

Nicolas Nagel

Praxishandbuch Datenschutz

Leitfaden zur DSGVO für Juristen und Laien

Impressum

Praxishandbuch Datenschutz

Leitfaden zur DSGVO für Juristen und Laien

1. Auflage 2019

ISBN 978-3-903255-05-0

Autor: Univ. Lekt. Nicolas Nagel, CIPP/E, CIPM, FIP, CDPO

Medieninhaber

TÜV AUSTRIA AKADEMIE GMBH

Leitung: Mag. (FH) Christian Bayer, Rob Bekkers, MSc BSc

2345 Brunn am Gebirge, TÜV AUSTRIA-Platz 1

Tel.: +43 5 0454-8000

E-Mail: akademie@tuv.at | www.tuv-akademie.at

Produktionsleitung: Mag. Judith Martiska

Layout, Satz & Grafiken: Markus Rothbauer, office@studio02.at,

Lukas Drechsel-Burkhard, lucdesign

Herstellung: Druckwelten, www.druckwelten.at

Cover: Adobe Stock

© 2019 TÜV AUSTRIA AKADEMIE GMBH

Das Werk ist urheberrechtlich geschützt. Alle Rechte, insbesondere die Rechte der Verbreitung, der Vervielfältigung, der Übersetzung, des Nachdrucks und der Wiedergabe bleiben – auch bei nur auszugsweiser Verwertung – dem Verlag vorbehalten.

Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Medieninhabers reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Trotz sorgfältiger Prüfung sämtlicher Beiträge in diesem Werk sind Fehler nicht auszuschließen. Die Richtigkeit des Inhalts ist daher ohne Gewähr. Eine Haftung des Herausgebers oder der Autoren ist ausgeschlossen.

Zur leichteren Lesbarkeit wurde die männliche Form gewählt. Selbstverständlich gelten alle Formulierungen für Männer und Frauen in gleicher Weise.

Vorwort

Liebe Leserinnen, liebe Leser,

die europäische Datenschutzgrundverordnung (DSGVO) gehört zu der bedeutendsten Gesetzesentwicklung der Europäischen Union in den letzten Jahren. Mit Stichtag 25. Mai 2018 wurden durch sie die nationalen Datenschutzgesetze abgelöst und musste sodann auch in Österreich und Deutschland unmittelbar angewendet werden.

Aber was wird sich damit für Unternehmen ändern?

Wie wird sich die Datenschutzgrundverordnung auf die vielen alltäglichen Datenverarbeitungen und Unternehmensabläufe konkret auswirken – und zwar europaweit, von Brüssel über Wien und Lissabon bis nach Warschau?

Wie immer bei gesetzlichen Neuerungen ist anfangs vieles unklar und es gibt viele offene Fragen – dieses Praxishandbuch liefert Ihnen dazu erste Antworten und Analysen, wie Datenverarbeitungen und Prozesse in diesem Bereich künftig vonstattengehen werden/müssen/sollten/können.

Checklisten, konkrete Beispiele, Übungen und Muster helfen Ihnen dabei, die DSGVO in Ihrem Unternehmen umzusetzen.

Sie, liebe Leserinnen, liebe Leser, finden hier hoffentlich für Sie hilfreiche Tipps und konkrete Hilfestellungen, wie Sie künftig personenbezogene Daten von Kunden, Geschäftspartnern, Lieferanten und deren Mitarbeitern sowie Ihren eigenen Mitarbeitern gesetzeskonform verarbeiten können.

Abschließend sei angemerkt, dass es sich dabei um Empfehlungen und oftmals um meine persönliche Sichtweise aus meinen bisherigen Erfahrungen und um keine abschließenden Anweisungen handelt. Dieses Buch soll letztendlich ein praktisches Hilfsmittel sein, damit Sie rasch und unkompliziert die neuen gesetzlichen Regelungen anwenden können.

Da der Datenschutz ein schnelllebiger und sich rasch verändernder Bereich ist, der stetigen Weiterentwicklung unterliegt und Entscheidungen der Behörden und Gerichte fortlaufend nun zu erwarten sind, ist es ratsam sich weiterhin intensiv und kontinuierlich mit der Datenschutz-Grundverordnung zu beschäftigen und – wo notwendig – professionelle Unterstützung zu Rate zu ziehen.

Zu guter Letzt gilt mein besonderer Dank meiner Familie, insbesondere meiner Frau Tanja und meinem kleinen Sohn Jonas, die stets verständnisvoll die Zeit mit ihrem Mann bzw. Papa während des Entstehens dieses Buches, das ich ihnen hiermit auch widmen möchte, entbehrt haben.



Univ. Lekt. Nicolas Nagel, CIPP/E, CIPM, FIP, CDPO
Head of Data Protection TÜV AUSTRIA GROUP
Senior Consultant für Datenschutz & externer Datenschutzbeauftragter
Wien, im Januar 2019

WIDMUNG

für
meine liebe Frau
Tanja
und
meinen bezaubernden Sohn
Jonas

Inhaltsverzeichnis

1 Einleitung	13
2 Welche Gesetze gilt es zu beachten?	14
2.1 Die EU-Datenschutzgrundverordnung (DSGVO)	14
2.2 Das österreichische Datenschutzgesetz „2018“ (DSG 2018)	15
2.3 Das deutsche Bundesdatenschutzgesetz	16
2.4 Das österreichische Telekommunikationsgesetz 2003 (TKG 2003)	16
2.5 Das österreichische Datenschutzgesetz 2000 (DSG 2000)	17
2.6 ePrivacy-Verordnung	17
3 Mythen rund um die DSGVO	19
4 Datenschutz – Worum geht es eigentlich?	23
4.1 Warum ist Datenschutz so wichtig für uns alle?	23
4.2 Datenschutz und Datensicherheit	26
4.3 Datenschutz – etwas gänzlich Neues?	27
5 Thema Strafen: Was habe ich zu befürchten?	29
5.1 Geldbußen	29
5.1.1 <i>Strafrahmen</i>	29
5.1.2 <i>Kriterien für die Strafbemessung</i>	30
5.2 Abhilfemaßnahme abseits von Strafen	31
5.3 Schadenersatz	32
5.4 Haftung	32
5.5 Strafrecht	33
5.6 Präventionsmaßnahmen	33
6 Definitionen und Grundbegriffe	35
6.1 Datenarten	35
6.1.1 <i>Personenbezogene Daten</i>	36
6.1.2 <i>Besondere Kategorien von Daten</i>	36
6.1.3 <i>Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten</i>	37
6.1.4 <i>Anonyme Daten</i>	37
6.1.5 <i>Genetische, biometrische und Gesundheitsdaten</i>	37
6.2 Verarbeitungsbegriffe	38
6.2.1 <i>Verarbeiten von Daten</i>	38

6.2.2	<i>Pseudonymisierung</i>	39
6.2.3	<i>Einschränkung der Verarbeitung</i>	39
6.2.4	<i>Profiling</i>	40
6.2.5	<i>Dateisystem</i>	40
6.3	Akteure im Datenschutz	41
6.3.1	<i>Verantwortlicher</i>	41
6.3.2	<i>Auftragsverarbeiter</i>	41
6.3.3	<i>Betroffene Person</i>	42
6.3.4	<i>Gemeinsame Verantwortliche</i>	42
6.3.5	<i>Dritter</i>	42
6.3.6	<i>Empfänger</i>	42
6.3.7	<i>Aufsichtsbehörde</i>	42
7	Prüfschema Datenschutz	44
8	Prüfpunkt I: Zweckdefinition und Rolle	46
8.1	Datenverarbeitung – Was ist damit gemeint?	46
8.2	Datenschutzrechtliche Rolle	48
9	Prüfpunkt II: Rechtsgrundlagen der Datenverarbeitung	54
9.1	Verarbeitungsverbot als Ausgangslage	54
9.2	Einwilligung	55
9.2.1	<i>Subsidiäre Anwendung</i>	55
9.2.2	<i>Definition</i>	56
9.2.3	<i>Bedingungen einer rechtmäßigen Einwilligung</i>	56
9.2.4	<i>Organisatorische Erfordernisse</i>	60
9.2.5	<i>Sonderregelung zu „elektronischer Post“</i>	61
9.2.5.1	<i>Österreich</i>	61
9.2.5.2	<i>Deutschland</i>	62
9.2.6	<i>Zusammenfassung</i>	64
9.3	Vertragserfüllung und Vertragsanbahnung	65
9.4	Rechtliche Verpflichtung	66
9.5	Lebenswichtige Interessen	66
9.6	Aufgabe im öffentlichen Interesse	67
9.7	Berechtigte Interessen	67
9.8	Rechtsgrundlagen für besondere Kategorien von Daten	68
9.9	Rechtsgrundlage für personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten	70
9.10	Beschäftigtenverhältnis (Deutschland)	71

10	Prüfpunkt III: Datenschutzgrundsätze	77
10.1	Rechtmäßigkeit	78
10.2	Zweckbindung	79
10.2.1	<i>Zweckspezifizierung</i>	79
10.2.2	<i>Verarbeitung für eigene Zwecke</i>	79
10.2.3	<i>Verarbeitung als Dienstleister</i>	80
10.2.4	<i>Weiterverarbeitung für andere Zwecke</i>	80
10.3	Datenminimierung	81
10.4	Prüfpunkt IV: Privacy by Design und Privacy by Default	82
10.4.1	<i>Privacy by Design (Datenschutz durch Technikgestaltung)</i>	82
10.4.2	<i>Privacy by Default (Datenschutzfreundliche Voreinstellungen)</i>	84
10.4.3	<i>Praktische Relevanz und Anwendung der Grundsätze</i>	84
10.5	Richtigkeit	85
10.6	Speicherbegrenzung	86
10.7	Integrität und Vertraulichkeit	88
10.8	Rechenschaftspflicht	89
11	Datenschutzmanagementsystem (DSMS)	96
11.1	Allgemein	96
11.2	Ziele	97
11.3	Implementierung	97
11.4	Inhalte	99
12	DSGVO-Implementierungsprojekt	101
12.1	Management Commitment und Ressourcen	101
12.2	Projektteam bilden	102
12.3	Initiale Schulung	105
12.4	Datenschutzorganisation etablieren	105
12.4.1	<i>Aufbau und Struktur</i>	105
12.4.2	<i>Interner Datenschutzausschuss</i>	106
12.4.3	<i>Internes Datenschutz-Wiki</i>	108
12.5	Status Quo feststellen	109
12.6	GAP-Analyse durchführen	114
12.7	Anpassungs- und Umsetzungsmaßnahmen abarbeiten	114
12.8	Übersicht DSGVO-Implementierungsprojekt	115
12.9	Laufenden Compliance-Prozess aufbauen	115
13	Prüfpunkt V: Informationspflichten	117
13.1	Allgemein	117

13.2	Situation neu vs. alt.	118
13.3	Formvorschriften	118
13.4	Datenerhebung bei der betroffenen Person	119
13.4.1	<i>Inhalt</i>	119
13.4.2	<i>Ausnahmen von der Informationsverpflichtung.</i>	121
13.5	Datenerhebung bei einem Dritten.	122
13.5.1	<i>Inhalt</i>	122
13.5.2	<i>Zeitpunkt und Fristen.</i>	123
13.5.3	<i>Ausnahmen von der Informationsverpflichtung.</i>	123
14	Prüfpunkt VI: Betroffenenrechte.	131
14.1	Recht auf Auskunft	131
14.1.1	<i>Auskunftsinhalt</i>	132
14.1.2	<i>Recht auf eine Kopie.</i>	132
14.1.3	<i>Ablauf, Form, Frist und Kosten.</i>	133
14.2	Recht auf Richtigstellung	136
14.3	Recht auf Löschung	137
14.3.1	<i>Wann besteht nun aber das Recht auf Löschung und die Pflicht zur Löschung?</i>	137
14.3.2	<i>Inhalt des Löschungsanspruchs.</i>	138
14.3.3	<i>Ausnahmen</i>	139
14.4	Recht auf Einschränkung	140
14.4.1	<i>Wann besteht das Recht auf Einschränkung?</i>	140
14.4.2	<i>Was nun?</i>	141
14.4.3	<i>Wie „schränkt“ man nun ein?</i>	141
14.5	Recht auf Widerspruch	142
14.5.1	<i>Direktmarketing.</i>	143
14.5.2	<i>Verarbeitung aufgrund „berechtigter Interessen“</i>	143
14.5.3	<i>Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder zu statistischen Zwecken</i>	143
14.6	Recht auf Datenübertragbarkeit	144
15	Prüfpunkt VII: Profiling und automatisierte Entscheidungen	149
15.1	Einschränkung der Anwendung	150
15.2	Ausnahmen.	150
15.3	Bedingungen.	151
15.4	Scoring- und Bonitätsauskünfte	152
15.5	Anwendbarkeit im Alltag	153
16	Verzeichnis von Verarbeitungstätigkeiten (VVV).	159
16.1	Pflicht zum Führen eines Verzeichnisses	159

16.2	Form	160
16.3	Inhalte	161
16.3.1	<i>Verzeichnis von Verarbeitungstätigkeiten (Verantwortlicher)</i>	161
16.3.2	<i>Verzeichnis von Verarbeitungstätigkeiten (Auftragsverarbeiter)</i>	162
17	Datenschutzbeauftragter	164
17.1	Bisherige Ausgangslage	164
17.2	Benennungspflicht nach der DSGVO	164
17.2.1	<i>Behörde</i>	165
17.2.2	<i>Öffentliche Stelle</i>	166
17.2.3	<i>Nicht-öffentliche Stellen (sprich „klassische“ privatrechtliche Unternehmen und Organisationen)</i>	168
17.3	Benennungspflicht nach nationaler Regelung	172
17.3.1	<i>Österreich</i>	172
17.3.2	<i>Deutschland</i>	173
17.4	Freiwillige Benennung	174
17.5	Aufgaben	174
17.6	Bestellung, Rechtsstellung und Sonstiges	176
17.7	Anforderungen an einen Datenschutzbeauftragten	177
17.7.1	<i>Fachlich</i>	177
17.7.2	<i>Persönlich</i>	179
17.8	Externe Benennung	179
17.9	Abschätzung für bestimmte Branchen	181
18	Prüfpunkt VIII: Auftragsverarbeiter	187
18.1	Auswahl eines Auftragsverarbeiters	187
18.2	Auftragsverarbeitervertrag (AVV)	188
18.2.1	<i>Mindestinhalt eines Auftragsverarbeitervertrags</i>	188
18.2.2	<i>Empfehlenswerte Inhalte</i>	189
18.2.3	<i>Sub-Auftragsverarbeiter</i>	189
18.3	Alltag im Unternehmen	190
19	Prüfpunkt IX: Internationaler Datenverkehr	195
19.1	Begriff „Datenübermittlung“	195
19.2	Datenübermittlung in ein „Drittland“	195
19.3	Konsequenz bei Datenübermittlungen in Drittländer	196
19.4	Vorteile gegenüber dem „alten“ Datenschutzgesetz in Österreich	196
19.5	Angemessenheit des Datenschutzniveaus	197
19.5.1	<i>Angemessenheitsbeschluss der EU-Kommission</i>	197
19.5.2	<i>Privacy Shield Framework</i>	198

19.5.3	<i>Binding Corporate Rules (BCRs)</i>	199
19.5.4	<i>Standarddatenschutzklauseln</i>	201
19.6	Ausnahmen.	202
19.7	Alltag im Unternehmen	203
20	Prüfpunkt X: Datenschutz-Folgenabschätzung.	209
20.1	Was ist eine Datenschutz-Folgenabschätzung?	209
20.2	Erstbeurteilung (Schwellenwertanalyse).	209
20.2.1	<i>Allgemein</i>	209
20.2.2	<i>Zwingende Gründe für eine Durchführung</i>	210
20.2.3	<i>Risiken</i>	211
20.2.4	<i>„Blacklists“</i>	211
20.2.5	<i>„Whitelists“</i>	217
20.2.6	<i>Risikoerhöhende Kriterien</i>	221
20.2.7	<i>Bewertungsbeispiele</i>	225
20.3	Ablauf eines Datenschutz-Folgenabschätzungsprozesses	227
20.4	Durchführung einer Datenschutz-Folgenabschätzung.	227
20.4.1	<i>Inhalt</i>	227
20.4.2	<i>Risikoermittlung</i>	228
20.4.3	<i>Fazit</i>	229
20.5	Auswirkungen auf Unternehmen.	229
21	Datenschutzverletzungen und Meldepflichten	234
21.1	Was tun, wenn dann mal doch etwas passiert?	234
21.2	Begriff der Datenschutzverletzung.	234
21.3	Welche Fälle sind zu unterscheiden?	235
21.4	Meldepflichten	235
21.4.1	<i>Auftragsverarbeiter gegenüber dem Verantwortlichen</i>	235
21.4.2	<i>Verantwortliche gegenüber der Aufsichtsbehörde</i>	236
21.4.3	<i>Verantwortliche gegenüber der betroffenen Person</i>	237
21.5	Wie kann ich ein Risiko nun konkret einstufen?	238
21.6	Sonstige Pflichten und Maßnahmen	239
21.7	Typischer Ablauf des Prozesses zu Datenschutzverletzungen	241
21.8	Anwendungsbeispiele	241
22	Fotos und Videos.	247
22.1	Allgemein	247
22.1.1	<i>Anwendbare Rechtsgebiete</i>	247
22.1.2	<i>Fotobegriff</i>	247
22.1.3	<i>Videobegriff</i>	248

22.2	Datenschutz	248
22.2.1	<i>DSGVO</i>	248
22.2.2	<i>DSG Österreich</i>	253
22.2.3	<i>BDSG Deutschland</i>	258
22.3	Urheberrecht	259
22.3.1	<i>Österreich</i>	259
22.3.2	<i>Deutschland</i>	261
22.3.3	<i>Sonstiges</i>	262
22.4	Arbeitsrecht	263
22.5	Allgemeines Persönlichkeitsrecht	263
22.6	Alltagsbeispiele	264
23	Zertifizierungen	268
23.1	Allgemeines	268
23.2	Vorteile	269
23.2.1	<i>Für Kunden</i>	269
23.2.2	<i>Für Anbieter</i>	269
23.3	Aktuelle Zertifizierungen	270
24	Behörden, europäische Stellen und Rechtsbehelfe von Betroffenen	272
24.1	Rechtsbehelfe von betroffenen Personen	272
24.2	Nationale Aufsichtsbehörde	273
24.2.1	<i>Österreich</i>	273
24.2.2	<i>Deutschland</i>	273
24.3	Europäischer Datenschutzausschuss	273
25	Anhang	275
25.1	DSGVO Artikel mit zugeordneten Erwägungsgründen	275
25.2	Vorlage Verzeichnis von Verarbeitungstätigkeiten	277
25.3	Speicher-, Aufbewahrungs- und Verjährungsfristen	280
25.4	Muster Meldung an die Aufsichtsbehörde im Falle von Datenschutzverletzungen	285
26	Über den Autor	286

Abkürzungsverzeichnis

A		ISO	International Organization for Standardization, Internationale Organisation für Normung
ABGB	Allgemeines Bürgerliches Gesetzbuch	IT	Informationstechnik, Informationstechnik im Zusammenhang mit
AGB	Allgemeine Geschäftsbedingungen	iZm	
Art.	Artikel	K	
B		KMU	Kleine und mittlere Unternehmen
BAO	Bundesabgabenordnung	KUG	Kunsturhebergesetz
BDSG	Bundesdatenschutzgesetz	P	
BGB	Bürgerliches Gesetzbuch	PDCA	Plan Do Check Act
BSI	Bundesamt für Sicherheit in der Informationstechnologie	PDF	Portable Document Format
C		PHG	Produkthaftungsgesetz
CNIL	Commission Nationale de l'Informatique et des Libertés	PR	Public Relations
CRM	Customer Relationship Management	PS	Privacy Shield
D		S	
d. h.	das heißt	SVG	Signatur- und Vertrauensdienstegesetz
DSG 2000	Datenschutzgesetz 2000	T	
DSG 2018	Datenschutzgesetz 2018	TKG	Telekommunikationsgesetz
DSGVO	Datenschutzgrundverordnung	TKG 2003	Telekommunikationsgesetz 2003
DSMS	Datenschutzmanagementsystem	TOMs	Technische und organisatorische Maßnahmen
E		U	
ECG	E-Commerce-Gesetz	UGB	Unternehmensgesetzbuch
EDA	Europäischer Datenschutz-ausschuss	UrhG	Urhebergesetz
ErwGr	Erwägungsgrund	USA	Vereinigte Staaten von Amerika
EU	Europäische Union	USB	Universal Serial Bus
EuGH	Europäischer Gerichtshof	UStG	Umsatzsteuergesetz
G		V	
gg	gegen	VVV-AV	Verzeichnis von Verarbeitungstätigkeiten Auftragsverarbeiter
GG	Grundgesetz	W	
GPS	Global Positioning System	WP29	Artikel 29 Datenschutzgruppe
I		Z	
IEC	Internationale Elektrotechnische Kommission	z. B.	zum Beispiel
ISMS	Informationssicherheitsmanagementsystem		

1 Einleitung

Sie werden sich fragen, was kann ich von diesem Buch nun wohl erwarten? Immerhin gibt es ja bereits das eine oder andere Buch zur Datenschutzgrundverordnung (DSGVO) am Markt.

„Praxis“ im Titel klingt ja schon mal nicht schlecht. Der Autor arbeitet sogar praktisch im Datenschutz und implementiert die DSGVO bei Unternehmen tagtäglich und der TÜV AUSTRIA steht zuletzt auch eher für die praxisorientierte Seite und nicht für allzu steif geführte akademische Hochschuldiskussionen.

Nun ja, lassen Sie es mich so ausdrücken: Ja, das praxisorientierte Näherbringen der DSGVO, kombiniert mit klassischen Problemstellungen des Alltags in Unternehmen samt möglichen Lösungswegen wäre sogar mein primäres Ziel dieses Buches.

Wenn ich Ihnen das Ganze zudem, unabhängig davon, ob Sie Jurist sind, näherbringen kann, und im Schreibstil nicht ganz so erzkonservativ und ernst bleiben muss bzw. darf, dann freut mich dies umso mehr. Die Juristen unter Ihnen verzeihen mir daher unter Umständen die eine oder andere nicht 100%ig exakt juristisch geprägte Ausdrucksweise oder Formulierung. Mir geht es vor allem auch darum, dass Personen ohne Jura-Studium den Inhalt dieses Buches verstehen und anwenden können. Vielleicht empfinden aber auch die Juristen unter Ihnen ein juristisches Fachbuch, das am Ende nicht ganz so steif juristisch geschrieben wurde, als erheiternde Abwechslung.

Natürlich kann ich es Ihnen (vor allem den Nicht-Juristen) nicht ersparen, dass der Inhalt dieses Buches ein rechtlicher ist (die DSGVO) und in weiten Teilen auch so behandelt werden muss. Aber ich versuche insbesondere auch den Nicht-Juristen in diesem Zuge ein paar Basics der Juristerei beizubringen. Womöglich empfinden Sie dies wiederum aber sogar als ansprechende Weiterbildung nebenher.

**„Wenn man alle Gesetze studieren wollte,
so hätte man gar keine Zeit, sie zu übertreten.“**

Johann Wolfgang von Goethe (1749–1832)

2 Welche Gesetze gilt es zu beachten?

Die Verarbeitung personenbezogener Daten einer Person unterliegt verschiedensten rechtlichen Regelungen. Die bedeutsamsten sind dabei sicherlich insbesondere ab dem 25.05.2018:

- ✓ die EU-Datenschutzgrundverordnung (DSGVO) und
- ✓ das österreichische Datenschutzgesetz („DSG 2018“ oder „DSG“),
- ✓ das österreichische Telekommunikationsgesetz 2003 (TKG 2003),
- ✓ das deutsche Bundesdatenschutzgesetz („BDSG 2018“ oder „BDSG neu“).

Ganz außer Acht sollte man die „alte“ Rechtslage jedoch auch nicht lassen, da diese in Vergleichen mit der DSGVO spannende Einblicke bieten, wenn man sich mit der Materie näher auseinandersetzen möchte:

- ✓ das österreichische Datenschutzgesetz (DSG 2000),
- ✓ das deutsche Bundesdatenschutzgesetz (BDSG alt).

Und um noch einen Ausblick für die Zukunft zu geben, sollte man durchaus in der nächsten Zeit erwarten dürfen

- ✓ die Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy Verordnung).

2.1 Die EU-Datenschutzgrundverordnung¹ (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

1 Vgl. <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&qid=1512933519199&from=EN>

Die Verordnung ersetzt ab 25. Mai 2018 die aus dem Jahr 1995 stammende EU Richtlinie 95/46/EG² zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr sowie das österreichische Datenschutzgesetz (DSG 2000).

Im Gegensatz zur EU Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018. Den Mitgliedstaaten ist es grundsätzlich nicht erlaubt, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken, auch wenn dies medial manchmal derart angedeutet wird. Allerdings enthält die Verordnung verschiedene Öffnungsklauseln, die es den einzelnen Mitgliedstaaten ermöglichen, bestimmte Aspekte des Datenschutzes auch im nationalen Alleingang zu regeln.

Die DSGVO regelt unter anderem die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen. Die bereits geltenden Betroffenenrechte werden erweitert und um neue Rechte ergänzt (z.B. um das Recht auf Datenübertragbarkeit oder das Recht auf Einschränkung).

Die Datenschutz-Grundverordnung gilt auch für Unternehmen, die ihren Sitz außerhalb der Europäischen Union haben, sich mit ihren Angeboten aber an EU-Bürger wenden (Marktortprinzip).

Das Datenschutzniveau wird mit der DSGVO nicht abgesenkt, sondern an einigen Stellen sogar weiter verschärft. Insbesondere bringt die DSGVO neue Transparenz- und Dokumentationsanforderungen für Verantwortliche der Datenverarbeitung und Auftragsverarbeiter mit sich. Ein gut strukturiertes Datenschutz-Managementsystem rückt dabei zusehends in den Fokus.

Die Aufsichtsbehörden haben bereits jetzt angekündigt, die Einhaltung der Datenschutzgrundverordnung verstärkt prüfen zu wollen – umso wichtiger ist es daher, sich mit den Neuerungen der DSGVO zu befassen und diese rasch umzusetzen. Zumal die Eingriffsrechte der Aufsichtsbehörden und die Sanktionen, die gegen die Unternehmen verhängt werden können, wesentlich verschärft wurden.

2 Vgl. <http://eur-lex.europa.eu/legal-content/DE/TEXT/?uri=celex%3A31995L0046>

2.2 Das österreichische Datenschutzgesetz „2018“ (DSG 2018)³



Das österreichische Datenschutzgesetz 2018 (oft hört und liest man auch vom Daten-
schutzanpassungsgesetz) trat ab 25. Mai 2018 gleichzeitig mit der DSGVO in Geltung.

Das DSG 2018 regelt insbesondere jene Bereiche des Datenschutzrechts, welche durch
die DSGVO den europäischen Staaten zur näheren Regelung überlassen wurden bzw.
einen Spielraum zur Ausgestaltung bieten oder ergänzende Regelungen vorschreiben.

Dieser Leitfaden geht in den nachstehenden Ausführungen und relevanten Bereichen
stets auch auf die Spezifika des DSG 2018 entsprechend ein. Im Bereich der Bildverar-
beitung, die wir besser unter „Videoüberwachung“ bis dato kannten, kommen etwa die
Regelungen des DSG 2018 intensiv zur Anwendung.

2.3 Das deutsche Bundesdatenschutzgesetz⁴



Das deutsche Bundesdatenschutzgesetz ist analog dem österreichischen Datenschutz-
gesetz ein nationales Anpassungs- und Ergänzungsgesetz zur DSGVO und trat ebenso
am 25. Mai 2018 in Kraft.

Seine Ursprünge hat das deutsche Bundesdatenschutzgesetz im Jahr 1977, welche
schlussendlich am 01. Januar 1978 zum ersten Datenschutzgesetz Deutschlands führ-
ten. Das Bundesland Hessen hatte hingegen 1970 bereits das erste Datenschutzgesetz
weltweit eingeführt.

Deutschland hat im Rahmen der Öffnungsklauseln die Themenbereiche Datenschutz-
beauftragter, Datenschutz im Beschäftigtenverhältnis, Scoring und Bonitätsauskünfte,
Verbraucherkredite und Freiheitsstrafen im „BDSG neu“ fokussiert.

2.4 Das österreichische Telekommunikationsgesetz 2003 (TKG 2003)⁵



Das Telekommunikationsgesetz 2003 ist ein österreichisches Gesetz und hat den grund-
sätzlichen Zweck, durch Förderung des Wettbewerbes im Bereich der elektronischen
Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen,

3 Vgl. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>

4 Vgl. https://www.bgbl.de/xaver/bgbl/stArtxav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf#_bgbl_%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1543010735482

5 Vgl. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849>

preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten.

Weitaus bekannter sind dennoch dessen Regelungen zur elektronischen Post und damit zusammenhängender Werbung. Eine Werbe- oder Massen-E-Mail muss insbesondere den Regelungen des TKG 2003 folgen. Näheres dazu im dazugehörigen Kapitel später.

2.5 Das österreichische Datenschutzgesetz 2000 (DSG 2000)⁶

Das Datenschutzgesetz 2000 war ein österreichisches Gesetz, welches auf Basis der Datenschutz EU Richtlinie 95/46/EG, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, etabliert wurde.

Dieses galt als Rechtsgrundlage, für die Verarbeitung personenbezogener Daten, bis zum 25. Mai 2018 in Österreich.

Aufgrund der Aufhebung des DSG 2000 mit gleichzeitigem Ingeltungtreten der Datenschutzgrundverordnung am 25. Mai 2018 wird grundsätzlich im Folgenden nicht mehr auf die Besonderheiten und Vorgaben des DSG 2000 näher eingegangen, sondern alle Ausführungen zu diesem Thema mit Bezug auf die DSGVO erläutert.



2.6 ePrivacy-Verordnung⁷

Langen Titels (Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation) kurzer Sinn ergibt die „ePrivacy-Verordnung der EU“.

Vorweg: Zum Zeitpunkt des Verfassens dieses Buches gibt es nur den durchaus im Endstadium befindlichen Entwurf dazu. In Kraft oder in Geltung getreten ist diese noch nicht. Ursprünglich war ein gleichzeitiges Ingeltungtreten mit der DSGVO geplant. Aufgrund der vielseitigen Verhandlungen wurde dies jedoch wieder verschoben.

Worum geht es? Im Grunde genommen möchte die EU mit der ePrivacy-Verordnung auf die Besonderheiten des Internets und der digitalen Welt eingehen und die Privatsphäre der Bürger in diesen Bereichen stärken. Ob jetzt die allseits bekannten Cookies (nein, nicht das leckere Backwerk), die Nutzung von Mobile Apps oder das Internet der Dinge⁸ (vernetzte physische und virtuelle Gegenstände), die ePrivacy-Verordnung soll

6 Vgl. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>

7 Vgl. <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017PC0010&from=EN>

8 Vgl. https://de.wikipedia.org/wiki/Internet_der_Dinge

dafür Regulatorien bieten. Daneben wird aber auch, wie bereits aktuell in Österreich durch das TKG 2003, das Direktmarketing geregelt.

Wie verhält sich die ePrivacy Verordnung nun gegenüber der DSGVO? Immerhin sind ja beide EU Verordnungen. Grundsätzlich ist die ePrivacy-Verordnung eine so genannte *lex specialis*. Und nun lernen Sie auch schon, wie versprochen/angedroht, Ihren ersten „hippen lateinischen juristischen Begriff“.

lex specialis

Eine *lex specialis* (hier unsere ePrivacy-Verordnung) ist ein spezielles Gesetz, das dem allgemeinen Gesetz (*lex generalis* = DSGVO) vorgeht. Dieses besondere Gesetz verdrängt das allgemeine Gesetz in bestimmten Bereichen. Die Spezialität des Gesetzes kann sich beispielsweise daraus ergeben, dass es nur einen bestimmten (speziellen) Sachbereich regelt, während die allgemeine Norm für mehrere Bereiche gilt.

3 Mythen rund um die DSGVO

Leider gibt es noch immer zahlreiche falsche Vorstellungen und gefährliche Halbwahrheiten über die DSGVO. Nicht zuletzt wegen der teilweise schlicht schlechten Berichterstattung, journalistisch reißerischen Überschriften und verkürzten Darstellungen der Thematik.

Mit einigen dieser Vorurteile möchte ich auf den folgenden Seiten nun aufräumen.

„Die DSGVO trifft mich als kleines Unternehmen doch nicht!“

Falsch!

Die Datenschutzgrundverordnung gilt für jede Person, jedes Ein-Mann-Unternehmen, jeden Klein- und Mittelständischen Betrieb und jeden Konzern, der personenbezogene Daten verarbeitet. Dabei ist es unerheblich, ob die Daten elektronisch (IT-Systeme) oder nicht-automatisiert (Papierakten) verarbeitet werden.

Ausnahmen bestehen nur eingeschränkt, etwa im persönlichen oder familiären Tätigkeitsbereich (z. B. das private Adressbuch von Freunden) oder im staatlichen Bereich der nationalen Sicherheit.

Die DSGVO gilt daher gleichermaßen für:

- ✓ Einzelpersonen
- ✓ Unternehmen
- ✓ Vereine
- ✓ Parteien
- ✓ Behörden
- ✓ Öffentliche Stellen
- ✓ Stiftungen
- ✓ Bund, Länder, Gemeinden

„Es hat bis jetzt niemanden interessiert – dies wird weiterhin so sein!“

Falsch!

Die Datenschutzgrundverordnung hat im Gegensatz zum bis 25.5.2018 geltenden DSG 2000 einen Strafraum von bis zu 20 Millionen Euro oder 4 % des weltweit erzielten Jahresumsatzes eines Unternehmens!

Das DSG 2000 hatte einen Strafraum von 25.000 Euro, das BDSG einen Strafraum von 300.000 Euro.

Für mich persönlich wäre dies bereits ein ausreichend großer Beweggrund, um sich mit den Regelungen der DSGVO auseinanderzusetzen.

Zudem führt das mediale und bei den Bürgern immer stärker werdende Interesse am Grundrecht auf Datenschutz dazu, dass die Einhaltung ein wichtiger Teil des Images eines Unternehmens wird und am Ende einen deutlichen Wettbewerbsvorteil darstellt.

„Die Aufsichtsbehörde kontrolliert doch niemanden!“

Falsch!

Die Datenschutzbehörden hatten in der Vergangenheit zwar durchaus keine üppige personelle Ausstattung, jedoch hat sich dies bereits seit 25.05.2018 geändert und wird mit Fortdauer der DSGVO sich noch weiter erheblich erweitern. Die Personalressourcen werden jedenfalls aufgestockt. Somit rücken flächendeckende Kontrollen deutlich näher.

Weiters muss sich eine Behörde zur Prüfung in einem ersten Schritt nicht aktiv vor Ort in die Unternehmen begeben, sondern kann sich aufgrund der Rechenschaftspflicht der Unternehmen die Einhaltung der DSGVO nachweisen lassen.

Zusätzlich können betroffene Personen mittels Beschwerde bei der Behörde vorstellig werden und auf Missstände hinweisen. Dazu reicht oftmals ein Screenshot von unzulässigen Vertragsformulierungen, Missachtung von detaillierten Informationspflichten oder unrechtmäßig ausgestalteten Einwilligungserklärungen. Dazu zählen insbesondere unzufriedene Kunden, Lieferanten, Mitarbeiter oder aber Wettbewerber!

Eine Behörde geht jeder Beschwerde von betroffenen Personen nach. Somit führt jede Beschwerde zu einer konkreten Untersuchung gegen das Unternehmen. Das Unternehmen muss dann nachweisen, dass entgegen der Beschwerde die Datenverarbeitung im Rahmen der DSGVO erfolgt ist.

Zum Zeitpunkt des Verfassens dieses Buches (Herbst 2018) waren bereits nach wenigen Monaten und über den Zeitraum des berühmten Sommerlochs hinweg, **in Österreich knapp 1000 und in Deutschland mehrere 10.000 Beschwerden** bei den Behörden eingelangt.

„Die DSGVO ändert ja nichts!“

Falsch!

Die Datenschutzgrundverordnung behält zwar viele Grundsätze des bestehenden Datenschutzrechts bei, führt allerdings auch zahlreiche Neuerungen für Unternehmen ein.

Dazu zählen insbesondere die zahlreichen Dokumentationspflichten, Verzeichnisse und Register neben den neu einzuführenden Unternehmensprozessen sowie Richtlinien und der Sicherstellung von Betroffenenrechten.

Unternehmen haben zukünftig durch eine geeignete Organisation die Einhaltung des Datenschutzes fortlaufend zu kontrollieren, adaptieren und proaktiv nachzuweisen (Stichwort: Datenschutz-Managementsystem).

Auch muss an die Datenschutzbehörde ein etwaiger Datenschutzbeauftragter gemeldet werden. Eine Behörde könnte dabei relativ einfach mit Unternehmens- und Branchenregistern feststellen, ob gegen eine Bestellopflicht verstoßen wurde.

„Schön und gut, aber wir verarbeiten ja gar keine Daten!“

Falsch!

Diese Meinung resultiert oftmals von einer falschen Vorstellung, was unter „personenbezogenen Daten“ oder „verarbeiten“ verstanden wird.

Personenbezogene Daten sind alle Informationen, welche man einer natürlichen Person zuordnen kann. Dazu zählen sowohl Mitarbeiter als auch Kunden, Lieferanten, Ansprechpartner in Unternehmen und Mitarbeiter und Kunden von Kunden.

Beispiele sind etwa Name, E-Mail-Adresse, Telefonnummer, Gehalt, Foto, erfasste Meinungen, Vermerke zu einer Person, ein Vertrag oder eine Rechnung mit einem Namen.

In der Praxis sind sehr viele Daten auch personenbezogene Daten!

Hinter dem Begriff „verarbeiten“ verbirgt sich nicht mehr und nicht weniger als ein Hilfsbegriff des Datenschutzrechts.

Denn unter einem Verarbeiten von Daten wird – Achtung: lange Aufzählung – erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenlegen, übermitteln, verbreiten, abgleichen oder verknüpfen, einschränken, löschen oder vernichten verstanden.

Wie Sie wohl schnell gemerkt haben: Im Endergebnis ist es all jenes, was man mit Daten anstellen kann.