

Datenschutz und IT-Compliance

Das Handbuch für Admins und IT-Leiter

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

1	Grundlagen: Was Sie über den Datenschutz wissen müssen	17
2	Das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)	47
3	Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb	61
4	Datenschutz beim Betrieb von Websites	123
5	Datenschutzverpflichtungen als Unternehmen umsetzen	163
6	Umgang mit Datenschutzvorfällen	219
7	Export von Daten in alle Welt: Was ist erlaubt?	239
8	Umgang mit den Daten von Mitarbeitern	265
9	Einführung Compliance	305
10	Folgen bei Datenschutzproblemen: Sanktionen, Abmahnungen und Schadenersatz	333
11	Strafrechtliche Risiken für Admins	355
12	Generative KI: Was bei der Nutzung von ChatGPT & Co. zu beachten ist	385

Inhalt

Vorwort	15
1 Grundlagen: Was Sie über den Datenschutz wissen müssen	17
1.1 Eine kleine Geschichte des Datenschutzes	17
1.2 Die Datenschutzgesetze im Überblick	19
1.3 Ein erster Blick: Aufbau und wichtige Begriffe in der DSGVO	20
1.4 Was ist überhaupt geschützt: personenbezogene Daten	22
1.5 Umgang mit personenbezogenen Daten: Verarbeitung & Co.	24
1.6 Grundsätze und Prinzipien des Datenschutzes	25
1.6.1 Rechtmäßigkeit der Verarbeitung	25
1.6.2 Verarbeitung nach Treu und Glauben	25
1.6.3 Transparenz	25
1.6.4 Zweckbindung	26
1.6.5 Datenminimierung	27
1.6.6 Richtigkeit der Datenverarbeitung	27
1.6.7 Speicherbegrenzung	28
1.6.8 Integrität und Vertraulichkeit	28
1.6.9 Rechenschaftspflicht	29
1.7 Abwägungssache: Der risikobasierte Ansatz in der DSGVO	29
1.8 Immer notwendig: Rechtsgrundlagen in der DSGVO	31
1.8.1 Die Einwilligung	31
1.8.2 Erfüllung eines Vertrags oder die Durchführung einer vorvertraglichen Maßnahme	34
1.8.3 Erfüllung einer rechtlichen Verpflichtung	35
1.8.4 Schutz lebenswichtiger Interessen	36
1.8.5 Wahrnehmung öffentlicher Interessen oder Ausübung öffentlicher Gewalt	36
1.8.6 Wahrung berechtigter Interessen	37
1.8.7 Ein Sonderfall: Datenverarbeitung für die Zwecke des Beschäftigungsverhältnisses	41
1.8.8 Höhere Anforderungen: Besondere Kategorien von personenbezogenen Daten	42
1.9 Die Haushaltsausnahme: Datenverarbeitung im privaten Bereich	44

2 Das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) 47

2.1 Hintergrund: Was regelt das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)? 47

2.2 Anwendungsfall »Telemedien« 49

2.2.1 Technische und organisatorische Vorkehrungen 49

2.2.2 Schutz der Privatsphäre bei Endeinrichtungen 52

2.2.3 Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen 55

2.3 Anwendungsfall Telekommunikation 56

2.3.1 Speicherung von Logdaten 57

2.3.2 Anwendungsbereich »interpersonelle Telekommunikationsdienste« 58

2.3.3 Muss der Arbeitgeber das Fernmeldegeheimnis beachten? 58

3 Technischer Datenschutz: Anforderungen der DSGVO an den IT-Betrieb 61

3.1 Die Grundlagen: Was ist technischer Datenschutz? 61

3.2 Sicher ausgewählt: Technische und organisatorische Maßnahmen (TOM) 65

3.2.1 Geeignetheit, Angemessenheit und Stand der Technik 65

3.2.2 Quellen zum Stand der Technik 68

3.2.3 Das Risiko als Bewertungskriterium 73

3.3 Systemprotokolle und Weblogs: Was ist notwendig, und was ist erlaubt? 76

3.3.1 Protokollierung zur Analyse von Webzugriffen 77

3.3.2 Protokollierung zur Analyse des E-Mail-Verkehrs 79

3.3.3 Protokollierung ohne konkreten Anlass 82

3.3.4 Protokollierung in besonderen Fällen 84

3.4 Verfügbar, wenn es notwendig ist: Backups und Archivierung 84

3.5 Nichts ist für die Ewigkeit: Löschpflichten und Löschkonzepte 88

3.6 Wolkige Aussichten: Anforderungen an die Datenverarbeitung in der Cloud 95

3.7	Arbeitsplatz »Home-Office«: Was ist zu beachten?	101
3.7.1	Grundsätzliche Überlegungen	102
3.7.2	Vorgaben für das Home-Office: ein Überblick	103
3.7.3	Regelungsbereiche der Anforderungen	104
3.7.4	Videokonferenzen als Sonderfall	109
3.8	Videoüberwachung: Voraussetzungen für den legalen Betrieb	114
4	Datenschutz beim Betrieb von Websites	123
<hr/>		
4.1	Grundlagen der technischen Gestaltung von Websites	123
4.2	Pflichtübung: Die aussagekräftige und rechtskonforme Datenschutzerklärung	124
4.2.1	Die rechtlichen Grundlagen der Datenschutzerklärung	126
4.2.2	Mindestinhalt einer Datenschutzerklärung	127
4.3	Newsletter	138
4.3.1	Rechtsgrundlage für den Newsletter-Versand	138
4.3.2	Kopplungsverbot	139
4.3.3	Anmeldung zum Newsletter: die Einwilligung	140
4.3.4	Auswertung des Nutzerverhaltens	143
4.3.5	Impressum und Abmelde-Link	144
4.3.6	Widerruf der Einwilligung	144
4.3.7	Einsatz von Dienstleistern für den Newsletter-Versand	146
4.4	Schlankheitskur: Datenschutzkonformer Umgang mit Cookies & Co.	146
4.4.1	Grundsatz: Einwilligungsbedürftigkeit	146
4.4.2	Cookie-Banner zur Einholung von Einwilligungen	147
4.4.3	Nachweis von Einwilligungen	156
4.5	Rechtmäßige Analyse: Richtiger Umgang mit Google Analytics & Co.	156
4.5.1	Webanalysen ohne Einwilligung?	156
4.5.2	Rechtsgrundlage für die weiteren Verarbeitungen	157
4.5.3	Eingeschränkte Analysemöglichkeiten ohne Einwilligung	158
4.6	Datenschutzaspekte im Zusammenhang mit HTML5 sowie bei Googles FLoC und Co.	159

5 Datenschutzverpflichtungen als Unternehmen umsetzen 163

5.1 Bestandsaufnahme der Daten im Unternehmen: So erstellen Sie ein Verarbeitungsverzeichnis (VVT)	164
5.1.1 Wer muss ein VVT führen?	164
5.1.2 Wer hat Einblick in das VVT?	165
5.1.3 Wie wird ein VVT erstellt und gepflegt?	165
5.1.4 Gesetzliche Mindestinhalte des VVT	168
5.1.5 Was passiert, wenn ich kein VVT führe bzw. es nicht pflege?	177
5.2 Technische und organisatorische Maßnahmen (TOM) festlegen und dokumentieren	178
5.3 Richtig informieren: Datenschutzhinweise für Betroffene	182
5.3.1 Transparenzgrundsatz	182
5.3.2 Allgemeine Regeln zu Betroffenenrechten in Art. 12 DSGVO	183
5.3.3 Datenschutzhinweise nach Art. 13 DSGVO	186
5.4 Wie Ihr Unternehmen seiner Auskunftspflicht richtig nachkommt	192
5.4.1 Auskunftsanspruch nach Art. 15 DSGVO	193
5.4.2 Anspruch auf Kopie?	195
5.4.3 Wie erfülle ich den Anspruch?	196
5.5 Die Auftragsverarbeitung: Was müssen Sie beachten?	197
5.6 Die Datenschutz-Folgenabschätzung: Notwendigkeit und Durchführung	202
5.6.1 Wann muss eine DSFA durchgeführt werden?	204
5.6.2 Wie wird eine DSFA durchgeführt?	206
5.7 Der Datenschutzbeauftragte: Notwendigkeit und Anforderungen	208
5.7.1 Wann muss ein DSB benannt werden?	208
5.7.2 Wie wird ein DSB benannt?	210
5.7.3 Interner oder externer DSB?	211
5.7.4 Konzerndatenschutzbeauftragte	213
5.7.5 Laufzeit der Benennung	213
5.7.6 Organisatorische Einordnung des DSB	213
5.7.7 Aufgaben des DSB	214
5.7.8 Wer kann DSB sein?	215
5.7.9 Wann haftet der DSB?	216

6	Umgang mit Datenschutzvorfällen	219
6.1	Wenn der IT-Vorfall zur Datenschutzkatastrophe wird	219
6.1.1	Richtig Vorbeugen: Aufbau eines interdisziplinären Incident-Response-Managements	220
6.1.2	Nehmen Sie Kontakt auf!	221
6.2	In der Krise: Wichtige Schritte planen!	222
6.3	Grundlagen der Meldepflicht von Datenschutzverstößen an die Aufsichtsbehörde	223
6.3.1	Art. 33: In welchen Fällen muss gemeldet werden?	224
6.3.2	Art. 33: Vorbereitung und Durchführung der Meldung	226
6.3.3	Aufsichtssache: Erstellen und Übersenden der Meldung an die Aufsichtsbehörde	228
6.4	Die Benachrichtigung an die Betroffenen nach Art. 34	230
6.4.1	Entstehen der Benachrichtigungspflicht an die Betroffenen	230
6.4.2	Ausnahmen der Benachrichtigungspflicht	231
6.4.3	Inhalt der Benachrichtigungen	232
6.5	Meldepflichten für Auftragsverarbeiter	233
6.6	Bußgelder im Kontext mit Meldepflichten	233
6.7	Schadensersatzansprüche bei Data Breaches	235
6.8	Damit es nicht nochmal passiert: Lessons Learned	236
6.9	Zwischenfazit und Checkliste	238
7	Export von Daten in alle Welt: Was ist erlaubt?	239
7.1	Der Datenschutz und die nationalen Grenzen	239
7.2	Die Welt in drei Zonen geteilt	240
7.2.1	Datentransfer innerhalb des EWR	240
7.2.2	Sichere Drittstaaten: Länder mit Angemessenheitsbeschluss	241
7.2.3	Unsichere Drittstaaten	242
7.2.4	Datenexport in die USA: Eine schwierige Geschichte	242
7.3	Datenexport in Drittstaaten am Beispiel der USA	246
7.3.1	Standarddatenschutzklauseln	247
7.3.2	Zusätzliche technische Maßnahmen bei Standarddatenschutzklauseln	250

7.3.3	Binding Corporate Rules (BCR)	253
7.3.4	Zertifizierung	254
7.3.5	Einwilligung	254
7.3.6	Weitere Sonderfälle nach Art. 49 DSGVO	256
7.4	Datenexport in andere Drittstaaten	256
7.5	Europäische Töchter von US-Unternehmen und der CLOUD Act	256
7.6	Privacy Shield 2.0: Alles neu durch das TADPF?	259
7.6.1	Grundgedanken des TADPF	259
7.6.2	Praktische Nutzung des TADPF	260
7.6.3	Wird der TADPF ein Erfolgsmodell?	260
7.7	Fallbeispiel Datentransfer: Massenabmahnungen für Google Fonts	261
7.8	Zwischenfazit	263
8	Umgang mit den Daten von Mitarbeitern	265
<hr/>		
8.1	Grundlage des Beschäftigtendatenschutzes: § 26 BDSG	266
8.1.1	Geltungsbereich	266
8.1.2	Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis	267
8.1.3	Begründung des Beschäftigungsverhältnisses: die Bewerbung	268
8.1.4	Informationssicherheit bei Bewerbungsverfahren	269
8.1.5	Durchführung des Beschäftigungsverhältnisses	270
8.1.6	Beendigung des Arbeitsverhältnisses	270
8.1.7	Einwilligung im Arbeitsverhältnis	271
8.1.8	Aufdecken von Straftaten	272
8.2	Nutzung von E-Mail, Chat und Internet im Unternehmen	272
8.2.1	Verbot der privaten Nutzung	273
8.2.2	Gestattung der privaten Nutzung	275
8.2.3	Protokolle aus Gründen der Informationssicherheit	276
8.2.4	Umgang mit den E-Mails von ausscheidenden Mitarbeitern	276
8.2.5	Erstellen und Durchsetzen von klaren Regeln	277
8.3	Chef liest mit! Möglichkeiten und Grenzen der Überwachung von Mitarbeitern	279
8.3.1	Der gläserne Mitarbeiter: Das höchste deutsche DSGVO-Bußgeld	279
8.3.2	Verführerische Technik	280
8.3.3	IT-Sicherheit vs. Privatsphäre	281
8.3.4	Elektronische Augen: Videoüberwachung am Arbeitsplatz	281

8.3.5	Bußgelder für die Mitarbeiterüberwachung	282
8.3.6	Sag mir wo und wann: Mitarbeiterüberwachung per GPS	282
8.3.7	Arbeitszeiterfassung	283
8.3.8	Überwachung im Home-Office	283
8.3.9	Komplette Selbstvermessung	284
8.4	Rechtsrisiken für Administratoren: Haftungsrisiken und Fallbeispiele	285
8.4.1	Arbeitsrechtliche Risiken im Bereich der IT	286
8.4.2	Missachtung des Datenschutzes	287
8.4.3	Kündigung wegen Vertrauensverstoß	288
8.4.4	Unerlaubte Installation von Software	288
8.4.5	Fallbeispiel: Der gelangweilte Admin	289
8.5	Bring Your Own Device (BYOD) und die Vermischung von Privatem und Geschäftlichem	290
8.6	Ärger mit dem Chef: Wie können sich Admins gegen zweifelhafte Anweisungen wehren?	292
8.6.1	Von der Neugier zum Kontrollwahn	293
8.6.2	Beschäftigte sind weisungsgebunden	293
8.6.3	Das Weisungsrecht des Arbeitgebers	294
8.6.4	Wenn Grenzen überschritten werden	294
8.6.5	Keine Pflicht zur Umsetzung rechtswidriger Anweisungen	295
8.6.6	Umsetzung und Widerstand in der Praxis	296
8.6.7	Sonderregeln bei Notfällen	297
8.6.8	Rechtssicherheit für alle Beteiligten schaffen	298
8.6.9	Schwieriger Umgang mit privaten Daten	299
8.6.10	Vertreterregelungen sind das A und O	299
8.7	Mitbestimmungsrecht der Arbeitnehmervertretungen	300
8.7.1	Einführung und Nutzung von technischen Einrichtungen	300
8.7.2	Mitarbeitervertretung und Überwachung	301
9	Einführung Compliance	305
9.1	Die Grundlagen: Was ist überhaupt Compliance?	305
9.2	Verletzung von Compliance-Vorgaben: Risiken für Unternehmen	309
9.3	Verletzung von Compliance-Vorgaben: Pflichten und Haftung von Führungskräften	310
9.3.1	Grundlagen der Geschäftsführerhaftung	310
9.3.2	Delegation von Verantwortlichkeit im Unternehmen	312

9.3.3	Haftung für Compliance-Versäumnisse	313
9.3.4	D&O-Versicherungen für Führungskräfte	315
9.4	Schutzmechanismen: Die Rolle von Compliance Management Systemen	315
9.4.1	Einrichtung eines CMS	316
9.4.2	Vorlagen für CMS	317
9.4.3	Mitbestimmungspflicht des Betriebsrats	322
9.5	Was ist IT-Compliance?	323
9.6	Aus dem Dunkeln holen: Der Umgang mit Schatten-IT	325
9.7	Umgang mit Whistleblowern: Hinweisgeber angemessen schützen	326
9.8	Wie sage ich es meinem Chef: Umgang mit fragwürdigen Arbeitsanweisungen	328
9.8.1	Weisungsrecht des Arbeitgebers	328
9.8.2	Rechte der Arbeitnehmer	329
9.8.3	Tipps für die Praxis zur Konfliktlösung und -prävention	330
9.8.4	Umgang mit Notfällen	332

10 Folgen bei Datenschutzproblemen: Sanktionen, Abmahnungen und Schadenersatz 333

10.1	Datenschutzverstöße werden bestraft: Sanktionsmöglichkeiten der DSGVO	333
10.1.1	Sanktionsmöglichkeiten der Aufsichtsbehörden	333
10.1.2	Rechte der Betroffenen	336
10.1.3	Abmahnungen durch Mitbewerber	337
10.2	Das Schwert der Aufsichtsbehörden: Bußgelder nach Art. 83 DSGVO	338
10.2.1	Zwei Bußgeldrahmen	338
10.2.2	Bestimmung der Bußgeldhöhe	339
10.2.3	Bußgeldkonzepte der Aufsichtsbehörden	340
10.2.4	Ein Sonderproblem: Rechtsträgerprinzip vs. Funktionsträgerprinzip	342
10.2.5	Beispiele für Bußgelder	344
10.3	Das kann teuer werden: Schadenersatzansprüche der Betroffenen	345
10.3.1	Art. 82 DSGVO als zentrale Anspruchsgrundlage	345
10.3.2	Verstoß gegen die DSGVO	345
10.3.3	Folgefragen	346

10.4 Böse Überraschung: Wann drohen Abmahnungen?	350
10.4.1 Rechtsgrundlage für Abmahnungen	350
10.4.2 Unterlassungsanspruch und strafbewehrte Unterlassungserklärung	352
10.4.3 Einstweiliges Verfügungsverfahren	352
10.4.4 Rechtsanwaltskosten	353
10.4.5 Rechtfertigung von Abmahnungen	353
11 Strafrechtliche Risiken für Admins	355
11.1 Das Computerstrafrecht: Konsequenzen für Admins und Pentester	355
11.1.1 Ausspähen von Daten (§ 202a StGB)	356
11.1.2 Abfangen von Daten (§ 202b StGB)	359
11.1.3 Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)	360
11.1.4 Datenhehlerei (§ 202d StGB)	364
11.1.5 Datenveränderung (§ 303a StGB)	365
11.1.6 Computersabotage (§ 303b StGB)	366
11.2 Geheimniskrämerei: der richtige Umgang mit Geheimnissen	367
11.2.1 Verletzung von Privatgeheimnissen (§ 203 StGB)	367
11.2.2 Abhören verboten: Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB)	370
11.2.3 Besser nicht verraten: Folgen bei Verrat von Geschäftsgeheimnissen	372
11.3 Missbrauch personenbezogener Daten: Strafbarkeiten und Ordnungswidrigkeiten	373
11.3.1 Strafbarkeiten nach § 42 BDSG	373
11.3.2 Ordnungswidrigkeiten	376
11.4 Richtiger Umgang mit Durchsuchungen, Durchsichten und Beschlagnahmen	376
11.4.1 Offene Ermittlungsmaßnahmen	377
11.4.2 Verdeckte Ermittlungsmaßnahmen: die Online-Durchsuchung	382
11.5 Fazit	383

12 Generative KI: Was bei der Nutzung von ChatGPT & Co. zu beachten ist	385
12.1 Grundlagen: Wie funktioniert ChatGPT eigentlich?	385
12.2 KI-Generatoren und das Urheberrecht	387
12.2.1 Welche Rechte bestehen an KI-Ergebnissen?	387
12.2.2 Gemischte Platte: Wie viel KI darf in einem Werk stecken?	389
12.2.3 Besonderheiten bei der Nutzung von KI für Code	391
12.2.4 KI von der eigenen Website aussperren?	392
12.3 KI-Generatoren und der Datenschutz	394
12.3.1 Datenschutz bei der geschäftlichen Nutzung der KI	394
12.3.2 Vertragliche Beziehung und Datenexport	394
12.3.3 Rechtsgrundlagen für die geschäftliche Nutzung	395
12.3.4 Datenschutzerfordernungen an die Betreiber der KI	395
12.3.5 Besonderheiten bei Bild-KI	396
12.4 Geschäftsgeheimnisschutz und KI	396
12.5 Richtlinien für die Nutzung von KI-Generatoren	397
Index	399