
EU-Datenschutz-Grundverordnung (DSGVO)

Paul Voigt • Axel von dem Bussche

EU-Datenschutz- Grundverordnung (DSGVO)

Praktikerhandbuch

2. Auflage

 Springer

Paul Voigt
Taylor Wessing
Berlin, Deutschland

Axel von dem Bussche
Taylor Wessing
Hamburg, Deutschland

ISBN 978-3-662-68819-9 ISBN 978-3-662-68820-5 (eBook)
<https://doi.org/10.1007/978-3-662-68820-5>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <https://portal.dnb.de> abrufbar.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer-Verlag GmbH, DE, ein Teil von Springer Nature 2018, 2024

Erweiterte Übersetzung der englischen Ausgabe: The EU General Data Protection Regulation (GDPR) von Paul Voigt und Axel von dem Bussche, © Springer International Publishing AG 2017. Alle Rechte vorbehalten.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Brigitte Reschke

Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

Vorwort

Sechs Jahre ist es her, seitdem die Erstauflage dieses Handbuchs erschienen ist. Seitdem hat sich viel getan. Waren datenschutzrechtliche EuGH-Urteile in Vor-DSGVO-Zeiten noch ein „Event“, auf das man sich monatelang „freuen“ und vorbereiten konnte, ist es inzwischen eine Herausforderung, der Masse an Datenschutzurteilen und Behördenentscheidungen Herr zu werden. Hinzu kommt eine deutlich zunehmende Digitalregulierung auf europäischer Ebene, die auch auf datenschutzrechtliche und IT-sicherheitsrechtliche Vorgaben Einfluss nimmt – NIS2, DORA, DSA, DMA, AI Act, CRA; die Liste ließe sich beliebig fortsetzen.

Kurzum, eine Neuauflage war angezeigt. Wie bereits in der Voraufgabe gehen wir nicht nur auf die DSGVO, sondern auch auf das begleitende deutsche Recht ein, und wie bei der Voraufgabe gibt es ein englischsprachiges „Schwesterbuch“, das parallel erscheint und die Befassung mit dem Datenschutz im internationalen Kontext erleichtern soll.

Auch in dieser Auflage ist dem Handbuch eine „Checkliste“ der wichtigsten Datenschutzpflichten vorangestellt, die maßgebliche Problemfelder in Kurzform darlegt und Verweise auf die entsprechenden Teile dieses Buches enthält.

Für die umfassende Unterstützung bei beiden Projekten möchten wir uns bei Frau Dr. Brigitte Reschke und Frau Julia Bieler vom Verlag Springer Nature, sowie unseren wissenschaftlichen Mitarbeitern Jin Fuhrken, Hannes Bastians, Albert Gutman und Alea Mostler bedanken.

Stets dankbar sind wir auch für Hinweise, Anregungen und Kritik zu diesem Buch, die Sie gerne per Email an p.voigt@taylorwessing.com oder a.bussche@taylorwessing.com richten können.

Berlin, Deutschland
Hamburg, Deutschland
Mai 2024

Paul Voigt
Axel Freiherr von dem Bussche

Inhaltsverzeichnis

1	Einleitung und „Checkliste“	1
1.1	Gesetzgeberischer Hintergrund und bisherige Rechtslage	1
1.1.1	Die EG-Datenschutzrichtlinie	1
1.1.2	Die Datenschutz-Grundverordnung	2
1.1.3	Das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU	3
1.2	Checkliste – Die wichtigsten datenschutzrechtlichen Pflichten	4
1.2.1	Datenschutzorganisation	4
1.2.2	Rechtmäßigkeit der Datenverarbeitung	7
	Referenzen	9
2	Anwendungsbereich der DSGVO	11
2.1	In welchen Fällen ist die Verordnung anwendbar? – sachlicher Anwendungsbereich	11
2.1.1	„Verarbeitung“	12
2.1.2	„Personenbezogene Daten“	14
2.1.3	Ausnahmen vom sachlichen Anwendungsbereich	22
2.2	Auf wen ist die Verordnung anwendbar? – persönlicher Anwendungsbereich	23
2.2.1	„Verantwortlicher“	23
2.2.2	„Auftragsverarbeiter“	28
2.2.3	Von der DSGVO geschützte Personen	29
2.3	Wo ist die Verordnung anwendbar? – räumlicher Anwendungsbereich	30
2.3.1	Datenverarbeitung im Rahmen der Tätigkeiten einer EU-Niederlassung	32
2.3.2	Verarbeitung personenbezogener Daten von innerhalb der EU befindlichen betroffenen Personen	36
2.4	Anwendungsbereich des BDSG	40
	Referenzen	43

3	Anforderungen an die Datenschutzorganisation	47
3.1	Rechenschaftspflicht	47
3.2	Allgemeine Pflichten	50
3.2.1	Risikobasierter Ansatz	51
3.2.2	Verantwortlichkeit, Haftung und allgemeine Pflichten des Verantwortlichen	53
3.2.3	Zusammenarbeit mit den Aufsichtsbehörden	55
3.3	Die Verteilung von Verantwortlichkeit zwischen gemeinsam Verantwortlichen („Joint controllers“)	57
3.3.1	Die Beziehung zwischen gemeinsam für die Verarbeitung Verantwortlichen	58
3.3.2	Rechtsfolgen gemeinsamer Verantwortung	61
3.4	Auftragsverarbeiter	63
3.4.1	Privilegierte Stellung des Auftragsverarbeiters	63
3.4.2	Verpflichtung des Verantwortlichen bei der Auswahl eines Auftragsverarbeiters	64
3.4.3	Pflichten des Auftragsverarbeiters	73
3.4.4	Hinzuziehung eines „Unter-Auftragsverarbeiters“	74
3.5	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy by Design and by Default“)	76
3.6	Verzeichnisse von Verarbeitungstätigkeiten	81
3.6.1	Inhalt und Zweck der Verzeichnisse	81
3.6.2	Dokumentation der Zwecke der Datenverarbeitung	83
3.6.3	Ausnahme von der Pflicht zum Führen der Verzeichnisse	84
3.7	Technische und organisatorische Maßnahmen	86
3.7.1	Angemessenes Datenschutzniveau	87
3.7.2	Maßnahmenkatalog	88
3.7.3	Andere EU-Vorschriften	90
3.8	Verletzungen des Schutzes personenbezogener Daten („Data Breach Notification“)	92
3.8.1	Verletzung des Schutzes personenbezogener Daten	92
3.8.2	Meldung an die Aufsichtsbehörde	94
3.8.3	Benachrichtigung der betroffenen Personen	101
3.9	Datenschutz-Folgenabschätzung („Data Protection Impact Assessment“) und vorherige Konsultation	106
3.9.1	Betroffene Arten von Verarbeitungstätigkeiten	107
3.9.2	Vornahme der Folgenabschätzung	112
3.10	Datenschutzbeauftragter	118
3.10.1	Pflicht zur Benennung	118
3.10.2	Anforderungen an den Datenschutzbeauftragten	126
3.10.3	Stellung des Datenschutzbeauftragten	129
3.10.4	Aufgaben des Datenschutzbeauftragten	135

3.11	Benennung eines Unionsvertreters	141
3.11.1	Voraussetzungen hinsichtlich des Vertreters	141
3.11.2	Ausnahmen von der Pflicht zur Benennung eines Vertreters	143
3.11.3	Pflichten des Vertreters	143
3.12	Verhaltensregeln, Zertifizierungen, Siegel, etc.	145
3.12.1	Verhaltensregeln („Codes of Conduct“)	146
3.12.2	Zertifizierungen, Datenschutzsiegel und -prüfzeichen („Certifications, seals and marks“)	152
	Referenzen	156
4	Materielle Anforderungen	163
4.1	Verarbeitungsgrundsätze	163
4.1.1	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	164
4.1.2	Zweckbindung	165
4.1.3	Datenminimierung	167
4.1.4	Richtigkeit	168
4.1.5	Speicherbegrenzung	169
4.1.6	Integrität und Vertraulichkeit	169
4.2	Rechtsgrundlagen für die Datenverarbeitung	170
4.2.1	Verarbeitung auf der Grundlage der Einwilligung der betroffenen Person	170
4.2.2	Verarbeitung auf der Grundlage eines gesetzlichen Erlaubnistatbestandes	181
4.2.3	Verarbeitung besonderer Kategorien personenbezogener Daten	195
4.3	Datenübermittlungen an Drittländer	207
4.3.1	Angemessenheitsbeschlüsse	208
4.3.2	Standardvertragsklauseln	210
4.3.3	Binding Corporate Rules	217
4.3.4	Verhaltensregeln, Zertifizierungsverfahren, etc.	222
4.3.5	Ausnahmen für bestimmte Fälle	223
4.3.6	Nach dem Unionsrecht nicht zulässige Übermittlungen oder Offenlegungen	230
4.4	Eingeschränktes „Konzernprivileg“	231
4.4.1	Eigenständige Datenschutzverantwortlichkeit jedes Gruppenunternehmens	232
4.4.2	Erleichterungen in Bezug auf die materiellen Anforderungen	233
4.4.3	Erleichterungen in Bezug auf die Datenschutzorganisation	234
	Referenzen	234

5	Rechte der betroffenen Personen	239
5.1	Allgemeine Vorgaben	239
5.1.1	Die Art und Weise der Kommunikation mit den betroffenen Personen	240
5.1.2	Die Form der Kommunikation	241
5.2	Informationspflicht des Verantwortlichen bei Erhebung der personenbezogenen Daten	242
5.2.1	Zeitpunkt der Information	242
5.2.2	Erhebung der Daten bei der betroffenen Person	243
5.2.3	Erhebung der Daten aus einer anderen Quelle	247
5.2.4	Einschränkung der Informationspflichten nach dem BDSG	248
5.2.5	Praxishinweise	253
5.3	Informationen über infolge eines Antrags ergriffene Maßnahmen	253
5.3.1	Art und Weise der Bereitstellung der Informationen	254
5.3.2	Frist für die Bereitstellung der Informationen	257
5.3.3	Unterrichtung im Falle des Nicht-Tätigwerdens	258
5.3.4	Bestätigung der Identität der betroffenen Person	258
5.4	Auskunftsrecht	259
5.4.1	Umfang des Auskunftsrechts	259
5.4.2	Recht auf Kopie	262
5.4.3	Einschränkungen des Auskunftsrechts nach dem BDSG	265
5.4.4	Praxishinweise	268
5.5	Recht auf Berichtigung, auf Löschung und auf Einschränkung der Verarbeitung	268
5.5.1	Recht auf Berichtigung	269
5.5.2	Recht auf Löschung	272
5.5.3	Recht auf Einschränkung der Verarbeitung	286
5.5.4	Mitteilungspflicht gegenüber Dritten im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung	290
5.6	Recht auf Datenübertragbarkeit	292
5.6.1	Anwendungsbereich & Ausübung des Rechts auf Datenübertragbarkeit	293
5.6.2	Technische Spezifikationen	299
5.6.3	Übermittlung der Daten	300
5.6.4	Verhältnis zum Recht auf Löschung	300
5.6.5	Vertraglicher Ausschluss des Rechts auf Datenübertragbarkeit	301
5.7	Widerspruchsrecht	302
5.7.1	Gründe für einen Widerspruch gegen die Verarbeitung	302
5.7.2	Einschränkungen im BDSG	305

5.7.3	Ausübung des Rechts & Rechtsfolgen	306
5.7.4	Informationspflicht	307
5.8	Automatisierte Entscheidungsfindung	307
5.8.1	Anwendungsbereich des Verbots	307
5.8.2	Ausnahmen vom Verbot nach der DSGVO	312
5.8.3	Ausnahme vom Verbot nach dem BDSG	313
5.8.4	Angemessene Schutzmaßnahmen	314
5.9	Beschränkungen der Betroffenenrechte	315
	Referenzen	316
6	Zusammenarbeit mit den Aufsichtsbehörden	321
6.1	Bestimmung der zuständigen Aufsichtsbehörde	321
6.2	One-Stop-Shop	322
6.2.1	Grenzüberschreitende Verarbeitungstätigkeit	324
6.2.2	Bestimmung der federführenden Aufsichtsbehörde	325
6.2.3	Bestimmung anhand der Hauptniederlassung des Unternehmens	325
6.2.4	Ausnahme: lokale Zuständigkeit	328
6.3	One-Stop-Shop auf nationaler Ebene nach dem BDSG	330
6.4	Bestimmung der zuständigen Aufsichtsbehörde bei Fehlen einer Niederlassung des Unternehmens in der EU	331
6.5	Zusammenarbeit und Kohärenzverfahren	332
6.5.1	Europäischer Datenschutzausschuss	332
6.5.2	Verfahren zur Zusammenarbeit	333
6.5.3	Kohärenzverfahren	334
	Referenzen	334
7	Rechtsdurchsetzung und Sanktionen nach der DSGVO	337
7.1	Aufgaben und Untersuchungsbefugnisse der Aufsichtsbehörden	337
7.1.1	Größere Konsistenz der Untersuchungsbefugnisse innerhalb der EU	337
7.1.2	Regelungen zu aufsichtsbehördlichen Befugnissen im BDSG	338
7.1.3	Umfang der Untersuchungsbefugnisse	339
7.1.4	Ausübung der Befugnisse	342
7.2	Zivilrechtliche Haftung	343
7.2.1	Recht auf Schadensersatz	343
7.2.2	Schadensersatzpflichtige	348
7.2.3	Exkulpationsmöglichkeit	349
7.3	Sanktionen	351
7.3.1	Abhilfebefugnisse der Aufsichtsbehörden	352
7.3.2	Gründe für Bußgelder und Bußgeldbeträge	353
7.3.3	Verhängung von Bußgeldern	355
7.3.4	Sanktionierung von Unternehmensgruppen	359

7.3.5	Sanktionen und Verfahrensvorschriften des BDSG und des OWiG	360
7.3.6	Praxishinweise	363
7.4	Rechtsbehelfe	364
7.4.1	Rechtsbehelfe von daten verarbeitenden Unternehmen	364
7.4.2	Rechtsbehelfe von betroffenen Personen	365
	Referenzen	370
8	Nationale Besonderheiten	373
8.1	Vielzahl von Öffnungsklauseln	373
8.1.1	Öffnungsklauseln innerhalb der allgemeinen Bestimmungen der DSGVO	373
8.1.2	Gesetzgebungskompetenz der EU-Mitgliedstaaten in besonderen Verarbeitungssituationen	377
8.1.3	Regelungen im BDSG zu besonderen Verarbeitungssituationen	379
8.2	Beschäftigtendatenschutz	380
8.2.1	Öffnungsklausel	381
8.2.2	Regelungen des § 26 BDSG	382
8.2.3	Kollektivvereinbarungen als Rechtsgrundlage	391
8.3	Telemedien- und Telekommunikationsdatenschutz	393
	Referenzen	397
9	Besondere Verarbeitungssituationen	401
9.1	Big Data	401
9.1.1	Anwendbarkeit der DSGVO	403
9.1.2	Rechenschaftspflicht	404
9.1.3	Besondere Herausforderungen für Verantwortliche	404
9.2	Künstliche Intelligenz	408
9.3	Cloud Computing	412
9.3.1	Verteilung der Verantwortlichkeiten	413
9.3.2	Auswahl eines geeigneten Cloud-Anbieters	414
9.3.3	Cloud-Serviceanbieter in Drittländern	415
9.4	Internet of Things	415
9.4.1	Rechtsgrundlage für Datenverarbeitungen im IoT	416
9.4.2	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	417
9.4.3	Der EU Data Act	418
	Referenzen	419
10	Audits als Mittel zur Selbstkontrolle	421
10.1	Vorteile eines Datenschutzaudits	421
10.2	Internes oder externes Audit?	422
10.3	Ablauf eines Datenschutzaudits	422
10.4	Ausblick: Zertifizierungsverfahren	424
	Referenzen	424
	Stichwortverzeichnis	425