[269] Deswegen verzichtet die Bundesnetzagentur bis zu einer endgültigen Entscheidung auf jegliche Anordnungen oder Maßnahmen, auch Bußgeldverfahren, zur Durchsetzung dieser Regelung.[270]

6.5 HGB, AO

Das Handelsgesetzbuch (HGB) und die Abgabenordnung (AO) kommen auf den ersten Blick überwiegend aufgrund der dort verankerten Aufbewahrungsfristen mit der DSGVO in Berührung. Laut §257 HGB gilt beispielsweise für Handelsbücher, Eröffnungsbilanzen, Lageberichte und Buchungsbelege eine Aufbewahrungspflicht von zehn Jahren, Handelsbriefe, also Schriftstücke, die ein Handelsgeschäft betreffen, müssen sechs Jahre lang aufbewahrt werden.[271] In §147 AO werden zusätzlich steuerrelevante Unterlagen aufgeführt, für die ebenfalls eine Aufbewahrungsfrist von sechs Jahren gilt, sofern nicht andere steuerrechtliche Regelungen eine kürzere Aufbewahrungsfrist zulassen.[272] Die

[266] vgl. §113d TKG, URL: https://dejure.org/gesetze/TKG/113d.html
[267] URL: https://www.datenschutz-notizen.de/eugh-allgemeine-verpflichtung-zur-vorratsdatenspeicherung-ist-unzulaessig-5417066/, 13.10.19
[268] URL: https://www.datenschutz-notizen.de/eugh-allgemeine-verpflichtung-zur-vorratsdatenspeicherung-ist-unzulaessig-5417066/, 13.10.19
[269] Bundesnetzagentur: Mitteilung, URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html, 13.10.19
[270] vgl. Bundesnetzagentur: Mitteilung, URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html, 13.10.19
[271] vgl. §257 HGB, URL: https://dejure.org/gesetze/HGB/257.html
[272] vgl. §147 AO, URL: https://dejure.org/gesetze/AO/147.html

DSGVO erklärt Datenverarbeitungen, worunter auch die bloße Speicherung fällt[273], auf der Grundlage einer rechtlichen Verpflichtung in Artikel 6 Absatz 1 Buchstabe c DSGVO für rechtmäßig.[274] Auch in Artikel 17 DSGVO, in dem das Recht einer Person auf Löschung der sie betreffenden personenbezogenen Daten festgehalten ist, wird eindeutig betont, dass auf das Löschen trotz des Wunsches des Betroffenen verzichtet werden kann, wenn dem die Erfüllung rechtlicher Verpflichtungen entgegen steht.[275] Im Anwendungsbereich der AO in §2a AO wird eine ausdrückliche Abgrenzung zur DSGVO mit Betonung ihrer Vorrangstellung vorgenommen, hier heißt es: „Die Vorschriften dieses Gesetzes und der Steuergesetze über die Verarbeitung personenbezogener Daten finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die [DSGVO] [...] in der jeweils geltenden Fassung unmittelbar [...] gilt.“[276] Im HGB in §10a HGB findet sich eher eine Einschränkung beziehungsweise Spezifizierung der aus der DSGVO abgeleiteten Betroffenenrechte, indem erklärt wird, dass das Auskunftsrecht nach Artikel 15 Absatz 1 DSGVO allein dadurch erfüllt wird, „dass die betroffene Person Einsicht in das Handelsregister und in die zum Handelsregister eingereichten Dokumente sowie in das für die Bekanntmachungen der Eintragungen bestimmte elektronische Informations- und Kommunikationssystem nehmen kann. Eine Information der betroffenen Person über konkrete Empfänger, gegenüber denen die im Register, in Bekanntmachungen der Eintragungen oder in zum Register einzureichenden Dokumenten enthaltenen personenbezogenen Daten offengelegt werden, erfolgt nicht.“[277] Zudem haben Betroffene nur unter gewissen Voraussetzungen, die in einigen Paragraphen des ‚Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der Freiwilligen Gerichtsbarkeit’ für eine Löschung beziehungsweise Berichtigung vorgesehen sind, das Recht auf Berichtigung der sie betreffenden Daten in Hinsicht auf das Handelsregister, Bekanntmachungen der Eintragungen oder auf zum Handelsregister einzureichenden Dokumente.[278] Auch das Widerspruchsrecht nach Artikel 21 DSGVO findet demnach keine Anwendung.[279] Dieses Widerspruchsrecht ergibt sich laut Artikel 21 DSGVO lediglich für diejenigen personenbezogenen Daten, die auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e oder f DSGVO verarbeitet werden, und führt zum Abbruch der Verarbeitung, sofern der Verantwortliche nicht „zwingende schutzwürdige

[273] vgl. Art. 4 Nr. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[274] vgl. Art. 6 Abs. 1 Buchstabe c DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[275] vgl. Art. 17 Abs. 3 Buchstabe b DSGVO, URL: https://dejure.org/gesetze/DSGVO/17.html
[276] §2a Abs.3 AO, URL: https://dejure.org/gesetze/AO/2a.html
[277] §10a Abs. 1 HGB, URL: https://dejure.org/gesetze/HGB/10a.html
[278] vgl. §10a Abs. 2 HGB, URL: https://dejure.org/gesetze/HGB/10a.html
[279] vgl. §10a Abs. 3 HGB, URL: https://dejure.org/gesetze/HGB/10a.html

Gründe für [diese] nachweisen [kann], die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.“[280] In Artikel 6 Absatz 1 Buchstaben e und f DSGVO werden Verarbeitungen aufgrund der Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen und dem Verantwortlichen übertragen wurden beziehungsweise Verarbeitungen zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, falls nicht die Interessen des Betroffenen überwiegen, für rechtmäßig erklärt.[281] Allerdings stellt Artikel 23 DSGVO eine weitere Öffnungsklausel dar, die die nationalgesetzliche Beschränkung einiger Betroffenenrechte, darunter auch das Widerspruchsrecht nach Artikel 21 DSGVO, neben anderen Schutzzielen auch zur Sicherstellung des Schutzes wichtiger Ziele des allgemeinen öffentlichen Interesses eines Mitgliedstaates oder zum Schutz der betroffenen Person sowie der Rechte und Freiheiten anderer Personen erlaubt.[282] Da also das Widerspruchsrecht aus Artikel 21 DSGVO nur dann nicht greift, wenn eine Verarbeitung im öffentlichen Interesse oder zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erfolgt, beides schutzwürdige Ziele, die eine Beschränkung nach Artikel 23 DSGVO ermöglichen, steht dieser Paragraph des HGB nicht grundsätzlich im Widerspruch zur DSGVO. Das Handelsregister dient durch zuverlässige und vollständige Daten der Transparenz und Sicherheit im Geschäftsverkehr und damit auch einem öffentlichen Interesse[283], was eine Beschränkung der Betroffenenrechte nach der DSGVO rechtfertigt.[284] Im zweiten Absatz des Artikels 23 DSGVO sind spezifische Inhalte genannt, zu denen eine solche Gesetzgebungsmaßnahme gegebenenfalls Informationen enthalten muss, darunter zum Beispiel die Zwecke der Verarbeitung oder die Verarbeitungskategorien, die Kategorien personenbezogener Daten, den Umfang der Beschränkungen, Angaben zum Verantwortlichen und die Risiken für die Rechte und Freiheiten der betroffenen Personen.[285]

Sowohl das HGB als auch die AO wurden durch das ‚Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften’, das ebenfalls am 25.05.2018 in Kraft trat, an die DSGVO angepasst. Beim HGB waren davon lediglich zwei Paragraphen betroffen, der bereits näher beschriebene §10a HGB, der die Betroffenenrechte der

[280] Art. 21 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/21.html
[281] vgl. Art. 6 Abs. 1 Buchstabe e und f DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[282] vgl. Art. 23 Abs. 1 Buchstabe e und j DSGVO, URL: https://dejure.org/gesetze/DSGVO/23.html
[283] vgl. URL: https://www.ihk-niederbayern.de/Beratung-Service/Recht/handelsregister/zweck-des-handelsregisters/4116878, 16.09.19
[284] vgl. Art. 23 Abs. 1 Buchstabe e DSGVO, URL: https://dejure.org/gesetze/DSGVO/23.html
[285] vgl. Art. 23 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/23.html

DSGVO beschränkt, und §320 HGB, in dem lediglich Absatz 5 Satz 2 formal angepasst wurde.[286] In der AO wurden dagegen 34 Paragraphen geändert.[287] Neben dem bereits genannten §2a AO wurden zum Beispiel auch die §§29b und c neu eingeführt. In §29b AO wird die Verarbeitung personenbezogener Daten durch eine Finanzbehörde für zulässig erklärt, „wenn sie zur Erfüllung der ihr obliegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die ihr übertragen wurde, erforderlich ist.“[288] Das entspricht formal und inhaltlich Artikel 6 Absatz 1 Buchstabe e DSGVO.[289] §29b Absatz 2 AO befasst sich mit der Verarbeitung besonderer Kategorien personenbezogener Daten durch Finanzbehörden, dieser Absatz ist durch Artikel 9 Absatz 2 Buchstabe g DSGVO mit der Verordnung vereinbar, wenn eine solche Verarbeitung auf Grundlage des Rechts eines Mitgliedstaates aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.[290] Die selbe Bedingung wird auch im zugehörigen Paragraphen der AO gefordert.[291] §29c AO regelt die Verarbeitung personenbezogener Daten durch Finanzbehörden zu anderen Zwecken als dem Erhebungszweck[292] und entspricht weitgehend dem §23 BDSG.[293] §31c AO befasst sich mit der Verarbeitung besonderer Kategorien personenbezogener Daten zu statistischen Zwecken[294], was in Artikel 9 Absatz 2 Buchstabe j DSGVO für zulässig erklärt wird[295], dabei wird ebenso §22 Absatz 2 Satz1 BDSG berücksichtigt[296], der das Ergreifen „angemessene[r] und spezifische[r] Maßnahmen zur Wahrung der Interessen der betroffenen Person“[297] fordert und in Absatz 3 des Paragraphen für diesen Fall noch verschärft zur Anwendung kommt.[298] Im darauf folgenden Sechsten Abschnitt des Ersten Teils der AO, der komplett neu eingefügt wurde[299], sind die Rechte der betroffenen Person geregelt. Hier wird beispielsweise die Informationspflicht der Finanzbehörde bei Erhebung personenbezogener Daten, entsprechend dem Artikel 23 Absatz 1 DSGVO, beschränkt[300], auch für den Fall, dass die Daten nicht beim Betroffenen selbst erhoben

[286] vgl. URLs: https://www.buzer.de/gesetz/3486/l.htm, https://www.buzer.de/gesetz/3486/v208257-2018-05-25.htm, 20.09.19
[287] vgl. URL: https://www.buzer.de/gesetz/1966/l.htm, 20.09.19
[288] §29b Abs. 1 AO, URL: https://dejure.org/gesetze/AO/29b.html
[289] vgl. Art. 6 Abs. 1 Buchstabe e DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[290] vgl. Art. 9 Abs. 2 Buchstabe g DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[291] vgl. §29b Abs. 2 S. 1 AO, URL: https://dejure.org/gesetze/AO/29b.html
[292] vgl. §29c AO, URL: https://dejure.org/gesetze/AO/29c.html
[293] vgl. §23 BDSG, URL: https://dejure.org/gesetze/BDSG/23.html
[294] vgl. §31c AO, URL: https://dejure.org/gesetze/AO/31c.html
[295] vgl. Art. 9 Abs. 2 Buchstabe j DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[296] vgl. §31c Abs. 1 S. 2 AO, URL: https://dejure.org/gesetze/AO/31c.html
[297] §22 Abs. 2 S. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/22.html
[298] vgl. §31c Abs. 3 AO, URL: https://dejure.org/gesetze/AO/31c.html
[299] vgl. URL: https://www.buzer.de/gesetz/1966/v208267-2018-05-25.htm, 20.09.19
[300] vgl. §32a Abs. 1 und 2 AO, URL: https://dejure.org/gesetze/AO/32a.html

werden.[301] Auch in der AO ist das Auskunftsrecht des Betroffenen beschränkt, beispielsweise ist eine Auskunft nicht nötig, falls die Daten nur aufgrund gesetzlicher Aufbewahrungsfristen gespeichert sind, die Auskunftserteilung einen unverhältnismäßig großen Aufwand erfordern würde und durch technische und organisatorische Mittel sichergestellt ist, dass die Daten nicht zu einem anderen Zweck verarbeitet werden.[302] „Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.“[303] Erfolgt eine solche Information des Betroffenen, so wird die Form, soweit durch die DSGVO nichts genaueres vorgegeben ist, durch die Finanzbehörde bestimmt[304], bei einer elektronischen Auskunftserteilung ist §87a AO zu beachten[305], der für die Übermittlung von Daten, die dem Steuergeheimnis unterliegen, die Verwendung eines geeigneten Verschlüsselungsverfahrens vorschreibt.[306] In §32f AO werden die Rechte auf Berichtigung, Löschung und Widerspruch näher spezifiziert. Finanzbehörden sind demnach befugt, von einer Löschung abzusehen, wenn diese „im Falle nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und [...] das Interesse der betroffenen Person an der Löschung als gering anzusehen [ist].“[307] In einem solchen Fall ist die Verarbeitung einzuschränken, beides ist hingegen bei einer unrechtmäßigen Verarbeitung nicht möglich.[308] Das Recht auf Widerspruch besteht gegenüber einer Finanzbehörde nicht, „soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.“[309] Sollten „die Daten einem Verwaltungsakt zugrunde liegen, der nicht mehr aufgehoben, geändert oder berichtigt werden kann“[310], wird auch dann, wenn der Betroffene die Richtigkeit der Daten bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen lässt, keine Einschränkung der Verarbeitung bewirkt, allerdings ist „[d]ie ungeklärte Sachlage [...] in geeigneter Weise

[301] vgl. §32b AO, URL: https://dejure.org/gesetze/AO/32b.html
[302] vgl. §32c Abs. 1 Nr. 3 AO, URL: https://dejure.org/gesetze/AO/32c.html
[303] §32c Abs. 4 S. 1 AO, URL: https://dejure.org/gesetze/AO/32c.html
[304] vgl. §32d Abs. 1 und 2 AO, URL: https://dejure.org/gesetze/AO/32d.html
[305] vgl. §32d Abs. 3 AO, URL: https://dejure.org/gesetze/AO/32d.html
[306] vgl. §87a Abs. 1 S. 3 AO, URL: https://dejure.org/gesetze/AO/87a.html
[307] §32f Abs. 2 S. 1 AO, URL: https://dejure.org/gesetze/AO/32f.html
[308] vgl. §32f Abs. 2 S. 2 und 3 AO, URL: https://dejure.org/gesetze/AO/32f.html
[309] §32f Abs. 5 AO, URL: https://dejure.org/gesetze/AO/32f.html
[310] §32f Abs. 1 S. 1 AO, URL: https://dejure.org/gesetze/AO/32f.html

festzuhalten.“[311] In §384a AO ist zusätzlich festgelegt, dass „Vorschriften dieses Gesetzes und der Steuergesetze über Steuerordnungswidrigkeiten [...] keine Anwendung [finden], soweit für eine Zuwiderhandlung zugleich Artikel 83 der [DSGVO] [...] unmittelbar oder nach § 2a Absatz 5 entsprechend gilt.“[312]

6.6 SGB

Zeitgleich mit der DSGVO traten im Mai 2018 auch die Änderungen des Ersten und Zehnten Buches Sozialgesetzbuch (SGB I und SGB X), ebenfalls durch das ‚Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften’, in Kraft.[313] Eine solche Einführung spezifischerer Bestimmungen zur Anpassung der Anwendung der DSGVO für konkrete Aufgaben ist über Artikel 6 Absatz 2 und 3 DSGVO dann möglich, wenn eine Verarbeitung auf Grundlage einer rechtlichen Verpflichtung oder der Aufgabenerfüllung im öffentlichen Interesse erfolgt.[314] Im SGB I wurde lediglich §35 SGB I geändert. Während Absatz 1 des Paragraphen nur geringförmig und überwiegend formal angepasst wurde, regelt Absatz 2 den Umgang mit der DSGVO[315], indem festgelegt wird, dass die Bestimmungen der Sozialgesetzbücher die Verarbeitung von Sozialdaten abschließend regeln, sofern nicht die DSGVO unmittelbar gilt.[316] Im SGB X dagegen wurden 36 Paragraphen geändert.[317] So werden nun zum Beispiel Sozialdaten in §67 SGB X als personenbezogene Daten nach Artikel 4 Nummer 1 DSGVO, „die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden“[318], definiert. Die hier erwähnten Stellen finden sich in §35 Absatz 1 SGB I und meinen zum Beispiel die Datenstelle der Rentenversicherung, Integrationsfachdienste, die Künstlersozialkasse oder anerkannte Adoptionsvermittlungsstellen.[319] Neben zahlreichen hauptsächlich formalen oder

[311] §32f Abs. 1 S. 2 AO, URL: https://dejure.org/gesetze/AO/32f.html
[312] §384a Abs. 1 AO, URL: https://dejure.org/gesetze/AO/384a.html
[313] vgl. Bayrischer Landesbeauftragter für Datenschutz: Datenschutzreform 2018, Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO), 25.09.2017, S. 1f., URL: https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf
[314] vgl. Art. 6 DSGVO, URL: https://dejure.org/gesetze/DSGVO/6.html
[315] vgl. URL: https://www.buzer.de/gesetz/3690/al66903-0.htm, 20.09.19
[316] vgl. §35 Abs. 2 SGB I, URL: https://dejure.org/gesetze/SGB_I/35.html
[317] vgl. URL: https://www.buzer.de/gesetz/3086/l.htm, 20.09.19
[318] §67 Abs. 2 S. 1 SGB X, URL: https://dejure.org/gesetze/SGB_X/67.html
[319] vgl. §35 Abs. 1 SGB I, URL: https://dejure.org/gesetze/SGB_I/35.html

redaktionellen Anpassungen[320] werden auch im SGB X die Betroffenenrechte gemäß Artikel 23 Absatz 1 Buchstabe e DSGVO eingeschränkt,[321] dies erfolgt in vergleichbarer Art und ähnlicher Ausprägung der Beschränkungen in der AO.[322] Wichtig ist auch, dass im Zusammenhang mit dem Erheben von Gesundheitsdaten, die eine besondere Kategorie personenbezogener Daten nach Artikel 9 DSGVO darstellen, keine neuen spezifischen Regelungen im SGB X erlassen wurden, so dass hier die DSGVO direkt zu beachten ist.[323]

6.7 IT-SiG

Die erste Version des ‚Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme', das IT-Sicherheitsgesetz (IT-SiG), trat im Juli 2015 in Kraft.[324] Dieses „ist ein Artikelgesetz, das neben dem BSI-Gesetz auch das Energiewirtschaftsgesetz, das Atomgesetz, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze"[325] geändert hat. Das BSI ist das Bundesamt für Sicherheit in der Informationstechnik. Das IT-SiG schreibt Betreibern Kritischer Infrastrukturen, zum Beispiel aus den Bereichen Energie, IT und Telekommunikation, Gesundheit, Wasser oder Finanz- und Versicherungswesen, ein Mindest-Niveau an IT-Sicherheit und die Meldung von erheblichen IT-Störungen an das BSI vor.[326] Das ‚Gesetz über das Bundesamt für Sicherheit in der Informationstechnik' (BSI-Gesetz, BSIG) wurde dadurch um einige Paragraphen und Regelungen erweitert. Neben dem Hinzufügen der Erklärung

[320] vgl. Bayrischer Landesbeauftragter für Datenschutz: Datenschutzreform 2018, Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO), 25.09.2017, S. 2, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf
[321] vgl. Art. 23 Abs. 1 Buchstabe e DSGVO und §§82ff. SGB X, URLs: https://dejure.org/gesetze/DSGVO/23.html, https://dejure.org/gesetze/SGB_X/82.html
[322] vgl. §§82ff. SGB X und §§32aff. AO, URLs: https://dejure.org/gesetze/SGB_X/82.html, https://dejure.org/gesetze/AO/32a.html
[323] vgl. Bayrischer Landesbeauftragter für Datenschutz: Datenschutzreform 2018, Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO), 25.09.2017, S. 3, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf
[324] vgl. URL: https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html, 20.09.19
[325] BSI: Schutz Kritischer Infrastrukturen – durch IT-Sicherheitsgesetz und UP KRITIS, Kapitel 3: Das IT-SiG ist Pflicht, 2017, S. 11, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=7F65543A03EE0395114CEC68CC88E11B.1_cid360?__blob=publicationFile&v=7
[326] BSI: Das IT-Sicherheitsgesetz, Kapitel 2: Zielgruppen und Neuregelungen, S. 7, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf;jsessionid=7F65543A03EE0395114CEC68CC88E11B.1_cid360?__blob=publicationFile&v=7

der Zuständigkeit für die Informationssicherheit auf nationaler Ebene in §1 BSIG wurde in §2 Absatz 10 BSIG auch eine Definition kritischer Infrastrukturen angefügt.[327] Dabei handelt es sich um Einrichtungen, Anlagen oder Teile davon, die zum einen bestimmten, teilweise bereits genannten Sektoren angehören und zum anderen auch „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“[328] Die Paragraphen §§8a – 8d BSIG wurden hinzugefügt. Diese verpflichten Betreiber kritischer Infrastrukturen dazu, nach dem Stand der Technik „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen“[329], die Erfüllung dieser Anforderungen mindestens alle zwei Jahre nachzuweisen[330] und „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“[331] an das BSI zu melden. Im Zuge dieser Vorschriften verarbeitete personenbezogene Daten dürfen nach §8b Absatz 7 BSIG nicht zu anderen Zwecken als den im Paragraphen genannten verarbeitet werden.[332] Neu war auch die Berichtspflicht des BSI gegenüber des Bundesministeriums des Innern und die Bußgeldvorschriften in §14 BSIG.[333] Demnach kann eine mangelnde Umsetzung geeigneter IT-Sicherheits-Maßnahmen oder das Ausbleiben der Meldung zu einer Geldbuße von bis zu fünfzigtausend Euro geahndet werden.[334] Aktuell wird ein IT-SiG 2.0 diskutiert, einen zugehörigen Referentenentwurf (BSIG-E) legte das Bundesministerium des Innern (BMI) am 27.03.2019 vor.[335] Danach soll zum Beispiel das BSIG dahingehend geändert werden, dass das BSI anfallende Protokolldaten länger als bisher, nämlich maximal 18 statt wie aktuell drei Monate, speichern darf, dabei kann durch eine Anordnung des Präsidenten des Bundesamtes der Erhalt oder die Wiederherstellung eines Personenbezugs pseudonymisierter Daten

[327] vgl. URL: https://www.buzer.de/gesetz/8987/v193756-2015-07-25.htm, 20.09.19
[328] §2 Abs. 10 Nr. 2 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[329] §8a Abs. 1 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[330] vgl. §8a Abs. 3 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[331] §8b Abs. 4 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[332] vgl. §8b Abs. 7 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[333] vgl. URL: https://www.buzer.de/gesetz/8987/v193756-2015-07-25.htm, 20.09.19
[334] vgl. §14 Abs. 2 BSIG, URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf
[335] vgl. BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf

erfolgen, soweit dies erforderlich ist.[336] Außerdem wird der Sektor Entsorgung als Kritische Infrastruktur hinzugefügt und Anlagen, die „dem Bereich Kultur und Medien angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind“[337] werden als Infrastrukturen von besonderem öffentlichen Interesse eingestuft[338] und damit ebenfalls zu einer gewissen IT-Sicherheit verpflichtet. Desweiteren wird vorgeschlagen, die Geldbußen an die in der DSGVO genannten Beträge anzupassen, also erheblich zu erhöhen.[339] Nach dem vorgeschlagenen §7b BSIG-E ist das BSI befugt, „zur Erfüllung seiner Aufgaben Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich erreichbaren informationstechnischen Systemen durch[zu]führen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können.“[340]

Außer dem BSIG ist im IT-SiG 2.0 auch die Änderung des TKG (TKG-E) und des TMG (TMG-E) vorgesehen. Demnach wird zum Beispiel für Betreiber öffentlicher Telekommunikationsnetze zusätzlich zu den in §109 TKG vorgeschriebenen technischen Schutzmaßnahmen[341] durch einen ergänzenden Absatz 2a für diesen Paragraphen ausdrücklich der Einsatz eines Systems zur Angriffserkennung (IDS – Intrusion Detection System) gefordert.[342] Laut TMG-E kann das BSI „zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für eine Infrastruktur im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter [...] anordnen, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann.“[343] Zudem sollen die für die IT-Sicherheit einschlägigen Paragraphen des StGB geändert beziehungsweise neue Paragraphen hinzugefügt werden (StGB-E). Der

[336] vgl. ebd. §5 Abs. 2 BSIG-E, S. 11f.
[337] BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, §2 Abs. 14 Nr. 1 BSIG-E, S. 8, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf
[338] vgl. ebd. §2 Abs. 13 und 14 BSIG-E, S. 8,
[339] vgl. ebd. §14 Abs. 2 BSIG-E, S. 24
[340] ebd. §7b Abs. 1 BSIG-E, S. 16
[341] vgl. §109 TKG, URL: https://dejure.org/gesetze/TKG/109.html
[342] vgl. BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, §109 Abs. 2a TKG-E, S. 25, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf
[343] vgl. ebd. §13 Abs. 7a TMG-E, S. 27

Referentenentwurf sieht hier unter anderem die Erhöhung der Strafe gemäß den Paragraphen §§202a bis 202 d StGB vor. Hierbei handelt es sich um das Ausspähen oder Abfangen von Daten, das Vorbereiten eines der beiden und Datenhehlerei. In allen Fällen soll die Strafe auf Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe statt wie bisher Freiheitsstrafe bis zu zwei beziehungsweise drei Jahren oder Geldstrafe angehoben werden. Gleiches gilt für §303a StGB, der die rechtswidrige Datenveränderung regelt. Im Falle des §303b StGB, der Computersabotage, soll die aktuelle Strafe von Freiheitsstrafe bis zu drei Jahren oder Geldstrafe auf sechs Monate bis zu fünf Jahre Freiheitsstrafe oder Geldstrafe erhöht werden.[344] Desweiteren ist das Hinzufügen der §§202e, 202f StGB-E geplant, die für die unbefugte Nutzung informationstechnischer Systeme eine Geldstrafe oder Freiheitsstrafe bis zu einem Jahr und für einen besonders schweren Fall einer Straftat gegen die Vertraulichkeit oder die Integrität von IT-Systemen, darunter fallen beispielsweise die Straftaten der §§202a bis 202e StGB-E bei gewerbsmäßigem Handeln oder Zugehörigkeit zu einer Bande, eine Freiheitsstrafe von sechs Monaten bis zu zehn Jahren vorsehen.[345] Eine Straftat nach §202f StGB-E in der Absicht, die Funktionsfähigkeit einer kritischen Infrastruktur zu beeinträchtigen oder zu gefährden, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft und damit zum Verbrechen deklariert.[346] Die Tatbestände der gerade genannten Paragraphen, §§202a bis 202e, 202f Absatz 2 und 3 StGB-E, sollen auch in die StPO als schwere Straftat nach §100a StPO aufgenommen werden und damit der Verdacht auf eine solche eine (Quellen-)TKÜ rechtfertigen. Eine Straftat nach §202f Absatz 2 StGB-E soll auch in den Staftatenkatalog des §100b StPO-E aufgenommen werden und damit eine Grundlage für eine Online-Durchsuchung darstellen können.[347] Interessant ist diesbezüglich auch der Abschlussbericht einer Fallstudie des BKA zu sogenannten ‚Hacktivisten', also Aktivisten, die bestimmte soziale oder politische Ziele und Ideologien mittels Hacking-Tools durchzusetzen versuchen.[348] Unter den 211 zwischen 2010 und 2012 festgenommenen Mitgliedern des Web-Kollektivs Anonymous[349] waren demnach 31, die

[344] vgl. ebd. §§202a bis 202d, 303a, 303b StGB-E, S. 29
[345] vgl. ebd. §§202e, 202f, S. 30f.
[346] vgl. ebd. §202f Abs. 2 StGB-E, S. 31
[347] vgl. BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, §§100a, 100b StPO-E, S. 32, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf
[348] vgl. BKA: Hacktivisten – Abschlussbericht, S. 18, Download möglich unter: URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2016HacktivistenqAbschlussbericht.html
[349] Hierbei handelt es sich um eine internationale, dezentrale Gruppe von ‚Hacktivisten', die sich für ein freies Internet ohne Zensur einsetzen und durch DOS-Attacken gegen Wikileaks-Gegner bekannt wurden.

unter 18 Jahre alt waren. Auch in der Fallstudie des BKA, in der 37 Beschuldigte betrachtet wurden, waren 16 zwischen 14 und 18 Jahre alt, eine Person sogar unter 14.[350] Der Datenschutz bei Minderjährigen ist allgemein eher strenger zu behandeln als der Erwachsener, eine Quellen-TKÜ, die bei einem Vergehen nach §202a StGB, also dem Zugänglichmachen geschützter Daten[351], nach IT-SiG 2.0 möglich wäre, ist, wie bereits erklärt, nach Einschätzung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ohnehin ein immenser Eingriff in die Privatsphäre Beschuldigter. Bei einem verhältnismäßig hohen Anteil minderjähriger Täter wäre ein solches Ausmaß möglicherweise noch kritischer zu betrachten.

Seit Februar 2019 werden Anträge unterschiedlicher Fraktionen zur Stärkung der IT-Sicherheit diskutiert.[352] Die Linke plädiert dabei gegen den Einsatz von Staatstrojanern sowie die Nutzung oder Anschaffung von Sicherheitslücken wie Backdoors[353] oder Zero-Day-Exploits[354]. Desweiteren argumentieren sie für die Umwandlung des BSI in eine eigenständige, vom BMI unabhängige Behörde, ein Verbot für den Export von Überwachungssoftware sowie den Ausschluss von Militär und Geheimdiensten aus der deutschen Cyber-Sicherheitsstrategie und die Förderung von Open-Source-Software[355] im Bereich der IT-Sicherheit.[356] Auch die FDP kritisiert in ihrem Antrag, dass das BSI dem BMI untersteht, das gleichzeitig für das BKA und das Bundesamt für Verfassungsschutz (BfV) zuständig ist. Daraus resultiert ein deutlicher Interessenkonflikt innerhalb des Ministeriums.[357]

---

[350] vgl. BKA: Hacktivisten – Abschlussbericht, S. 50f., Download möglich unter: URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2016HacktivistenqAbschlussbericht.html

[351] vgl. §202a StGB, URL: https://dejure.org/gesetze/StGB/202a.html

[352] vgl. URL: https://kripoz.de/Kategorie/gesetzentwuerfe/page/2/, 24.10.19

[353] „Hintertüren" zu Programmen oder Hardwaresystemen, übliche Sicherheitsmechanismen werden dabei umgangen, auch für Service- oder Reparaturzwecken von Herstellern genutz, kann gewollt implementiert oder heimlich installiert sein, weitere Informationen: URL: https://www.security-insider.de/was-ist-eine-backdoor-a-676126/, 03.11.19

[354] Hierbei werden dem Hersteller noch unbekannte Schwachstellen ausgenutzt, für die es deswegen auch noch kein Patch gibt, die Sicherheitslücke also nicht einfach durch Installation einer bekannten Korrektur geschlossen werden kann. So kann unterschiedliche Malware auf dem System zum Einsatz kommen. Weitere Informationen: URL: https://www.security-insider.de/was-ist-ein-zero-day-exploit-a-648117/, 03.11.19

[355] Open-Source-Software ist quelloffen, das bedeutet, der zugrundeliegende Code ist zugänglich, kann und darf verändert beziehungsweise angepasst werden. Die Software darf weiter verteilt werden, muss allerdings nicht kostenfrei sein. Weitere Informationen: URL: https://opensource.org/docs/osd, 03.11.19

[356] vgl. Die Linke: Antrag: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, Drucksache 19/7705, 13.02.19, II. 5., S. 1f., URL: https://kripoz.de/wp-content/uploads/2019/02/bt-drs-19-7705.pdf

[357] vgl. FDP: Antrag: Digitalisierung ernst nehmen – IT-Sicherheit stärken, Drucksache 19/7698, 12.02.19, S. 2, URL: https://kripoz.de/wp-content/uploads/2019/02/bt-drs-19-7698.pdf

Dieselbe Forderung nach der Unabhängigkeit der Behörden mit Ziel IT-Sicherheit von Ermittlungsbehörden und Geheimdiensten unterstützt eco, Verband der Internetwirtschaft e.V., in seiner Stellungnahme zu den Anträgen der Fraktionen.[358] Desweiteren wird darin für eine allgemeine Pflicht für alle staatlichen Behörden ebenso wie für KRITIS Betreiber plädiert, bekannte Sicherheitslücken zwingend zu melden.[359] Außerdem ist es laut eco „[v]or dem Hintergrund der Bedeutung des Schutzes personenbezogener Daten und datensparsamer Ansätze bei Ermittlungen und bei staatlichem Handeln [...] auch wegen des massiven Eingriffs in die Vertraulichkeit der Kommunikation von Bürgerinnen und Bürgern dringend erforderlich, dass die Vorratsdatenspeicherung abgeschafft wird.“[360] Auch Dr. Sven Herpig, Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, hat in seiner Stellungnahme die stärkere Unabhängigkeit des BSI von anderen Behörden des BMI als wichtiges Ziel genannt. Daneben empfiehlt er eine Erhöhung der Schutzmaßnahmen gegen invasive staatliche Überwachungsmaßnahmen wie Quellen-TKÜ oder Online-Durchsuchung.[361] Im IT-SiG 2.0 wird §1 BSIG, in dem eindeutig geregelt ist, dass das BSI dem BMI untersteht, nicht geändert.[362] Demnach bleibt der Interessenkonflikt innerhalb des BMI weiterhin bestehen. Auch werden weder die Paragraphen §§113a bis 113g TKG[363], die die Vorratsdatenspeicherung betreffen, noch die Paragraphen der StPO[364], die den Einsatz von Staatstrojanern ermöglichen, in die von den Sachverständigen gewünschte Richtung geändert.[365]

[358] vgl. eco: Stellungnahme zu den Anträgen: 19/7698: Digitalisierung ernst nehmen – IT-Sicherheit stärken, 19/7705: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, und 19/1328: IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern, Ausschussdrucksache 19(4)255 B, 04.04.19, S. 2f, URL: https://kripoz.de/wp-content/uploads/2019/04/a-drs-19-4-255-b-landefeld.pdf
[359] vgl. ebd. S. 4
[360] ebd. S. 6
[361] vgl. Dr. Herpig, Sven, Stiftung Neue Verantwortung: Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema "ITSicherheit", Ausschussdrucksache 19(4)255 A, 08.04.19, S. 2 Nr. 1 und 3, URL: https://kripoz.de/wp-content/uploads/2019/04/a-drs-19-4-255-a-herpig.pdf
[362] vgl. BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, S. 7, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf
[363] vgl. ebd. S. 26
[364] §§100a, 100b StPO, beide werden im Referentenentwurf lediglich um weitere Straftaten, die einen solchen Eingriff rechtfertigen, erweitert.
[365] vgl. BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, S. 32, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf

6.8 Andere Gesetze

Noch nicht vollständig geklärt ist, ob DSGVO-Verstöße auch über das Gesetz gegen den unlauteren Wettbewerb abgemahnt werden können.[366] In den in Kapitel 2 des UWG festgelegten Rechtsfolgen wird festgehalten, dass nach den Paragraphen §§3, 7 UWG unzulässige Handlungen Abmahnungen nach sich ziehen können.[367] Für datenschutzrechtliche Verstöße dürften §3 UWG, der „[u]nlautere geschäftliche Handlungen“[368] für unzulässig erklärt in Verbindung mit §3a UWG herangezogen werden. Dieser definiert eine Handlung gegen eine gesetzliche Vorschrift, „ die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln“[369] für unlauter, wenn „der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen“.[370] Es soll also nicht jeder Rechtsverstoß auch wettbewerbswidrig sein; Stattdessen muss für jeden Einzelfall entschieden werden, „ob es sich bei der angeblich verletzten Norm [...] um eine sog[enannte] „Marktverhaltensregel“ im Sinne des § 3 a) UWG handelt.“[371] Relevant ist eine Klärung dieser Fragestellung insbesondere deshalb, da nach den Paragraphen §§8 und 9 UWG jeder Mitbewerber bei nach §§3 oder 7 UWG unzulässigen Handlungen Ansprüche auf Beseitigung oder auch Unterlassung[372] beziehungsweise Schadensersatzansprüche[373] geltend machen kann.[374]

Auch im Betriebsverfassungsgesetz (BetrVG) sind datenschutzrechtliche Aspekte verankert. So schreibt §75 BetrVG vor, dass Arbeitgeber und Betriebsrat sowohl dafür Sorge zu tragen haben, dass die Mitarbeiter nach den Grundsätzen von Recht und Billigkeit behandelt werden, als auch die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern haben.[375] Desweiteren ist es nach §80 BetrVG allgemeine Aufgabe des Betriebsrats, „darüber zu wachen, dass die zugunsten der

[366] vgl. Kann die DSGVO über das UWG abgemahnt werden? – Neue Gerichtsentscheidungen, 07.05.19, URL: https://www.wbs-law.de/wettbewerbsrecht/kann-die-dsgvo-ueber-das-uwg-abgemahnt-werden-lg-wuerzburg-trifft-erste-entscheidung-23849/, 29.10.19
[367] vgl. §§8, 9, 10 UWG, URL: https://dejure.org/gesetze/UWG
[368] §3 Abs. 1 UWG, URL: https://dejure.org/gesetze/UWG/3.html
[369] §3a UWG, URL: https://dejure.org/gesetze/UWG/3a.html
[370] §3a UWG, URL: https://dejure.org/gesetze/UWG/3a.html
[371] URL: https://www.datenschutzbeauftragter-info.de/wettbewerbsrechtliche-abmahnung-wegen-dsgvo-verstoessen/, 29.10.19
[372] vgl. §8 UWG, URL: https://dejure.org/gesetze/UWG/8.html
[373] vgl. §9 UWG, URL: https://dejure.org/gesetze/UWG/9.html
[374] vgl. Stolze, Michael: Der Datenschutz als Marktverhaltensregel im Wettbewerbsrecht, 2012, URL: https://www.iitr.de/veroeffentlichungen/der-datenschutz-als-marktverhaltensregel-im-wettbewerbsrecht.html, 29.10.19
[375] vgl. §75 BetrVG, URL: https://dejure.org/gesetze/BetrVG/75.html

Arbeitnehmer geltenden Gesetze [und] Verordnungen [...] durchgeführt werden".[376] Beide Vorschriften beinhalten auch, den im Betrieb beschäftigten Personen das Recht auf informationelle Selbstbestimmung zuzugestehen.[377]

Der Geschäftsführer einer Gesellschaft mit beschränkter Haftung (GmbH) ist in den Angelegenheiten der Gesellschaft zur Sorgfalt eines ordentlichen Geschäftsmannes verpflichtet, bei Nicht-Beachten ist er der Gesellschaft gegenüber für entstandene Schäden haftbar[378] und bei Datenschutzverletzungen können, wie bereits mehrfach aufgezeigt, erhebliche finanzielle Strafen die Folge sein.

7 Compliance-Maßnahmen

Compliance kann rechtlich aus zahlreichen Paragraphen abgeleitet werden. So handelt nach §130 OWiG der Inhaber eines Betriebes oder Unternehmens, „der vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, [...] ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre."[379] Desweiteren schreibt §43 GmbHG „in Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes"[380] vor, dies bezieht sich allerdings auf Geschäftsführer.[381] §93 AktG verpflichtet Vorstandsmitglieder bei ihrer Geschäftsführung zur „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters"[382], in §116 AktG werden Sorgfaltspflicht und Verantwortlichkeit von Aufsichtsratsmitgliedern geregelt[383] und §347 HGB sagt aus, dass „[w]er aus einem Geschäfte, das auf seiner Seite ein Handelsgeschäft ist, einem anderen zur Sorgfalt verpflichtet ist, [...] für die Sorgfalt eines ordentlichen Kaufmanns einzustehen [hat]."[384] §91 AktG fordert geeignete Maßnahmen, insbesondere ein

[376] §80 Abs. 1 Nr. 1 BetrVG, URL: https://dejure.org/gesetze/BetrVG/80.html
[377] vgl. URL: https://www.felser.de/blog/betriebsrat-und-datenschutz/, 29.10.19
[378] vgl. §43 GmbHG, URL: https://dejure.org/gesetze/GmbHG/43.html
[379] §130 Abs. 1 S. 1 OWiG, URL: https://dejure.org/gesetze/OWiG/130.html
[380] §43 Abs. 1 GmbHG, URL: https://dejure.org/gesetze/GmbHG/43.html
[381] vgl. §43 Abs. 1 GmbHG, URL: https://dejure.org/gesetze/GmbHG/43.html
[382] §93 Abs. 1 S. 1 AktG, URL: https://dejure.org/gesetze/AktG/93.html
[383] vgl. §116 AktG, URL: https://dejure.org/gesetze/AktG/116.html
[384] §347 Abs. 1 HGB, URL: https://dejure.org/gesetze/HGB/347.html

Überwachungssystem, um den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkennen zu können, und damit auch Compliance.[385]

Empfehlungen und Orientierungshilfen zur guten Unternehmensführung börsennotierter Gesellschaften werden im Deutschen Corporate Governance Kodex (DCGK) beschrieben.[386] Darin wird unter 4.1.3 Compliance als Aufgabe des Vorstands aufgeführt. Seit 2017 soll dieser ebenfalls „für angemessene, an der Risikolage des Unternehmens ausgerichtete Maßnahmen (Compliance Management System) sorgen und deren Grundzüge offenlegen.“[387] In der neuen Fassung des DCGK vom 9. Mai 2019, die allerdings noch nicht in Kraft getreten ist, finden sich Compliance und das zugehörige Management System unter Grundsatz 5.[388]

Ein solches Compliance Management Systems (CMS) bezeichnet „alle Prozesse und Maßnahmen [...], die das Ziel haben, die Regelkonformität einer Organisation (z.B. Unternehmen) zu unterstützen“.[389] Verantwortlich für die Einrichtung, Aufrechterhaltung und ständige Verbesserung des CMS ist die oberste Leitung. „Als Querschnittsthema betrifft Compliance alle Bereiche und Funktionen einer Organisation.“[390] Es gibt keine konkreten rechtlichen Vorgaben bezüglich eines solchen CMS[391], allerdings sind mit der ISO[392] 19600 Richtlinien für Aufbau und Betrieb gegeben.[393] Demnach basiert ein CMS auf fünf gleichwertigen Säulen: Erstens der Bewertung des Umfeldes und der Compliance Risiken. „Hier geht es zunächst darum, die organisatorischen Rahmenbedingungen sowie das rechtliche Umfeld des Unternehmens zu analysieren und die Compliance-Verpflichtungen zu identifizieren.“[394] Dabei wird in der Praxis meist nur eine begrenzte Anzahl rechtlicher Regelungen einbezogen, nämlich die, deren Nicht-Befolgen durch einzelne Mitarbeiter besonders gravierende Konsequenzen für das ganze Unternehmen

[385] vgl. §91 Abs. 2 AktG, URL: https://dejure.org/gesetze/AktG/91.html
[386] vgl. URL: https://www.dcgk.de/de/, 03.10.19
[387] Deutscher Corporate Governance Kodex, 07.02.2017, 4.1.3, S. 6, URL: https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/170424_Kodex_Mark_up.pdf
[388] vgl. DCGK 2019 mit Begründungen, Deutscher Corporate Governance Kodex wie von der Regierungskommission am 9. Mai 2019 beschlossen, Grundsatz 5, S. 9f., Download möglich unter: URL: https://www.dcgk.de/de/kodex/dcgk-2019.html
[389] vgl. URL: https://www.otris.de/wiki/richtlinienmanagement/compliance-management-system/, 07.10.19
[390] TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 3, URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf
[391] vgl. URL: https://www.otris.de/wiki/richtlinienmanagement/compliance-management-system/, 07.10.19
[392] International Standards Organization, Entwicklung internationaler Standardnormen, weitere Informationen: URL: https://wirtschaftslexikon.gabler.de/definition/iso-40855/version-264231, 07.10.19
[393] vgl. Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.60, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156
[394] Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.62, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156

zur Folge hätte.[395] Gerade in Hinsicht auf die Rechenschaftspflicht in Verbindung mit den hohen Anforderungen der DSGVO sowie die hohen möglichen Bußgelder und Strafen bei Verstößen gegen diese ist der Schutz personenbezogener Daten definitiv ein Compliance Thema und sollte in einem CMS umgesetzt werden.[396]

Die zweite Säule stellt die Führung des Unternehmens dar. Diese muss zum einen die Entscheidung zur Einführung eines CMS treffen, sowie dessen Ziele und den Rahmen festlegen und die dafür benötigten Ressourcen bereitstellen.[397] Zum anderen entscheidet die Unternehmensleitung „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten“[398], ist demnach nach der DSGVO für selbige verantwortlich[399] und damit rechenschaftspflichtig[400] und haftbar.[401] Systemische Steuerungs- und Kontrollmaßnahmen stellen die dritte Säule dar. Darunter fallen interne Regelwerke wie ein Verhaltenskodex und Handlungsanweisungen,[402] worunter auch die Zugriffskontrolle einzuordnen ist. Training und Kommunikation ist die vierte Säule eines CMS. Die ISO verlangt Maßnahmen zur Mitarbeiter-Schulung, sodass jeder Beschäftigte die für seine Zuständigkeit zu beachtenden Regelungen kennt und umzusetzen weiß. Außerdem ist es wichtig, dass das Top-Management sich aktiv zum regelkonformen Verhalten bekennt und dies nach unten kommuniziert.[403] Die fünfte und letzte Säule besteht aus Monitoring, internen Audits und der Reaktion. Monitoring beschreibt dabei „die Beobachtung des laufenden Betriebs des Compliance-Systems“[404], also interne stichprobenhafte Kontrollen, die auf das Verhalten im Unternehmen abzielen. Bei internen Audits handelt es sich um Systemchecks, die das CMS selbst, auch in Hinsicht auf eventuell geändertes rechtliches Umfeld und regelmäßige Anpassungen der

[395] vgl. ebd. S. 62
[396] vgl. Gierschmann, Markus: Datenschutz-Managementsystem zur Sicherstellung der Compliance nach DS-GVO - Bestandsaufnahme und Blick in die Zukunft, BvD-Verbandstage 2018 Berlin, S. 2, URL: https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Verbandstage_Markus-Gierschmann.pdf
[397] vgl. Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.62, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156
[398] Art. 4 Nr. 7 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[399] vgl. Art. 4 Nr. 7 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html
[400] vgl. Art. 5 Abs. 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/5.html
[401] vgl. Art. 82 DSGVO, URL: https://dejure.org/gesetze/DSGVO/82.html
[402] vgl. Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.62, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156
[403] vgl. Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.63, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156
[404] Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.63, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156

Risikoanalyse, überprüfen.[405] „Festgestellte Compliance-Verstöße erfordern eine Reaktion des Unternehmens. Dazu gehören die Untersuchung des Vorfalls, die Festlegung der Konsequenzen des festgestellten Fehlverhaltens, sowie die Entscheidung über das weitere Vorgehen.“[406] Diese müssen im konkreten Einzelfall getroffen werden, Präventivmaßnahmen gegen eine Wiederholung eines solchen Vorfalls wären eine mögliche Konsequenz, an die das CMS angepasst werden müsste.[407] Durch die ständige Beobachtung und Anpassung des CMS ergibt sich ein dynamischer Prozess, der im folgenden Modell dargestallt ist.

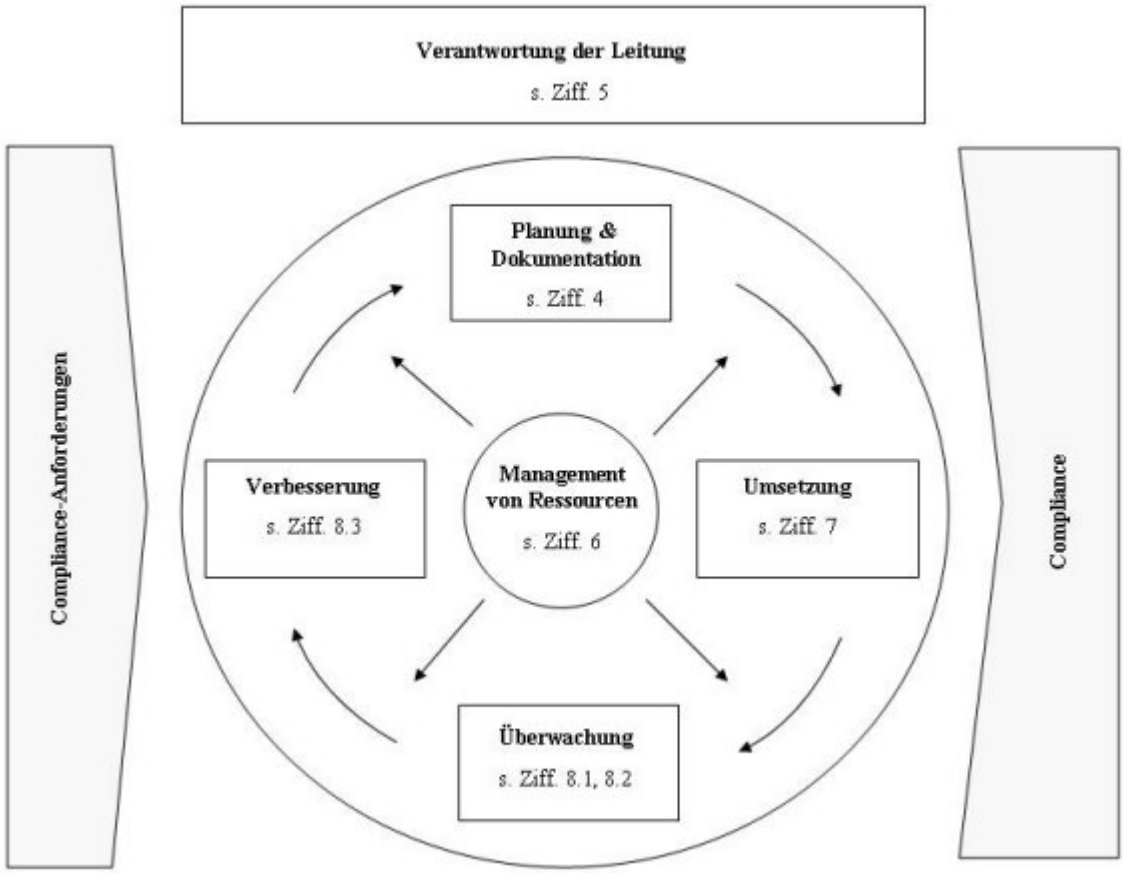

Abbildung 1: Modell eines (prozessorientierten) CMS[408]

[405] vgl. Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.63, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156

[406] Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, S.63, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156

[407] vgl. ebd. S. 63

[408] TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 4, URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf, 12.10.19

Das zentral dargestellte Management von Ressourcen beinhaltet zum einen das Ermitteln, Bereitstellen und Aufrechterhalten der für die Erfüllung der Compliance-Anforderungen benötigten Infrastruktur und zum anderen die Durchführung regelmäßiger Compliance-Schulungen für die betroffenen Mitarbeiter.[409]

Die Dokumentation setzt sich aus den notwendigen Vorgabe- und Nachweisdokumenten zusammen. Erstere sind üblicherweise unter anderem Rechtsquellen wie Gesetze, Satzungen oder Kodizes, Handbücher oder Richtlinien, die eine Aufzählung der spezifischen Compliance-Anforderungen eines Unternehmens enthalten, sowie eine Beschreibung des CMS. Bei Nachweisdokumenten handelt es sich beispielsweise um Compliance-Berichte, Risikoanalysen, Dokumente über die Durchführung von Compliance-Schulungen und gesetzlich vorgeschriebene Nachweisdokumente.[410] In Hinsicht auf den Datenschutz ist in diesem Zusammenhang besonders Artikel 30 DSGVO zu nennen, der Unternehmen ab 250 Mitarbeitern oder unabhängig von der Anzahl der Beschäftigten solche Unternehmen, die sensible Daten nach Artikel 9 DSGVO oder Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Artikel 10 DSGVO verarbeiten, zum Führen eines Verzeichnisses aller Verarbeitungstätigkeiten verpflichtet. Ein derartiges Verzeichnis muss Namen und Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung, die Kategorien der verarbeiteten Daten, der betroffenen Personen sowie der Empfänger und wenn möglich vorgesehene Fristen zu Löschung und die zur Sicherheit der Verarbeitungen ergriffenen technischen und organisatorischen Maßnahmen enthalten.[411] Damit beinhaltet dieses Verzeichnis automatisch Inhalte des in der Abbildung nächsten Schrittes: der Umsetzung. Diese enthält die spezifischen Compliance-Risiken und -Anforderungen des expliziten Unternehmens, entsprechende Maßnahmen zur Eindämmung beziehungsweise Erfüllung derselben sowie ihre Integration in die Arbeitsabläufe. Zudem ist eine Anlaufstelle für mögliche compliance-relevante Hinweise sinnvoll und für eine Zertifizierung des CMS durch TÜV Rheinland notwendig.[412] Zur Überwachung, der Analyse und der Verbesserung der Wirksamkeit des CMS werden neben internen Audits insbesondere Korrekturmaßnahmen durch

[409] vgl. TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 13f., URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf

[410] vgl. TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 8f., URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf

[411] vgl. Art. 30 DSGVO, URL: https://dejure.org/gesetze/DSGVO/30.html

[412] vgl. TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 15ff., URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf

Anpassungen des CMS nach Verstößen gegen die Compliance-Anforderungen des Unternehmens und daraus abgeleitete Vorbeugungsmaßnahmen genannt.[413]
Die bereits mehrfach genannten Compliance-Verpflichtungen setzen sich dabei, wie aus der Definition von Compliance abzuleiten ist, aus gesetzlichen Vorschriften, vertraglich festgelegten Regelungen, externen und internen Regelwerken zusammen, die alle im CMS berücksichtigt, dokumentiert und eingehalten werden müssen. Neben dem eigentlichen CMS können auch viele weitere Bestandteile beziehungsweise Prozesse im Zusammenhang mit Compliance zertifiziert werden. Darunter fallen beispielsweise auch ein Managementsystem für Informationssicherheit (ISMS), Risiko- oder Notfallmanagement. Für jedes der gerade genannten besteht neben den zugehörigen international geltenden und zertifizierbaren ISO-Standards auch je ein BSI-Standard, an dem sich Unternehmen orientieren können. Während diese Managementsysteme zunächst als internes Regelwerk anzusehen sind, sind die jeweiligen Standards, nach denen diese zertifiziert werden können und die spezifische, nicht vom Unternehmen selbst festgelegte Regelungen enthalten, externe Regelwerke.

7.1 Externe Regelwerke

Im Folgenden sollen sowohl für Informationssicherheit als auch das Risikomanagement die jeweiligen ISO Standards dargelegt und erläutert werden.
Managementsysteme für Informationssicherheit werden durch eine ganze Familie an ISO Standards näher beschrieben, wie in der nachfolgenden Abbildung dargestellt ist.

[413] vgl. TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, S. 18ff., URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf

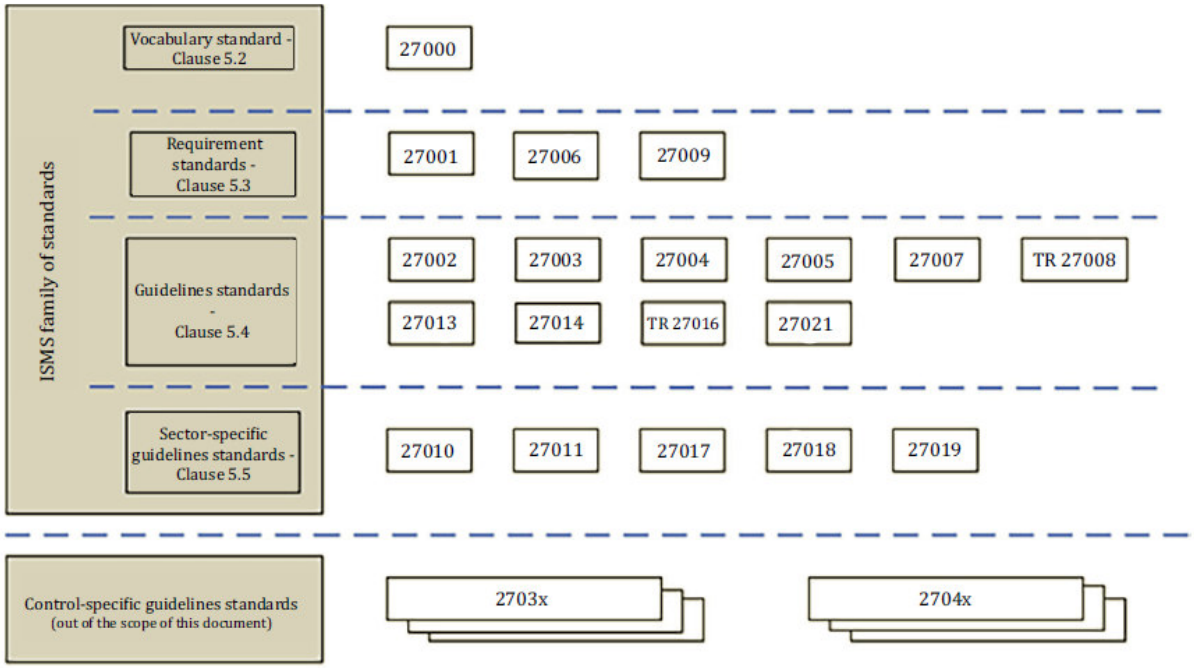

Abbildung 2 ISO-27000 Familie (ISMS-Standards)[414]

Wie aus Abbildung 2 zu entnehmen ist, legt ISO 27000 Begriffsbestimmungen und Definitionen fest, die auch in den anderen zugehörigen Standards verwendet werden, bietet einen Überblick über die Inhalte der weiteren ein ISMS betreffenden Standards und beschreibt die Grundlagen eines ISMS.[415] Im Folgenden sollen einige der dieser ISO-Reihe zugehörigen Standards knapp beschrieben werden.

Die ISO 27001, die nicht kostenlos zur Verfügung steht, beschreibt „die Anforderungen an die Umsetzung sowie die Dokumentation eines Informationssicherheits-Managementsystems (ISMS).“[416] Ein wirksames ISMS stärkt den Schutz gegen Cyberangriffe und Datendiebstahl.[417] Die ursprüngliche Ausgabe der ISO 27001 von 2005 basierte zu großen Teilen auf dem PDCA-Modell[418], das in der aktuellen Version von

[414] ISO/IEC: ISO/IEC 27000:2018, 5.1 General information, 2018, S. 19, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
[415] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 19, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
[416] vgl. URL: https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html, 10.10.19
[417] vgl. TÜV SÜD Management Service GmbH: Whitepaper: ISO 27001: Informationssicherheit und Zertifizierungsprozess, 2015, S. 2, URL: https://www.tuev-sued.de/uploads/images/1464955241375022630318/iso-27001-white-paper-vm-de-screen2.pdf
[418] Plan – Do – Check – Act

2013 lediglich als zugrundeliegendes Prinzip ohne direkten Verweis enthalten ist.[419] Die ISO 27001 wird als bedeutendster Standard für ein ISMS betrachtet, das IT-Grundschutzhandbuch des BSI ist mit dieser Norm kompatibel. Die darin genannten Anforderungen sind technisch nicht detailliert beschrieben sondern eher allgemein gehalten, um auf jede Organisation angewendet werden zu können.[420] ISO 27001 ist nach den Vorgaben des Anhang SL[421] aufgebaut und nennt die ISO 27000:2013 als einzige normative Referenz, alle dort festgelegten Begriffe und Definitionen werden übernommen. Bei der Umsetzung eines ISMS wird ein prozessorientierter Ansatz verfolgt. Alle relevanten externen oder internen Themen des Unternehmens, die die Fähigkeit zu einer erfolgreichen Implementierung eines ISMS beeinträchtigen könnten, müssen bestimmt und berücksichtigt werden. Die oberste Managementebene muss nach ISO 27001 eine Informationssicherheitspolitik festlegen und das Bewusstsein für Informationssicherheit im ganzen Unternehmen aktiv fördern. Die spezifischen Risiken in Bezug auf die Informationssicherheit müssen bewertet und für den Umgang mit denselben ein Plan ausgearbeitet werden, die Festlegung bestimmter geeigneter Maßnahmen liegt in der Verantwortung des Unternehmens. Zudem werden das Bereitstellen aller für das ISMS erforderlichen Ressourcen, die Dokumentation und die regelmäßige Beurteilung von Eignung und Wirksamkeit des ISMS gefordert. Das Feststellen von Nichtkonformitäten sowie das Ergreifen von Korrekturmaßnahmen werden als besonders wichtig für die fortlaufende Verbesserung des ISMS genannt.[422] Die ISO 27001 richtet sich an die Geschäftsleitung und IT-Sicherheitsbeauftragte.[423] Als diejenige Norm, die die durch ein Unternehmen zu erfüllenden Anforderungen an ein ISMS festlegt, ist ISO 27001 die einzige aus der ISO 27000-Familie, für deren Erfüllung ein Unternehmen

[419] vgl. TÜV SÜD Management Service GmbH: Whitepaper: ISO 27001: Informationssicherheit und Zertifizierungsprozess, 2015, S. 5f., URL: https://www.tuev-sued.de/uploads/images/14649552413750226303 18/iso-27001-white-paper-vm-de-screen2.pdf
[420] vgl. BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 23, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf
[421] vgl. URL: https://www.bsigroup.com/LocalFiles/nl-nl/iso-9001/BSI-Annex-SL-Whitepaper.pdf, 11.10.19
[422] vgl. TÜV SÜD Management Service GmbH: Whitepaper: ISO 27001: Informationssicherheit und Zertifizierungsprozess, 2015, S. 6, URL: https://www.tuev-sued.de/uploads/images/14649552413750226303 18/iso-27001-white-paper-vm-de-screen2.pdf
[423] vgl. BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 24, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

zertifiziert werden kann.[424] Die anderen beiden „Requirement Standards“ dieser ISO-Reihe sind nicht so allgemein, sondern nur für bestimmte Unternehmen anzuwenden. ISO 27006 spezifiziert Anforderungen an die Zertifizierungsstellen für ISMSs und erweitert ISO 17021 in Hinsicht auf die Akkreditierung dieser Stellen. ISO 27009 ist für die Anwendung in spezifischen Sektoren gedacht und stellt sicher, dass zusätzliche oder konkretere Anforderungen nicht in Konflikt mit den Anforderungen aus ISO 27001 stehen.[425]

Wie aus Abbildung 2 zu entnehmen ist, sind ISO 27002 bis ISO 27005 als „Guideline Standards“ eingeordnet. Als solcher legt ISO 27002 „Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in einer Organisation fest.“[426] ISO 27002 ist damit wesentlich detaillierter und konkreter als ISO 27001[427] und richtet sich an IT-Sicherheitsbeauftragte. Der Standard beschäftigt sich mit 14 Überwachungsbereichen in Bezug auf das Sicherheitsmanagement, darunter Personalsicherheit, Zugangskontrolle, Kryptographie, Kommunikationssicherheit, Compliance und der Umgang mit Informationssicherheitsvorfällen.[428] ISO 27003 liefert Erklärungen und Handlungsempfehlungen zur ISO 27001, ISO 27004 dient als Unterstützung bei der Evaluierung und Feststellung der Effektivität des ISMS.[429] ISO 27005 stellt Richtlinien für die Implementierung eines die Konzepte aus ISO 27001 unterstützenden, prozessorientierten Informationssicherheits-Risikomanagements.[430] Demnach werden Informationssicherheitsrisiken systematisch anhand der folgenden konkreten Schritte

[424] vgl. URLs: https://www.imsm.de.com/iso-normen/?msclkid=0b6977f7ad95142ab5382a52d1a74352&utm_source=bing&utm_medium=cpc&utm_campaign=NEU_ISO_Allgemein&utm_term=%2Biso%20%2Bzertifizierung&utm_content=ISO_Zertifizierung, https://advisera.com/27001academy/de/knowledgebase/iso-27001-im-vergleich-zu-iso-27002/, 12.10.19

[425] vgl. ISO/IEC 27000:2018, 5.3 Standards Specifying Requirements, 2018, S. 20, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[426] BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 24, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

[427] vgl. URL: https://advisera.com/27001academy/de/knowledgebase/iso-27001-im-vergleich-zu-iso-27002, 12.10.19

[428] vgl. BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 24f., URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

[429] vgl. ISO/IEC 27000:2018, 5.4 Standards Describing General Guidelines, 2018, S. 20f., kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[430] vgl. ISO/IEC 27000:2018, 5.4 Standards Describing General Guidelines, 2018, S. 21, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

identifiziert, bewertet und behandelt. Zunächst werden die Rahmenbedingungen bestimmt, worunter „die Festlegung von Kriterien zur Bewertung und Akzeptanz von Risiken, die Abgrenzung des Betrachtungsbereiches sowie die Etablierung einer Organisation für das Risikomanagement“[431] fallen. Dann werden die Risiken unter Berücksichtigung der Unternehmenswerte im Betrachtungsbereich identifiziert. Unternehmenswerte können beispielsweise Hardware, Software, Informationen und Geschäftsprozesse sein. Auch relevante Bedrohungen, vorhandene Schwachstellen und bestehende oder geplante Sicherheitsmaßnahmen müssen berücksichtigt werden, da diese die Eintrittswahrscheinlichkeit oder das Ausmaß des Schadens beeinflussen können. Daraus müssen im Anschluss mögliche Konsequenzen abgeleitet werden, wie beispielsweise Reputationsverlust. Nach ihrer Identifikation werden die Risiken bewertet, wobei aus Eintrittswahrscheinlichkeit und Schadensausmaß bei Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität ein zugehöriges Risikoniveau bestimmt wird. Im Anschluss an die darauf dolgende Priorisierung erfolgt nun die Risikobehandlung. Dabei werden die ermittelten Risiken reduziert, akzeptiert, vermieden oder übertragen. Reduziert bedeutet, dass geeignete Sicherheitsmaßnahmen zur Verringerung des Risikos getroffen werden, akzeptiert meint, dass Risiken, die gewisse festgelegte Akzeptanzkriterien erfüllen, unbehandelt bestehen bleiben können, vermieden werden Risiken beispielsweise durch das Auslagern kritischer Systeme an gesondert gesicherte Umgebungen und übertragen werden können Risiken an Dritte mittels Vertragsformulierungen oder Versicherungen. Aus der Risikobehandlung ergibt sich eine Zuordnung der jeweiligen Risiken zur bestimmten Handlungsempfehlung. Relevante Mitarbeiter und weitere Entscheidungsträger sollten über diese Risiken informiert sein. Die Risiken, Bedrohungen, Schwachstellen und Maßnahmen müssen immer wieder auf Änderungen untersucht, und das Risikomanagement auf Angemessenheit überprüft werden.[432] Die hier genannten Risiken beziehen sich auf die Informationssicherheit, also die Verfügbarkeit, Vertraulichkeit und Integrität der technischen Systeme und gespeicherten Daten.

[431] BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 26, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

[432] vgl. BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 26f., URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

Für ein allgemeines Risikomanagement besteht ein eigener ISO Standard, ISO 31000, dessen aktuelle Version im Februar 2018 veröffentlicht wurde. Das Vorgehen entspricht im Groben dem eben beschriebenen[433] und ist laut ISO 31000 in alle Entscheidungsfindungen in jedem Bereich des Unternehmens zu integrieren. Im Vergleich zur Vorgängerversion von 2009 wird besonders der zyklische und iterative Charakter des Risikomanagements, also zum Beispiel das Reagieren auf regelmäßige Kontrollen oder Feedback, betont.[434] Auch nach ISO 31000 wird nicht zertifiziert, es handelt sich hier um Handlungsempfehlungen.[435]

ISO 27007 liefert Richtlinien für die Durchführung von internen und externen Audits,[436] der Standard ISO 27014 definiert sechs Grundsätze für die Governance von Informationssicherheit, darunter beispielsweise die Verfolgung eines risikobasierten Ansatzes oder die Konformität mit internen oder externen Anforderungen, also Compliance.[437]

Auch wenn ein Unternehmen mehreren oder auch sämtlichen Standards aus der ISO 27000-Familie entsprechen kann, kann es ausschließlich auf Grundlage von ISO 27001 zertifiziert werden. Alternativ ist eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz möglich, in diesem Fall kann eine umfassende Risikoanalyse entfallen, da das BSI die typischen Gefährdungen bewertet.[438]

Das Definieren, Einrichten, Erhalten und Verbessern der Informationssicherheit und damit auch die erfolgreiche Umsetzung eines ISMS sind demnach für die Compliance und das Image eines Unternehmens notwendig und förderlich.[439] In einer so vernetzten Welt stellen Informationen und damit zusammenhängende Prozesse einen wesentlichen

---

[433] vgl. PWMP Management- und Organisations-Beratung: Risikomanagement nach ISO 31000 Umsetzung in der Organisation, 2018, URL: http://www.pwmp.de/files/181102-Risikomanagement-nach-ISO-31000.pdf

[434] vgl. Veltsos, Christophe: 10 Takeaways From the ISO 31000:2018 Risk Management Guidelines, in: SecurityIntelligence, 2018, URL: https://securityintelligence.com/10-takeaways-from-the-iso-310002018-risk-management-guidelines/, 13.10.19

[435] vgl. PWMP Management- und Organisations-Beratung: Risikomanagement nach ISO 31000 Umsetzung in der Organisation, 2018, S. 2, URL: http://www.pwmp.de/files/181102-Risikomanagement-nach-ISO-31000.pdf

[436] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 21, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[437] vgl. BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, S. 28, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

[438] vgl. URL: https://www.datenschutzbeauftragter-info.de/isms-dsgvo-moeglichkeiten-der-zertifizierung/, 13.10.19

[439] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 11 und 14, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Unternehmenswert dar.[440] Informationssicherheit sorgt für Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, minimiert die Konsequenzen von betreffenden Sicherheitsvorfällen[441] und ist damit ein grundlegendes Unternehmensziel.

Um dies erreichen zu können, ist ein Risikomanagement vonnöten und es müssen alle physischen, menschlichen und technischen Bedrohungen betrachtet werden.[442] In Hinblick auf die Verarbeitung personenbezogener Daten schreibt die DSGVO „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“[443], vor. Ein Verstoß gegen diese Vorschrift kann nach Artikel 83 DSGVO eine Geldbuße bis zu 10 Millionen Euro oder 2% des Jahresumsatzes zur Folge haben.[444] Zusätzlich haftet ein Verantwortlicher bei Verstoß gegen die DSGVO für dadurch entstandene Schäden und materiell oder immateriell geschädigte Personen haben Schadensersatzansprüche gegen den Verantwortlichen.[445] Ein ISMS dürfte auch für den Nachweis der Integrität und Vertraulichkeit der verarbeiteten Daten hilfreich sein, der in Artikel 5 DSGVO gefordert wird.[446]

Auch für einen Rahmen für Datenschutz im Bereich der Informationstechnologie besteht seit 2011 ein ISO Standard, ISO 29100, der ebenfall kostenlos erhältlich ist.[447] Hier werden einige wichtige Begrifflichkeiten im Zusammenhang mit Datenschutz geklärt, Akteure und ihre Rollen bei der Verarbeitung personenbezogener Daten definiert, Überlegungen zur Sicherung der Privatsphäre beschrieben und Bezüge zu bestehenden Datenschutzprinzipien in der Informationstechnologie hergestellt.[448] Die im Standard genannten grundsätzlichen Datenschutz Prinzipien entsprechen inhaltlich in etwa den in der DSGVO geforderten Grundsätzen. So findet sich zum Beispiel die informierte Einwilligung nach Artikel 6 und 7 DSGVO unter dem Prinzip ‚Consent and Choice’ in Kapitel 5.2, die Rechtmäßigkeit (Art. 5 Abs. 1 Buchstabe a und Art. 6 DSGVO) sowie die

[440] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 13, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[441] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 12, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[442] vgl. ISO/IEC 27000:2018, 5.1 General information, 2018, S. 13, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[443] Art. 32 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/32.html

[444] vgl. Art. 83 Abs. 4 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html

[445] vgl. Art. 82 Abs. 1 und 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/82.html

[446] vgl. Art. 5 Abs. 1 Buchstabe f DSGVO, Art. 5 Abs. 2 DSGVO, URLs: https://dejure.org/gesetze/DSGVO/5.html, https://www.datenschutz-notizen.de/iso-iec-27001-vs-dsgvo-1022677/, 13.10.19

[447] vgl. URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html, 14.10.19

[448] vgl. ISO/IEC 29100:2011, 1. Scope, 2011, S. 11, kostenloser Download in englischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Pflicht zur Mitteilung des Zwecks der Verarbeitung (Art. 13 DSGVO) in ‚Purpose legitimacy and specification', Kapitel 5.3, die Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e DSGVO) in Kapitel 5.4 unter ‚Collection limitation', die Datenminimierung (Art. 5 Abs. 1 Buchstabe c DSGVO) unter ‚Data minimization' in Kapitel 5.5, die Zweckbindung (Art. 5 Abs. 1 Buchstabe b DSGVO) bei ‚Use, retention and disclosure limitation', Kapitel 5.6, die Richtigkeit aus Artikel 5 Absatz 1 Buchstabe d DSGVO unter ‚Accuracy and quality' in Kapitel 5.7 und Kapitel 5.8 ‚Openness, transparency and notice' und 5.9 ‚Individual participation and access' beschreiben inhaltlich in etwa die Forderungen der DSGVO nach Transparenz (Art. 12 bis 15 DSGVO). Auch die in Artikel 5 Absatz 2 DSGVO verlangte Rechenschaftspflicht des Verantwortlichen, im Standard als ‚PII controller'[449] bezeichnet, stellt in ISO 29100, Kapitel 5.10 ‚Accountability' ein grundlegendes Prinzip dar.[450] Kapitel 5.11 fordert technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit, vergleichbar mit Artikel 32 DSGVO, in beiden Fällen werden die Hauptschutzziele der IT-Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, konkret genannt. Zuletzt verlangt ISO 29100 ‚Privacy Compliance', also das Einhalten rechtlicher oder anderweitig bestehender Vorschriften und Regelungen im Zusammenhang mit Datenschutz.[451] Es beinhalten auch weitere ISO-Standards datenschutzspezifische Bestimmungen. Im August 2019 wurde die Norm ISO 27701 veröffentlicht, die eine Erweiterung der Standards ISO 27001 und ISO 27002 für das Datenschutzmanagement darstellt.[452] Im Anhang enthält diese ISO-Norm eine Tabelle, die den Anforderungen der DSGVO konkrete Maßnahmen zuordnet, genannt werden beispielsweise Datenschutz-Schulungen für Mitarbeiter, der „Privacy by Design"-Grundsatz aus Artikel 25 Absatz 1 DSGVO und die Überprüfung von Sicherheitsvorfällen auf Datenschutzverletzungen.

Zumindest aktuell kann ISO 27701 jedenfalls nicht als Basis für ein Zertifikat über die Einhaltung der DSGVO dienen. Zum einen ist ISO 27001 der einzige zertifizierbare Standard dieser Reihe,[453] zum anderen ist in Artikel 43 DSGVO, der die Anforderungen an die Zertifizierungsstellen in Hinsicht auf die Vorgaben der DSGVO regelt, festgelegt, dass diese von einer zuständigen Aufsichtsbehörde oder einer nationalen

[449] PII: Personally Identifiable Information, aus dem Abkürzungsverzeichnis der ISO zu entnehmen
[450] vgl. ISO/IEC 29100:2011, 1. Scope, 2011, S. 14ff., kostenloser Download in englischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
[451] vgl. ISO/IEC 29100:2011, 1. Scope, 2011, S. 18f., kostenloser Download in englischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html und Art. 32 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/32.html
[452] vgl. URL: https://www.beuth.de/de/norm/iso-iec-27701/312455765, 15.10.19
[453] vgl. URL: https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, 13.10.19

Akkreditierungsstelle gemäß ISO 17065 akkreditiert werden kann.[454] ISO 27001 und damit auch ISO 27701, die darauf aufbaut und lediglich eine Erweiterung dazu darstellt, richtet sich allerdings nach ISO 17021. Gegenüber Aufsichtsbehörden kann eine Zertifizierung nach ISO 27001 auch mit der Erweiterung nach 27701 damit nicht als Nachweis für DSGVO-konformes Verhalten dienen. Aktuell besteht noch keine Zertifizierungsmöglichkeit nach Artikel 42 DSGVO.[455]
Nichtsdestotrotz zeigt die Erweiterung von ISO 27001 durch ISO 27701 im Hinblick auf den Datenschutz den engen Zusammenhang zwischen Datenschutz und Informationssicherheit, der sich auch in den gemeinsamen, bereits mehrfach behandelten Schutzzielen der Vertraulichkeit, Verfügbarkeit und Integrität zeigt.[456]

7.2 Interne Regelwerke

Zusätzlich zu den bereits beschriebenen externen Regelwerken bestehen auch sinnvolle intern umzusetzende Richtlinien, die nicht zertifiziert werden aber dennoch eine Hilfe darstellen können. Für die Datensicherheit, die zum einen für das Unternehmen an sich, zum anderen aber auch aus datenschutzrechtlicher Sicht eine bedeutende Rolle einnimmt, sind im Anschluss an die bereits diskutierte Risikoanalyse und -bewertung, wobei neben von Menschen ausgelösten Schwierigkeiten auch Störungen aufgrund höherer Gewalt oder technischen Problemen wie Stromausfällen berücksichtigt werden,[457] auch weitere technische und organisatorische Maßnahmen (TOMs) zur Vermeidung von Vorfällen gegen die genannten Schutzziele zu treffen. Dies ist gesetzlich in der DSGVO in Artikel 32 DSGVO[458] und konkret in §64 BDSG vorgeschrieben.[459] Speziell genannt werden hier Pseudonymisierung und Verschlüsselung. Für automatisierte Verarbeitungen werden zum Erreichen der grundsätzlichen Schutzziele 14 Umsetzungsmaßnahmen genannt.[460] Im Folgenden soll sich mit einigen davon näher auseinander gesetzt werden. Diese sind sowohl inhaltlich als auch in der Umsetzung teilweise sehr eng verbunden, und die

[454] vgl. Art. 43 Abs. 1 Buchstabe b DSGVO, URL: https://dejure.org/gesetze/DSGVO/43.html
[455] vgl. URL: https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, 13.10.19
[456] vgl. URL: https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, 13.10.19
[457] vgl. URL: https://www.business-wissen.de/hb/ziele-und-aufgaben-des-risikomanagements-im-unternehmen/, 13.10.19
[458] vgl. Art. 32 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/32.html
[459] vgl. §64 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html
[460] vgl. §64 Abs. 2 und 3 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html

Begrifflichkeiten werden allgemein häufig anders oder weiter ausgelegt als im BDSG. Auch im Vergleich zur Anlage zu §9 BDSG_alt gibt es einige Abweichungen.

Beispielsweise ist in der neuen Fassung des BDSG die Zutrittskontrolle nicht aufgeführt, die nach BDSG_alt „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, [...] verwehr[t]“[461], allerdings weist die Definition der Zugangskontrolle in §64 BDSG eine gewisse Ähnlichkeit mit der Zutrittskontrolle auf. Die Zugangskontrolle im BDSG meint die „Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte“[462], in der alten Fassung war darunter das „[V]erhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können“[463], zu verstehen. In der neuen Version des BDSG werden beide Begriffe also unter der Zugangskontrolle zusammengefasst, praktische Maßnahmen hierfür sind unter anderem Passwortrichtlinien, digitale Zertifikate oder Firewalls, aber eben auch Alarmanlagen, Zutrittskontrollsysteme mit Chipkarten-Leser oder Videoüberwachungs-Anlagen.[464] Die Zugriffskontrolle war in der alten Fassung ein weiter gefasster Begriff, der beinhaltete, „dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“[465], während in der aktuellen Version lediglich die „Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben“[466] umfasst wird. Grundsätzlich wird in beiden Versionen das Need-to-Know-Prinzip umgesetzt, das besagt, dass jeder Mitarbeiter eben nur genau die Berechtigungen erhält, die er für die Erfüllung seiner Aufgaben tatsächlich braucht, in vielen Fällen genügt beispielsweise eine Leseberechtigung für einige Daten aus, wenn der Mitarbeiter zwar Kenntnis über die Informationen benötigt, sie aber nicht verändern soll.[467] Damit ist allerdings auch das Berechtigten-Management eingeschlossen, das schon bei kleinen Unternehmen, auch

[461] S. 2 Nr. 1 Anlage zu §9 S. 1 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./Anlage.html
[462] §64 Abs. 3 Nr. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html
[463] S. 2 Nr. 2 Anlage zu §9 S. 1 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./Anlage.html
[464] vgl. Schonschek, Oliver: DSGVO: So setzen Sie die erweiterte Zugangskontrolle um, 2017, URL: https://www.datenschutz-praxis.de/fachartikel/dsgvo-setzen-sie-erweiterte-zugangskontrolle-um/, 13.10.19
[465] S. 2 Nr. 3 Anlage zu §9 S. 1 BDSG_alt, URL: https://dejure.org/gesetze/BDSG_a.F./Anlage.html
[466] §64 Abs. 3 Nr. 5 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html
[467] vgl. Brinks, Cornelia: Zugriffskontrolle – TOM und der Datenschutz Teil 3, 2015, URL: https://www.datenschutz-notizen.de/11496-4211496/, 18.10.19

aufgrund der benötigten Dynamik, kompliziert sein kann.[468] Es gibt unterschiedliche Ansätze hierfür. Dabei lässt sich zwischen benutzerbestimmter und systembestimmter Zugriffskontrolle unterscheiden. Erstere beinhaltet zum Beispiel die intuitive Darstellung als Zugriffsmatrix, die allerdings in der Praxis zu speicherintensiv ist, die häufig verwendeten Zugriffskontrolllisten (access control lists, ACLs), die zu jedem Objekt[469] eine Liste mit den Subjekten[470] und deren jeweiligen Berechtigungen speichern, oder Capabilities, die für jedes Subjekt eine Liste mit den Objekten und den Berechtigungen speichern. Die systembestimmte Zugriffskontrolle liegt dem Bell-LaPadula-Modell zugrunde, das die Berechtigungen über Label regelt, die jedem Objekt und jedem Subjekt zugeordnet werden. Bekannt ist auch die rollenbasierte Zugriffskontrolle (RBAC), bei der die Berechtigungen nicht fest einem Subjekt, sondern einer Rolle, also einer Funktion oder Aufgabe, die ein Subjekt einnehmen kann, zugeordnet werden. Dies eignet sich insbesondere für die Abbildung hierarchischer Organisationsstrukturen.[471]

Die ebenfalls in §64 BDSG aufgeführte Datenträgerkontrolle, also die „Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern“[472], ebenso die Speicherkontrolle, die „Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten“[473] waren sowohl im allgemeinen technischen Verständnis als auch in der alten Fassung des BDSG unter dem Begriff Zugriffskontrolle mit abgedeckt[474] und sind damit grundsätzlich nicht als neue Erweiterung anzusehen. Desweiteren ist §64 BDSG in Teil 3 des BDSG einzuordnen, der laut §45 BDSG „für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten“[475], gilt und damit für die meisten Unternehmen nicht verpflichtend sein dürfte, während §9 BDSG_alt im ersten Abschnitt mit den allgemeinen und gemeinsamen Bestimmungen zu finden ist.

---

[468] vgl. URL: https://www.datenschutz-praxis.de/fachartikel/zugriffskontrolle-unerlaubten-zugriffen-auf-der-spur/, 18.10.19
[469] zum Beispiel einer Datei, einem Konto oder einem kompletten Verzeichnis
[470] also den Nutzern oder auch anderen verbundenen Systemen
[471] vgl. Center for Computing Technologies, Universität Bremen: IT-Sicherheit: Zugriffskontrolle, URL: http://www-rn.informatik.uni-bremen.de/lehre/itsec/itsec05-1a.pdf, 18.10.19
[472] §64 Abs. 3 Nr. 2 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html
[473] §64 Abs. 3 Nr. 3 BDSG, URL: https://dejure.org/gesetze/BDSG/64.html
[474] vgl. Brinks, Cornelia: Zugriffskontrolle – TOM und der Datenschutz Teil 3, 2015, URL: https://www.datenschutz-notizen.de/11496-4211496/, 18.10.19
[475] §45 S. 1 BDSG, URL: https://dejure.org/gesetze/BDSG/45.html

Die DSGVO schreibt einerseits die Information betroffener Personen über die Dauer der geplanten Speicherung[476] und andererseits die sofortige Löschung als Rechte der Betroffenen beziehungsweise dadurch als Pflichten des Verantwortlichen vor, falls die Daten zum Beispiel für den Zweck der Erhebung nicht mehr notwendig sind, die Einwilligung die Rechtsgrundlage der Verarbeitung darstellte und widerrufen wird oder die Löschung aufgrund des Rechts der Mitgliedstaaten vorgeschrieben ist.[477] Die Umsetzung der verbindlichen Lösch- und Aufbewahrungspflichten führt unter Umständen zu extrem hohem Arbeits- und Zeitaufwand, weswegen sich die Aufstellung und Nutzung eines Löschkonzepts lohnen und zu Compliance in diesem Bereich des Unternehmens führen kann. Dazu sind die gespeicherten Daten zunächst zu lokalisieren, also eine Übersicht zu verschaffen, welche Daten im Unternehmen wo gespeichert sind. Dann ist sich über die im konkreten Fall geltenden Aufbewahrungs- und Löschpflichten zu informieren und eine Löschregel, die sich aus Lösch- beziehungsweise Aufbewahrungsfrist und Startzeitpunkt der Speicherung zusammensetzt, zu definieren. Zusätzlich sind diejenigen Löschpflichten zu berücksichtigen, die jederzeit beispielsweise durch einen Widerruf der Einwilligung in die Verarbeitung durch den Betroffenen oder anderweitiges Wegfallen der Rechtsgrundlage der Verarbeitung auftreten können. Hierzu sind spezifische Regeln und deren Umsetzung festzulegen. Daraus kann dann für jede Abteilung eine Tabelle aufgestellt werden. Auch Sonderfälle wie Auftragsdatenverarbeitungen sollten bedacht werden. Zuletzt ist das Löschkonzept und der Vorgang des Löschens zu implementieren, auch hier ist regelmäßiges Testen und Überprüfen, auch hinsichtlich möglicher relevanter rechtlicher Änderungen, nötig.[478]

Auf verschiedene Lösch- und Aufbewahrungspflichten sowie mögliche Konflikte wurde bereits eingegangen. Wichtig ist in diesem Zusammenhang allerdings auch die Frage, was dieses „Löschen“ nun genau bedeutet. Gerade bei elektronisch gesicherten Daten ist bekannt, dass „Löschen“ nicht gleich „Auslöschen“ ist. Die DSGVO definiert den Begriff nicht, allerdings geht aus Artikel 4 Nummer 2 DSGVO hervor, dass das „Löschen“ und die „Vernichtung“ von Daten nicht gleichzusetzen sind.[479] Nach Meinung des österreichischen Datenschutzbeauftragten kann die Anonymisierung personenbezogener Daten bereits als Löschung ausreichen, sofern der Personenbezug nicht ohne

[476] vgl. Art. 13 Abs. 2 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/13.html
[477] vgl. Art. 17 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/17.html
[478] vgl. URL: https://www.isico-datenschutz.de/blog/2019/07/30/loeschkonzept-dsgvo/, 26.10.19
[479] vgl. Art. 4 Nummer 2 DSGVO, URL: https://dejure.org/gesetze/DSGVO/4.html

unverhältnismäßig hohen Aufwand wiederhergestellt werden kann.[480] Zudem ist in Erwägungsgrund 26 festgehalten, dass die DSGVO nicht auf anonyme Informationen angewendet werden sollte.[481]

Prinzipiell kann ein Unternehmen alle zertifizierbaren Maßnahmen auch ausschließlich durch interne Regelungen umsetzen, es fehlt dann lediglich die Kontrolle von außen, die als Nachweis dienen kann. Deswegen ist es nicht ganz leicht, nach internen und externen Regelwerken zu trennen, hier wurde davon ausgegangen, dass lediglich diejenigen Bereiche, für die es keine Möglichkeit zur Zertifizierung nach einem ISO Standard gibt, ausschließlich durch interne Vorschriften umgesetzt, während in den anderen Fällen zusätzlich die internationalen Standards eingehalten werden.

8 DSGVO-Urteile

Im Zusammenhang mit dem „Recht auf Vergessenwerden“ ist besonders ein aufsehenerregender Fall aus Spanien sehr bekannt geworden. Im Jahr 2010 hat Costeja González bei der spanischen Datenschutzbehörde (AEPD) Beschwerde gegen Google Spain und Google Inc. eingereicht, da bei einer Suche nach seinem Namen noch immer Ergebnisse bezüglich einer Zwangsversteigerung seines Hauses aufgrund einer Pfändung wegen ausstehender Forderungen der Sozialversicherung von 1998 angeboten wurden. Die Behörde sollte Google auffordern, die Links zu entfernen. Die AEPD setzte daraufhin 2012 das Verfahren aus und legte dem EuGH im Rahmen eines Vorabentscheidungsverfahrens Fragen zur Auslegung der zu diesem Zeitpunkt gültigen Datenschutzrichtlinie von 1995 vor. Am 13. Mai 2014 erließ der EuGH das Urteil, dass Suchmaschinen-Anbieter zur Löschung von Suchergebnissen aufgrund einer Namenssuche aus der Trefferliste verpflichtet werden können.[482] Obwohl dieses Verfahren vor Inkrafttreten oder Veröffentlichung der DSGVO stattfand, hat es eindeutig

[480] vgl.: DSB, Bescheid v. 5.12.2018, Gz. D123.270/0009-DSB/2018, European Case Law Identifier: ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018, URL: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html, URLs: https://www.e-recht24.de/news/datenschutz/11269-dsgvo-daten-loeschen-heisst-nicht-unbedingt-daten-vernichten.html, https://www.lhr-law.de/magazin/datenschutzrecht/daten-loeschen-bedeutet-nicht-unbedingt-daten-vernichten

[481] vgl. Erwägungsgrund 26, URL: https://dsgvo-gesetz.de/erwaegungsgruende/nr-26/

[482] vgl. DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.24,
Vollständiges Urteil des EuGH unter: URL:
http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=DE

datenschutzrechtliche Relevanz. Zum einen wird deutlich, dass viele Schutzrechte betroffener Personen nicht erst durch die DSGVO bestehen, zum anderen spielte in diesem konkreten Fall die genaue Auslegung der Richtlinie für die nationale Anwendung eine bedeutende Rolle, obgleich diese nicht unmittelbar anwendbar war. Die Reaktionen auf das Urteil waren eher kontrovers. Rechtsanwalt Joerg Heidrich, zu dieser Zeit Datenschutzbeauftragter des Heise Zeitschriften Verlags, kritisierte in einem Interview die Grundsatzentscheidung des EuGH als fragwürdiges Urteil, das die Maxime ‚im Zweifellsfall für den Datenschutz' statt eines Abwägens konkreter betroffener Interessen begünstigt. Auch für die Praxis hält er dieses Vorgehen für schwierig.[483] Tatsächlich gingen bei Google nach dem Urteil bis Februar 2015, also innerhalb von etwa neun Monaten, bereits über 200.000 Löschanträge ein.[484] Auch Prof. Dr. Wolfgang Hoffmann-Riem, ehemaliger Justizsenator und Richter des Bundesverfassungsgerichts, hält die Differenzierungen im EuGH-Urteil für unzureichend und misst dem Abwägen des Persönlichkeitsschutzes betroffener Personen gegen die Interessen anderer an der freien Zugänglichkeit solcher Informationen einen hohen Stellenwert bei. Er betont dabei die Bedeutung des öffentlichen Diskurses für einen demokratischen Staat, in dem eine möglicherweise pauschal angewandte Löschpflicht problematisch sein könnte, sowie die Funktion des Internets als eine Art kollektives Gedächtnis. Kritisch sieht er besonders die Tatsache, dass die Umsetzung des Urteils, also die Entscheidung, welche Informationen zugänglich sind und welche nicht, Google selbst überlassen wurde.[485] Unabhängige Schiedsinstanzen hätten wohl einige Fachleute bevorzugt, da Google durch diese Ermächtigung zu einem privaten Rechtsdurchsetzer wird.[486] Richtlinien hierfür erarbeitete ein eigens eingerichteter Expertenbeirat, dessen Abschlussbericht im Februar 2015 veröffentlicht wurde. Hier wird ausdrücklich betont, dass der EuGH „dem Recht auf Privatsphäre jedenfalls in der gegebenen Konstellation einen grundsätzlichen Vorrang vor den Kommunikationsgrundrechten eingeräumt"[487] hat. Es werden vier materiell-rechtliche Hauptkriterien vorgeschlagen, die bei einer solchen Abwägung beachtet werden sollten. Als erstes Kriterium wird die Rolle des Antragstellers im öffentlichen Leben aufgeführt,

[483] vgl. DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.32
[484] vgl. DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.24
[485] vgl. DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.50f.
[486] vgl. URL: https://www.handelszeitung.ch/unternehmen/google-droht-neue-klage-wegen-loeschungsstreit-631485, 27.10.19
[487] DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.64

wobei eine sehr kleine Rolle zu einem sehr großen Anspruch auf Privatheit führt. Als zweites wird die Natur der bestimmten betroffenen Information betrachtet, wobei beispielsweise Daten über das Sexual- oder Intimleben für einen Vorrang des Rechts auf Privatheit sprechen. Dann ist die Quelle der Information zu berücksichtigen, wobei seriöse Quellen stärker gewichtet werden als zum Beispiel Social Media-Seiten. Als viertes Kriterium wird der Zeitfaktor aufgeführt, wonach das berechtigte Interesse der Öffentlichkeit an der Information im Laufe der Zeit abnimmt. Zusätzlich wurden fünf prozedurale Aspekte ausgearbeitet, die vom EuGH nicht benannt wurden. So soll beispielsweise das Formular für Löschanträge gut zugänglich und verständlich sein, eine Entscheidung durch Google soll vom Antragsteller beziehungsweise dem Betreiber der Webseite anfechtbar sein und eine Löschung aus dem jeweiligen nationalen Angebot von Google wurde als ausreichend erachtet.[488] Diese räumliche Beschränkung wird wiederum ebenfalls kritisiert.[489]

Im September 2019 hat der EuGH allerdings dazu entschieden, dass dieses Vorgehen den Anforderungen des „Rechts auf Vergessenwerden“ genügt.[490]

Hinsichtlich der umstrittenen Möglichkeit, Datenschutzrechtsverletzungen nach dem UWG abzumahnen, finden sich einige Urteile. Während zum Beispiel das Landgericht Magdeburg im Urteil vom 18.01.19 die DSGVO bezüglich möglicher Sanktionen für abschließend und damit Verstöße gegen dieselbe für nicht über das UWG abstrafbar erklärt,[491] schätzt das Landgericht Würzburg im Beschluss vom 13.09.18 die Nichteinhaltung der DSGVO als wettbewerbsrechtlich relevant ein.[492] Das Oberlandesgericht Hamburg hat diese Ansicht in einem Urteil vom 25.10.2018 insbesondere darauf gestützt, dass die DSGVO zum einen in Artikel 77 DSGVO zwar nur jeder betroffenen Person, dafür allerdings „unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde“[493] einräumt und zum anderen ausdrücklich „[j]ede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller

[488] vgl. DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015, S.64

[489] vgl. URL: https://www.handelszeitung.ch/unternehmen/google-droht-neue-klage-wegen-loeschungsstreit-631485, 27.10.19

[490] vgl. EuGH-Urteil vom 24.09.2019, Rechtssache C-507/17, URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=1473662

[491] vgl. LG Magdeburg, Urteil vom 18.01.19, Az.: 36 O 48/18, URL: http://www.landesrecht.sachsen-anhalt.de/jportal/?quelle=jlink&docid=JURE190001056&psml=bssahprod.psml&max=true

[492] vgl. LG Würzburg, Beschluss vom 13.09.18, Az.: 11 O 1741/18 UWG, URL: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-22735?hl=true

[493] Art. 77 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/77.html

Schaden entstanden ist, [...] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter [hat]“[494], also nicht ausschließlich die betroffenen Personen, deren Daten verarbeitet werden. Daraus leitet sich aus Sicht des genannten Gerichts ab, dass die DSGVO in den Vorschriften zu den Sanktionen nicht abschließend ist.[495]

Gegen die Österreichische Post AG (ÖPAG) wurde von der Datenschutzbehörde eine Verwaltungsstrafe in Höhe von 18 Millionen Euro verhängt, weil diese wohl personenbezogene Daten über die vermeintliche politische Affinität von Betroffenen verarbeitet hat.[496] Artikel 9 DSGVO verbietet, mit Ausnahme der in Absatz 2 genannten Erlaubnistatbestände, die Verarbeitung personenbezogener Daten, aus denen „politische Meinungen [...] oder weltanschauliche Überzeugungen [...] hervorgehen“[497], nach Artikel 83 DSGVO ist bei einem Verstoß gegen Artikel 9 DSGVO eine Geldbuße von bis zu 20 Millionen Euro oder 4% des Jahresumsatzes möglich.[498] Zusätzlich wurden weitere Rechtsverletzungen in Hinsicht auf die Verwendung für das Direktmarketing festgestellt.[499] Hierzu besteht noch keine rechtskräftige Entscheidung, die ÖPAG hat Rechtsmittel angekündigt.[500] Gleichzeitig werden zivilrechtliche Schadensansprüche verhandelt, das Landgericht Feldkirch hat im August 2019 einem Betroffenen Schadensersatz in Höhe von 800 Euro zugesprochen, da der Kläger nicht in die Verarbeitung der ihn betreffenden Parteiaffinitäten eingewilligt hatte und die anderen Erlaubnistatbestände aus Artikel 9 DSGVO in diesem Fall nicht einschlägig waren. Zusätzlich wurde der Betroffene nicht persönlich über diese Verarbeitung informiert.[501] Auch dieses Urteil ist noch nicht rechtskräftig.[502]

---

[494] Art. 82 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/82.html
[495] vgl. OLG Hamburg, Urteil vom 25.10.2018, Az.: 3 U 66/17, URL: https://www.datenschutz.eu/urteile/Bestimmte-DSGVO-Verletzungen-sind-Wettbewerbsverstoesse-Oberlandesgericht-Hamburg-20181025/
[496] vgl. URL: https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag, 27.10.19
[497] Art. 9 Abs. 1 DSGVO, URL: https://dejure.org/gesetze/DSGVO/9.html
[498] vgl. Art. 83 Abs. 5 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html
[499] vgl. URL: https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag, 27.10.19
[500] vgl. URLs : https://wien.orf.at/stories/3019396/, https://www.dr-bahr.com/news/oesterreichische-datenschutzbehoerde-18-mio-eur-dsgvo-bussgeld-gegen-oesterreichische-post.html, 27.10.19
[501] vgl. URL: https://www.datenschutz.eu/urteile/800-EUR-Schadensersatz-wegen-unerlaubter-DSGVO-Verarbeitung-Landgericht-Feldkirch-20190807/, 27.10.19
[502] vgl. URL: https://www.dr-bahr.com/news/800-eur-schadensersatz-fuer-betroffenen-wegen-dsgvo-verletzung.html, 27.10.19

Die in Deutschland verhängten Bußgelder bewegten sich bisher in einem weit niedrigeren Bereich, mit Höchstwerten von etwa 200.000 Euro.[503] Verhängt wurde diese Strafe von Maja Smoltczyk, der Berliner Datenschutzbeauftragten, gegen den Lieferdienst Delievery Hero Germany GmbH wegen Nichtachtung der Betroffenenrechte.[504] Allerdings hat Frau Smoltczyk im August bereits angekündigt, ein Bußgeld in zweistelliger Millionenhöhe erlassen zu wollen.[505] Im November hat sie dies nun umgesetzt und gegen die Immobiliengesellschaft ‚Deutsche Wohnen' ein Bußgeld von 14,5 Millionen Euro erlassen. Das Unternehmen hat ein Archivsystem zur Speicherung von personenbezogenen Daten seiner Mieter, darunter zum Beispiel auch Gehaltsbescheinigungen oder Kontoauszüge, verwendet, das keine Möglichkeit zur Löschung der Daten vorsah. Zusätzlich wurde nicht geprüft, ob die weitere Speicherung der Daten zulässig war. Einige der Informationen waren etliche Jahre alt und dienten nicht mehr dem Zweck der Erhebung. Die Datenschutzbehörde forderte bereits 2017 eine Umstellung des Archivsystems, dem kam ‚Deutsche Wohnen' allerdings nicht nach.[506] Das Urteil ist noch nichts rechtskräftig, das Unternehmen kann noch Einspruch einlegen.[507]

Die aktuell höchsten Geldstrafen wurden von der Britischen Datenschutzaufsichtsbehörde ICO verhängt. So könnte British Airways aufgrund zu schwacher Sicherheitsvorkehrungen, die zu einer Verletzung des Schutzes personenbezogener Daten führten, zu einer Zahlung von 1,5% ihres weltweiten Umsatzes im Jahr 2017 verpflichtet werden. Das wären etwa 183 Millionen Pfund,[508] was umgerechnet fast 213 Millionen Euro sind. Ein angemessener Schutz der personenbezogenen Daten ist einer der Verarbeitungsgrundsätze nach Artikel 5 DSGVO,[509] ein Verstoß gegen diesen Artikel kann nach Artikel 83 DSGVO ebenso wie ein Verstoß gegen Artikel 9 DSGVO geahndet

[503] vgl. URL: https://www.datenschutzbeauftragter-info.de/rekord-bussgelder-auch-in-deutschland/, 07.11.19
[504] vgl. Pressemitteilung vom 19.09.19, URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf, 28.10.19
[505] vgl. URL: https://www.datenschutzbeauftragter-info.de/rekord-bussgelder-auch-in-deutschland/, 07.11.19
[506] vgl. Tremmel, Moritz: Millionen-Bußgeld gegen Deutsche Wohnen verhängt, in: golem.de, 05.11.19, URL: https://www.golem.de/news/landesdatenschutzbeauftragte-dsgvo-bussgeld-gegen-deutsche-wohnen-verhaengt-1911-144810.html, 06.11.19
[507] vgl. Schäfer, Jan: DSGVO: Immobiliengesellschaft soll 14,5 Millionen Euro Strafe zahlen, in: eRecht24, 06.11.19, URL: https://www.e-recht24.de/news/datenschutz/11721-dsgvo-immobiliengesellschaft.html, 06.11.19
[508] vgl. URL: https://www.datenschutzbeauftragter-info.de/datenschutzaufsichtsbehoerde-kuendigt-dsgvo-rekord-bussgelder-an/, 07.11.19
[509] vgl. Art. 5 Abs. 1 Buchstabe f DSGVO, URL: https://dejure.org/gesetze/DSGVO/5.html

werden.[510] Ungefähr 3% des Jahresumsatzes soll die Hotelkette Marriot, ebenfalls nach einem Datenschutzvorfall, zahlen, was etwa 99 Millionen Pfund entspricht, also 115 Millionen Euro. Die Urteile sind noch nicht rechtskräftig und beide Unternehmen haben angekündigt, rechtliche Schritte gegen die Strafen einzuleiten.[511]

Auch wenn in der Praxis der Großteil der Geldbußen bisher vergleichsweise eher geringer ausgefallen ist als vor Inkrafttreten der DSGVO befürchtet wurde, könnte sich das jetzt im weiteren Verlauf ändern. Einige aktuelle Entwicklungen könnten den Schluss zulassen, dass die Aufsichtsbehörden mittlerweile dazu übergehen, den von der DSGVO gegebenen Bußgeldrahmen voll auszuschöpfen.[512]

9 Fazit – DSGVO als Herausforderung für Compliance

Zusammenfassend ist festzuhalten, dass die Einhaltung datenschutzrechtlicher Vorschriften in Hinsicht sowohl auf mögliche rechtliche Konsequenzen als auch auf gesellschaftliche Folgen wie Imageverlust als wichtiges, ja erfolgsentscheidendes Unternehmensziel anzusehen ist.

Durch die zahlreichen rechtlichen Vorgaben, wie hier allein in Hinsicht auf den Datenschutz aufgezeigt, entsteht ein äußerst komplexes Gefüge, in dem es für einen Großteil der Unternehmen zusätzlich spezifische Gesetzestexte oder Sonderregelungen zu beachten gilt. Den Datenschutz betreffend ist besonders zu betonen, dass im Falle eines Widerspruchs die DSGVO gegenüber nationalen Gesetzen eine Vorrangstellung hat, sofern sie nicht selbst Abweichungen zulässt. Dadurch ist die Anwendbarkeit einiger nationaler Gesetze, beispielsweise wie bereits dargelegt aus dem TMG und dem TKG, umstritten oder nicht mehr gegeben.

Datenschutz und IT-Sicherheit sind in einer globalen, vernetzten Welt stark miteinander verbunden, da ersterer ohne eine technische Absicherung durch zweitere nicht gegeben sein kann.

Transparenz und Möglichkeiten für die Kontrolle durch den Betroffenen bezüglich der Verarbeitung seiner personenbezogenen Daten spielen gerade dadurch eine entscheidende Rolle, dass leicht der Überblick verloren gehen kann. Das Recht auf informationelle

[510] vgl. Art. 83 Abs. 5 Buchstabe a DSGVO, URL: https://dejure.org/gesetze/DSGVO/83.html
[511] vgl. URL: https://www.datenschutzbeauftragter-info.de/datenschutzaufsichtsbehoerde-kuendigt-dsgvo-rekord-bussgelder-an/, 07.11.19
[512] vgl. URL: https://www.datenschutzbeauftragter-info.de/rekord-bussgelder-auch-in-deutschland/, 07.11.19

Selbstbestimmung beinhaltet schließlich zwangsläufig auch das Wissen, wer die eigenen Daten wo und wie zu welchem Zweck und in welchem Umfang nutzt oder verarbeitet. Durch die Unübersichtlichkeit und die mangelnden Kontrollmöglichkeiten des Einzelnen sind Regelungen, Überwachungsmöglichkeiten und eine Strafbarkeit von Verstößen durch eine andere Instanz nötig.

Für die Praxis empfiehlt sich für Unternehmen sowohl aus organisatorischen Gründen als auch zur rechtlichen Absicherung, zum Beispiel im Hinblick auf die in der DSGVO geregelte Rechenschaftspflicht des Verantwortlichen, der Einsatz eines Compliance Management Systems. Dabei ist auf ein entsprechendes Verzeichnis, das die Einhaltung bestehender Lösch- und Aufbewahrungsfristen gewährleistet, sowie ein geeignetes Risikomanagement und für den Datenschutz unabdingbare Datensicherheitsmaßnahmen zu achten. Zudem sind einige gesetzliche Regelungen von der Größe des Unternehmens abhängig oder davon, ob ein Betrieb börsennotiert ist oder nicht.

10 Aktuelle Situation

Nach der repräsentativen, branchenübergreifenden Studie ‚CMS Compliance-Barometer', die jährlich von der Wirtschaftskanzlei CMS Deutschland erhoben wird, steht Datenschutz besonders durch die DSGVO und die verschärften Sanktionsmöglichkeiten im Fokus der Compliance-Verantwortlichen und wurde von 35 Prozent der befragten Unternehmer als Compliance-Risiko an erster Stelle genannt. Das Bewusstsein für Compliance ist über die letzten Jahre im Management leicht rückläufig, während es bei den Mitarbeitern zunimmt. Gleichzeitig sinkt die Bereitschaft letzterer, in Compliance-Fragen Entscheidungen zu treffen. Mängel in der Compliance-Kultur und in der Compliance-Kommunikation werden als wesentliche Schwachstelle in vielen Unternehmen gesehen. Gut vier von zehn Großunternehmen haben eine eigene Compliance-Abteilung. Vermutlich unter anderem auch auf das Inkrafttreten der DSGVO zurückzuführen ist zudem der Anstieg der Unternehmen, die externe Berater einbinden, um etwa 20 Prozent.[513] Diese Umfrage zeigt nun deutlich, als welche enorme Herausforderung die neuen Datenschutzrichtlinien für Unternehmen einzuordnen sind. Hieraus resultieren eben derartige von Firmen getroffene Anpassungsversuche wie die

[513] vgl. CMS: 4. CMS Compliance-Barometer: Unternehmen unterschätzen wesentliche Risiken, 22.05.19, URL: https://cms.law/de/deu/news-information/4.-cms-compliance-barometer-unternehmen-unterschaetzen-wesentliche-risiken, 10.11.19

Miteinbeziehung externer Berater oder das Aufbauen eigener Compliance-Abteilungen. Die ausufernde Wichtigkeit von Compliance als solches geht aus der Umfrage ebenfalls hervor, da eine mangelnde Kommunikation sowie eine nicht hinreichende Kultur diesbezüglich als erfolgsentscheidende Herausforderung für die Firma erachtet wird. Dies ist nicht verwunderlich, da Compliance, als Einhaltung rechtlicher wie unternehmensinterner Regelungen, der Sicherheit sowohl des Unternehmens selbst als auch der Mitbewerber und Kunden dient. Um die gesamte Problematik in einem etwas größer gefassten Rahmen zu betrachten, ist wohl zu erwähnen, dass insbesondere auch der Datenschutz eine Art von Sicherheit darstellt, auch wenn diese sich selbstredend auf einer anderen Ebene einordnen lässt als die von Hobbes in „Der Staatsvertrag" durch Gesetze angestrebte. Das dürfte sich allein schon zeitlich ergeben, da das Recht auf informationelle Selbstbestimmung durch die zunehmende Digitalisierung zum einen an Bedeutung gewinnt und zum anderen schwerer durchzusetzen ist. Dennoch zeigt sich auch hier das von Hobbes als Grundlage für die Notwendigkeit eines Staates genannte Bedürfnis der Menschen nach Sicherheit, eines der zentralsten Güter im juristischen Bereich. Ein Staat, der diese Aufgabe erfüllt, indem er nämlich dem Einzelnen ein ausreichendes Maß an Sicherheit, eben auch an die jeweiligen Situationen und neuen Bedrohungen angepasst, zu gewähren vermag, kann selbstredend nicht willkürlich agieren, sondern muss bestimmten Regeln folgen. Ein nicht willkürlicher Staat, der (Rechts-)Sicherheit und Gerechtigkeit gewährleistet und bestimmte Grundrechte wahrt, ist per Definition ein Rechtsstaat.[514]

„Demokratie ist gewiss ein preisenswertes Gut, Rechtsstaat ist aber wie das tägliche Brot, wie Wasser zum Trinken und wie Luft zum Atmen, und das Beste an der Demokratie gerade dieses, dass nur sie geeignet ist, den Rechtsstaat zu sichern ."[515]

[514] vgl. Gabler Wirtschaftslexikon: Rechtsstaat, URL: https://wirtschaftslexikon.gabler.de/definition/rechtsstaat-46650/version-269928, 10.11.19

[515] Radbruch, Prof. Dr. Gustav (1878 - 1949), https://legalcareers.de/static_pages/Juristische_Zitate_02, 06.11.19

Literaturverzeichnis

Gesetzestexte: URL: https://dejure.org/, https://www.gesetze-im-internet.de/

Artikel 29-Datenschutzgruppe: Fünfter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Gemeinschaft und in Drittländern, 2002, URL: https://www.zaftda.de/tb-artikel-29-gruppe/143-05-ii-jahresbericht-art-29-gruppe-2000-06-03-2002/file

Aure, Andreas H., Der säkularisierte und subjektivierte Naturrechtsbegriff bei Hugo Grotius, URL: https://forhistiur.de/2008-02-aure/

Dr. Basar, Eren, Dr. Hiéramente, Mayeul: Datensparsamkeit in der StPO – Die Möglichkeit der Löschung, in: HRRS (Höchstrichterliche Rechtsprechung zum Strafrecht), Aug./Sept. 2018, S. 336 – 342, S. 336, URL: https://www.hrr-strafrecht.de/hrr/archiv/18-08/index.php?sz=8#336

Bayrischer Landesbeauftragter für Datenschutz: Datenschutzreform 2018, Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO), 25.09.2017, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf

BITKOM, DIN: Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten, 2014, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

Bitkom: Stellungnahme zur Positionsbestimmung der Datenschutzkonferenz vom 26. April 2018 zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, 09.05.2018, URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2018/Positionspapiere/180511-Positionsbestimmung-der-Datenschutzkonferenz-vom-26-April-2018/Bitkom-Stellungnahme-Position-DSK-DSGVO-TMG.pdf

BKA: Hacktivisten – Abschlussbericht, Download möglich unter: URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2016HacktivistenqAbschlussbericht.html

BMI: Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat - Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), 27.03.2019, URL: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf

Brinks, Cornelia: Zugriffskontrolle – TOM und der Datenschutz Teil 3, 2015, URL: https://www.datenschutz-notizen.de/11496-4211496/

BSI: Das IT-Sicherheitsgesetz, Kapitel 2: Zielgruppen und Neuregelungen, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf;jsessionid=7F65543A03EE0395114CEC68CC88E11B.1_cid360?__blob=publicationFile&v=7

BSI: Schutz Kritischer Infrastrukturen – durch IT-Sicherheitsgesetz und UP KRITIS, Kapitel 3: Das IT-SiG ist Pflicht, 2017, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=7F65543A03EE0395114CEC68CC88E11B.1_cid360?__blob=publicationFile&v=7

Buchmann, Erik, Eichhorn, Susanne: Auskunftsersuchen nach Art. 15 DSGVO – Wie leicht machen es Unternehmen ihren Kunden, ihre Rechte nach Art. 15 DSGVO auszuüben?, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S.65-70

Bundesnetzagentur: Mitteilung, URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html

BverG, Urteil des Ersten Senats vom 27. Februar 2008, -1 BvR 370/07-, Rn. (1-333), URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

Center for Computing Technologies, Universität Bremen: IT-Sicherheit: Zugriffskontrolle, URL: http://www-rn.informatik.uni-bremen.de/lehre/itsec/itsec05-1a.pdf

CMS: 4. CMS Compliance-Barometer: Unternehmen unterschätzen wesentliche Risiken, 22.05.19, URL: https://cms.law/de/deu/news-information/4.-cms-compliance-barometer-unternehmen-unterschaetzen-wesentliche-risiken

2017/0003 (COD), Vorschlag für die Verordnung über Privatsphäre und elektronische Kommunikation, 10.1.2017, von https://www.datenschutz-bayern.de/0/eprivacyVO.html

DCGK 2019 mit Begründungen, Deutscher Corporate Governance Kodex wie von der Regierungskommission am 9. Mai 2019 beschlossen, Grundsatz 5, Download möglich unter: URL: https://www.dcgk.de/de/kodex/dcgk-2019.html

Deuse, Klaus : Intelligente Helfer – Halbleiter im Auto, 2014, URL: https://p.dw.com/p/1CgV1

Deutscher Bundestag: Stenografischer Bericht, 155. Sitzung, Plenarprotokoll 17/155, 26.01.2012, URL: http://dipbt.bundestag.de/doc/btp/17/17155.pdf

Deutscher Corporate Governance Kodex, 07.02.2017, URL: https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/170424_Kodex_Mark_up.pdf

Die Linke: Antrag: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, Drucksache 19/7705, 13.02.19, II. 5., S. 1f., URL: https://kripoz.de/wp-content/uploads/2019/02/bt-drs-19-7705.pdf

DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet: Das Recht auf Vergessenwerden, Hamburg, Oktober 2015

DSB, Bescheid v. 5.12.2018, Gz. D123.270/0009-DSB/2018, European Case Law Identifier: ECLI:AT:DSB:2018:DSB.D123.270.0009.DSB.2018, URL: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

DSK: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, URL: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

DSK: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 26.04.2018, URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf

eco: Stellungnahme zu den Anträgen: 19/7698: Digitalisierung ernst nehmen – IT-Sicherheit stärken, 19/7705: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, und 19/1328: IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern, Ausschussdrucksache 19(4)255 B, 04.04.19, URL: https://kripoz.de/wp-content/uploads/2019/04/a-drs-19-4-255-b-landefeld.pdf

EuGH-Urteil vom 24.09.2019, Rechtssache C-507/17, URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=1473662

FDP: Antrag: Digitalisierung ernst nehmen – IT-Sicherheit stärken, Drucksache 19/7698, 12.02.19, URL: https://kripoz.de/wp-content/uploads/2019/02/bt-drs-19-7698.pdf

Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 15.05.2017, URL: https://www.bundestag.de/resource/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf

Gesetzesentwurf der Bundesregierung, Drucksache 18/11272, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 22.02.2017, URL: http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf

Gierschmann, Markus: Datenschutz-Managementsystem zur Sicherstellung der Compliance nach DS-GVO - Bestandsaufnahme und Blick in die Zukunft, BvD-Verbandstage 2018 Berlin, URL: https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Verbandstage_Markus-Gierschmann.pdf

Harrer, Julia: Jean-Jacques Rousseau: Der Gesellschaftsvertrag, studienarbeit, 2012, Grin, URL: https://www.grin.com/document/205970

Dr. Herpig, Sven, Stiftung Neue Verantwortung: Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema "ITSicherheit", Ausschussdrucksache 19(4)255 A, 08.04.19, URL: https://kripoz.de/wp-content/uploads/2019/04/a-drs-19-4-255-a-herpig.pdf

Hobbes, Thomas: Der Staatsvertrag, Von den beiden ersten natürlichen Gesetzen und den Verträgen, in: Horster, Detlef: Texte zur Ethik, Reclam, Stuttgart 2012

Hobbes, Thomas: Leviathan, Hamburg, Meiner, 1996, S. 4, URL: https://homepage.univie.ac.at/charlotte.annerl/texte/hobbes.pdf

Horster, Detlef: Texte zur Ethik, Zu den Autorinnen und Autoren, Reclam, Stuttgart 2012

Hotter, Maximilian : Privatsphäre – Der Wandel eines liberalen Rechts im Zeitalter des Internets, Campus Verlag GmbH, Frankfurt am Main, 2011

Hume, David: Der Ursprung von Rechtsordnung und Eigentum, in in: Horster, Detlef: Texte zur Ethik, Reclam, Stuttgart 2012

ISO/IEC: ISO/IEC 27000:2018, 2018, kostenloser Download in englischer oder französischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

ISO/IEC 29100:2011, 2011, kostenloser Download in englischer Sprache möglich unter: URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Dr. Jonas, Peter: Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, in: Austrian Law Journal, ALJ 1/2016, S. 60–67, URL: https://alj.uni-graz.at/index.php/alj/article/view/62/156

Kant, Immanuel (1724 - 1804) : Über den Gemeinspruch: Das mag in der Theorie richtig sein, taugt aber nicht für die Praxis, URL: http://www.zeno.org/Philosophie/M/Kant,+Immanuel/Über+den+Gemeinspruch%3A+Das+mag+in+der+Theorie+richtig+sein,+taugt+aber+nicht+für+die+Praxis/II.+Vom+Verhältnis+der+Theorie+zur+Praxis+im+Staatsrecht

Kuhnigk, Nadine : Künstliche Intelligenz und Datenschutz: Passt nicht immer, in: Mainpost, 26.9.19, URL: https://www.mainpost.de/ueberregional/wirtschaft/mainpostwirtschaft/Kuenstliche-Intelligenz-und-Datenschutz-Passt-nicht-immer;art9485,10305975

Ladenthin, Volker: Eine Gesellschaft braucht Gesetze, netzwerk ethik heute, URL: https://ethik-heute.org/eine-gesellschaft-braucht-gesetze/

LG Magdeburg, Urteil vom 18.01.19, Az.: 36 O 48/18, URL: http://www.landesrecht.sachsen-anhalt.de/jportal/?quelle=jlink&docid=JURE190001056&psml=bssahprod.psml&max=true

LG Würzburg, Beschluss vom 13.09.18, Az.: 11 O 1741/18 UWG, URL: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-22735?hl=true

Lischka, Konrad : Zahlung per EC-Karte – Was die Datensammler wirklich wissen, Spiegel online, 2010, URL: https://www.spiegel.de/netzwelt/web/zahlung-per-ec-karte-was-die-datensammler-wirklich-wissen-a-719168.html

Mylonas, Alexios: Security and Privacy in Ubiquitous Computing: The Smart Mobile Equipment Case, 2013

Mylonas et al.: Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition, 2011

OLG Hamburg, Urteil vom 25.10.2018, Az.: 3 U 66/17, URL: https://www.datenschutz.eu/urteile/Bestimmte-DSGVO-Verletzungen-sind-Wettbewerbsverstoesse-Oberlandesgericht-Hamburg-20181025/

Petrlic, Ronald: Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO – Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden, in: DuD – Datenschutz und Datensicherheit, Februar 2019, S. 71-75

Platon: Nomoi, Die Gesetze, URL: http://www.opera-platonis.de/Nomoi.pdf

Pressemitteilung vom 19.09.19, URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf

PWMP Management- und Organisations-Beratung: Risikomanagement nach ISO 31000 Umsetzung in der Organisation, 2018, URL: http://www.pwmp.de/files/181102-Risikomanagement-nach-ISO-31000.pdf

Radbruch, Prof. Dr. Gustav (1878 - 1949), URL: https://legalcareers.de/static_pages/Juristische_Zitate_02

Schaar, Peter : Datenschutz in Zeiten von Big Data, in: HMD Praxis der Wirtschaftsinformatik, 2014, S.840-852

Schäfer, Jan: DSGVO: Immobiliengesellschaft soll 14,5 Millionen Euro Strafe zahlen, in: eRecht24, 06.11.19, URL: https://www.e-recht24.de/news/datenschutz/11721-dsgvo-immobiliengesellschaft.html

Schonschek, Oliver: DSGVO: So setzen Sie die erweiterte Zugangskontrolle um, 2017, URL: https://www.datenschutz-praxis.de/fachartikel/dsgvo-setzen-sie-erweiterte-zugangskontrolle-um/

Stolze, Michael: Der Datenschutz als Marktverhaltensregel im Wettbewerbsrecht, 2012, URL: https://www.iitr.de/veroeffentlichungen/der-datenschutz-als-marktverhaltensregel-im-wettbewerbsrecht.html

Tremmel, Moritz: Millionen-Bußgeld gegen Deutsche Wohnen verhängt, in: golem.de, 05.11.19, URL: https://www.golem.de/news/landesdatenschutzbeauftragte-dsgvo-bussgeld-gegen-deutsche-wohnen-verhaengt-1911-144810.html

TÜV Rheinland: TR CMS 101:2011 – Standard für Compliance Management Systeme (CMS), 2011, URL: https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf

TÜV SÜD Management Service GmbH: Whitepaper: ISO 27001: Informationssicherheit und Zertifizierungsprozess, 2015, URL: https://www.tuev-sued.de/uploads/images/1464955241375022630318/iso-27001-white-paper-vm-de-screen2.pdf

Unterrichtung durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit, 27.Tätigkeitsbericht, Drucksache 19/9800, 08.05.2019, URL: http://dip21.bundestag.de/dip21/btd/19/098/1909800.pdf

Veltsos, Christophe: 10 Takeaways From the ISO 31000:2018 Risk Management Guidelines, in: SecurityIntelligence, 2018, URL: https://securityintelligence.com/10-takeaways-from-the-iso-310002018-risk-management-guidelines/

Voßhoff, Andrea: Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272 und der Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334, 29.05.2017, URL: https://freiheitsrechte.org/home/wp-content/uploads/2017/05/186346_Stellungnahme_BfDI_zu_18-11272_und_186334.pdf

vzbv: Anwendbarkeit des Telemediengesetzes, 28.06.2018, URL: https://www.vzbv.de/sites/default/files/downloads/2018/06/29/18-06-28_vzbv-stellungnahme_dsk_tmg-dsgvo.pdf

Webseiten

https://advisera.com/27001academy/de/knowledgebase/iso-27001-im-vergleich-zu-iso-27002

https://www.beuth.de/de/norm/iso-iec-27701/312455765

https://bitcoin.org/de/

https://www.bits.gmbh/die-rechenschaftspflicht-nach-der-DSGVO/

https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html

https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/AbteilungenReferate/IVA6_42GGO.pdf?__blob=publicationFile&v=4

https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html

https://www.bsigroup.com/LocalFiles/nl-nl/iso-9001/BSI-Annex-SL-Whitepaper.pdf

https://www.business-wissen.de/hb/ziele-und-aufgaben-des-risikomanagements-im-unternehmen/

https://www.buzer.de/gesetz/1966/l.htm

https://www.buzer.de/gesetz/1966/v208267-2018-05-25.htm

https://www.buzer.de/gesetz/3086/l.htm

https://www.buzer.de/gesetz/3486/l.htm

https://www.buzer.de/gesetz/3486/v208257-2018-05-25.htm

https://www.buzer.de/gesetz/3690/al66903-0.htm

https://www.buzer.de/gesetz/5815/l.htm

https://www.buzer.de/gesetz/6165/l.htm

https://www.buzer.de/gesetz/7616/l.htm

https://www.buzer.de/gesetz/8987/v193756-2015-07-25.htm

http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=DE

https://datenschutzbeauftragter-hamburg.de/2016/03/weitergabe-personenbezogener-daten-an-ermittlungsbehoerden/

https://www.datenschutzbeauftragter-info.de/anforderungen-an-die-einwilligung-von-kindern-nach-der-dsgvo/

https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/

https://www.datenschutzbeauftragter-info.de/datenschutzaufsichtsbehoerde-kuendigt-dsgvo-rekord-bussgelder-an/

https://www.datenschutzbeauftragter-info.de/dsgvo-grundsaetze-fuer-die-verarbeitung-personenbezogener-daten/

https://www.datenschutzbeauftragter-info.de/isms-dsgvo-moeglichkeiten-der-zertifizierung/

https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/

https://www.datenschutzbeauftragter-info.de/polizeianfragen-rechtskonforme-datenweitergabe-nach-der-dsgvo/

https://www.datenschutzbeauftragter-info.de/rekord-bussgelder-auch-in-deutschland/

https://www.datenschutzbeauftragter-info.de/wettbewerbsrechtliche-abmahnung-wegen-dsgvo-verstoessen/

https://www.datenschutz.eu/urteile/800-EUR-Schadensersatz-wegen-unerlaubter-DSGVO-Verarbeitung-Landgericht-Feldkirch-20190807/

https://www.datenschutzexperte.de/telekommunikationsgesetz-tkg/

https://www.datenschutz-grundverordnung.eu/rechtsnormen-der-dsgvo/art-99-eu-dsgvo/

https://www.datenschutz-notizen.de/eugh-allgemeine-verpflichtung-zur-vorratsdatenspeicherung-ist-unzulaessig-5417066/

https://www.datenschutz-notizen.de/iso-iec-27001-vs-dsgvo-1022677/

https://www.datenschutz-praxis.de/fachartikel/zugriffskontrolle-unerlaubten-zugriffen-auf-der-spur/

https://www.dcgk.de/de/

https://www.dcgk.de/de/kodex/archiv.html

https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/170424_Kodex.pdf

https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html

https://www.dirks-computerseite.de/smart-tv-vorteile/#:~:text=Vorteile%20und%20Nachteile%20der%20Smart%20TV%20Ger%C3%A4te&text=Daf%C3%BCr%20bekommt%20man%20mit%20den,das%20Budget%20im%20Auge%20beh%C3%A4lt.

https://www.dr-bahr.com/news/800-eur-schadensersatz-fuer-betroffenen-wegen-dsgvo-verletzung.html

https://www.dr-bahr.com/news/oesterreichische-datenschutzbehoerde-18-mio-eur-dsgvo-bussgeld-gegen-oesterreichische-post.html

https://dsgvo-gesetz.de/erwaegungsgruende/

https://www.e-recht24.de/news/datenschutz/11269-dsgvo-daten-loeschen-heisst-nicht-unbedingt-daten-vernichten.html

http://www.eugrz.info/PDF/EGMR1/Konvent.pdf

https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31995L0046

https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015L1535

https://europa.eu/european-union/eu-law/legal-acts_de

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_de

https://www.fachportal-steuerrecht.de/jportal/portal/page/fpsteuerrecht.psml?nid=jpr-NLBAADG000818&cmsuri=%2Ffachportal_steuerrecht%2Fde%2Fr17%2Fnachrichten_1%2Fzeige_nachricht.jsp

https://www.felser.de/blog/betriebsrat-und-datenschutz/

https://freiheitsrechte.org/trojaner/

https://www.gabler-banklexikon.de/definition/europaeische-datenschutzgrundverordnung-eu-dsgvo-81652

https://www.gesetze-bayern.de/Content/Document/BayDSG

https://www.gesetze-im-internet.de/

https://www.getabstract.com/de/zusammenfassung/nomoi/35632

https://www.handelszeitung.ch/unternehmen/google-droht-neue-klage-wegen-loeschungsstreit-631485

https://www.heise.de/tipps-tricks/WhatsApp-Alternativen-Welche-Messenger-gibt-es-3976153.html

http://hoganlovells-blog.de/2018/06/11/dsgvo-oder-tmg-was-muessen-unternehmen-beim-einsatz-von-cookies-beachten/

https://www.ihk-niederbayern.de/Beratung-Service/Recht/handelsregister/zweck-des-handelsregisters/4116878

https://www.imsm.de.com/iso-normen/?msclkid=0b6977f7ad95142ab5382a52d1a74352&utm_source=bing&utm_medium=cpc&utm_campaign=NEU_ISO_Allgemein&utm_term=%2Biso%20%2Bzertifizierung&utm_content=ISO_Zertifizierung

https://www.infolaw.at/downloads/mag_georg_fellner_ll_m-oeffnungsklauseln_der_dsgvo-2017-05-05.pdf

https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/PDF-Dateien/Factsheets/factsheet_grundrecht_auf_datenschutz_07_05_2010.pdf

https://www.isico-datenschutz.de/blog/2019/07/30/loeschkonzept-dsgvo/

https://www.juraforum.de/lexikon/straftat-abgrenzung-zur-ordnungswidrigkeit

https://www.juraforum.de/lexikon/telekommunikationsueberwachung

https://kripoz.de/Kategorie/gesetzentwuerfe/page/2/

http://lexikon.jura-basic.de/aufruf.php?file=1&art=&find=Telemedien%20%3E%3EAbgrenzung%20zu%20Telekommunikation%20und%20Rundfunk

https://www.lhr-law.de/magazin/datenschutzrecht/daten-loeschen-bedeutet-nicht-unbedingt-daten-vernichten

https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-gff-staatstrojaner-ueberwachung-software-ermittlungen/, https://freiheitsrechte.org/trojaner/

https://www.lto.de/recht/hintergruende/h/verfassungsbeschwerde-staatstrojaner-fdp-anwalt-interview-online-durchsuchung/

http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DSGVO.pdf

https://opensource.org/docs/osd

https://www.otris.de/wiki/richtlinienmanagement/compliance-management-system/

https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag

http://rechtslexikon.net/d/qualifizierte-straftat/qualifizierte-straftat.htm

http://www.rechtslexikon.net/d/tatbestand/tatbestand.htm

http://www.rechtzweinull.de/telemediengesetz

https://www.revosax.sachsen.de/vorschrift/1672-Saechsisches-Datenschutzgesetz

https://www.security-insider.de/was-ist-eine-backdoor-a-676126/

https://www.security-insider.de/was-ist-ein-zero-day-exploit-a-648117/

https://www.springerprofessional.de/datenschutz-und-datensicherheit-dud/7466274

https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

https://www.telemedicus.info/article/3342-OEffnungsklauseln-und-Drittstaaten-Eine-uebersehene-Luecke.html

https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html

https://www.wbs-law.de/wettbewerbsrecht/kann-die-dsgvo-ueber-das-uwg-abgemahnt-werden-lg-wuerzburg-trifft-erste-entscheidung-23849/

https://wien.orf.at/stories/3019396/

https://wirtschaftslexikon.gabler.de/definition/iso-40855/version-264231

https://wirtschaftslexikon.gabler.de/definition/rechtsstaat-46650/version-269928

https://www.zeit.de/digital/datenschutz/2019-05/baltimore-nsa-tool-hackerangriff-ransomware-wannacry-usa, https://www.pandasecurity.com/de/security-info/wannacry/

https://www.zeit.de/politik/deutschland/2018-08/staatstrojaner-verfassungsbeschwerde-ueberwachungsinstrument-hajo-seppelt-can-duendar

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, Datum Vorname Nachname