

Inhaltsverzeichnis

Vorwort	5
Abbildungsverzeichnis	13
Abkürzungsverzeichnis	15
Quellenverzeichnis	19
 1 Einleitung	 23
 2 Der Begriff des Datenschutz-Management-Systems ..	 26
2.1 Gesetzliche Definition	26
2.2 Definitionen in der Literatur	28
2.3 Definition nach nationalen oder internationalen Standards	29
2.3.1 Vielfältige Ansätze	29
2.3.2 ISO 27701	30
2.4 Eigene Definition eines Datenschutz-Management-Systems	31
 3 Chancen und Risiken von Datenschutz- Management-Systemen	 33
3.1 Chancen von Datenschutz-Management-Systemen	33
3.1.1 Organisationsvorteile	34
3.1.2 Qualitätssicherung	36
3.1.3 Risikoprävention	36
3.1.4 Marketingvorteile	37
3.1.5 Wettbewerbsvorteile	37
3.2 Risiken von Datenschutzverletzungen	38
3.2.1 Schadensersatzansprüche von Geschädigten	39
3.2.2 Arbeitsrechtliche Maßnahmen	41
3.2.3 Organisations- und Beratungskosten	42
3.2.4 Straf- und Bußgeldverfahren	42
3.2.5 Reputationsschäden	45

- 4 Anforderungen an Datenschutz-Management-Systeme** 47
 - 4.1 Gesetzliche Anforderungen** 47
 - 4.1.1 Anforderungen nach der DS-GVO 47
 - 4.1.2 Grundsätze der Verarbeitung von personenbezogenen Daten 48
 - 4.1.2.1 Rechtmäßigkeit 48
 - 4.1.2.2 Verarbeitung nach Treu und Glauben 49
 - 4.1.2.3 Transparenz 49
 - 4.1.2.4 Zweckbindung 50
 - 4.1.2.5 Datenminimierung 51
 - 4.1.2.6 Richtigkeit 51
 - 4.1.2.7 Speicherbegrenzung 52
 - 4.1.2.8 Integrität und Vertraulichkeit 53
 - 4.1.2.9 Rechenschaftspflicht 53
 - 4.1.3 Beschränkungen der Grundsätze und Betroffenenrechte 54
 - 4.1.4 Weitere Pflichten des Verantwortlichen 54
 - 4.1.4.1 Auftragsverarbeitung 55
 - 4.1.4.2 Verzeichnis von Verarbeitungstätigkeiten 56
 - 4.1.4.3 Sicherheit der Verarbeitung 58
 - 4.1.4.4 Umgang mit Datenschutzverletzungen 58
 - 4.1.4.5 Datenschutz-Folgenabschätzung 60
 - 4.1.4.6 Datenschutzbeauftragter 61
 - 4.1.4.7 Datentransfers 61
 - 4.1.5 Anforderungen nach Spezialgesetzen 63
 - 4.1.5.1 Europäische Richtlinien und Verordnungen 64
 - 4.1.5.2 Deutsche Gesetze 64
 - 4.1.6 Anforderungen durch das BDSG 65
 - 4.1.6.1 Modifizierungen 66
 - 4.1.6.2 Konkretisierungen 67
 - 4.1.7 Gerichtliche Anforderungen 68
 - 4.2 Anforderungen von Datenschutz-Aufsichtsbehörden** 69
 - 4.2.1 Europäischer Datenschutzausschuss 70
 - 4.2.2 Datenschutzkonferenz des Bundes und der Länder 71
 - 4.2.3 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 73

4.2.4	Landesdatenschutz-Aufsichtsbehörden	73
4.3	Anforderungen von Unternehmen	74
4.3.1	Geschäftsmodell	75
4.3.2	Unternehmenskultur in puncto Datenschutz	76
4.3.3	Geografische Verteilung der Standorte	78
4.3.4	Struktur und Organisation	79
4.4	Anforderungen von Kunden	80
5	Komponenten von Datenschutz-Management-Systemen	81
5.1	Datenschutzziele	82
5.1.1	Öffentliche Datenschutzziele	83
5.1.2	Unternehmensinterne Datenschutzziele	84
5.2	Datenschutzstrategie	85
5.2.1	Einhaltung aller datenschutzrechtlichen Bestimmungen	86
5.2.1.1	Identifikation der gesetzlichen Anforderungen	87
5.2.1.2	Implementierung und Änderung relevanter Prozesse	87
5.2.1.3	Kommunikation und Schulung	87
5.2.1.4	Kultur und Mindset	88
5.2.1.5	Kontrolle	89
5.2.2	Aufbau einer Datenschutzorganisation	89
5.2.2.1	Intern oder extern	89
5.2.2.2	Zentral oder Dezentral	91
5.2.2.3	Alleine oder gemeinschaftlich	91
5.2.3	Weltweit einheitlicher Datenschutzstandard	92
5.2.3.1	Identifizierung der einschlägigen Rechtsnormen	93
5.2.3.2	Schaffung eines einheitlichen Verständnisses	94
5.2.4	Umsetzung der digitalen Transformation	94
5.2.4.1	Identifizierung der digitalen Projekte	95
5.2.4.2	Datenethik	95
5.2.4.3	Kommunikation	95
5.2.5	Gestaltung des legislativen und regulativen Datenschutzzumfeldes	96
5.2.5.1	Entwicklung der Unternehmensstandpunkte	97
5.2.5.2	Beratungen mit dem Gesetzgeber oder Behördenvertretern	97
5.2.6	Notfall-Datenschutzstrategie	97

- 5.3 Datenschutzorganisation 98
 - 5.3.1 Personelle Ausstattung 99
 - 5.3.2 Ressourcen 101
 - 5.3.3 Integration 102
 - 5.3.4 Berichtslinien 103
- 5.4 Datenschutzprogramm 103
 - 5.4.1 Richtlinien 105
 - 5.4.1.1 Code of Conduct 105
 - 5.4.1.2 Globale Datenschutzrichtlinie 105
 - 5.4.1.3 Globale Richtlinien zu Spezialthemen 106
 - 5.4.1.4 Lokale Datenschutzrichtlinie 106
 - 5.4.1.5 Einzelfallspezifische lokale Richtlinien und
Arbeitsanweisungen 108
 - 5.4.2 Verzeichnisse 108
 - 5.4.2.1 Verzeichnis von Verarbeitungstätigkeiten 109
 - 5.4.2.2 Datenschutz-Folgenabschätzung (DSFA) 111
 - 5.4.2.3 IT-Inventar und Datenflüsse 114
 - 5.4.3 Betroffenenrechte 114
 - 5.4.3.1 Informationspflichten 114
 - 5.4.3.2 Recht auf Auskunft, Berichtigung und Löschung 117
 - 5.4.4 Meldesystem für Datenschutzvorfälle 118
 - 5.4.5 Vertragswesen 119
 - 5.4.5.1 Einwilligungen und Verträge mit dem Betroffenen 120
 - 5.4.5.2 Betriebsvereinbarungen 121
 - 5.4.5.3 Datenübermittlungen in Deutschland 122
 - 5.4.5.4 Standardvertragsklauseln 126
 - 5.4.5.5 Binding Corporate Rules 127
 - 5.4.6 Technische und organisatorische Maßnahmen 127
 - 5.4.6.1 Data Privacy by Design 130
 - 5.4.6.2 Data Privacy by Default 130
 - 5.4.6.3 Risikobasierter Ansatz 131
 - 5.4.7 Schulung & Sensibilisierung 133
 - 5.4.7.1 Arbeitsvertragliche Unterlagen 134
 - 5.4.7.2 Einführungsveranstaltungen 134
 - 5.4.7.3 Regelmäßige Schulungen für alle Mitarbeiter 135
 - 5.4.7.4 Spezialschulungen für einzelne Bereiche 136

5.4.7.5	Intranetseite	136
5.4.7.6	Sensibilisierungsmaßnahmen	136
5.4.8	Überwachung	137
5.4.8.1	Kontrollen	138
5.4.8.2	Audits	139
5.4.9	Zertifizierung	139
5.4.10	Berichtswesen	140
5.4.10.1	Ad-hoc-Mitteilungen	142
5.4.10.2	Monatsberichte	142
5.4.10.3	Jahresbericht	143
5.5	Datenschutzberatung	144
5.5.1	Anfragen	146
5.5.1.1	Interne Anfragen	146
5.5.1.2	Externe Anfragen	147
5.5.1.3	Vertraulichkeit	147
5.5.2	Bearbeitung von Anfragen	149
5.5.2.1	Eruierung des Sachverhalts	149
5.5.2.2	Datenschutzrechtliche Beurteilung	150
5.5.2.3	Beantwortung von Anfragen	152
5.5.2.4	Dokumentation und Analyse	156
5.5.3	Delegation	159
6	Implementierung von Datenschutz-Management-Systemen	160
6.1	Projektplanung	161
6.2	Verwendung behördlicher Materialien	164
6.3	Wirksamkeitserfordernis	164
6.4	Erwartungshaltung	165
6.5	Das Kostenargument	166
6.6	Rechtsunsicherheiten	167
6.6.1	Gründe für Rechtsunsicherheiten	168
6.6.2	Umgang mit Rechtsunsicherheiten	168

**7 Kontinuierliche Weiterentwicklung von
Datenschutz-Management-Systemen 170**

7.1 Kenntnis von neuen Entwicklungen 171

7.2 Bestimmung der Relevanz 172

7.3 Konsequente Umsetzung 173

Stichwortverzeichnis 175