

ESV ERICH
SCHMIDT
VERLAG

Handbuch Kundendatenschutz

Von

Dr. Simon Menke

Leiter Konzerndatenschutz/Syndikus

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 <https://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

<https://ESV.info/978-3-503-20938-5>

Zitiervorschlag:

Menke, Handbuch Kundendatenschutz

ISBN 978-3-503-20938-5 (gedrucktes Werk)

ISBN 978-3-503-20939-2 (eBook)

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022

www.ESV.info

Druck: Hubert & Co., Göttingen

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, noch nicht abschließend geklärt ist. Zwar haben sowohl die deutschen als auch andere europäische Aufsichtsbehörden und der Europäische Datenschutzausschuss bereits einige Orientierungshilfen sowie Leitlinien veröffentlicht, die in diesen dargelegten (zumeist strengen) Positionen müssen aber naturgemäß nicht vollständig korrekt sein. Darüber hinaus vertreten einzelne Aufsichtsbehörden zum Teil voneinander abweichende Rechtsansichten.

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. Auch ist die Schaffung eines „Level-Playingfield“ im Datenschutz ein wesentliches Ziel der Datenschutz-Grundverordnung. Dieses Ziel wurde bisher jedoch nicht erreicht.

Die rechtliche Bewertung von Datenverarbeitungen wird in der Praxis regelmäßig dadurch erschwert, dass die Verarbeitungen im Rahmen technischer 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 sind. Die Erläuterungen erfolgen unter anderem im Rahmen 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 fast vier 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“ stets 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. 12. 2021 berücksichtigt werden.

Hamburg, im Februar 2022

Dr. Simon Menke

Inhaltsverzeichnis

Vorwort	5
Abkürzungsverzeichnis	15
Teil I Grundlagen	19
A. Relevante Gesetze	21
I. Datenschutz-Grundverordnung (DSGVO)	21
1. Einheitlicher Rechtsrahmen	21
2. „Level-Playingfield“/Kohärenzmechanismus	21
3. Relevanz der Erwägungsgründe	23
4. Unbestimmtheit	23
II. Bundesdatenschutzgesetz (BDSG 2018)	24
III. Telemediengesetz/Telekommunikation-Telemedien- Datenschutzgesetz (TTDSG)	25
IV. Bürgerliches Gesetzbuch (BGB)	26
V. Gesetz gegen den Unlauteren Wettbewerb (UWG)	26
VI. Gesetz gegen Wettbewerbsbeschränkungen (GWB)	27
1. Verfahren des Bundeskartellamts gegen Facebook	27
2. Regelbeispiele in § 19a GWB	28
B. Anwendungsbereich der DSGVO	30
I. Sachlicher Anwendungsbereich/Personenbezug	30
1. Rechtslage nach dem BDSG 2009	30
2. Rechtslage nach der DSGVO	31
3. „Pseudonyme“/pseudonymisierte Daten	32
4. Anonymisierung	37
5. Daten Verstorbener	40
II. Räumlicher Anwendungsbereich	41
III. Begriff der Verarbeitung	41
C. Grundsatz der „Accountability“	44
I. Einzelne gesetzliche Vorgaben	44
II. Datenschutz-Managementsystem (DSMS)	45
D. Alleinige Verantwortlichkeit	46
E. Auftragsverarbeitung	46
I. Einzelne Datenverarbeitungen	48
II. Versendung von Lieferankündigungen	49
III. Grenzfälle	50
IV. „Multifunktionale Stelle“	51
V. „Privilegierung“	53
VI. Abrede zur Auftragsverarbeitung	54
1. Abschluss von SDK	55
2. Unteraufnehmer	55
VII. Eigenständige Haftung des Auftragsverarbeiters	56

VIII. Gesetzliche Verpflichtungen des Auftragsverarbeiters/Vertragliche Haftung	56
IX. „Exzess“ des Auftragsverarbeiters	58
F. „Controller to Controller“	59
G. Gemeinsame Verantwortlichkeit	60
I. Anwendungsbereich	61
1. Fortbestand der Rechtsprechungen zur Richtlinie 95/46/EG?	62
2. Zweck der Regelungen zur gemeinsamen Verantwortlichkeit	64
3. Sinn und Zweck der konkreten Datenverarbeitung	65
II. „Phasenbezug“	65
III. „Joint-Controller-Agreement“	66
IV. Transparenz	67
V. Haftung	67
H. Datenminimierung	68
I. Speicherung in mehreren Datenbanken	69
II. „Gastzugang“	70
I. Grundsatz der Zweckbindung	71
J. Verbot mit Erlaubnisvorbehalt/Rechtsgrundlagen	72
I. Kein „Konzernprivileg“	73
II. Etwaige Nachteile für Konzerne	73
Teil 2 Rechtsgrundlagen	75
A. Einzelne Rechtsgrundlagen	77
I. Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO)	77
1. Freiwilligkeit der Einwilligung	77
2. Für den bestimmten Fall	84
3. Unmissverständlich abgegebene Willensbekundung	86
4. Dauer der Gültigkeit von Einwilligungen	87
5. Alter der Einwilligenden	88
6. Nachweis der Einwilligung	89
7. Einwilligung und AGB-Kontrolle	90
8. Widerruf der Einwilligung	92
II. Vertragserfüllung/vorvertragliche Maßnahmen (Art. 6 Abs. 1 S. 1 lit. b) DSGVO)	92
1. Vertrag/Vertragsparteien	93
2. Vorvertragliche Maßnahmen	94
3. Erforderlichkeit	95
III. Rechtliche Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c) DSGVO)	97
IV. Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO)	99
1. Berechtigtes Interesse	99
2. „Eigentliche Interessenabwägung“	108
3. Vernünftige Erwartungen der Betroffenen	115
B. Verhältnis der Rechtsgrundlagen zueinander	121

C. Zweckänderung	122
I. „Zweckkompatibilität“	123
II. Eigene Rechtsgrundlage?	125
III. Information über Zweckänderung	126
Teil 3 Informationspflichten	129
A. Schaffung von Transparenz als ein wesentliches Ziel der DSGVO	131
B. Erhebung von Daten beim Betroffenen (Art. 13 DSGVO)	132
I. Verhältnis von Art. 13 Abs. 1 DSGVO zu Art. 13 Abs. 2 DSGVO	133
II. Die einzelnen Informationen	134
1. Name und Kontaktdaten des Verantwortlichen	134
2. Kontaktdaten des Datenschutzbeauftragten	134
3. Zweck der Datenverarbeitung sowie Rechtsgrundlage	135
4. Berechtigtes Interesse an der Datenverarbeitung	135
5. Empfänger oder Kategorien von Empfängern	136
6. Absicht der Übermittlung der Daten in unsichere Drittländer	138
7. Dauer der Speicherung/Verarbeitung bzw. Kriterien für die Dauer	139
8. Hinweis auf Betroffenenrechte	140
9. Automatisierte Einzelfallentscheidung inklusive „Profiling“ ...	141
10. Zweckänderung	144
III. Ausnahme: Betroffener verfügt bereits über die Informationen ...	144
C. Nicht beim Betroffenen erhobene Daten (Art. 14 DSGVO)	145
I. Kategorien personenbezogener Daten	146
II. Quelle für die Datenerhebung	147
III. „Frist“ zur Erteilung der Informationen	147
1. Kommunikation mit den Betroffenen	147
2. Offenlegung gegenüber Empfängern	147
3. Verhältnis der Regelungen zueinander	148
IV. Informationen sind bereits bekannt	149
V. Unmöglichkeit/unverhältnismäßiger Aufwand	150
D. Rechtsfolge bei Verstoß gegen die Informationspflichten	151
Teil 4 Rechte der Betroffenen/Automatisierte Einzelfallent- scheidungen	153
A. Allgemeines zu den Rechten der Betroffenen	155
B. Die einzelnen Rechte	155
I. Recht auf Auskunft	155
1. Systematik	156
2. Recht auf Bestätigung sowie auf weitere Informationen	156
3. Informationen zum Drittlanddatentransfer	156
4. Der Betroffene verfügt bereits über die Informationen	157
5. Kopie der verarbeiteten Daten	157
6. Ausnahmen	159
II. Recht auf Berichtigung	160

III.	Recht auf Löschung	161
1.	Zweckerreichung	162
2.	Gesetzliche Verpflichtungen zur Aufbewahrung	162
3.	Recht auf Löschung und Werbewiderspruch	163
4.	Pflicht zur Löschung und „Accountability“	163
5.	Anonymisierung	163
IV.	Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)	165
V.	Mitteilungspflicht gegenüber Datenempfängern (Art. 19 DSGVO)	167
VI.	Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	168
1.	Datenkategorien/Art der Verarbeitung	168
2.	Format	169
3.	Übertragung an Dritte	170
4.	Rechte Dritter	170
VII.	Widerspruchsrecht	170
1.	Widerspruch nach Art. 21 Abs. 1 DSGVO	171
2.	Widerspruch nach Art. 21 Abs. 2 DSGVO („Direktwerbung“) ...	172
3.	Widerspruch mittels automatisierter Verfahren	172
4.	Rechtsfolge eines umzusetzenden Widerspruchs	173
5.	Praktische Grenzen der Umsetzbarkeit	173
C.	Vollmacht	176
D.	Umsetzungsfrist	176
I.	Information über ergriffene Maßnahmen	177
II.	Monatsfrist	177
III.	Verlängerung der Frist	177
E.	Form der Information	178
F.	Betroffenenrechte bei der Verarbeitung pseudonymer Daten	178
I.	Vorschrift in Art. 11 Abs. 2 DSGVO	179
II.	Einzelne Konstellationen	180
1.	Nutzung von Endgeräten durch unterschiedliche Personen ...	180
2.	„Third-Party-Konstellationen“	181
3.	Verarbeitung von Daten durch Datentreuhänder	182
4.	Verschlüsselung von Identifiern durch eine „Third-Party“	182
5.	Online-Tracking durch Websitebetreiber	183
6.	Verarbeitung von Trackingdaten in gemeinsamer Verantwortlichkeit	184
7.	Pseudonymisierung durch ausschließlich interne Maßnahmen	186
G.	Automatisierte Einzelfallentscheidung (Art. 22 DSGVO)	187
I.	Automatisierte Einzelfallentscheidung	187
II.	Rechtliche Wirkung/Beeinträchtigung in ähnlicher Weise	187

III. Ausnahmen	188
1. Erforderlichkeit der automatisierten Einzelfallentscheidung (Art. 22 Abs. 2 Ziffer a) DSGVO)	189
2. Zulässigkeit aufgrund europäischer/nationaler Regelungen (Art. 22 Abs. 2 Ziffer b) DSGVO)	189
3. Einwilligung (Art. 22 Abs. 2 Ziffer c) DSGVO)	190
IV. Weitere Anforderungen (Art. 22 Abs. 3 DSGVO)	190
V. Besondere Kategorien personenbezogener Daten	191
Teil 5 Technische und organisatorische Maßnahmen	193
A. Regelung in Art. 32 DSGVO	195
I. „Risikobasierter Ansatz“	195
II. Adressaten	196
III. Einzelne Maßnahmen	196
B. Berechtigungskonzepte	197
C. Faktische Bewertung/Qualifikation	197
D. Identifizierung	198
E. Geschäftsgeheimnisgesetz (GeschGehG)	199
Teil 6 Datenpannen	201
A. Allgemeines	203
B. Adressaten der Regelungen	203
C. Verletzung des Schutzes personenbezogener Daten	204
D. Verantwortungsbereich	204
E. Keine Differenzierung nach Datenkategorien	205
F. Verschulden	205
G. Ausnahme von der Meldepflicht gegenüber der Aufsichtsbehörde	206
H. Inhalt der Meldung an die Aufsichtsbehörde	207
I. Verpflichtung zur Benachrichtigung der Betroffenen	207
J. Inhalt der Benachrichtigung	208
K. Melde-/Benachrichtigungsfrist	208
L. Dokumentation	209
M. Verwertungsverbot	209
Teil 7 Drittlanddatentransfer	211
A. „Übermittlung“ in unsichere Drittländer	213
I. „Übermittlung“	213
II. Unsicheres Drittland	214
B. Geeignete Garantien	215
I. Entscheidung des EuGH in der Rechtssache „Schrems II“	215
II. Binding-Corporate-Rules	216
III. EU-Standarddatenschutzklauseln	216
C. Cloud-Infrastrukturen	217
I. Section 702 des FISA	218
II. Schutzmaßnahmen	218
III. Modell der „geteilten Verantwortlichkeit“	220
IV. Richtlinien für die Praxis	220

D. Tracking-/Marketing-Tools	221
E. „Content-Delivery-Networks“	222
Teil 8 Online-Tracking/Online-Marketing	225
A. Online-Tracking	227
I. ePrivacy-Richtlinie (Richtlinie 2002/58/EG)	227
1. Technikneutralität	228
2. Ausnahmen vom Einwilligungserfordernis	228
II. „Umsetzung“ im Telemediengesetz (TMG)	232
III. Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)	233
IV. Entwürfe einer ePrivacy-Verordnung	233
V. Privacy-Sandbox-Projekt	234
VI. Einwilligung	235
1. Einwilligungserteilung mittels eines „Weitersurfens“	236
2. „Nudging“/„Cookie-Walls“	238
3. Verlinkung von Einwilligungstexten/1st-Layer-Text	242
4. Erteilung von Einwilligungen mittels Browser-Settings	243
5. Privacy Information Management Systeme (PIMS)	244
6. Nachweis der Erteilung von Einwilligungen	245
7. Userverhalten vor Erteilung der Einwilligung	249
VII. Verhältnis der ePrivacy-Richtlinie zur DSGVO	250
VIII. Diskussion um Google-Analytics	252
IX. Cross-Device-Tracking	253
B. Spezielle Online-Marketing-Verfahren	254
I. Realtime-Bidding-Verfahren	254
1. Einzelne technische Dienstleister/Infrastrukturen	255
2. Rechtliche Beurteilung	258
II. Audience-Matching	260
1. Funktionsweise der Tools	261
2. Rechtsgrundlage für die Datenverarbeitung durch den Werbetreibenden	261
3. Ausgestaltung des Abgleichs als Auftragsverarbeitung	262
4. Interessenabwägung	266
5. Betroffenenrechte	267
III. Vorteilsangebote auf Websites	268
IV. „Dynamic Pricing“	270
Teil 9 Direktmarketing	273
A. Printwerbung	275
I. Rechtslage unter Geltung des BDSG 2009	275
II. Rechtslage unter Geltung der DSGVO	276
1. Rechtsgrundlage	276
2. Keine Beschränkung auf „Listendaten“	276
3. Mehrere „Selektionskriterien“	277
4. „Lettershopverfahren“	278

5.	Keine ausdrückliche Regelung einer „Andruckpflicht“	280
6.	Hinweis auf das Widerspruchsrecht	280
III.	Weitergabe von Daten an „Adressverlage“	281
IV.	Verwendung von Daten aus dem Online-Impressum	282
B.	Werbung mittels „elektronischer Post“ (u. a. E-Mail)	283
I.	Verhältnis zur DSGVO	283
II.	Werbung	283
1.	„Feedbackanfragen“	283
2.	Gesetzlich vorgeschriebene Kommunikation	284
III.	Ausdrückliche Einwilligung	284
IV.	Elektronische Post	284
1.	Push-Nachrichten	285
2.	„Inbox-Ads“	285
V.	„Tell-a-Friend-Funktionen“	286
VI.	Nachweis der Erteilung der Einwilligung	286
VII.	Bewerbung „ähnlicher Waren und Dienstleistungen“ (§ 7 Abs. 3 UWG)	287
1.	Elektronische Post	288
2.	Erhebung der Adresse	288
3.	„Ähnliche Waren und Dienstleistungen“	288
4.	„Feedbackanfragen“	289
5.	Hinweis bei Erhebung der elektronischen Postadresse	290
6.	Hinweis auf das Widerspruchsrecht in jeder Werbung	291
7.	Zeitliche Beschränkung?	291
C.	Telefonwerbung	291
I.	„Mutmaßliche Einwilligung“	292
II.	Nachweis der ausdrücklichen Einwilligung	292
III.	Ordnungswidrigkeit (§ 20 UWG)	293
Teil 10	Bonitätsprüfung/Factoring/Inkasso	297
A.	Bonitätsprüfung	299
I.	Zeitpunkt der Bonitätsprüfung	299
II.	Bestandteile der Bonitätsprüfung	299
1.	Auskunfteiabfrage	300
2.	Internes Scoring	302
3.	Nutzung eigener Informationen zum Zahlungsverhalten	304
III.	Automatisierte Einzelfallentscheidung	305
IV.	Übermittlung von Bonitätsdaten an Auskunfteien	305
1.	Gesetzliche Vorgaben	305
2.	Übermittlung von Positivdaten	308
3.	Nachmeldeverpflichtung	309
V.	Konzerninterne „Warndienste“	309
VI.	Aktive Zahlungsartensteuerung	310
1.	Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f) DSGVO)	310
2.	Einwilligung	311

B. Factoring-Dienstleister	312
I. Verantwortlichkeiten	313
II. Übersicht Datenflüsse/Rechtsgrundlagen	315
Risikoprüfung	315
Verarbeitung von Daten nach dem Ankauf	315
C. Refinanzierung/stilles Factoring	316
D. Abgabe von Forderungen an Inkassounternehmen	317
I. Verantwortlichkeit	317
II. Rechtsgrundlagen	317
III. Datenkategorien	318
IV. Informationspflichten	319
V. Zusammenarbeit mit Auskunfteien	319
Teil 11 Gesellschaftsrechtliche Konstellationen	321
A. Share-Deal/Übertragungen nach dem UmWG	323
B. Asset-Deal	324
I. Vertragsübernahme	324
II. Übermittlung von Postadressdaten	325
III. Widerspruchslösung	325
Teil 12 Folge von Datenschutzverstößen	327
A. Ansprüche von Betroffenen aus dem BGB	329
B. Ansprüche aus dem UWG	330
C. Aktivlegitimation von Verbänden nach dem UKlaG	331
D. Schadensersatzansprüche der Betroffenen aus der DSGVO	332
I. Materieller Schaden	332
II. Immaterieller Schaden	333
III. Beweislast	334
E. „Instrumentarien“ der Aufsichtsbehörden	335
I. Verwarnung	335
II. Untersagung	335
III. Bußgeld	336
1. Berücksichtigung des Konzernumsatzes	336
2. Bußgeldzumessungskonzept der DSK	337
Literaturverzeichnis	339
Stichwortverzeichnis	349