

Inhalt

6 Abbildungsverzeichnis

7 Abkürzungsverzeichnis

12 Vorwort

16 1 Begrifflichkeiten und Grundprinzipien der DSGVO

- 17 1.1 Der Weg zur Datenschutz-Grundverordnung (DSGVO)
- 18 1.2 Anwendungsbereich der DSGVO und des DSG
- 23 1.3 Wesentliche Begriffe der DSGVO
- 25 1.4 Grundprinzipien der DSGVO
- 29 1.5 Überblick über das Sanktionen- und Haftungsregime
- 30 1.6 Fazit

32 2 Art 82 DSGVO und Haftungsszenarien

- 33 2.1 Augsgangspunkt
- 33 2.2 Art 82 DSGVO – Haftung und Recht auf Schadenersatz
- 34 2.3 Art 82 DSGVO vs § 33 DSG 2000 – alles beim Alten?
- 34 2.4 Aktivlegitimation
- 38 2.5 Schaden
- 41 2.6 Verschulden und Haftungsbefreiung
- 42 2.7 Die Passivlegitimation
- 43 2.8 Gesamtschuldnerschaft
- 43 2.9 Fazit

44 3 Projektmanagement im Datenschutz

- 45 3.1 Herausforderungen
- 46 3.2 Projektformat
- 46 3.3 Projektmanagement
- 55 3.4 Fazit

58 4 Die Datenschutzorganisation

- 59 4.1 Die Notwendigkeit einer Datenschutzorganisation
- 60 4.2 Data-Protection-Management-System (DPMS)
- 61 4.3 Praktische Umsetzung eines DPMS
- 79 4.4 Das Projektsetup
- 83 4.5 Rollen des DPMS
- 85 4.6 Fazit

88 5 Vereinbarungen nach Art 28 DSGVO

- 89 5.1 Augsgangspunkt
- 89 5.2 Abgrenzung zum Verantwortlichen
- 90 5.3 Auswahl des Auftragsverarbeiters
- 91 5.4 Die Grundlage der Auftragsverarbeitung
- 93 5.5 Zwingende Mindestinhalte
- 97 5.6 Besondere Informationspflicht bei rechtswidriger Weisung
- 98 5.7 Subbeauftragung und Formerfordernis
- 99 5.8 Fazit

100	6	Datenschutz im Konzern
101	6.1	Konzerninterner Datenaustausch
102	6.2	Konzernbegriff in der DSGVO
102	6.3	Konzerninterne Datentransfers innerhalb der Europäischen Union
107	6.4	Konzerninterne Datentransfers in Drittstaaten
108	6.5	Abgrenzung – Gemeinsame Verantwortlichkeit und Auftragsverarbeitung
109	6.6	Konzerndatenschutzbeauftragter
110	6.7	Fazit
112	7	Datenübermittlungen an Drittländer oder internationale Organisationen
113	7.1	Einleitung
113	7.2	Begrifflichkeiten
115	7.3	Zulässigkeit der Datenübermittlung
126	7.4	Aktuelle Entwicklungen
127	7.5	Fazit
130	8	Der One-Stop-Shop und die Zusammenarbeit zwischen Aufsichtsbehörden
131	8.1	Einleitung
131	8.2	Allgemeine Zuständigkeit
133	8.3	Prinzip der „federführenden Aufsichtsbehörde“ („One-Stop-Shop“)
147	8.4	Zusammenarbeit und Kohärenz
158	8.5	Fazit
160	9	Verarbeitungsverzeichnis und DS-FA
161	9.1	Einleitung
161	9.2	Das Verarbeitungsverzeichnis
172	9.3	Die DS-FA
179	9.4	Fazit
180	10	Betroffenenrechte
181	10.1	Einleitung
181	10.2	Die Betroffenenrechte im Überblick
183	10.3	Informationspflicht
188	10.4	Recht auf Auskunft
190	10.5	Recht auf Berichtigung
191	10.6	Recht auf Löschung und Recht auf Vergessenwerden
193	10.7	Recht auf Einschränkung der Verarbeitung
195	10.8	Recht auf Datenübertragbarkeit
196	10.9	Widerspruchsrecht
197	10.10	Recht, keiner Entscheidung aufgrund automatisierter Verarbeitung unterworfen zu werden
198	10.11	Fazit
200	11	Datenschutzvorfall
201	11.1	Definition
204	11.2	Erkennung und Umgang
212	11.3	Meldepflichten
219	11.4	Fazit
220	12	Informationssicherheit
221	12.1	Begriffsklärung

223 12.2 Das Informationssicherheitsmanagementsystem (ISMS)
240 12.3 Fazit

242 13 Technische und organisatorische Maßnahmen

243 13.1 Einleitung
244 13.2 Was sind TOMs?
250 13.3 Privacy-by-design und privacy-by-default
251 13.4 Die DSGVO und TOMs – Weitere Vorgaben
255 13.5 Case Study: Technische und organisatorische Maßnahmen umsetzen
261 13.6 Fazit

262 14 Datenschutzaudit und Zertifizierungen

263 14.1 Einleitung
265 14.2 Vor- und Nachteile einer Zertifizierung
270 14.3 Grundsätze einer Zertifizierung
276 14.4 Vorbereitungen und Voraussetzungen für eine Zertifizierung
280 14.5 Der Zertifizierungsprozess
285 14.6 Fazit

286 15 Datenschutz im Dienstverhältnis

287 15.1 Einleitung
287 15.2 Von der Bewerbung bis zum Eintritt
295 15.3 Datenschutz im laufenden Dienstverhältnis
300 15.4 Beendigung des Dienstverhältnisses
302 15.5 Fazit

304 16 Interne Untersuchungen und Datenschutz

305 16.1 Einleitung
306 16.2 Ablauf einer internen Untersuchung mit dem Schwerpunkt e-Discovery
308 16.3 Zulässigkeit von e-Discovery-Maßnahmen
314 16.4 Umgang mit privaten Informationen
315 16.5 Policies
316 16.6 Forensic Readiness für den Ernstfall
316 16.7 Fazit

318 17 Ausblick

322 Anhang

328 Literaturverzeichnis

342 Die Autoren