

Datenschutz- Compliance nach der DS-GVO

Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden

Thomas Kranig, Jurist, Präsident des Bayerischen Landesamtes für
Datenschutzaufsicht (BayLDA),

Andreas Sachs, Dipl.-Informatiker, Leiter des technischen Referats sowie
Vertreter des Präsidenten beim Bayerischen Landesamt für Datenschutz-
aufsicht (BayLDA) und

Markus Gierschmann, Dipl.-Wirtschaftsingenieur, Finanzökonom (ebs),
CIPP/E, CIPM, Datenschutzbeauftragter (udis, TÜV), Datenschutzauditor
(TÜV), Unternehmensberater

2. Auflage

Inhaltsverzeichnis

Vorworte	5
Abkürzungen	23

Teil I: Einführung in die DS-GVO

1	Einleitung	29
1.1	An wen richtet sich diese Handlungshilfe	29
1.2	Was beinhaltet diese Handlungshilfe und was nicht	29
2	Allgemeines zur DS-GVO	31
3	Wesentliche Anforderungen der DS-GVO	32
3.1	Wesentliche Datenschutzvorschriften der DS-GVO	32
3.1.1	Wesentliche Regelungen für den Verantwortlichen	32
3.1.2	Wesentliche Regelungen zur Auftragsverarbeitung	33
3.1.3	Wesentliche Ausnahmen und Ergänzungen im BDSG	34
3.2	Wesentliche Datenschutzprozesse (Ablauforganisation)	36
3.3	Wesentliche Datenschutzstrukturen (Aufbauorganisation)	37

Teil II: Sicherstellung der Datenschutz-Compliance

4	Datenschutzstrukturen (Aufbauorganisation)	41
4.1	Datenschutzziele	42
4.2	Datenschutz-Governance-Struktur	44
4.3	Datenschutzleitlinie	49

5	Datenschutzprozesse (Ablauforganisation)	51
5.1	Kernprozess: „Datenschutzkonforme Datenverarbeitung“	51
5.1.1	Überblick Datenverarbeitung	51
5.1.2	Anforderungen an die Datenverarbeitung	52
5.1.2.1	Einhaltung der Datenschutzgrundsätze	52
5.1.2.2	Rechtmäßigkeit der Verarbeitung	53
5.1.2.3	Transparenz	54
5.1.2.4	Datenschutz durch Technikgestaltung und Voreinstellung	55
5.1.2.5	Sicherheit der Verarbeitung	61
	5.1.2.5.1 Ermittlung des Schutzniveaus	63
	5.1.2.5.2 Auswahl geeigneter technischer und organisatorischer Maßnahmen	65
	5.1.2.5.3 Bewertung von Datensicherheitsrisiken	68
5.1.2.6	Auftragsverarbeitung und gemeinsam Verantwortliche	70
5.1.2.7	Übermittlung in Drittländer	72
5.1.2.8	Dokumentation der Verarbeitungstätigkeiten	74
5.1.3	Einbindung Auftragsverarbeiter	75
5.1.4	Datenverarbeitung – PDCA	79
	5.1.4.1 Planung	79
	5.1.4.2 Betrieb	83
	5.1.4.3 Bewertung	83
	5.1.4.4 Verbesserung	84
5.2	Kernprozess: „Sicherstellung der Betroffenenrechte“	85
5.2.1	Überblick Betroffenenrechte	85
5.2.2	Anforderungen an das Management von Betroffenenrechten	86
	5.2.2.1 Antragsbearbeitung durch den Verantwortlichen	86
	5.2.2.2 Auskunftsrecht (Art. 15)	87
	5.2.2.3 Recht auf Berichtigung (Art. 16)	88
	5.2.2.4 Recht auf Löschung („Recht auf Vergessenwerden“) (Art. 17)	89
	5.2.2.5 Recht auf Einschränkung der Verarbeitung (Art. 18)	90
	5.2.2.6 Recht auf Datenübertragbarkeit (Art. 20)	90
	5.2.2.7 Widerspruchsrecht (Art. 21)	91
	5.2.2.8 Automatisierte Entscheidungen im Einzelfall (Art. 22)	91
	5.2.2.9 Recht auf Widerruf einer Einwilligung	91

5.2.3	Einbindung Auftragsverarbeiter	92
5.2.4	Betroffenenrechte – PDCA	92
5.2.4.1	Planung	92
5.2.4.2	Betrieb	96
5.2.4.3	Bewertung	97
5.2.4.4	Verbesserung	98
5.3	Kernprozess: „Handhabung von Datenschutzverletzungen“	99
5.3.1	Überblick Datenschutzverletzung	99
5.3.2	Anforderungen bei Vorliegen einer Datenschutzverletzung	100
5.3.2.1	Meldepflicht gegenüber der Aufsichtsbehörde	100
5.3.2.1.1	Fristen für die Meldung	100
5.3.2.1.2	Inhalt der Meldung	101
5.3.2.1.3	Dokumentationspflichten	102
5.3.2.2	Benachrichtigungspflicht gegenüber den betroffenen Personen	102
5.3.2.2.1	Zeitpunkt der Benachrichtigung	103
5.3.2.2.2	Inhalt der Benachrichtigung	103
5.3.3	Einbindung Auftragsverarbeiter	103
5.3.4	Datenschutzverletzung – PDCA	105
5.3.4.1	Planung	105
5.3.4.2	Betrieb	113
5.3.4.3	Bewertung	114
5.3.4.4	Verbesserung	118
6	Datenschutz-Risikomanagement	119
6.1	Risikobezug in der DS-GVO	119
6.1.1	Risiken bei der Datenverarbeitung	120
6.1.2	Risiken einer Datenschutzverletzung	124
6.1.3	Beispiele aus der DS-GVO für Risiko, hohes Risiko und Schaden	125
6.1.4	Risikobasierter Ansatz	127
6.2	Risikomanagement	129
6.2.1	Risiko	129
6.2.2	Risikomanagement	130
6.2.2.1	Risikomanagementgrundsätze	131
6.2.2.2	Risikomanagementsystem	132

6.2.2.3	Risikomanagementprozess	133
6.2.2.4	Techniken zur Risikobeurteilung	134
6.3	Datenschutz-Risikomanagement	135
6.3.1	Datenschutzrisiko	136
6.3.2	Datenschutz-und Compliance-Risiken	138
6.3.3	Datenschutz-Risikomanagementprozess	139
6.3.4	Datenschutz-Folgenabschätzung	140
6.3.4.1	DSFA in Anlehnung an die ISO 29134	141
6.3.4.1.1	DSFA-Prozess	141
6.3.4.1.2	DSFA-Bericht	143
6.3.4.2	Datenschutzrisikobeurteilung und-behandlung	144
6.3.4.2.1	Risikobeurteilung	144
6.3.4.2.2	Risikobehandlung	148
6.3.5	Umgang mit Risiken nach der DS-GVO	150
7	Datenschutzdokumentation	153
7.1	Dokumentations- und Nachweispflichten	153
7.1.1	Dokumentation der Datenverarbeitung	153
7.1.2	Dokumentation der Sicherstellung der Betroffenenrechte	155
7.1.3	Dokumentation der Handhabung von Datenschutzverletzungen	156
7.1.4	Zentrale Bedeutung des Verzeichnisses aller Verarbeitungstätigkeiten ...	156
7.1.5	Nachweiserbringung durch Zertifizierung und Verhaltensregeln	158
7.2	Datenschutzdokumentationsmanagement	159
7.2.1	Zwecke der Dokumentation	159
7.2.2	Dokumentationsstandards	161
7.2.3	Dokumentationsstruktur	162
7.2.4	Dokumentationsprozess	165
7.2.4.1	Dokumenten-Lebenszyklus	165
7.2.4.2	Dokumentation der Datenschutzdokumente und PDCA-Zyklus	165
7.2.5	Dokumentenmanagementsystem	166

8	Datenschutzsensibilisierung, -training und -Schulungen	167
8.1	Notwendigkeit von Schulungen als organisatorische Maßnahme	167
8.2	Datenschutzbewusstsein (Awareness)	167
8.3	Maßnahmen zur Förderung des Datenschutzbewusstseins	169
8.3.1	Datenschutzschulung und -training	169
8.3.2	Weitergehende Maßnahmen	170
8.4	Datenschutzbewusstsein – PDCA	171
8.4.1	Planung	171
8.4.2	Betrieb	172
8.4.3	Bewertung und Verbesserung	173
9	Datenschutzaudit/-zertifizierung	174
9.1	Überprüfung und Nachweiserbringung	174
9.1.1	Datenschutzkonforme Verarbeitung	178
9.1.2	Auftragsverarbeitung	178
9.1.3	Sicherheit der Verarbeitung	179
9.1.4	Datenschutz durch Technikgestaltung	179
9.1.5	Datenschutzfreundliche Voreinstellung	180
9.1.6	Datenschutz-Folgenabschätzung	181
9.1.7	Datenübermittlung vorbehaltlich geeigneter Garantien	181
9.1.8	Profiling	181
9.2	Datenschutzaudits	181
9.2.1	Audit	181
9.2.1.1	Interne und externe Audits	182
9.2.1.2	Audittypen	183
9.2.1.3	Anforderungen an einen Auditor	184
9.2.2	Auditplanung	185
9.2.3	Auditprogramm	186
9.2.4	Auditprozess	188
9.2.4.1	Vorbereitung	188
9.2.4.2	Durchführung	190
9.2.4.3	Nachbereitung	191

9.3	Datenschutz-zertifizierung	192
9.3.1	Akkreditierung	192
9.3.2	Datenschutz-zertifikate	194
9.3.3	Zertifizierungsverfahren	197
10	Datenschutz-Managementssystem	198
10.1	Umsetzung der Rechenschaftspflicht	198
10.1.1	Erforderlichkeit eines Datenschutz-Management-systems	198
10.1.2	Verantwortung für ein Datenschutz-Management-system	201
10.2	Anforderungen an ein Datenschutz-Management-system	201
10.2.1	Prinzipien für ein Datenschutz-Management-system	202
10.2.2	Elemente eines Datenschutz-Management-systems	204
10.3	Corporate Governance und Management-systeme	209
10.3.1	Corporate Governance	209
10.3.2	Management-systeme	210
10.3.3	Management-systemstandards	210
10.3.4	Ansätze für ein Datenschutz-Management-system	212
10.4	Datenschutzstandards	214
10.4.1	Internationale, europäische und nationale Normung	214
10.4.2	ISO-Datenschutzstandards	216
10.4.3	ISO-Datenschutzprojekte	217
10.5	Datenschutz-Management-system nach ISO 27701	220
10.5.1	Ansatz und Aufbau	220
10.5.2	DSMS-spezifische Anforderungen – Erweiterung der ISO 27001	221
10.5.3	DSMS-spezifische Empfehlungen – Erweiterung der ISO 27002	224
10.5.4	Zusätzliche Empfehlungen – Erweiterung der ISO 29100	227
10.5.5	Zertifizierung nach ISO und DS-GVO	230

Teil III: Überwachung der Datenschutz-Compliance

11 Rolle der Aufsichtsbehörde gegenüber den Unternehmen	235
11.1 Aufgaben der Aufsichtsbehörde	235
11.2 Befugnisse der Aufsichtsbehörde	236
11.2.1 Untersuchungsbefugnisse	236
11.2.2 Abhilfebefugnisse	237
11.2.3 Genehmigungs- und Beratungsbefugnisse	238
11.3 Zusammenarbeit der Aufsichtsbehörden	239
11.3.1 Zusammenarbeit der deutschen Aufsichtsbehörden	240
11.3.2 Zusammenarbeit der EU-Aufsichtsbehörden	241
12 Überwachung durch Aufsichtsbehörden	242
12.1 Überwachungspraxis durch Aufsichtsbehörden	242
12.1.1 Zielsetzung und Vorgehen	242
12.1.2 Praxisbeispiele	243
12.2 Prüffragen von Aufsichtsbehörden	243
12.2.1 Erläuterungen zu den Prüffragen	243
12.2.2 Prüffragen zur Datenschutzstruktur	244
12.2.3 Prüffragen zur datenschutzkonformen Datenverarbeitung	246
12.2.4 Prüffragen zur Sicherstellung der Betroffenenrechte	249
12.2.5 Prüffragen zur Handhabung von Datenschutzverletzungen	252
12.3 Checkliste Erfüllung der „Rechenschaftspflicht“	255
Abbildungsverzeichnis	261
Tabellenverzeichnis	265
Literatur	267
Stichwortverzeichnis	273