

Datenschutz-Compliance nach der DS-GVO

Handlungshilfe für Verantwortliche
inklusive Prüffragen für
Aufsichtsbehörden

Autoren:

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

Andreas Sachs, Dipl.-Informatiker, Leiter des technischen Referats
beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und

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



Bundesanzeiger
Verlag

Inhaltsverzeichnis

Vorwort	5
Abkürzungen	15

Teil I: Einführung in die DS-GVO

1 Einleitung	21
1.1 An wen richtet sich diese Handlungshilfe	21
1.2 Was beinhaltet diese Handlungshilfe und was nicht	21
2 Allgemeines zur DS-GVO	23
3 Wesentliche Anforderungen der DS-GVO an den Verantwortlichen	24
3.1 Wesentliche Datenschutzvorschriften der DS-GVO	24
3.2 Wesentliche Datenschutzprozesse (Ablauforganisation)	25
3.3 Wesentliche Datenschutzstrukturen (Aufbauorganisation)	27

Teil II: Sicherstellung der Datenschutz-Compliance

4 Datenschutzstrukturen (Aufbauorganisation)	31
4.1 Datenschutzziele	31
4.2 Datenschutz-Governance-Struktur	33
4.3 Datenschutzleitlinie	35
5 Datenschutzprozesse (Ablauforganisation)	37
5.1 Kernprozess: „Datenschutzkonforme Datenverarbeitung“	37
5.1.1 Überblick Datenverarbeitung	37
5.1.2 Anforderungen an die Datenverarbeitung	38
5.1.2.1 Einhaltung der Datenschutzgrundsätze	38
5.1.2.2 Rechtmäßigkeit der Verarbeitung	39
5.1.2.3 Transparenz	40
5.1.2.4 Sicherheit der Verarbeitung	41
5.1.2.5 Auftragsverarbeitung	43
5.1.2.6 Übermittlung in Drittländer	45
5.1.2.7 Dokumentation der Verarbeitungstätigkeiten	46

5.1.3	Datenverarbeitung – PDCA	47
5.1.3.1	Planung	48
5.1.3.2	Betrieb	51
5.1.3.3	Bewertung	51
5.1.3.4	Verbesserung	53
5.2	Kernprozess: „Sicherstellung der Betroffenenrechte“	53
5.2.1	Überblick Betroffenenrechte	54
5.2.2	Anforderungen an das Management von Betroffenenrechten	55
5.2.2.1	Antragsbearbeitung durch den Verantwortlichen	55
5.2.2.2	Auskunftsrecht	56
5.2.2.3	Recht auf Berichtigung	57
5.2.2.4	Recht auf Löschung („Recht auf Vergessenwerden“)	57
5.2.2.5	Recht auf Einschränkung der Verarbeitung	58
5.2.2.6	Recht auf Datenübertragbarkeit	59
5.2.2.7	Widerspruchsrecht	59
5.2.2.8	Automatisierte Entscheidungen im Einzelfall	60
5.2.2.9	Recht auf Widerruf einer Einwilligung	60
5.2.3	Betroffenenrechte – PDCA	61
5.2.3.1	Planung	61
5.2.3.2	Betrieb	65
5.2.3.3	Bewertung	66
5.2.3.4	Verbesserung	67
5.3	Kernprozess: „Handhabung von Datenschutzverletzungen“	68
5.3.1	Überblick Datenschutzverletzung	68
5.3.2	Anforderungen bei Vorliegen einer Datenschutzverletzung	69
5.3.2.1	Meldepflicht gegenüber der Aufsichtsbehörde	69
5.3.2.1.1	Fristen für die Meldung	69
5.3.2.1.2	Inhalt der Meldung	69
5.3.2.1.3	Dokumentationspflichten	70
5.3.2.2	Benachrichtigungspflicht gegenüber den betroffenen Personen	70
5.3.2.2.1	Zeitpunkt der Benachrichtigung	71
5.3.2.2.2	Inhalt der Benachrichtigung	71
5.3.3	Datenschutzverletzung – PDCA	71
5.3.3.1	Planung	71
5.3.3.2	Betrieb	74
5.3.3.3	Bewertung	75
5.3.3.4	Verbesserung	77

6	Datenschutz-Risikomanagement	78
6.1	Risikobezug in der DS-GVO	78
6.1.1	Risiken bei der Datenverarbeitung	79
6.1.2	Risiken einer Datenschutzverletzung	83
6.1.3	Beispiele aus der DS-GVO für Risiko, Schaden und hohes Risiko	84
6.1.4	Risikobasierter Ansatz	87
6.2	Risikomanagement	88
6.2.1	Risiko	88
6.2.2	Risikomanagement	89
6.2.2.1	Risikomanagementgrundsätze	90
6.2.2.2	Risikomanagementsystem	91
6.2.2.3	Risikomanagementprozess	92
6.2.2.4	Techniken zur Risikobeurteilung	93
6.3	Datenschutz-Risikomanagement	94
6.3.1	Datenschutzrisiko	95
6.3.2	Datenschutz- und Compliance-Risiken	96
6.3.3	Datenschutz-Risikomanagementprozess	97
6.3.4	Datenschutz-Folgenabschätzung	99
6.3.4.1	DSFA in Anlehnung an die ISO 29134	99
6.3.4.1.1	DSFA-Prozess	100
6.3.4.1.2	DSFA-Bericht	101
6.3.4.2	Datenschutzrisikobeurteilung und Datenschutzrisikobehandlung	102
6.3.4.2.1	Risikobeurteilung	102
6.3.4.2.2	Risikobehandlung	106
6.3.5	Umgang mit Risiken nach der DS-GVO	109
7	Datenschutzdokumentation	110
7.1	Dokumentations- und Nachweispflichten	110
7.1.1	Dokumentation der Datenverarbeitung	110
7.1.2	Dokumentation der Sicherstellung der Betroffenenrechte	112
7.1.3	Dokumentation der Handhabung von Datenschutzverletzungen	113
7.1.4	Zentrale Bedeutung des Verzeichnisses aller Verarbeitungstätigkeiten	113
7.1.5	Nachweiserbringung durch Zertifizierung und Verhaltensregeln	115
7.2	Datenschutzdokumentationsmanagement	116
7.2.1	Zwecke der Dokumentation	116
7.2.2	Dokumentationsstandards	118
7.2.3	Dokumentationsstruktur	119

7.2.4	Dokumentationsprozess	122
7.2.4.1	Dokumenten-Lebenszyklus	122
7.2.4.2	Dokumentation der Datenschutzdokumente und PDCA-Zyklus	122
7.2.5	Dokumentenmanagementsystem	123
8	Datenschutzsensibilisierung, -training und -schulungen	124
8.1	Notwendigkeit von Schulungen als organisatorische Maßnahme	124
8.2	Datenschutzbewusstsein (Awareness)	125
8.3	Maßnahmen zur Förderung des Datenschutzbewusstseins	126
8.3.1	Datenschutzschulung und -training	126
8.3.2	Weitergehende Maßnahmen	127
8.4	Datenschutzbewusstsein – PDCA	128
8.4.1	Planung	128
8.4.2	Betrieb	129
8.4.3	Bewertung und Verbesserung	130
9	Datenschutzaudit/-zertifizierung	131
9.1	Überprüfung und Nachweiserbringung	131
9.1.1	Datenschutzkonforme Verarbeitung	133
9.1.2	Auftragsverarbeitung	134
9.1.3	Sicherheit der Verarbeitung	135
9.1.3.1	Ermittlung des Schutzniveaus	135
9.1.3.2	Auswahl geeigneter technischer und organisatorischer Maßnahmen	137
9.1.3.3	Bewertung von Datensicherheitsrisiken	140
9.1.4	Datenschutz durch Technikgestaltung	142
9.1.5	Datenschutzfreundliche Voreinstellung	144
9.1.6	Datenschutz-Folgenabschätzung	144
9.1.7	Datenübermittlung vorbehaltlich geeigneter Garantien	145
9.1.8	Profiling	145
9.2	Datenschutzaudits	145
9.2.1	Audit	145
9.2.1.1	Interne und externe Audits	146
9.2.1.2	Audittypen	146
9.2.1.3	Anforderungen an einen Auditor	148
9.2.2	Auditplanung	149
9.2.3	Auditprogramm	150
9.2.4	Auditprozess	152
9.2.4.1	Vorbereitung	152
9.2.4.2	Durchführung	154
9.2.4.3	Nachbereitung	155

9.3	Datenschutz Zertifizierung	157
9.3.1	Akkreditierung	157
9.3.2	Datenschutz Zertifikate	158
9.3.3	Zertifizierungsverfahren	160
10	Datenschutz-Managementsystem	162
10.1	Umsetzung der Rechenschaftspflicht	162
10.2	Corporate Governance und Managementsysteme	164
10.2.1	Corporate Governance	164
10.2.2	Managementsysteme	165
10.2.3	Managementsystemstandard	166
10.3	Datenschutzstandards	167
10.3.1	ISO-Datenschutzstandards	168
10.3.2	ISO-Datenschutzprojekte	169
10.3.3	ISO-Leitfaden für den Schutz personenbezogener Daten	171
10.3.4	Entwicklung eines ISO-Datenschutz-Managementsystems	174
10.4	Ansatz eines „Integrierten Datenschutz-Managementsystems“	175
10.4.1	Komponenten eines Datenschutz-Managementsystems	175
10.4.2	Elemente eines Datenschutz-Managementsystems	177
10.4.3	Ausblick	182

Teil III: Überwachung der Datenschutz-Compliance

11	Rolle der Aufsichtsbehörde gegenüber den Unternehmen	187
11.1	Aufgaben der Aufsichtsbehörde	187
11.2	Befugnisse der Aufsichtsbehörde	187
11.2.1	Untersuchungsbefugnisse	188
11.2.2	Abhilfebefugnisse	188
11.2.3	Genehmigungs- und Beratungsbefugnisse	190
11.3	Zusammenarbeit, Kohärenz	190
12	Prüffragen für Aufsichtsbehörden	192
12.1	Erläuterungen zu den Prüffragen	192
12.2	Prüffragen und Maßnahmen zur Datenschutzstruktur (Corporate Governance) ..	194
12.3	Prüffragen und Maßnahmen zur Datenverarbeitung	196
12.4	Prüffragen und Maßnahmen zur Sicherstellung der Betroffenenrechte	199
12.5	Prüffragen und Maßnahmen zur Handhabung von Datenschutzverletzungen	202

13 Ausblick	206
13.1 (R)Evolution im Datenschutz	206
13.2 Schritte zur Erfüllung der „Rechenschaftspflicht“	207
Abbildungsverzeichnis	213
Tabellenverzeichnis	217
Literatur	219
Stichwortverzeichnis	225