
Inhaltsverzeichnis

Vorwort	11
1 Basiswissen Datenschutz	13
1.1 Ziele und Zusammenwirken DSGVO/BDSG n. F.	13
1.2 Persönlichkeitsrecht	15
1.3 Datenschutz – warum betrifft das Thema auch Sie?	15
1.4 Satte Strafen bei Verstößen	16
2 Datenschutzbeauftragter	21
2.1 Pflicht zur Benennung	21
2.2 Wer kann zum Datenschutzbeauftragten benannt werden?	24
2.3 Aufgaben eines Datenschutzbeauftragten	25
3 Anforderungen an Unternehmen aus der DSGVO/BDSG n. F.	27
3.1 Pflichten und Verantwortlichkeiten – ein Überblick	27
3.2 Verzeichnis von Verarbeitungstätigkeiten	31
3.2.1 VVT für Auftragsverarbeiter?	32
3.2.2 Inhalt des Verzeichnisses und der Einzelbeschreibungen	33
3.2.3 Erklärung der einzelnen Einträge	36
3.2.3.1 Einträge, die für alle Verarbeitungen identisch sind	36
3.2.3.2 Einträge je Verfahren	37
3.2.4 Rechtsgrundlagen	39
3.3 Sicherheit der Verarbeitung inkl. Risikobewertung	47
3.3.1 Geeignete Maßnahmen	47
3.3.2 Angemessenes Schutzniveau	51
3.3.3 Nachweismöglichkeiten	51
3.3.4 Pflichten gegenüber den Mitarbeitern	52
3.4 Technische und organisatorische Maßnahmen	53
3.4.1 Pflicht zur Risikobegrenzung durch TOM	53
3.4.2 Auswahl der geeigneten Maßnahmen	55
3.4.3 Spezialfall Löschrufen/Löschkonzept	57
3.5 Organisation der Rechte der Betroffenen	59
3.5.1 Rechte der betroffenen Person	60
3.5.1.1 Artikel 15 DSGVO »Recht auf Auskunft«	60
3.5.1.2 Artikel 16 DSGVO »Recht auf Berichtigung«	61
3.5.1.3 Artikel 17 DSGVO »Recht auf Löschung«	61
3.5.1.4 Artikel 18 DSGVO »Recht auf Einschränkung der Verarbeitung«	64

3.5.1.5	Artikel 19 DSGVO »Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung«	66
3.5.1.6	Artikel 20 DSGVO »Recht auf Datenübertragbarkeit«	67
3.5.1.7	Artikel 21 DSGVO »Widerspruchsrecht«	68
3.5.1.8	Artikel 22 DSGVO »Automatisierte Entscheidungen im Einzelfall einschließlich Profiling«	71
3.5.2	Informationspflicht nach Artikel 13 und 14 DSGVO	74
3.5.3	Was tun, wenn eine betroffene Person ihre Rechte wahrnimmt?	77
3.6	Umgang mit externen Dienstleistern	82
3.7	Datenschutz im Beschäftigtenverhältnis	87
3.7.1	Geltende Gesetze	87
3.7.2	Einwilligung	87
3.7.3	Rechte der Mitarbeiter	89
3.8	Sensibilisierung von Mitarbeitern	90
3.9	Datenschutz-Folgenabschätzung	93
3.9.1	Risikobewertung/Risikoermittlung	94
3.9.2	Unterstützungsmöglichkeiten für die Durchführung der DSFA	97
3.9.3	Vorherige Konsultation	97
3.10	Meldepflicht bei Datenschutzverletzungen	98
3.11	Dokumentation und Erfüllung der Nachweispflicht	101
3.11.1	Verzeichnis von Verarbeitungstätigkeiten	102
3.11.2	Grundsätze der Verarbeitung	102
3.11.2.1	Grundsatz 1: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	104
3.11.2.2	Grundsatz 2: Zweckbindung	104
3.11.2.3	Grundsatz 3: Daten-Minimierung	105
3.11.2.4	Grundsatz 4: Richtigkeit	106
3.11.2.5	Grundsatz 5: Speicherbegrenzung	108
3.11.2.6	Grundsatz 6: Integrität und Vertraulichkeit	109
3.11.3	Einwilligung mit Nachweis	110
3.11.4	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	112
3.11.5	Datenschutzverletzungen	113
3.11.6	Empfehlung	114
3.12	Unternehmen ist Auftragsverarbeiter	114
3.12.1	Begriffsbestimmung: Auftragsverarbeiter	114
3.12.2	Zusätzliche bzw. geänderte Aufgaben	115
3.12.2.1	Verzeichnis von Verarbeitungstätigkeiten als Auftragsverarbeiter	115
3.12.2.2	Vereinbarungen zur Verarbeitung im Auftrag (Artikel 28 DSGVO)	117

3.12.2.3	Bearbeitung von Betroffenenrechten	117
3.12.2.4	Meldepflicht bei Datenschutzverletzungen	118
3.12.3	Haftung	118
4	Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde	121
4.1	Pflicht zur Kontaktaufnahme mit der Aufsichtsbehörde	121
4.2	Kontaktaufnahme mit der Aufsichtsbehörde	122
4.3	Kontaktaufnahme durch die Aufsichtsbehörde	122
5	Praxisbeispiele	125
5.1	Aufgabenliste für kleine Unternehmen	125
5.1.1	Anforderung A: Datenschutzbeauftragter (DSB)	126
5.1.2	Anforderung B: Verzeichnis von Verarbeitungstätigkeiten	127
5.1.3	Anforderung C: Datenschutz-Verpflichtung von Beschäftigten	127
5.1.4	Anforderung D: Informations- und Auskunftspflichten	128
5.1.5	Anforderung E: Löschen von Daten	129
5.1.6	Anforderung F: Sicherheit	129
5.1.7	Anforderung G: Auftragsverarbeitung	130
5.1.8	Anforderung H: Datenschutzverletzungen	130
5.1.9	Anforderung I: Datenschutz-Folgeabschätzung (DSFA)	131
5.1.10	Anforderung J: Videoüberwachung (VÜ)	132
5.2	Eigene Unternehmens-Webseite: Worauf Sie unbedingt achten sollten	132
5.3	Nutzung von Internet und E-Mail am Arbeitsplatz	135
5.3.1	Private Nutzung der dienstlichen Kommunikationsmittel	136
5.3.1.1	Telekommunikationsgesetze	136
5.3.1.2	Unternehmensregelungen	137
5.3.1.3	Datenschutzgesetze	138
5.3.1.4	Zusammenfassung und Aufgabenliste	138
5.3.1.5	Sonderbehandlung	139
5.3.1.6	Besondere Maßnahmen	139
5.3.2	Sichere Nutzung von Internet und E-Mail	140
5.3.2.1	Internet-Nutzung	140
5.3.2.2	E-Mail-Nutzung	141
5.4	Verpflichtung von Mitarbeitern auf Vertraulichkeit	144
5.5	Risikomanagement/IT-Sicherheit/Technische und organisatorische Maßnahmen	146
5.5.1	PDCA-Methode	146
5.5.2	Risiken der Verarbeitungen erkennen und Maßnahmen zur Minimierung planen	147
5.5.3	Geeignete Maßnahmen einführen	149
5.5.4	Wirksamkeit der Maßnahmen überprüfen	150
5.5.5	Maßnahmen ggfs. anpassen	151

5.6	Berührungspunkte mit Datenschutz im Arbeitsalltag	151
5.6.1	Umgang mit Visitenkarten	151
5.6.2	Kunde kommt ins Unternehmen	152
5.6.3	Verhalten am Telefon	155
5.6.4	Elektronischer Datenaustausch	158
5.6.5	Ausgestaltung des Arbeitsplatzes	159
5.7	Datenschutz-Managementsystem	161
5.7.1	Auswahl eines Datenschutz-Managementsystems	163
5.7.2	Eignung für den Einsatz in Kleinbetrieben	163
	Glossar	175
	Literaturverzeichnis und Links	179
	Stichwortverzeichnis	183