

Handbuch Kundendatenschutz

Von

Dr. Simon Menke

Co-General Counsel

2., neu bearbeitete Auflage

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

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

Weitere Informationen zu diesem Titel finden Sie im Internet unter

<https://ESV.info/978-3-503-24203-0>

Zitiervorschlag:

Menke, Handbuch Kundendatenschutz, 2. Aufl. 2026

1. Auflage 2022

2. Auflage 2026

ISBN 978-3-503-24203-0 (gedrucktes Werk)

ISBN 978-3-503-24204-7 (eBook)

DOI <https://doi.org/10.37307/b.978-3-503-24204-7>

Alle Rechte vorbehalten.

© 2026 Erich Schmidt Verlag GmbH & Co. KG

Genthiner Straße 30 G, 10785 Berlin

info@ESVmedien.de, www.ESV.info

Die Nutzung für das Text und Data Mining ist ausschließlich dem Erich Schmidt Verlag GmbH & Co. KG vorbehalten. Der Verlag untersagt eine Vervielfältigung gemäß § 44b UrhG ausdrücklich.

Druck: Beltz, Bad Langensalza

Vorwort

Die Verarbeitung von Kundendaten spielt in der Praxis für eine Vielzahl von Unternehmen eine wichtige Rolle. Zu diesen Unternehmen gehören unter anderem Betreiber von Online-Shops, Auskunftsteilen, Anbieter von Online-Marketing-Tools und Betreiber von Plattform-Ökosystemen.

Spätestens seit der Anwendung der Datenschutz-Grundverordnung im Jahr 2018 ist der Datenschutz in aller Regel wesentlicher Bestandteil des Compliance-Management-Systems solcher Unternehmen, die eine relevante Anzahl an Endkundendaten verarbeiten. Dies liegt zum einen daran, dass für den Fall einer Verletzung gesetzlicher datenschutzrechtlicher Vorgaben empfindliche Geldbußen drohen. Zum anderen gehen mit Verfahren wegen (möglicherweise) begangener Datenschutzverstöße in aller Regel kommunikative Risiken einher. Dies ist insbesondere dann der Fall, wenn die Verarbeitung von Endkundendaten Gegenstand eines Verfahrens ist.

Vor dem Hintergrund der zuvor genannten Risiken ist es für Datenschutzberater in der Praxis häufig misslich, dass eine Vielzahl relevanter Fragestellungen, die im Zusammenhang mit der Auslegung einzelner Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes 2018 bestehen, auch zum Zeitpunkt des Erscheinens dieser 2. Auflage noch nicht abschließend geklärt ist. Zwar haben sowohl die deutschen als auch andere europäische Aufsichtsbehörden und der Europäische Datenschutzausschuss einige Orientierungshilfen sowie Leitlinien veröffentlicht; die in diesen dargelegten Positionen müssen aber naturgemäß nicht vollständig korrekt sein. Darüber hinaus vertreten einzelne Aufsichtsbehörden zum Teil voneinander abweichende Rechtsansichten. Wegweisende Entscheidungen des EuGH haben mittlerweile dazu beigetragen, dass in der Praxis im Zusammenhang mit der Verarbeitung von Kundendaten mehr Rechtssicherheit erreicht werden kann. Viele in dem genannten Zusammenhang bestehende Rechtsfragen müssen aber noch durch den EuGH beantwortet werden.

Die Möglichkeit der Verarbeitung von Daten stellt in einer digitalisierten Welt regelmäßig einen wesentlichen Wettbewerbsfaktor dar. Aufgrund dieses Umstands ist es eine zentrale Aufgabe von Datenschutzberatern, datenschutzkonforme Lösungen in Bezug auf geplante Vorhaben aufzuzeigen. Folge des genannten Umstands ist außerdem, dass in der Praxis das Kartell- und das Datenschutzrecht relevante Berührungspunkte zueinander aufweisen. Hinzugekommen sind seit dem Erscheinen der 1. Auflage weitere europäische „Schnittstellenregulierungen“, wie z.B. die KI-Verordnung. Die Schaffung eines „Level-Playingfield“ im Datenschutz, die ein wesentliches Ziel der Datenschutz-Grundverordnung (gewesen) ist, wurde leider weiterhin nicht erreicht.

Die rechtliche Bewertung von Datenverarbeitungen wird in der Praxis regelmäßig dadurch erschwert, dass die Verarbeitungen im Rahmen technisch komple-

Der Vorgänge erfolgen. Solche Vorgänge bestehen z.B. häufig im Bereich des Online-Marketing. Datenschutzberater sehen sich vermehrt mit Schlagwörtern wie „Browser-Fingerprinting“, „Realtime-Bidding“ oder „Audience-Matching“ konfrontiert.

Dieses Handbuch soll Datenschutzberater dabei unterstützen, in der Praxis auftretende Verarbeitungen von Kundendaten rechtlich zu bewerten. In diesem Zusammenhang werden auch Vorgänge erläutert, die zumindest für solche Berater, die keinen technischen „Background“ aufweisen, auf den ersten Blick schwer nachzuvollziehen und die bisher nicht Gegenstand umfangreicher rechtlicher Diskussionen oder gerichtlicher Entscheidungen sind. Die Erläuterungen erfolgen unter anderem mittels der Darlegung von Beispielen. Darüber hinaus beinhaltet dieses Handbuch eine Vielzahl an Praxishinweisen, insbesondere zum strategischen Umgang mit noch nicht geklärten Rechtsfragen.

Auch wenn die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz 2018 bereits seit mehr als sieben Jahren geltendes Recht sind, bestehen – wie bereits erwähnt – immer noch relevante Unsicherheiten im Bereich der Auslegung. Für die Beantwortung solcher Fragestellungen, zu denen es noch keine abschließenden Rechtsprechungen gibt, ist die „Arbeit mit dem Gesetz“ von besonderer Relevanz. Aus diesem Grund werden in diesem Handbuch unter anderem einzelne Normen aus der sowie Erwägungsgründe zur Datenschutz-Grundverordnung zitiert. Dies erfolgt auch vor dem Hintergrund, dass in der juristischen Diskussion teilweise Ansichten vertreten werden, die mit dem jeweiligen Gesetzeswortlaut nicht oder nur schwer vereinbar sind.

Bei der Erstellung dieses Handbuchs konnten Entwicklungen in der Gesetzgebung, der Rechtsprechung und der Literatur bis zum 31.07.2025 berücksichtigt werden.

München, im September 2025

Dr. Simon Menke

Inhaltsverzeichnis

Vorwort	5
Abkürzungsverzeichnis	15
Teil I Grundlagen	21
A. Relevante Gesetze	23
I. Datenschutz-Grundverordnung (DSGVO)	23
1. Einheitlicher Rechtsrahmen	23
2. „Level-Playingfield“/Kohärenzmechanismus	23
3. Relevanz der Erwägungsgründe	25
4. Unbestimmtheit	25
II. Bundesdatenschutzgesetz (BDSG 2018)	27
III. Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG)	28
IV. Bürgerliches Gesetzbuch (BGB)	28
V. Gesetz gegen den Unlauteren Wettbewerb (UWG)	29
VI. Gesetz gegen Wettbewerbsbeschränkungen (GWB) / Digital Markets Act (DMA)	30
1. Verfahren des Bundeskartellamts gegen Meta	30
2. Untersagungstatbestände in § 19a GWB	31
3. Digital Markets Act (DMA)	33
4. Verhältnis des DMA zu § 19a GWB	35
VII. KI-Verordnung	36
B. Anwendungsbereich der DSGVO	39
I. Sachlicher Anwendungsbereich/Personenbezug	39
1. Rechtslage nach dem BDSG 2009	39
2. Rechtslage nach der DSGVO	40
3. „Pseudonyme“/pseudonymisierte Daten	42
4. Anonymisierung	47
5. Daten Verstorbener	51
II. Räumlicher Anwendungsbereich	51
III. Begriff der Verarbeitung	52
C. Grundsatz der „Accountability“	54
I. Einzelne gesetzliche Vorgaben	55
II. Datenschutz-Managementsystem (DSMS)	55
D. Alleinige Verantwortlichkeit	56
E. Auftragsverarbeitung	57
I. Einzelne Datenverarbeitungen	58
II. Versendung von Lieferankündigungen	59
III. Grenzfälle	61
IV. „Multifunktionale Stelle“	62
V. „Privilegierung“	63

VI. Abrede zur Auftragsverarbeitung	64
1. Abschluss von SDK	66
2. Unterauftragnehmer	66
VII. Eigenständige Haftung des Auftragsverarbeiters	67
VIII. Gesetzliche Verpflichtungen des Auftragsverarbeiters/ Vertragliche Haftung	67
IX. „Exzess“ des Auftragsverarbeiters	68
F. „Controller to Controller“	69
G. Gemeinsame Verantwortlichkeit	71
I. Anwendungsbereich	71
1. Fortbestand der Rechtsprechungen zur Richtlinie 95/46/EG?	73
2. Zweck der Regelungen zur gemeinsamen Verantwort- lichkeit	76
3. Sinn und Zweck der konkreten Datenverarbeitung	76
II. „Phasenbezug“	77
III. „Joint-Controller-Agreement“	78
IV. Transparenz	79
V. Haftung	79
H. Datenminimierung	80
I. Speicherung in mehreren Datenbanken	81
II. „Gastzugang“	81
I. Grundsatz der Zweckbindung	84
J. Verbot mit Erlaubnisvorbehalt/Rechtsgrundlagen	85
I. Kein „Konzernprivileg“	85
II. Etwaige Nachteile für Konzerne	86
Teil 2 Rechtsgrundlagen	87
A. Einzelne Rechtsgrundlagen	89
I. Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO)	89
1. Freiwilligkeit der Einwilligung	90
2. Für den bestimmten Fall	97
3. Unmissverständlich abgegebene Willensbekundung	100
4. Dauer der Gültigkeit von Einwilligungen	101
5. Alter der Einwilligenden	102
6. Nachweis der Einwilligung	103
7. Einwilligung und AGB-Kontrolle	104
8. Widerruf der Einwilligung	106
II. Vertragserfüllung/vorvertragliche Maßnahmen (Art. 6 Abs. 1 S. 1 lit. b) DSGVO)	107
1. Vertrag/Vertragsparteien	107
2. Vorvertragliche Maßnahmen	108
3. Erforderlichkeit	110
III. Rechtliche Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c) DSGVO)	112
IV. Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO)	114
1. Berechtigtes Interesse	115

2. „Eigentliche Interessenabwägung“	124
3. Vernünftige Erwartungen der Betroffenen	131
V. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)	137
B. Verhältnis der Rechtsgrundlagen zueinander	138
C. Zweckänderung	141
I. „Zweckkompatibilität“	141
II. Eigene Rechtsgrundlage?	143
III. Information über Zweckänderung	144
Teil 3 Informationspflichten	147
A. Schaffung von Transparenz als ein wesentliches Ziel der DSGVO	149
B. Erhebung von Daten beim Betroffenen (Art. 13 DSGVO)	150
I. Verhältnis von Art. 13 Abs. 1 DSGVO zu Art. 13 Abs. 2 DSGVO	151
II. Die einzelnen Informationen	152
1. Name und Kontaktdaten des Verantwortlichen	152
2. Kontaktdaten des Datenschutzbeauftragten	152
3. Zweck der Datenverarbeitung sowie Rechtsgrundlage	153
4. Berechtigtes Interesse an der Datenverarbeitung	153
5. Empfänger oder Kategorien von Empfängern	154
6. Absicht der Übermittlung der Daten in unsichere Drittländer	157
7. Dauer der Speicherung/Verarbeitung bzw. Kriterien für die Dauer	157
8. Hinweis auf Betroffenenrechte	159
9. Automatisierte Einzelfallentscheidung inklusive „Profiling“	160
10. Zweckänderung	162
III. Ausnahme: Betroffener verfügt bereits über die Informationen	162
C. Nicht beim Betroffenen erhobene Daten (Art. 14 DSGVO)	163
I. Kategorien personenbezogener Daten	165
II. Quelle für die Datenerhebung	165
III. „Frist“ zur Erteilung der Informationen	165
1. Kommunikation mit den Betroffenen	165
2. Offenlegung gegenüber Empfängern	166
3. Verhältnis der Regelungen zueinander	166
IV. Informationen sind bereits bekannt	167
V. Unmöglichkeit/unverhältnismäßiger Aufwand	168
D. Rechtsfolge bei Verstoß gegen die Informationspflichten	169
Teil 4 Rechte der Betroffenen/Automatisierte Einzelfall- scheidungen	171
A. Allgemeines zu den Rechten der Betroffenen	173
B. Die einzelnen Rechte	173
I. Recht auf Auskunft	173
1. Systematik	173
2. Recht auf Bestätigung sowie auf weitere Informationen	174

3. Informationen zum Drittlanddatentransfer	174
4. Der Betroffene verfügt bereits über die Informationen	175
5. Kopie der verarbeiteten Daten	175
6. Ausnahmen	177
II. Recht auf Berichtigung	178
III. Recht auf Löschung	179
1. Zweckerreichung	180
2. Gesetzliche Verpflichtungen zur Aufbewahrung	181
3. Recht auf Löschung und Werbewiderspruch	182
4. Pflicht zur Löschung und „Accountability“	182
5. Anonymisierung	182
IV. Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	184
V. Mitteilungspflicht gegenüber Datenempfängern (Art. 19 DSGVO)	186
VI. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	187
1. Datenkategorien/Art der Verarbeitung	187
2. Format	188
3. Übertragung an Dritte	189
4. Rechte Dritter	189
VII. Widerspruchsrecht	189
1. Widerspruch nach Art. 21 Abs. 1 DSGVO	190
2. Widerspruch nach Art. 21 Abs. 2 DSGVO („Direktwerbung“)	191
3. Widerspruch mittels automatisierter Verfahren	191
4. Rechtsfolge eines umzusetzenden Widerspruchs	192
5. Praktische Grenzen der Umsetzbarkeit	192
C. Vollmacht	195
D. Umsetzungsfrist	195
I. Information über ergriffene Maßnahmen	196
II. Monatsfrist	196
III. Verlängerung der Frist	196
E. Form der Information	197
F. Betroffenenrechte bei der Verarbeitung pseudonymer Daten	197
I. Vorschrift in Art. 11 Abs. 2 DSGVO	198
II. Einzelne Konstellationen	199
1. Nutzung von Endgeräten durch unterschiedliche Personen	199
2. „Third-Party-Konstellationen“	200
3. Verarbeitung von Daten durch Datentreuhänder	201
4. Verschlüsselung von Identifiern durch eine „Third-Party“	201
5. Online-Tracking durch Websitebetreiber	202
6. Verarbeitung von Trackingdaten in gemeinsamer Verantwortlichkeit	203
7. Pseudonymisierung durch ausschließlich interne Maßnahmen	205

G. Automatisierte Einzelfallentscheidung (Art. 22 DSGVO)	206
I. Automatisierte Einzelfallentscheidung	206
II. Rechtliche Wirkung/Beeinträchtigung in ähnlicher Weise	206
III. Ausnahmen	208
1. Erforderlichkeit der automatisierten Einzelfallentscheidung (Art. 22 Abs. 2 Ziffer a) DSGVO)	208
2. Zulässigkeit aufgrund europäischer/nationaler Regelungen (Art. 22 Abs. 2 Ziffer b) DSGVO)	209
3. Einwilligung (Art. 22 Abs. 2 Ziffer c) DSGVO)	210
IV. Weitere Anforderungen (Art. 22 Abs. 3 DSGVO)	211
V. Besondere Kategorien personenbezogener Daten	211
Teil 5 Technische und organisatorische Maßnahmen	213
A. Regelung in Art. 32 DSGVO	215
I. „Risikobasierter Ansatz“	215
II. Adressaten	216
III. Einzelne Maßnahmen	216
B. Berechtigungskonzepte	217
C. Faktische Bewertung/Qualifikation	217
D. Identifizierung	218
E. Geschäftsgeheimnisgesetz (GeschGehG)	220
Teil 6 Datenpannen	221
A. Allgemeines	223
B. Adressaten der Regelungen	223
C. Verletzung des Schutzes personenbezogener Daten	224
D. Verantwortungsbereich	224
E. Keine Differenzierung nach Datenkategorien	225
F. Verschulden	225
G. Ausnahme von der Meldepflicht gegenüber der Aufsichtsbehörde	225
H. Inhalt der Meldung an die Aufsichtsbehörde	227
I. Verpflichtung zur Benachrichtigung der Betroffenen	227
J. Inhalt der Benachrichtigung	228
K. Melde-/Benachrichtigungsfrist	228
L. Dokumentation	229
M. Verwertungsverbot	229
Teil 7 Drittlanddatentransfer	231
A. „Übermittlung“ in unsichere Drittländer	233
I. „Übermittlung“	233
II. Unsicheres Drittland	234
B. Geeignete Garantien	235
I. Entscheidung des EuGH in der Rechtssache „Schrems II“ / Privacy Framework	235
II. Binding-Corporate-Rules	237
III. EU-Standarddatenschutzklauseln	237

C. Cloud-Infrastrukturen	238
I. Section 702 des FISA	239
II. Schutzmaßnahmen	239
III. Modell der „geteilten Verantwortlichkeit“	241
IV. Richtlinien für die Praxis	241
D. Tracking-/Marketing-Tools	242
E. „Content-Delivery-Networks“	243
Teil 8 Online-Tracking/Online-Marketing	245
A. Online-Tracking	247
I. ePrivacy-Richtlinie (Richtlinie 2002/58/EG)	247
1. Technikneutralität	248
2. Ausnahmen vom Einwilligungserfordernis	248
II. „Umsetzung“ im Telemediengesetz (TMG)	252
III. Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG)	253
IV. Entwürfe einer ePrivacy-Verordnung	253
V. Abkehr vom Privacy-Sandbox-Projekt	254
VI. Einwilligung	256
1. Einwilligungserteilung mittels eines „Weitersurfens“	256
2. „Nudging“/„Cookie-Walls“	258
3. Verlinkung von Einwilligungstexten/1st-Layer-Text	262
4. Erteilung von Einwilligungen mittels Browser-Settings	263
5. Privacy Information Management Systeme (PIMS) / Verordnung über Dienste zur Einwilligungsverwaltung (EinwV)	265
6. Nachweis der Erteilung von Einwilligungen	266
7. Userverhalten vor Erteilung der Einwilligung	270
VII. Verhältnis der ePrivacy-Richtlinie zur DSGVO	271
VIII. Diskussion um Google-Analytics	273
IX. Cross-Device-Tracking	275
B. Spezielle Online-Marketing-Verfahren	276
I. Realtime-Bidding-Verfahren	276
1. Einzelne technische Dienstleister/Infrastrukturen	277
2. Rechtliche Beurteilung	280
II. Audience-Matching	282
1. Funktionsweise der Tools	283
2. Rechtsgrundlage für die Datenverarbeitung durch den Werbetreibenden	283
3. Ausgestaltung des Abgleichs als Auftragsverarbeitung	284
4. Interessenabwägung	288
5. Betroffenenrechte	289
III. Vorteilsangebote auf Websites	290
IV. „Dynamic Pricing“	292

Teil 9 Direktmarketing	295
A. Printwerbung	297
I. Rechtslage unter Geltung des BDSG 2009	297
II. Rechtslage unter Geltung der DSGVO	298
1. Rechtsgrundlage	298
2. Keine Beschränkung auf „Listendaten“	298
3. Mehrere „Selektionskriterien“	299
4. „Lettershopverfahren“	300
5. Keine ausdrückliche Regelung einer „Andruckpflicht“	302
6. Hinweis auf das Widerspruchsrecht	303
III. Weitergabe von Daten an „Adressverlage“	303
IV. Verwendung von Daten aus dem Online-Impressum	304
B. Werbung mittels „elektronischer Post“ (u. a. E-Mail)	305
I. Verhältnis zur DSGVO	305
II. Werbung	306
1. „Feedbackanfragen“	306
2. Gesetzlich vorgeschriebene Kommunikation	306
III. Ausdrückliche Einwilligung	307
IV. Elektronische Post	307
1. Push-Nachrichten	307
2. „Inbox-Ads“	307
V. „Tell-a-Friend-Funktionen“	308
VI. Nachweis der Erteilung der Einwilligung	309
VII. Bewerbung „ähnlicher Waren und Dienstleistungen“ (§ 7 Abs. 3 UWG)	310
1. Elektronische Post	311
2. Erhebung der Adresse	311
3. „Ähnliche Waren und Dienstleistungen“	311
4. „Feedbackanfragen“	312
5. Hinweis bei Erhebung der elektronischen Postadresse	313
6. Hinweis auf das Widerspruchsrecht in jeder Werbung	314
7. Zeitliche Beschränkung?	314
C. Telefonwerbung	314
I. „Mutmaßliche Einwilligung“	315
II. Nachweis der ausdrücklichen Einwilligung	315
III. Ordnungswidrigkeit (§ 20 UWG)	316
Teil 10 Bonitätsprüfung/Factoring/Inkasso	319
A. Bonitätsprüfung	321
I. Zeitpunkt der Bonitätsprüfung	321
II. Bestandteile der Bonitätsprüfung	321
1. Auskunftabfrage	322
2. Internes Scoring	325
3. Nutzung eigener Informationen zum Zahlungsverhalten	327
III. Automatisierte Einzelfallentscheidung	327

IV.	Übermittlung von Bonitätsdaten an Auskunftfeien	328
1.	Gesetzliche Vorgaben	328
2.	Übermittlung von Positivdaten	330
3.	Nachmeldeverpflichtung	332
V.	Konzerninterne „Warndienste“	332
VI.	Aktive Zahlungsartensteuerung	334
1.	Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO)	334
2.	Einwilligung	335
B.	Factoring-Dienstleister	336
I.	Verantwortlichkeiten	337
II.	Übersicht Datenflüsse/Rechtsgrundlagen	338
	Risikoprüfung	339
	Verarbeitung von Daten nach dem Ankauf	339
C.	Refinanzierung/stilles Factoring	340
D.	Abgabe von Forderungen an Inkassounternehmen	341
I.	Verantwortlichkeit	341
II.	Rechtsgrundlagen	341
III.	Datenkategorien	342
IV.	Informationspflichten	343
V.	Zusammenarbeit mit Auskunftfeien	343
Teil 11 Gesellschaftsrechtliche Konstellationen		345
A.	Share-Deal/Übertragungen nach dem UmwG	347
B.	Asset-Deal	348
I.	Vertragsübernahme	348
II.	Übermittlung von Postadressdaten	349
III.	Widerspruchslösung	350
Teil 12 Folge von Datenschutzverstößen		353
A.	Ansprüche von Betroffenen aus dem BGB	355
B.	Ansprüche aus dem UWG	356
C.	Aktivlegitimation von Verbänden nach dem UKlaG	358
D.	Schadensersatzansprüche der Betroffenen aus der DSGVO	359
I.	Materieller Schaden	360
II.	Immaterieller Schaden	360
III.	Beweislast	362
E.	„Instrumentarien“ der Aufsichtsbehörden	362
I.	Verwarnung	363
II.	Untersagung	363
III.	Bußgeld	364
1.	Berücksichtigung des Konzernumsatzes	364
2.	Bußgeldzumessungskonzepte	365
Literaturverzeichnis		369
Stichwortverzeichnis		381