

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von

Dr. Uwe Schläger

Jan-Christoph Thode

Unter Mitarbeit von

Dr. Christian Borchers; Conrad S. Conrad; Michael Cyl; Dr. Sebastian Ertel;
Annika Freund; Clemens Grünwald; Jennifer Jähn-Nguyen; Dr. Irene Karper;
Jan-Roman Kitzinger; Dr. Martin Klein-Hennig; Dr. Bettina Kraft;
Dr. Sanela Kühn; Dr. Sönke Maseberg; Dr. Britta Mester; Lars Meyer;
Dr. M. J. Kolodziej; Christin Münzberg; Lea Paschke; Jan Peplow; Olaf Rossow;
Jan Schirmacher; Dr. Uwe Schläger; Felix Schmidt; Dr. Torge Schmidt;
Markus Schönmann; Stefan R. Seiter; Daniel Stolper; Oliver Stutz;
Jan-Christoph Thode; Sven Venzke-Caprarese; Ralf von Rahden

2., neu bearbeitete und erweiterte 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.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

<http://ESV.info/978-3-503-20533-2>

Zitiervorschlag:

Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 2. Aufl.

1. Auflage 2018

2. Auflage 2022

ISBN 978-3-503-20533-2 (gedrucktes Werk)

ISBN 978-3-503-20534-9 (eBook)

Alle Rechte vorbehalten

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

www.ESV.info

Druck: Hubert & Co., Göttingen

Vorwort

Rechtzeitig zum Inkrafttreten der EU-Datenschutz-Grundverordnung hatten wir im März 2018 erstmals unser Handbuch zum Datenschutz und zur IT-Sicherheit herausgegeben. Zielsetzung war es damals, Unternehmen, aber auch öffentlichen Stellen einen Werkzeugkasten an die Hand zu geben, um die Vorschriften der Datenschutz-Grundverordnung praxisgerecht umzusetzen und die Herausforderungen der Datenschutz-Grundverordnung zu bewältigen. Diese Zielsetzung ist auch mehr als drei Jahre nach Inkrafttreten der Datenschutz-Grundverordnung wichtiger denn je.

Nicht zuletzt aufgrund der deutlich erhöhten Bußgelder, die von Datenschutz-Aufsichtsbehörden bereits mehrfach verhängt wurden, sehen sich Unternehmen weiterhin mit enormen Herausforderungen konfrontiert: Neben erweiterten Informations-, Rechenschafts- und Meldepflichten gilt es, für Verfahren mit hohen Risiken für die Persönlichkeitsrechte der Betroffenen eine Datenschutz-Folgenabschätzung durchzuführen. Auftragsverarbeiter müssen ebenso wie Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Auch die Eignung technischer und organisatorischer Sicherheitsmaßnahmen muss regelmäßig überprüft und dokumentiert werden.

Die nunmehr vorliegende zweite Auflage unseres Handbuchs stellt eine inhaltlich überarbeitete Auflage dar, die sowohl auf zwischenzeitliche Urteile zum Datenschutz als auch auf Best-Practice-Ansätze Bezug nimmt, die sich in den letzten Jahren entwickelt und bewährt haben. Erstellt und aktualisiert wurde das Handbuch von erfahrenen Beraterinnen und Beratern der datenschutz nord Gruppe, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit als Consultant tätig sind.

Das vorliegende Datenschutz-Handbuch richtet sich an betriebliche Datenschutzbeauftragte, IT-Administratoren, Unternehmensleitungen, Betriebs- oder Personalräte, aber auch an datenschutzinteressierte Beschäftigte und Kunden, die sich entweder einen Überblick über die neuen gesetzlichen Regelungen verschaffen wollen oder praxisgerechte Vorschläge zur Umsetzung der Datenschutz-Grundverordnung nachlesen möchten.

Das Handbuch gliedert sich im Wesentlichen in zwei Hauptteile: Die Kapitel A bis F sind datenschutzrechtlich geprägte Kapitel, während die Kapitel G bis J sicherheitstechnische Aspekte in den Vordergrund stellen. Nachdem wir in Kapitel A zunächst auf die datenschutzrechtlichen Grundlagen eingehen, stellen wir in Kapitel B vor, wie ein betriebliches Datenschutz-Management umgesetzt werden sollte. In Kapitel C steht die gesetzeskonforme Verarbeitung von Beschäftigtendaten im Vordergrund, in Kapitel D die gesetzeskonforme Verarbeitung von Kundendaten. Kapitel E beschäftigt sich mit der Verarbeitung personenbezogener Daten im Internet, in sozialen Netzwerken und in unterneh-

menseigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuches beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informationssicherheits-Managements beschrieben. Kapitel I stellt geeignete technisch-organisatorische Maßnahmen vor, und zwar übergreifende Maßnahmen, Infrastrukturmaßnahmen, Maßnahmen seitens der IT-Systeme, Netzwerkmaßnahmen und Maßnahmen auf Anwendungsebene. Und schließlich wird in Kapitel J beschrieben, in welcher Form Penetrationstest zur Evaluierung einer angemessenen IT-Sicherheit durchgeführt werden können.

Trotz der zahlreichen Verweise auf andere Kapitel dieses Buches sind sämtliche Hauptkapitel in sich abgeschlossen und können separat ohne Kenntnis der anderen Kapitel als Erkenntnisquelle dienen.

In diesem Sinne wünschen wir Ihnen als Herausgeber dieses Datenschutz-Handbuchs viel Spaß beim Lesen und Nachschlagen.

Bremen und Berlin, im Oktober 2021 Uwe Schläger und Jan-Christoph Thode

Inhaltsverzeichnis

Vorwort	V
Bearbeiterverzeichnis	XV
Abkürzungsverzeichnis	XVII
Literaturverzeichnis	XXI
Kapitel A Datenschutzrechtliche Grundlagen	1
1 Geschichte des Datenschutzrechts	3
1.1 Erste Entwicklungen	3
1.2 Das Volkszählungsurteil des Bundesverfassungsgerichts	4
1.3 Entwicklung der Datenschutzgesetze in Deutschland	9
2 Datenschutzrecht in Deutschland und in der EU	25
2.1 Maßgebliche Rechtsquellen	25
2.2 Grundlagen der Datenverarbeitung	28
2.3 Datenschutzrechtliche Grundsätze	37
2.4 Betroffenenrechte	44
2.5 Sanktionen	54
3 Anwendungsbereich der DSGVO	57
3.1 Niederlassungsprinzip	59
3.2 Marktortprinzip	62
3.3 Sonderfall Völkerrecht	67
3.4 Öffnungsklauseln	67
4 Datenschutzrecht außerhalb von Europa	71
4.1 USA	71
4.2 Japan	79
4.3 Russland	88
Kapitel B Datenschutzmanagement im Unternehmen	97
1 Der betriebliche Datenschutzbeauftragte	99
1.1 Bestellpflicht	99
1.2 Mitteilungspflicht gegenüber der Aufsichtsbehörde	108
1.3 Qualifikation	109
1.4 Wahrnehmung durch natürliche oder auch juristische Person?	111
1.5 Stellung im Unternehmen	112
1.6 Aufgaben	115
1.7 Abberufung	123
2 Verzeichnis von Verarbeitungstätigkeiten	125
2.1 Sinn und Zweck der Dokumentation	125
2.2 Zuständigkeit	125
2.3 Adressaten	126

2.4	Inhalt und Form	126
2.5	Historie und Aktualisierungsintervall	129
3	Datenschutz-Folgenabschätzung	131
3.1	Anwendungsbereich	131
3.2	Schwellenwert-Analyse	132
3.3	Durchführungsphase	133
3.4	Dokumentation	137
4	Verpflichtung auf das Datengeheimnis	139
4.1	Die Verpflichtung und die DSGVO	139
4.2	Praxisnahe Umsetzung im Unternehmensumfeld	139
4.3	Adressaten	140
4.4	Sanktionen bei Verletzung	141
5	Meldepflicht bei Datenpannen	143
5.1	Inhalt, Art und Weise und Frist der Meldung an die Aufsichtsbehörde	145
5.2	Inhalt, Art und Weise und Frist der Meldung an Betroffene	146
5.3	Ausnahme – Risikoabwägung	147
5.4	Dokumentation	147
5.5	Ausschlussgründe	148
6	Outsourcing	151
6.1	Auftragsverarbeitung – Chancen und Risiken	151
6.2	Abgrenzung zur eigenen Verantwortlichkeit	156
6.3	Gemeinsam für die Verarbeitung Verantwortliche	157
6.4	Übermittlung an Drittländer außerhalb der EU	157
7	Kontrolle des Datenschutzniveaus	165
7.1	Rolle des Datenschutzbeauftragten	165
7.2	Abgleich der Verfahrenspraxis mit Verzeichnissen	165
7.3	Abgleich der Verfahrenspraxis mit Betriebsvereinbarungen oder Richtlinien	165
7.4	Auditierung der Auftragsverarbeiter	166
7.5	Nachweis durch Zertifikate	167
7.6	Dokumentation	168
8	Datenlöschung	169
8.1	Das Praxisproblem – Warum soll ich Daten löschen?	169
8.2	Bestandsaufnahme für Löschfristen	170
8.3	Erstellung eines Löschkonzepts	171
9	Datenweitergabe im Konzern	173
9.1	Konzernprivileg	174
9.2	Auftragsverarbeitung im Konzern	175
9.3	Gemeinsame Verantwortlichkeit	176
9.4	Übermittlung innerhalb Europas	179
9.5	Beschäftigtendaten	182
9.6	Übermittlung außerhalb Europas	184

Kapitel C Verarbeitung von Beschäftigendaten	187
1 Regelungen zum Beschäftigendatenschutz	189
1.1 Öffnungsklausel	189
1.2 Regelungen im BDSG-neu	190
1.3 Betriebsvereinbarungen	191
2 Bewerbermanagement	193
2.1 Zulässigkeit der Datenverarbeitung im Bewerbungsverfahren	193
2.2 Dauer der Speicherung von Bewerberdaten	198
2.3 Informationspflichten	200
3 Personalakten	201
3.1 Inhalte	201
3.2 Zugriffsrechte	203
3.3 Aufbewahrungsdauer	203
3.4 Rechte des Mitarbeiters	204
3.5 Best Practice	205
4 Zeiterfassung	209
4.1 Abhängigkeit vom Arbeitszeitmodell	209
4.2 Erfassung der Kommt-, Geht- und Pausenzeiten	209
4.3 Zugriffsrechte	210
4.4 Aufbewahrungszeiten	210
5 Personalentwicklung	211
5.1 Schulungssysteme/Learning-Management-Systems	212
5.2 Mitarbeitergespräche	214
5.3 Arbeitszeugnisse und Performance-Management	215
5.4 Mitarbeiterprofile (Persönlichkeitsprofile)	217
5.5 Mitarbeiterbefragungen	220
5.6 360-Grad-Feedback	223
5.7 Outplacement	226
6 Nutzung von Internet, E-Mail und Telefon	227
6.1 Internet- und E-Mail-Nutzung	227
6.2 Telefonie	235
7 Ortung von Mitarbeitern	241
7.1 Ortung von Mobiltelefonen/GPS-Ortung	241
7.2 Betriebsvereinbarung/Einwilligung	242
7.3 Gesetzliche Grenzen	242
7.4 Transparenzpflichten	245
7.5 Aufdeckung von Straftaten	246
7.6 Sonstige Anforderungen	246
8 Auskunftersuchen von Behörden und sonstigen Dritten	247
8.1 Spezialgesetzliche Normen	247
8.2 Einwilligung	247
8.3 Berechtigtes Interesse an einer Datenherausgabe	247
8.4 Rahmenbedingungen und Umfang einer Datenherausgabe	248

9	Compliance-Maßnahmen	251
9.1	Der Begriff Compliance	251
9.2	Konfliktpotential zum Datenschutz	255
9.3	Datenschutzrechtliche Erlaubnisnormen	256
9.4	Best Practice	260
9.5	Sonstiges	277
10	Verarbeitung von Gesundheitsdaten	279
10.1	Rechtliche Grundlagen	279
10.2	Betriebsärztliche Untersuchungen	285
10.3	Eignungstests	288
10.4	Betriebliches Eingliederungsmanagement	289
11	Betriebsrat und Datenschutz	295
11.1	Stellung des Betriebsrats im Betriebsverfassungsgesetz	295
11.2	Aufgaben des Betriebsrats	295
11.3	Verwendung von Beschäftigtendaten im BetrVG	296
11.4	Stellung des Betriebsrats im BDSG	302
11.5	Verantwortung des Betriebsrats für den Datenschutz	305
11.6	Verwendung von Beschäftigtendaten durch den Betriebsrat	307
11.7	Kontrolle des Betriebsrats durch den Datenschutzbeauftragten	308
	Kapitel D Verarbeitung von Kundendaten	311
1	CRM-Systeme	313
1.1	Ausgestaltung und Anforderungen	313
1.2	Erfüllung eines Vertrages	315
1.3	Vorvertragliche Maßnahmen	317
1.4	Erforderlichkeit	318
1.5	Einzelne Kategorien von Daten	320
1.6	Nutzung innerhalb eines Konzerns	321
2	Marketing und Werbung	327
2.1	Regelungen in der DSGVO	327
2.2	Verschiedene Werbemaßnahmen	328
2.3	Widerspruchsrecht	343
2.4	Dokumentationspflichten	344
2.5	Geldbußen	344
3	Kundenbindungssysteme	347
3.1	Kundenbindung versus Datenschutz	347
3.2	Datenverarbeitung zur Programmabwicklung	351
3.3	Datenverarbeitung für Werbung und Marktforschung	353
3.4	Betroffenenrechte der Kundenkartenteilnehmer	357
3.5	Kundenkartensysteme in der Praxis	358
4	Unternehmenskauf	361
4.1	Einwilligung und Betriebsübergang	361
4.2	Datenaustausch vor einer Transaktion (Due-Diligence-Phase)	362
4.3	Informationspflichten gegenüber der betroffenen Person	364
4.4	Vollzug einer Transaktion	366

5	Bonitätsmanagement (einschl. Scoring)	369
5.1	Beteiligte des Bonitätsmanagements	370
5.2	Datenübermittlung an eine Auskunftfei	371
5.3	Allgemeine Bonitätsbewertung	378
5.4	Bonitätsbewertung mittels Scoring-Verfahren	381
5.5	Auskunfteien	390
5.6	Datenschutz-Folgenabschätzung	392
5.7	Bestellung eines Datenschutzbeauftragten	392
5.8	Konsultation der Aufsichtsbehörde	393
5.9	Rechte der betroffenen Person	393
5.10	Best Practice	401
	Kapitel E Datenverarbeitung im Internet und Intranet	405
1	Webseiten	407
1.1	Anwendbares Recht	407
1.2	Informationspflichten	408
1.3	Datenschutzerklärung	411
1.4	Disclaimer	414
1.5	Einwilligung auf Webseiten	415
1.6	Der Einsatz von Cookies	419
1.7	Tracking-Tools	429
1.8	Device-Fingerprinting	433
1.9	Newsletter	434
1.10	Kontaktformular	435
1.11	Tell-a-Friend-Funktion	436
1.12	Social-Media-Plugins	437
1.13	Veröffentlichung von Mitarbeiterdaten und -fotos	438
1.14	Gästebuch und Foren	440
1.15	Bewerbungsportal	441
1.16	Rechtspflichten zur Sicherung von Webseiten	443
1.17	Recht auf Datenübertragbarkeit	446
2	Soziale Netzwerke	449
2.1	Social-Media-Auftritt des Unternehmens	449
2.2	Social-Media-Plugins und eingebettete Inhalte	461
2.3	Marketing auf Social-Media-Plattformen	466
2.4	Social-Media-Recruiting	479
2.5	Nutzung von Social-Media-Diensten	480
2.6	Unternehmensinterne Social-Media-Nutzung	484
2.7	Künftige Entwicklungen	486
3	Intranet-Portale	489
3.1	Datenschutzrechtliche Rahmenbedingungen	490
3.2	Veröffentlichung von Kontaktdaten	492
3.3	Veröffentlichung von Bildnissen	492
3.4	Veröffentlichung von Qualifikationen und Lebensläufen	494
3.5	Veröffentlichung von Geburtstagen	494
3.6	Kalenderfunktion	495

3.7	Unternehmensinterne Kommunikationsplattformen am Beispiel von Microsoft Teams	495
3.8	Unternehmensinterne Intranet-Anwendungen am Beispiel von Microsoft Yammer	501
3.9	Künftige Entwicklungen	503
Kapitel F Videoüberwachung im Unternehmen		505
1	Personenbeziehbarkeit und Verarbeitung von Bilddaten	507
2	Rechtliche Grundlagen für Unternehmen	511
2.1	Videoüberwachung mit Einwilligung	512
2.2	Videoüberwachung aufgrund rechtlicher Verpflichtung	513
2.3	Videoüberwachung im öffentlichen Interesse	513
2.4	Videoüberwachung aufgrund Interessenabwägung	515
2.5	Videoüberwachung im Beschäftigungskontext	518
2.6	Videokonferenz und Videoidentifizierung	521
2.7	Videoüberwachung von Kindern	524
2.8	Verdeckte Videoüberwachung	525
3	Sicherheitsmaßnahmen für Videosysteme	527
3.1	Hinweisschilder	527
3.2	Löschung der Bilddaten	529
3.3	Sonstige technische und organisatorische Pflichten	531
4	Beispiele aus der Praxis	533
4.1	Supermärkte und Einkaufszentren	533
4.2	Gastronomie	533
4.3	Banken, Spielhallen, Tankstellen	534
4.4	Krankenhäuser, Praxen, Heime, Videosprechstunden	534
4.5	Wohnobjekte und Hotels	535
4.6	Baustellen	536
4.7	Abfallbeseitigung, Müllcontainer	537
4.8	Parkplätze, Parkhäuser, Kennzeichenerfassung	537
4.9	Öffentliche Verkehrsmittel	537
4.10	Dashcams in Unternehmensfahrzeugen	538
4.11	Außenfassaden und Perimeterschutz	539
4.12	Rechenzentren und Serverräume	540
Kapitel G Rechtliche Grundlagen der Informationssicherheit		541
1	Datenschutzgrundverordnung	543
1.1	Technische und organisatorische Maßnahmen	543
1.2	Pseudonymisierung	552
1.3	Anonymisierung	554
1.4	Verschlüsselung	555
1.5	Durchführung von Tests	556
1.6	Nachweispflichten	556
2	IT-Sicherheitsgesetz, europäische NIS-Richtlinie	561
2.1	Betreiber kritischer Infrastrukturen	561
2.2	Betreiber von Webseiten	563

2.3	Anbieter digitaler Dienste	564
2.4	EU Cybersecurity Act	565
3	Bereichsspezifische Normen	567
3.1	Energiewirtschafts- und Messstellenbetriebsgesetz	567
3.2	Kreditwesengesetz	567
3.3	Glücksspielstaatsvertrag	569
Kapitel H IT-Sicherheitsmanagement im Unternehmen		571
1	Vorgehensweise	573
2	Merkmale eines ISMS	575
2.1	Management-Prinzipien	575
2.2	Ressourcen	577
2.3	Mitarbeiter	577
2.4	Strategie	578
3	ISO/IEC 27001 und IT-Grundschutz	581
3.1	Unterschiede und Gemeinsamkeiten	581
3.2	ISO/IEC 27000-er Normenreihe	582
3.3	ISO 27001 auf der Basis von IT-Grundschutz	587
4	Bedeutung von Zertifikaten	593
Kapitel I Technische und organisatorische Maßnahmen		595
1	Übergreifende Aspekte	597
1.1	Behandlung von Sicherheitsvorfällen	597
1.2	Hardware und Software Management	599
1.3	Personal Management	602
1.4	Datensicherung	605
1.5	Archivierung	610
1.6	Datenlöschung	613
1.7	Verschlüsselung	618
1.8	Getrennte Test- und Produktivsysteme	628
1.9	Cloud-Computing	630
2	Infrastruktur	637
2.1	Zutrittskontrollsysteme	637
2.2	Brandschutzmaßnahmen	639
2.3	Maßnahmen gegen Über- und Unterspannung	640
2.4	Klimageräte	642
2.5	Vermeidung wasserführender Leitungen	642
3	IT-Systeme	643
3.1	Serversysteme	643
3.2	Clientsysteme	648
3.3	Mobile Endgeräte und Mobile-Device-Management	650
3.4	Verteilung und Verwaltung privilegierter Zugänge	651
4	Netze	653
4.1	Internetanbindung	653
4.2	Intranet	657

4.3	Verzeichnisdienste	660
4.4	Administration	663
5	Anwendungen	665
5.1	Identifizierung, Authentisierung und Autorisierung	665
5.2	Berechtigungs- und Rollenkonzepte	670
5.3	Mandantentrennung	672
5.4	Protokollierung von Anwendungsaktivitäten	673
Kapitel J	Penetrationstest	675
1	Vorgehensweise	677
1.1	Kickoff	678
1.2	Durchführung der Tests	679
1.3	Auswertung und Dokumentation	680
1.4	Ergebnispräsentation	680
1.5	Prüfung der Verbesserungsmaßnahmen	680
2	Testszzenarien	683
2.1	Black-Box	683
2.2	White-Box	683
2.3	Grey-Box	683
3	Testmodule und Prüff Themen	685
3.1	Systeme und Netzwerke	685
3.2	Anwendungen	689
Stichwortverzeichnis		697