Jacqueline Vogel

Lehrbuch für Datenschutzbeauftragte

Basiswissen

Vogel-Verlag

Impressum

Autorin: Jacqueline Vogel

Verlag: Vogel-Verlag, 97532 Üchtelhausen
ISBN: 978-3-9824784-5-6

3. Auflage 2024

Über mich

Meine ersten beruflich bedingten Berührungen mit dem Datenschutz hatte ich bereits im Jahre 2002. Als Personalsachbearbeiterin war ich nebenamtlich im behördlichen Datenschutz tätig. Zwischenzeitlich habe ich diverse Aufstiegsfortbildungen genossen und bin staatlich geprüfte Betriebswirtin, was es mir unheimlich erleichtert, sämtliche Prozesse im Unternehmen aus der Sicht des Datenschutzes zu beleuchten. Ich übernehmen im kleinen Familienunternehmen der IT und Datensicherheit den Fachbereich „Datenschutz“. Als Beraterin und Datenschutzbeauftragte betreue ich Unternehmen jeder Größe. angefangen vom Handwerker über Gesundheitspraxen bis hin zu Konzernen. Meine Aufträge umfassen meist die Erstellung datenschutzrechtlicher Unterlagen, die Durchführung von Mitarbeiterschulungen, Vertragsprüfungen oder interne Audits. Wenn es meine Zeit hergibt, bilde ich als Referentin neue Datenschutzbeauftragte aus und bereite neue Kollegen auf die IHK- oder TÜV-Prüfung vor. Die Tätigkeit als Referentin für Vorträge und Weiterbildungen führte auch dazu, dass ich ein eigenes Lehrbuch entwickelt habe. Ich habe meine Passion in der Vermittlung von Fachwissen gefunden. Es macht mir sehr viel Spaß meine Erfahrungen weiterzugeben und dem komplexen Fachwissen ein bisschen mehr Leichtigkeit zu verleihen. Neben meinen Zertifizierungen als Datenschutzbeauftragte für Unternehmen und Behörden (TÜV) und Datenschutzauditorin (TÜV) bin ich auch Mitglied im ERFA-Kreis Bayern der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) und Mitglied der offiziellen Allianz für Cyber-Sicherheit.

Bei Fragen zum Buch oder Verbesserungsvorschlägen können Sie mich gerne persönlich kontaktieren über *j.vogel@tencos.de*

Gender Hinweis:

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Buch die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Zielgruppe

- (angehende) Datenschutzbeauftragte
- Datenschutzkoordinatoren
- Datenschutzmanager
- Geschäftsführer, Inhaber und Vorstandsmitglieder als Hauptverantwortliche im Datenschutz
- Interessierte Datenschützer

Dieses Buch vermittelt erste Fachkenntnisse zum Thema Datenschutz anhand der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG). Sie erhalten umfassende Informationen, worauf Sie bei der Verarbeitung von personenbezogenen Daten achten müssen. Durch verständliche Texte und anschauliche Grafiken ist das Basisbuch auch für Einsteiger sehr gut geeignet. Das Buch setzt keinerlei rechtliche Kenntnisse voraus. Bereits in den ersten Kapiteln wird Ihnen der Umgang mit Rechtstexten erläutert, so dass ein leichter Einstieg in die Thematik gewährleistet wird. Es wird bewusst auf eine umfangreiche juristische Fachsprache verzichtet. Zahlreiche Tipps und praktische Hinweise helfen Ihnen bei der Umsetzung der Forderungen im Unternehmen oder Verein. Mit anschaulichen Übungen können Sie außerdem Ihr Wissen testen.

Das Buch bereitet auf die Prüfung zum betrieblichen Datenschutzbeauftragten vor. Egal ob Sie die Prüfung bei der Industrie- und Handelskammer, bei TÜV, DEKRA oder bei sonstigen Bildungsträgern ablegen, mit diesem Lehrbuch eignen Sie sich das grundlegende Fachwissen im Datenschutz an und testen das neu Erlernte anhand der Übungsaufgaben. Zusätzlich enthält das Buch zahlreiche Vorlagen und Muster, damit Sie nach der Prüfung den Datenschutz gleich in die Praxis umsetzen können.

Für Unternehmer, Geschäftsführer und Vereinsvorstände bietet dieses Buch einen ersten Überblick über die datenschutzrechtlichen Anforderungen, die in ihren Verantwortungsbereich fallen. Sie lernen dabei verständlich, was Sie eventuell noch in Ihrem Aufgabenbereich zu tun haben und welche Dokumente noch fehlen.

Was vermittelt dieses Buch NICHT?

Dieses Basisbuch beinhaltet die grundlegenden Themen, Begriffe und Anforderungen aus der DSGVO und dem BDSG. Komplexe Themengebiete wie Auftragsverarbeitungen, Datenübermittlungen in Drittländer, Datenschutzfolgenabschätzungen und Datensicherheit werden im weiterführenden Lehrbuch „Expertenwissen“ vermittelt. Diese Inhalte sind sehr komplex und bauen auf dem Grundlagenwissen aus diesem Basisbuch auf.

Inhalte der Fortsetzung „Expertenwissen“:

- Was ist eine Auftragsverarbeitung?
- Darf man Daten in das Ausland übertragen?
- Wie gestaltet man eine Datenschutz-Folgenabschätzung?
- Wie kann man eine Videoüberwachung datenschutzkonform realisieren?
- Welche Besonderheiten gibt es für Konzerne oder Unternehmensgruppen?
- Was ist Datensicherheit? Welche Maßnahmen sind zum Schutz der Daten zu ergreifen?

Inhaltsverzeichnis

Zeichenerklärungen:

Diese Erklärung bringt etwas Licht in das Dunkel.

Hier finden Sie wichtige Informationen oder Hinweise oder eine kurze Zusammenfassung wesentlicher Inhalte.

Empfehlungen:

Hier finden Sie nützliche Quellen für zusätzliche Informationen oder Hin weise zu einem systematischen Vorgehen.

Abkürzungen

ADV/AVV	Auftragsdatenverarbeitung, Vertrag zur Auftragsverarbeitung
AG	Aktiengesellschaft
AO	Abgabenordnung
Art.	Artikel
Az	Aktenzeichen
BayDSG	Bayerisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
DDG	Digitale-Dienste-Gesetz
DSA	Digital-Service-Act (Verordnung)
DSAnpUG	Datenschutz Anpassungs- und Umsetzungsgesetz
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz-Grundverordnung (EU-DSGVO)
DSK	Datenschutzkonferenz
DSMS	Datenschutz-Management-System
EDSA	Europäischer Datenschutzausschuss (eigentlich EDPB = european data protection board)
EG	Erwägungsgrund
EnEV	Energieeinsparverordnung
EU	Europäische Union
EU-DSRL	Europäische Datenschutzrichtlinie
GG	Grundgesetz

GmbH	Gesellschaft mit beschränkter Haftung
IDS	Intrusion-Detection-System
IHK	Industrie- und Handelskammer
KDG	Gesetz über den kirchlichen Datenschutz
KG	Kommanditgesellschaft
KI	Künstliche Intelligenz
KunstUrhG	Kunsturhebergesetz
LDSG	Landesdatenschutzgesetz
LMHV	Lebensmittelhygieneverordnung
OHG	Offene Handelsgesellschaft
QM	Qualitätsmanagement
PAuswG	Personalausweisgesetz
SSO	Single Sign-On (Einmalanmeldung)
StG	Strafgesetzbuch
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (vormals als TTDSG)
TKG	Telekommunikationsgesetz (außer Kraft)
TMG	Telemediengesetz
TOMs	Technische und Organisatorische Maßnahmen
TTDSG	TTDSG Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (2024 umbenannt in TDDDG)
TÜV	Technischer Überwachungsverein
UWG	Gesetz gegen den unlauteren Wettbewerb
VVT/VVZ	Verzeichnis der Verarbeitungstätigkeiten

1. Einführung

In diesem Kapitel lernen Sie...

- Die geschichtliche Entwicklung vom Bundesdatenschutzgesetz zur Datenschutzgrundverordnung.
- Worum es beim Datenschutz überhaupt geht.
- Was Daten sind und wo Unternehmen/Vereine überall mit Daten in Berührung kommen.

Die Datenschutzgrundverordnung

Kaum ein anderes Gesetz sorgt für so viel Chaos, Frust und Unverständnis. Dabei ist das Recht, welches mit diesem Gesetz gestärkt werden soll, nicht neu. Es geht um den Schutz der privaten Daten eines jeden Bürgers. Das bisherige Bundesdatenschutzgesetz (BDSG) hat dieses Recht der Bürger schon 1977 [1]sehr ernst genommen. Die gesetzlichen Forderungen der EU-Datenschutzgrundverordnung (EU-DSGVO), welche die Unternehmen zum Umdenken bewegen sollen, sind auch zu großen Teilen Bestandteil der Rechte von 1977. Bereits in der ersten Fassung des BDSG ist die Rede von einem Datenschutzbeauftragten, vom Auskunftsrecht oder von komplexen technischen und organisatorischen Maßnahmen (TOMs). Aber wieso sorgt genau jetzt die Neuauflage dieser Rechte für Aufregung? Dafür gibt es viele Gründe. Die Reichweite des Rechts hat sich erhöht. Datenschutz ist nun in der ganzen Europäischen Union und sogar über deren Grenzen hinaus ein schwerwiegendes Recht geworden. Um die Einhaltung des Gesetzes noch stärker überwachen zu können, wurde in den Behörden mehr

Sehr hohe Bußgelder seit der DSGVO.

10 Mio. bzw.
20 Mio. Euro.

[1] Das erste Bundesdatenschutzgesetz ist 1977 in Kraft getreten.

Personal eingestellt. Und nicht zuletzt sind die Strafen[2] immens gestiegen.

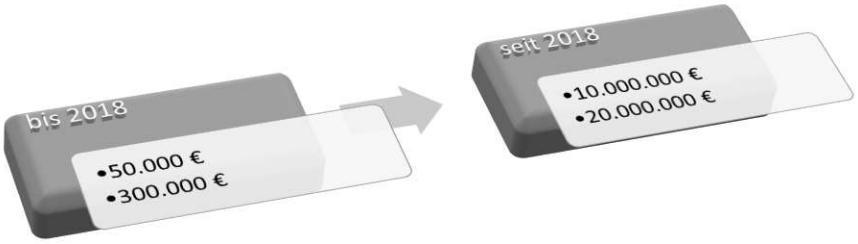

Abbildung 1: Bußgeldhöhe vor 2018 und nach 2018

1.1 Die geschichtliche Entwicklung

Das Bundesdatenschutzgesetz, in der Fassung von 1977, umfasste noch lange nicht so viele Forderungen und Regelungen wie jetzt. Aber schon damals hat die Regierung die Notwendigkeit zum Schutz der Bürger erkannt. Der Grundgedanke das Datenschutzes wurde aus dem **Grundgesetz** (GG) abgeleitet, in dem es heißt:

Art. 1 Abs. 1 Grundgesetz

„Die Würde des Menschen ist unantastbar."

Art. 2 Abs. 1 Grundgesetz

„Jeder Mensch hat das Recht auf die freie Entfaltung seiner Persönlichkeit..."

[2] Siehe auch Kapitel 6.5

Darin steckt das (ungeschriebene) höchstpersönliche

Recht eines jeden Bürgers auf

i**nformationeller Selbstbestimmung**

und das Persönlichkeitsrecht.

Wie das Persönlichkeitsrecht genau geschützt wird, was Unternehmen, Vereine oder Behörden mit den Daten der Bürger tun dürfen und was nicht, das regelt das BDSG bereits seit 1977.

Das informationelle Selbstbestimmungsrecht besagt, dass jeder Bürger über die Preisgabe ihn betreffender persönlicher Informationen grundsätzlich frei entscheiden darf.

Aufgrund des Prinzips des Föderalismus in Deutschland können die einzelnen Bundesländer eigene **Landesgesetze** erlassen. Diese wiederum dürfen weder gegen Bundesgesetze, das Grundgesetz oder Europarecht verstoßen. Jedes Bundesland für sich hat ein eigenes Landesgesetz für den Datenschutz (LDSG) z.B. Bayerisches Datenschutzgesetz, Thüringer Datenschutzgesetz. Das Landesdatenschutzrecht spielt vor allem für öffentliche Stellen (Gemeinde, Landratsamt, Agentur für Arbeit usw.) eine wichtige Rolle und muss durch die zuständigen Datenschutzbeauftragten berücksichtigt werden.

BDSG regelt den Datenschutz innerhalb Deutschlands und für Bundebehörden. LDSG regeln den Datenschutz für öffentliche Stellen innerhalb des Bundeslandes.

1995 versuchte die Europäische Union (EU) eine einheitliche Regelung für den Umgang mit persönlichen Daten in der gesamten Union zu schaffen. Dazu wurde die EU-Richtline 95/46/EG verabschiedet. Inhaltlich ähnelt diese Richtlinie unserem alten BDSG in der Ausführung von 1995. Eine Richtlinie der EU ist aber nicht automatisch für alle Mitgliedsländer bindend. Die EU fordert mit einer Richtlinie alle Mitgliedsstaaten dazu auf, die Inhalte in nationalen Gesetzen umzusetzen so z.B. für Deutschland im BDSG, im Kunsturhebergesetz (KunstUrhG), im Telemediengesetz (TMG), im Personalausweisgesetz (PAuswG) u.v.a. geschehen.

EU-DSRL
=
Datenschutz-richtlinie von 1995
=
Richtline 95/46/EG

Zwischenzeitlich wurde die Richtlinie erweitert. So wurde in der Union erkannt, dass die neuen Techniken, der Onlinehandel, Daten im Internet, künstliche Intelligenz oder internetfähige Geräte zu einer neuen Betrachtung des bisherigen Datenschutzes führen muss. Deshalb wurde 2002 die EU-Datenschutzrichtlinie 95/46/EG (EU-DSRL) um die E-Privacy Richtlinie erweitert/novelliert. Diese Richtlinie sollte ebenfalls angepasst und am 25.05.2018 als Verordnung in Kraft treten. Eine Einigung konnte aber nicht pünktlich erzielt werden.

2009 hat die Union noch einmal Veränderungen an der EU-DSRL vorgenommen und die sogenannte Cookie-Richtlinie hinzugefügt. Diese fordert z.B. die Webseitenbetreiber im Internet auf, Kunden/User der Webseite auf genutzte Cookies hinzuweisen. Diese Richtlinie der EU wurde in Deutschland nur teilweise umgesetzt. Eine weitere Umsetzung wurde zunächst nicht angestrebt.

Eine EU-Richtlinie muss zunächst in nationales Recht umgesetzt werden. Eine EU-Verordnung gilt unmittelbar (sofort, direkt) für alle Mitgliedstaaten.

Der Vorstoß der EU eine einheitliche Regelung zum Datenschutz in allen Mitgliedstaaten zu bewirken hat leider nur bedingt zur gewünschten Umsetzung geführt. Daher kam es in der EU im Jahr 2013 zu einem ersten Entwurf für eine Datenschutz-Grundverordnung. Der letzte Entwurf wurde dann schließlich nach langen Abstimmungsprozessen 2016 verabschiedet. Nach der Veröffentlichung im Amtsblatt der EU am 4. Mai 2016 trat die EU-DSGVO am 24. Mai 2016 in Kraft. Um allen Mitgliedsstaaten, deren Unternehmen und Behörden noch eine Übergangfrist zu gewähren wurde die EU-DSGVO erst ab den 25. Mai 2018 gültig.

Expertenwissen.

Wie wirken Verordnungen und Richtlinien?

Die EU-Kommission kann Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen erlassen.

Diese verschiedenen Rechtsakte haben unterschiedliche rechtlichen Bindungscharakter.

Verordnungen
gelten direkt in allen EU-Mitgliedstaaten, sobald sie im EU-Amtsblatt veröffentlicht werden. Sie sind für alle Mitgliedstaaten und deren Behörden verbindlich und benötigen keine zusätzliche nationale Umsetzung. Eine Verordnung ist ein Gesetz auf europäischer Ebene. Wenn eine Verordnung mit einem nationalen Gesetz in Konflikt steht, hat die Verordnung Vorrang. Ein Beispiel für eine Verordnung ist die DSGVO.
Richtlinien
setzen ein Ziel und einen Zeitrahmen für dessen Umsetzung fest und müssen von den Mitgliedstaaten in nationales Recht umgesetzt werden. Die Inhalte der Richtlinie sind meist nur grob beschrieben. Die Mitgliedsländer müssen die groben Ziele mittels eigener Gesetze konkretisieren. Deshalb wirkt eine Richtlinie nicht wie ein Gesetz. Die Umsetzungsfrist ist in der Richtlinie angegeben. Ein Beispiel ist die EU-Richtlinie 95/46/EG (Datenschutzrichtlinie. Richtlinien wirken nicht automatisch, sondern müssen durch nationale Gesetze verbindlich gemacht werden (mit Ausnahmen in besonderen Fällen).
Beschlüsse
regeln konkrete Sachverhalte und können, ähnlich wie Richtlinien, Verpflichtungen für einen Mitgliedstaat enthalten. Diese müssen ebenfalls durch nationale Gesetze umgesetzt werden, um verbindlich zu sein.

Eine Rechtsakt ist ein allgemeiner Begriff für Schriftstücke, die eine Rechtslage beschreiben. Manche Rechtsakte sind Gesetze und manche sind nur Beschlüsse.

Empfehlungen und Stellungnahmen
sind nicht verbindlich und auferlegen den Empfängern keine Rechte oder Pflichten. Sie helfen beim Verständnis der gesetzlichen Regelungen und beinhalten oft Konkretisierungen oder Anwendungsbeispiele. Im Datenschutz werden derartige Beschlüsse, Stellungnahme und Empfehlungen häufig durch den EDSA oder die DSK erstellt.

Zwischen 2021 und 2024 hieß das Gesetz „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG).

Ergänzend zur DSGVO wurden einige datenschutzrechtliche Regelungen auf nationaler Ebene in einem neuen Bundesdatenschutzgesetz festgehalten.
Am 20.05.2021 wurden letztendlich die übrigen Anforderungen der EU-Privacy-Richtlinie im neuen Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umgesetzt.

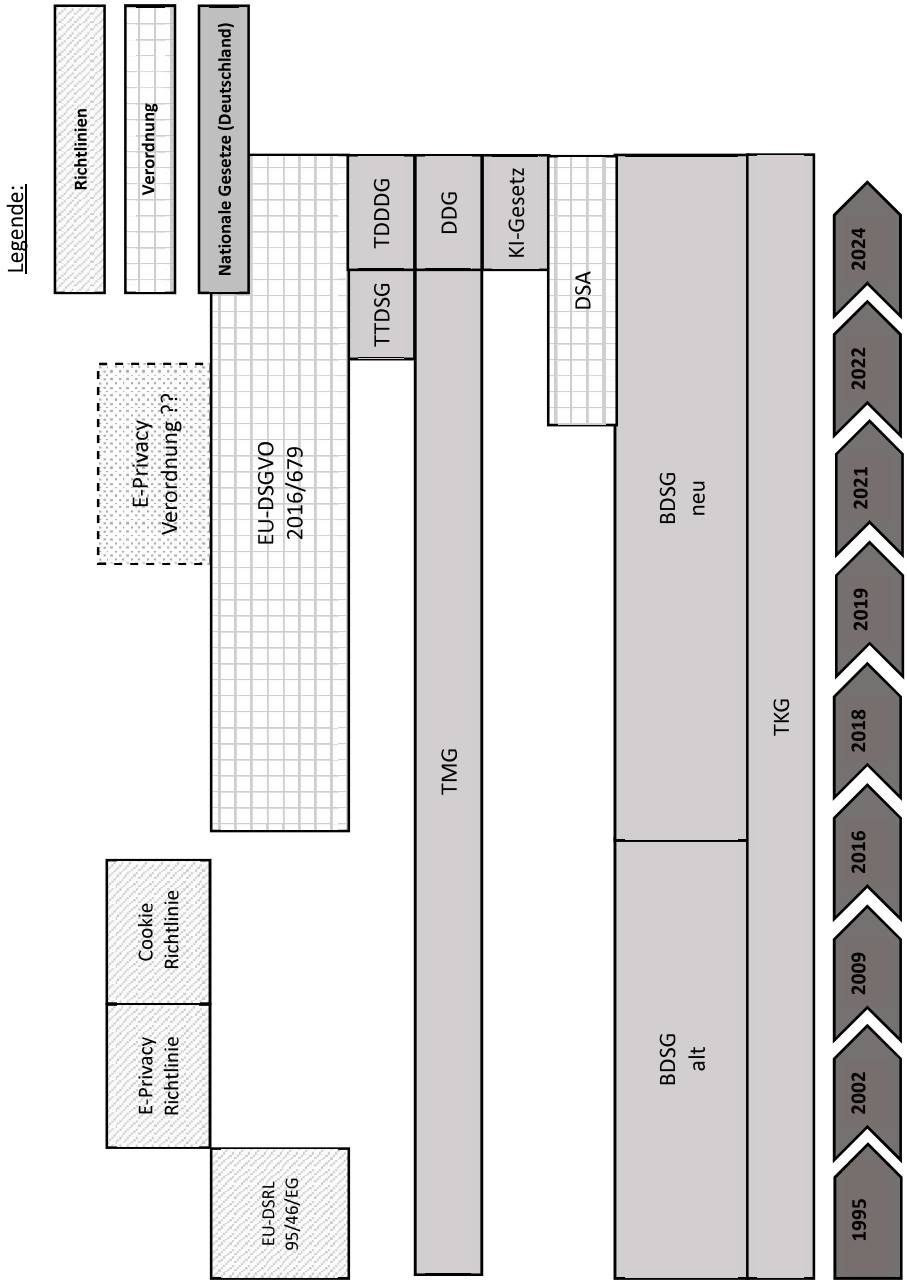

Abbildung 2: Zeitliche Entwicklung des Datenschutzrechtes

Das TTDSG trat zum 01.12.2021 in Kraft und ergänzt das neue Telemediengesetz, das BDSG und die DSGVO.

Viele Änderungen in den letzten Jahren

Die EU hatte 2022 beschlossen eine zusätzliche **Verordnung** „Digital Service Act" (DSA) – „Gesetz[3] über digitale Dienste" zu erlassen. Ziel der Verordnung war die Schaffung eines sicheren und verantwortungsvollen Online-Marktes. Die Verordnung ist seit 17.02.2024 vollumfassend anzuwenden. Ähnlich wie bei der DSGVO mussten die Mitgliedsländer der EU einige Anforderungen aus dem DSA in nationales Recht überführen. Dazu hat die Bundesregierung das neue **Digitale-Dienste-Gesetz** (DDG) erlassen, welches am 14.05.2024 in Kraft getreten ist. Das Gesetz dient der Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und Suchmaschinen. Es gilt für viele digitale Dienste z.B. Apps, Onlineshops oder auch Webseiten. Die frühere Impressumspflicht aus dem TMG ging in das DDG über. Im § 5 DDG ist die bekannten Impressumspflicht fast wortgetreu aus dem TMG zu finden.
Das **TMG** ist gleichzeitig außer Kraft getreten. Die übrig gebliebenen Reglungen wurden in das Digitale-Dienste-Gesetz übernommen.

Wir haben in der EU seit einigen Jahren einen einheitlichen Binnenmarkt für Waren und Dienstleistungen. Das bedeutet, dass Produkte ohne Beschränkungen und Zöllen die Grenzen innerhalb der EU passieren können. Nur die Daten durften bis 2018 die Grenzen nicht überschreiten. Erst die DSGVO hat dies möglich gemacht. Im Zeitalter der Digitalisierung war dieser Schritt längst nötig. Mit dem Gesetz über digitale Dienste wurde der Datenaustausch einheitlich reguliert und der Verbraucher ist bei

[3] Übersetzung „Gesetz über digitale Dienste". Dennoch handelt es sich um eine Verordnung. Nähere Erläuterungen finden Sie im Lehrbuch Teil 2 Kapitel 7.

der Nutzung digitaler Dienste (z.B. Social Media, Onlineplattformen) besser geschützt.

Zum 13.05.2024 wurde das TTDSG in das **TDDDG** - Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz umbenannt.

Neu: TDDDG, DDG und KI-Gesetz

TMG ist außer Kraft getreten.

Neben den Änderungen zum TMG und TKG ist am 1. August 2024 die neue **KI-Verordnung** (KI-Act, KI-Gesetz) in Kraft getreten. Diese Verordnung zielt darauf ab, die Regelungen zum Umgang mit künstlicher Intelligenz innerhalb der EU zu vereinheitlichen. Ähnlich wie bei der DSGVO hat die EU auch hier einen Umsetzungsspielraum von zwei Jahren eingeräumt. Die ersten Maßnahmen müssen daher bis August 2026 umgesetzt sein.

Inwieweit die neuen Gesetze die Arbeit des Datenschutzbeauftragten tangieren, bleibt noch abzuwarten.

Trotz der vielen Regelungen in Verordnungen, Richtlinien und Gesetzen gibt es genügend Lücken im Datenschutzrecht. Diese Lücken werden dann häufig durch Richterrecht (Urteile) oder Stellungnahmen, Empfehlungen und Whitepaper des Europäischen Datenschutzauschusses (EDSA) geschlossen. Aber auch die deutschen Aufsichtsbehörden teilen über Pressemeldungen ihre Ansichten und Interpretationen, die den Anwendern des Datenschutzrechtes etwas mehr Sicherheit geben sollen.

Nach der Veröffentlichung im Amtsblatt der EU am 4. Mai 2016 trat die EU-DSGVO am 24. Mai 2016 in Kraft. Um allen Mitgliedsstaaten, deren Unternehmen und Behörden noch eine Übergangfrist zu gewähren wurde die EU-DSGVO erst ab den 25. Mai 2018 gültig.

Art. 99 DSGVO

1. Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

2. Sie gilt ab dem 25. Mai 2018.

EU Datenschutzgrundverordnung

- 24.05.2016 Inkrafttreten
- 25.05.2018 Gültigkeit

Bundesdatenschutzgesetz

- neu vom 24.02.2017
- 25.05.2018 Gültigkeit

Als Datenschutzbeauftragter müssen Sie sowohl die Regelungen der DSGVO als auch des BDSGs berücksichtigen.

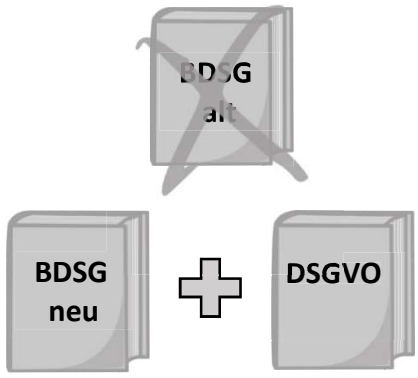

Abbildung 3: Zusammenhang der Datenschutzgesetze

Für die Sicherstellung des Datenschutzes in Unternehmen, Behörden oder Vereinen ist es also wichtig die grundlegenden Gesetze wie die DSGVO und das BDSG (neu) einzuhalten.

Weniger als die Hälfte der Paragrafen und Artikel sind für die Tätigkeit als Datenschutzbeauftragter wesentlich. Die übrigen Inhalte regeln die Aufgaben der Aufsichtsbehörden oder anderer Personen und Institute.

Gesetz	Anzahl der Paragrafen/Artikel	Anzahl der relevanten Paragrafen/Artikel
DSGVO	99	ca. 40
BDSG	85	ca. 16

In den folgenden Kapiteln werden wir uns den relevanten Paragrafen und Artikeln im Einzelnen widmen.

1.2 Was sind Daten?

Daten = allgemeine Angaben oder Informationen zu Messungen, Beobachtungen oder Befunden.

„Daten sind das Gold von Morgen".

Alle Einrichtungen sammeln über Menschen täglich, minütlich, sekündlich ... eine unendliche Anzahl von Daten. Daten begegnen uns den ganzen Tag zum Beispiel in der Buchhaltung, im Marketing, in der Verwaltung, in der Post, beim Arzt, beim Einkaufen, in der Schule u.v.m.
Und überall dort erzeugen wir wieder neue Daten, besonders im Zuge der zunehmenden Digitalisierung und des „Internets of Things" (IoT). Mit unserem Smartphone können Einkäufe getätigt, das Licht und die Heizung gesteuert werden und Autos werden zunehmend autonomer. Die Datenflut nimmt zu und das Interesse an einem Missbrauch der Daten wächst täglich.

BIG DATA

Big Data ist nichts anderes als die Sammlung all der erzeugten Daten. Die Einrichtungen haben die Daten entweder irgendwo gespeichert oder teilen Ihre Daten mit anderen Einrichtungen. Viele dieser Datenbanken stehen im ständigen Austausch oder werden regelmäßig von Unternehmen und Einrichtungen genutzt. Durch das Verknüpfen dieser Daten entstehen dann ganze Profile von unseren Mitmenschen. Mit diesen Profilen können Unternehmen sehr viel Geld verdienen, indem Marketingmaßnahmen (z.B. Werbung) speziell auf ein Profil zugeschnitten werden.

Sie sehen in dem Schaubild wie die einzelnen Einrichtungen (Apotheke, Onlinebank, Gemeinde und Pflegeheim) Daten von Herrn Müller sammeln. Das Speichern dieser Daten ist für diese Einrichtungen enorm wichtig und dient grundsätzlich der Verwaltung und Sicherstellung von Servicediensten.

Diese Daten können nun aufgrund der Gemeinsamkeit des Namens zu einem gesamten Profil zusammengefasst werden.

So können z.B. Kreditinstitute diese Daten kaufen und Herrn Müller regelmäßig ein verlockendes Kreditangebot zukommen lassen. Herr Müller könnte einen Kredit sicherlich gut gebrauchen, zumal die Überziehungszinsen oft teurer sind als die angebotenen Kreditzinsen. Diese Werbemaßnahme funktioniert allerdings nicht zwangsläufig bei Mitmenschen, die gerade im Lotto gewonnen haben oder aufgrund einer Erbschaft sehr viel Geld auf einem Konto haben. Daher macht es sich für die Unternehmen durchaus bezahlt maßgeschneiderte Werbemaßnahmen zu nutzen. Dazu müssen die Unternehmen aber erst einmal ihre potenziellen Kunden kennen. Und dazu nutzen sie Big Data.

Sämtliche Einrichtungen füttern diese riesigen Datenbanken immer weiter (legal oder illegal) und nutzen natürlich auch die daraus resultierenden Profile.

Fallbeispiel 1

Was weiß man nun alles über Herrn Müller?

Herr Josef Müller ist am 05.08.1960 geboren und Sohn von Gerda Müller, die aktuell in einem Pflegeheim untergebracht ist. Wir kennen seine Telefon-nummer (Pflegeheim) und seine Anschrift (Gemeinde).

Offensichtlich muss Herr Müller für die Pflege der Mutter allein aufkommen (Onlinebanking), was regelmäßig ein großes Loch in seine Finanzkasse reißt (aktuell - 1.261 €). Ohne den Pflegeaufwand hätte Herr Müller keinen Verlust auf seinem Bankkonto zu verzeichnen. Herr Müller ist verheiratet mit Elfriede Müller und er hat vermutlich ein Auto (Abbuchung Tankstelle).

Wir kennen nun aber auch ein paar sensible Daten:
Herr Müller geht regelmäßig in die Apotheke und besorgt Medikamente, auch für seine kranke Mutter, die offensichtlich an einem Tumor leidet (Pflegeheim).

Da sich Herr Müller auch Blutdruckmedikamente in der Apotheke besorgt hat, haben vermutlich er oder seine Ehefrau ein Leiden mit dem Blutdruck.

Die Lösung liegt also nahe. Die Gesetzgeber und die Europäische Union haben schon frühzeitig die Tücken dieser Datensammelwut einiger Einrichtungen erkannt. Jedes Unternehmen, jede Behörde, jeder Verein, jede Arztpraxis, jeder Supermarkt, ... letztlich alle Datensammler füttern das BIG DATA immer weiter. An sich ist das nicht verwerflich. Nur wie mit diesen Daten umgegangen wird, wer sie alles erhält und dass diese Daten kaum geschützt werden, dass ist sehr wohl verwerflich. Über die

Konsequenzen macht sich kaum eine Privatperson Gedanken, geschweige denn die Datensammler selbst. Meist sind die Auswirkungen auch noch gar nicht abschätzbar. Hier noch ein banales, aber reales Beispiel, was das Ergebnis dieser BIG DATA Ansammlungen sein kann. Diese Geschichte war auch die Grundlage des o.g. Fallbeispiels.

Ein treuer Bürger hatte nach vielen Jahren harter Arbeit seinen Job nicht mehr ausüben können. Zu allem Übel litt seine Mutter an einer Tumorerkrankung und befand sich seit vielen Monaten in einem Krankenhaus und musste dort gepflegt werden. Darunter litt natürlich auch die Gesundheit des Mannes. Glücklicherweise hatte er schon sehr früh das Risiko einer Berufsunfähigkeit erkannt und eine entsprechende Versicherung abgeschlossen. Nachdem er keine andere Wahl hatte, stellte er einen Antrag bei der Versicherung auf Zahlung der regelmäßigen Berufsunfähigkeitsrente. Dieser Antrag wurde prompt von der Versicherung abgelehnt, mit der Begründung, dass falsche Angaben bei der damaligen Gesundheitsprüfung gemacht wurden.

Die Existenz dieses Mannes war bedroht. Er hatte scheinbar an alle Risiken gedacht und jahrelang seine Versicherungsbeiträge bezahlt und steht nun ohne Unterstützung da. Vernünftiger Weise suchte sich der Mann Hilfe bei einem Anwalt. Der Anwalt beantragte Akteneinsicht und das Trauerspiel kam zum Vorschein.

Die Begründung der Versicherung beruhte auf verschiedenen Ergebnissen aus diversen Datensammlungen, die sie nutzten. Sie hatten Erkenntnisse darüber, dass der Mann regelmäßig Tumormedikamente in einer Apotheke besorgte. Zudem hatten sie Lokalisationsdaten erhalten, die zeigten, dass er sich regelmäßig im Krankenhaus aufhielt.
Die Zusammensetzung der diversen Daten ließ sie zu dem Schluss kommen, dass der Mann an einem Tumor

litt, und zwar seit mehreren Jahren. Diese vermutliche Tumorerkrankung hatte er bei der Gesundheitsprüfung nicht angegeben.
Erfreulicherweise konnte man die Missverständnisse schnell aufklären und der Mann erhielt seine ihm zustehende Berufsunfähigkeitsrente.

Es passiert mehrmals täglich, dass Daten über uns ausgewertet werden und Entscheidungen darauf beruhen, die nicht immer zu unseren Gunsten ausfallen. Diese Entscheidungen bekommen wir häufig gar nicht mit. Oder wussten Sie, dass Ihnen im Internet aufgrund Ihres Profils ganz andere Preise angezeigt werden als z.B. Ihrem Nachbarn?
Und wer sagt denn nun, dass all diese Daten richtig sind oder richtig interpretiert werden? Diese Gefahren wurden alle erkannt. Traurigerweise nicht von den Bürgern, sondern von einigen Abgeordneten der Partei „Bündnis 90/die Grünen“. Diese Abgeordneten haben hart für die Bürgerrechte vor dem Europäischen Parlament gekämpft. Hier ging es eben um das Recht, dass Bürger selbst entscheiden dürfen, wenn es um Ihre Daten geht und nicht irgendwelche Unternehmen oder Einrichtungen. Zu diesem Zeitpunkt ist das Recht auf informationelle Selbstbestimmung geboren und der Startschuss für die DSGVO gefallen.

Wer sich genauer mit den Datenschutzgesetzen auseinander setzt, wird aber merken, dass diese Gesetze in erster Linie eine Menge an Auflagen und Pflichten für die Unternehmen und Einrichtungen beinhalten. Wo geht es da um den Schutz der Bürger? Die Abgeordneten haben erkannt, dass die Bürger (egal in welchem Mitgliedsland) sich kaum für den Schutz Ihrer Daten interessieren. Es geht auch nicht um Geld, Steuern oder sonstige offensichtliche Einschränkungen. Den Bürgern sind die Konsequenzen aus ihrem unbedarften Handeln mit ihren Daten schlichtweg nicht bekannt. Zudem scheinen die Auswirkungen surreal und viel zu weit weg.

Informative Filmempfehlung:

DEMOCRACY - Im Rausch der Daten von David Bernet

Leider gehen nur wenige Bürger umsichtig und zurückhaltend mit ihren Daten um. Kaum ein Nutzer wird skeptisch, wenn er im Internet nach seiner E-Mail-Adresse, seinem Lieblingstier oder nach dem Wohnort gefragt wird. Über Social-Media-Kanäle werden pausenlos private Informationen preisgegeben und mit der ganzen Welt geteilt, ohne sich darüber bewusst zu sein, dass all diese Daten gegen die eigene Person erpresserisch verwendet werden können. So wie im Fallbeispiel gibt es tagtäglich Einrichtungen die unsere Daten liebend gern auswerten und verwenden, und da steckt immer eine Absicht dahinter. Häufig liegen die Absichten aber zu großen Teilen im Interesse dieser Einrichtung und nicht im Interesse der Nutzer. Das Datensammeln und Auswerten ist ein Geschäftsmodell geworden. Deshalb sind die Daten das „Gold von Morgen“.

Preise für Daten aus dem Darknet

Spotify Mitgliedschaft	2,00 €
Netflix Abo	3,00 €
Kreditkartennummer	27,00 €
Kreditkarte + Geburtsdatum	32,00 €
PayPal Kontodaten + Kreditkartendaten + Bankdaten	180,00 €

Tabelle 1: Preisübersicht gestohlener Daten im Darknet

Die Daten stammen aus einem Report den McAfee zur Aufklärung ihrer Kunden veröffentlicht hat (siehe „The Hidden Data Economy[4]“).

Auch wenn der Bericht schon etwas älter ist (2013), ist die Tatsache, dass Daten wertvolle Ware sind, immer noch gegeben. Jeder könnte im Darknet also einfach Kreditkartendaten kaufen und damit shoppen gehen. Natürlich sind das Kaufen und Verkaufen illegal. Aber Sie sehen, diese Daten haben einen entsprechenden Wert und Hacker verdienen mit dem Diebstahl dieser Daten Geld.

Die unbedarften Aussagen und oft gehörte Fragen einiger unwissender Mitmenschen...

[4] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf

... zeigen also sehr deutlich, dass das Europäische Parlament klug gehandelt hat und den unbedachten Bürger schützen muss, weil er es selbst offenbar nicht kann. Also hat man den Unternehmen und Einrichtungen die Verantwortung übertragen mit den Daten ihrer Kunden, Patienten, Schüler und Bürger umsichtig umzugehen.

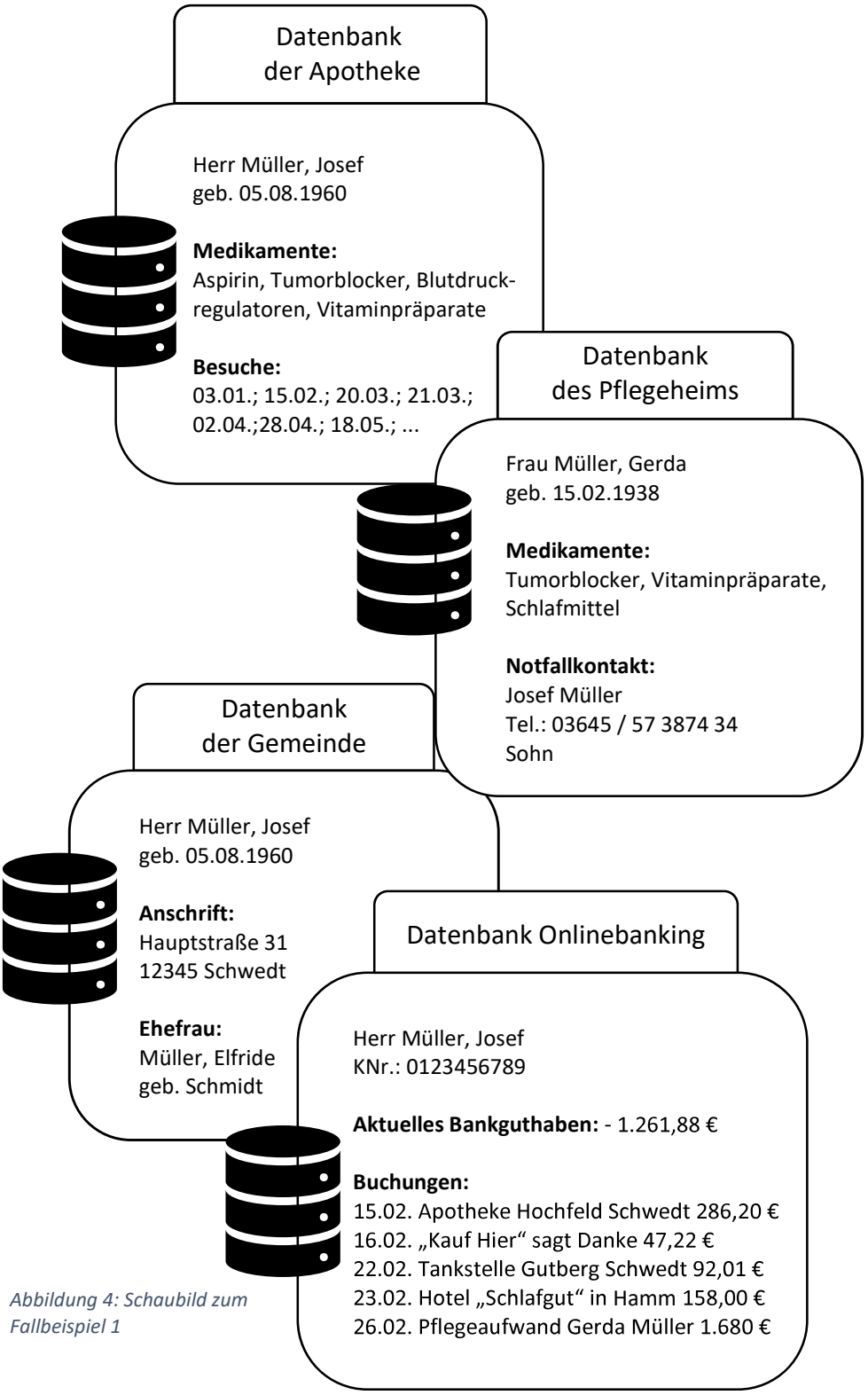

Abbildung 4: Schaubild zum Fallbeispiel 1

1.3 Datenschutz vs. Datensicherheit

Die DSGVO hat sich sowohl dem Datenschutz als auch der Datensicherheit gewidmet. In den verschiedenen Artikeln der Verordnung werden entsprechende Maßnahmen gefordert, die beide Bereiche gleichermaßen betreffen. Was ist aber nun der Unterschied?

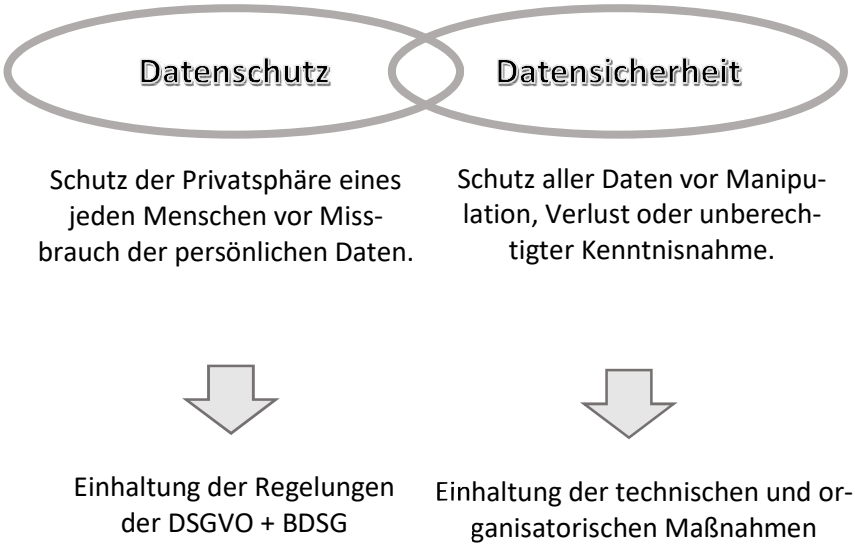

Abbildung 5: Unterschied Datenschutz und Datensicherheit

Beim **Datenschutz** geht es grundsätzlich nur um die privaten Daten einer natürlichen Person. Diese sollen um jeden Preis geschützt werden, von jeder Einrichtung, die diese Daten besitzen. Die Verantwortung wird per Gesetz auf jede Einrichtung übertragen. Wie diese Daten zu schützen sind bzw. was der Gesetzgeber konkret unter diesem Schutz versteht ist in den Artikeln der DSGVO konkret geregelt. Es geht also z.B. darum, dass die Einrichtungen erst einmal prüfen müssen, ob sie die persönlichen Daten der Menschen überhaupt besitzen dürfen. Dann geht es aber auch darum Abläufe zu realisieren, die ein regelmäßiges Aktualisieren oder Löschen der Daten sicherstellen. Zudem müssen einige Einrichtungen einen

Datenschutzbeauftragten benennen, der die Umsetzung der Regelungen der DSGVO überwacht. Es gibt also zahlreiche Schritte, bis zur vollumfänglichen Umsetzung des Datenschutzes.

Bei der **Datensicherheit** geht es nicht konkret um die persönlichen Daten der Mitmenschen. Es geht um alle Daten, die eine Einrichtung besitzt. Also auch z.B. Produktdaten, Entwicklungsdaten, Unternehmensdaten, usw.
Um diese Daten vor Manipulation, Verlust oder unberechtigter Kenntnisnahme zu schützen, müssen Unternehmen zahlreiche Sicherheitsvorkehrungen treffen. Die Einsicht seine Daten vor dem Wettbewerber zu schützen ist schon lange bei allen Unternehmen angekommen. Hier wird schon immer viel Wert auf die sogenannten Betriebsgeheimnisse gelegt. Die DSGVO fordert aber auch, persönliche Daten von Kunden, Lieferanten und Mitarbeitern durch technische und organisatorische Maßnahmen (Sicherheitsvorkehrungen) entsprechend zu sichern.
Letztlich gehen Datenschutz und Datensicherheit Hand in Hand.

1.4 Datenflüsse in Unternehmen

Die erste Aufgabe jedes Datenschutzbeauftragten ist es, sämtliche Datenflüsse in der Einrichtung zu analysieren. Um alle Forderungen der DSGVO umsetzen zu können, muss erst einmal eine Bestandsaufnahme aller Daten gemacht werden.

Welche Daten werden WO, von WEM, WOZU, WANN, WIE LANGE erfasst und wo fließen die Daten als nächstes hin?