

Inhalt

| | |
|---------------|----|
| Vorwort | 13 |
|---------------|----|

Teil I Einleitung 15

| | |
|--|-----------|
| 1 Einführung in die Datenschutz-Grundverordnung (DS-GVO) | 17 |
| 1.1 Die Ausgangslage | 17 |
| 1.2 Neuregelungen des Datenschutzes durch die DS-GVO | 17 |
| 1.2.1 Allgemeines | 17 |
| 1.2.2 Geltungsbereich | 18 |
| 1.2.3 Normadressaten | 20 |
| 1.2.4 Zulässigkeit der Verarbeitung | 21 |
| 1.2.5 Transparenzpflichten | 25 |
| 1.2.6 Korrekturrechte | 28 |
| 1.3 Fazit | 30 |
| 2 Häufig gestellte Fragen und Irrtümer zur DS-GVO | 31 |
| 2.1 „Die Datenschutz-Grundverordnung gilt nicht für kleine Unternehmen.“ | 31 |
| 2.2 „Vereine sind von der DS-GVO nicht betroffen.“ | 31 |
| 2.3 „Der deutsche Gesetzgeber wird für Ausnahmen sorgen.“ | 32 |
| 2.4 „Mit der DS-GVO ändert sich nichts.“ | 32 |
| 2.5 „Die Einhaltung kontrolliert doch keiner.“ | 32 |
| 2.6 „Wir verarbeiten keine personenbezogenen Daten.“ | 33 |
| 3 Warum Datenschutzverstöße kein Kavaliersdelikt (mehr) sind | 35 |
| 3.1 Einleitung | 35 |
| 3.2 Die Datenschutz-Grundverordnung | 35 |
| 3.3 Was sich ändern wird | 36 |
| 3.4 Rechtsgrundlagen: Wann dürfen Daten verarbeitet werden? | 37 |
| 3.5 Betroffenenrechte: mehr Transparenz | 39 |
| 3.6 Dokumentationspflichten | 40 |
| 3.7 IT-Sicherheit | 40 |
| 3.8 Neuerungen im Outsourcing | 42 |
| 3.9 Haftung & Bußgelder | 42 |
| 3.10 Datenschutzaufsicht | 43 |
| 3.11 Paradigmenwechsel: Beweise die Unschuld | 43 |
| 3.12 Fazit: erste Schritte zur Umsetzung | 44 |

| | | |
|----------|--|-----------|
| 4 | Neue Aufgaben für (HR-)Fach- und Führungskräfte | 45 |
| 4.1 | Erweiterung des Aufgabenspektrums | 45 |
| 4.2 | Prozessanforderungen | 46 |
| 4.3 | Einkauf von Produkten und Dienstleistungen..... | 48 |
| 4.4 | Zusammenarbeit mit dem Betriebsrat | 49 |
| 4.5 | Fazit | 49 |
| 5 | Assessment-Tool zur DS-GVO-Readiness..... | 51 |
| 6 | Merkblatt Projektorganisation: Einführung der Datenschutz- Grundverordnung im Unternehmen | 55 |
| 6.1 | Hintergrundwissen: Projektorganisation | 55 |
| 6.2 | Phase: Awareness schaffen | 56 |
| 6.3 | Phase: Projekt strukturieren | 58 |
| 6.4 | Phase: Projekt planen | 59 |
| 6.5 | Phase: Projekt beginnt | 61 |
| 6.6 | Argumentationshilfen..... | 61 |

Teil II Von der Rechenschaftspflicht zur Dokumentation 63

| | | |
|----------|--|-----------|
| 7 | Dokumentationspflichten in der DS-GVO | 65 |
| 7.1 | Einleitung..... | 65 |
| 7.2 | Anforderungen an ein Dokumentationssystem | 66 |
| 7.3 | Inhalte der Dokumentation | 68 |
| 7.4 | Phase Planung | 69 |
| 7.5 | Zwecke und Rechtsgrundlagen..... | 69 |
| 7.6 | Interessenabwägung | 69 |
| 7.7 | Sicherheitskonzept | 69 |
| 7.8 | Beschreibung der Unternehmensprozesse | 70 |
| 7.9 | Phase Umsetzung | 72 |
| 7.10 | Phase Kontrolle | 73 |
| 7.11 | Phase Mängelbeseitigung | 74 |
| 7.12 | Das Verzeichnis von Verarbeitungstätigkeiten..... | 74 |
| 7.13 | Fazit | 75 |

Teil III Die Arbeit des Datenschutzbeauftragten 77

| | | |
|----------|---|-----------|
| 8 | Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben | 79 |
| 8.1 | Bestellung eines Datenschutzbeauftragten..... | 79 |
| 8.1.1 | Voraussetzungen der Bestellpflicht nach der DS-GVO | 79 |
| 8.1.2 | Reichweite der Öffnungsklausel nach Art. 37 Abs. 4 DS-GVO | 81 |

| | | |
|---|---|------------|
| 8.1.3 | Anforderungen an die Bestellung | 81 |
| 8.2 | Rechtsstellung des Datenschutzbeauftragten | 84 |
| 8.2.1 | Unabhängigkeit und Stellung | 84 |
| 8.2.2 | Abberufungsschutz..... | 85 |
| 8.2.3 | Einbindung und Unterstützung des Datenschutzbeauftragten | 86 |
| 8.2.4 | Datenschutzbeauftragter als „Anwalt der Betroffenen“/ Pflicht zur Geheimhaltung bzw. Vertraulichkeit | 86 |
| 8.2.5 | Publizität der Person des Datenschutzbeauftragten/ Kontaktdaten | 87 |
| 8.3 | Aufgaben des Datenschutzbeauftragten | 87 |
| 8.3.1 | Grundsätzliches zur DS-GVO..... | 87 |
| 8.3.2 | Unterrichtung und Beratung | 88 |
| 8.3.3 | Überwachung der Einhaltung des Datenschutzes..... | 89 |
| 8.3.4 | Aufgaben des Datenschutzbeauftragten im Zusammenhang mit der Datenschutz-Folgenabschätzung... .. | 89 |
| 8.3.5 | Zusammenarbeit mit der Datenschutzaufsichtsbehörde | 90 |
| 8.3.6 | Pflicht zur risikoorientierten Tätigkeit..... | 91 |
| 8.4 | Wegfall der Ermächtigungen zum Erlass delegierter Rechtsakte | 91 |
| 8.5 | Fazit | 92 |
| 9 | Die grundrechtskonforme Ausgestaltung der Datenschutz- Folgenabschätzung nach der neuen europäischen Datenschutz- Grundverordnung..... | 93 |
| 9.1 | Eine grundrechtskonforme Datenschutz-Folgenabschätzung..... | 94 |
| 9.1.1 | Vorbereitungsphase | 94 |
| 9.1.2 | Bewertungsphase..... | 99 |
| 9.1.3 | Maßnahmenphase | 104 |
| 9.1.4 | Berichtsphase..... | 107 |
| 9.1.5 | Überwachung und Fortschreibung | 108 |
| 9.2 | Übergang in die neue Welt der DS-GVO | 108 |
| 9.3 | Fazit | 109 |
| Teil IV Spezialgebiete: Werbung und Gesundheitswesen | | 111 |
| 10 | Datenverarbeitung zu Werbezwecken nach der Datenschutz- Grundverordnung..... | 113 |
| 10.1 | Ausgangslage und Grundbedingungen der Rechtsanwendung unter der DS-GVO..... | 114 |
| 10.1.1 | Der (voraussichtliche) Normenbestand ab dem 25.5.2018 | 115 |
| 10.1.2 | Bewertung | 117 |
| 10.2 | Grundprinzipien des werbewirtschaftlichen Datenschutzes nach DS-GVO | 118 |

| | | |
|-----------|--|------------|
| 10.3 | Die materiellen Regelungen des werbewirtschaftlichen Datenschutzes nach der DS-GVO | 119 |
| 10.3.1 | Verhältnis der Erlaubnistatbestände zueinander..... | 119 |
| 10.3.2 | Einwilligungsbasierte Datenverarbeitung | 120 |
| 10.4 | Zwischenfazit..... | 130 |
| 10.5 | Datenverarbeitung zu Vertragszwecken oder für die Durchführung vorvertraglicher Maßnahmen..... | 131 |
| 10.6 | Datenverarbeitung aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten unter Abwägung mit den Interessen der betroffenen Person..... | 133 |
| 10.6.1 | Das berechnigte Interesse | 134 |
| 10.6.2 | Abwägung mit den Interessen der betroffenen Person | 137 |
| 10.7 | Informationspflichten nach der DS-GVO | 140 |
| 10.7.1 | Ausgewählte Pflichten nach dem Informationsprogramm der Art. 13, 14..... | 140 |
| 10.7.2 | Informationszeitpunkte | 141 |
| 10.7.3 | Die Modalitäten der Informationsvermittlung..... | 142 |
| 10.7.4 | Folgen von Transparenzverstößen..... | 144 |
| 10.8 | Werbewiderspruch | 144 |
| 10.9 | Szenarien werbewirtschaftlicher Datenverarbeitung unter der DS-GVO | 146 |
| 10.9.1 | Bestandkundenwerbung..... | 146 |
| 10.9.2 | Selektionsmaßnahmen und Werbescoring..... | 148 |
| 10.9.3 | Werbung für fremde Angebote (Nutzung oder Übermittlung von Daten zu Werbezwecken Dritter) | 149 |
| 10.9.4 | Nutzungsbasierte Online-Werbung (Targeting)..... | 151 |
| 10.10 | Fazit | 153 |
| 11 | DS-GVO – Was ändert sich im Gesundheitswesen? | 155 |
| 11.1 | Begriffsbestimmungen..... | 156 |
| 11.2 | Rechtsgrundlagen für die Verarbeitung..... | 157 |
| 11.3 | Betroffenenrechte | 159 |
| 11.4 | Berufsgeheimnisträger | 161 |
| 11.5 | Vorgaben für das Unternehmen „Krankenhaus“ bzw. die „ambulante Versorgung“ | 162 |
| 11.5.1 | Rechenschaftspflicht | 162 |
| 11.5.2 | Data protection by design and by default | 162 |
| 11.5.3 | Verarbeitungstätigkeitenverzeichnis..... | 163 |
| 11.5.4 | Datensicherheit | 163 |
| 11.5.5 | Datenschutz-Folgenabschätzung | 165 |
| 11.5.6 | Auftragsverarbeitung | 166 |
| 11.5.7 | Meldepflichten | 168 |
| 11.6 | Forschung | 169 |

| | | |
|------|----------------------------------|-----|
| 11.7 | Sanktionen/Strafregelungen | 172 |
| 11.8 | Fazit | 173 |

Teil V Betroffenenrechte **175**

| | | |
|-----------|---|------------|
| 12 | Das System der Betroffenenrechte nach DS-GVO | 177 |
| 12.1 | Überblick | 177 |
| 12.2 | Betroffenenrechte nach Zielen | 178 |
| 12.2.1 | Permission | 178 |
| 12.2.2 | Intervention | 181 |
| 12.2.3 | Information | 185 |
| 12.2.4 | Petition | 191 |
| 12.2.5 | Kompensation | 192 |
| 12.3 | Zusammenfassung und Ausblick | 193 |
| 13 | Warum die neuen Betroffenenrechte im Datenschutz zur Falle werden können | 195 |
| 13.1 | Einleitung | 195 |
| 13.2 | Das Recht auf Datenübertragbarkeit in der Praxis | 196 |
| 13.3 | Verhinderung automatischer Entscheidungen | 197 |
| 13.4 | Fazit | 197 |
| 14 | Wie sag ich's nur? – Informationspflichten | 199 |
| 14.1 | Einleitung | 199 |
| 14.2 | Direkte und indirekte Erhebung | 200 |
| 14.3 | Zeitpunkt | 201 |
| 14.4 | Direkterhebung | 201 |
| 14.5 | Indirekte Erhebung | 202 |
| 14.6 | Form und Sprache | 203 |
| 14.7 | Inhalt | 204 |
| 14.8 | Ausnahmen | 208 |
| 14.9 | Informationspflichten bei neuen Zwecken | 208 |
| 14.10 | Notwendige Vorarbeiten | 209 |
| 14.11 | Folgen bei einem Verstoß | 210 |
| 14.12 | Fazit | 210 |

Teil VI Auswirkungen auf die Personalwirtschaft **211**

| | | |
|-----------|---|------------|
| 15 | Was bleibt und was ist neu? Die EU-DS-GVO und der Beschäftigtendatenschutz | 213 |
| 15.1 | Die Ausgangslage | 213 |
| 15.2 | Nationale Beschäftigtendatenschutzregelungen | 214 |
| 15.2.1 | Die Öffnungsklausel des Art. 88 Abs. 1 DS-GVO | 214 |

| | | |
|-----------|---|------------|
| 15.2.2 | Subsidiarität der DS-GVO gegenüber sonstigen auch die Beschäftigtendatenverarbeitung betreffenden Normen..... | 216 |
| 15.3 | Neuregelungen der DS-GVO für den Beschäftigtendatenschutz | 217 |
| 15.3.1 | Allgemeines | 217 |
| 15.3.2 | Geltungsbereich | 217 |
| 15.3.3 | Räumlicher Anwendungsbereich..... | 218 |
| 15.3.4 | Normadressaten | 219 |
| 15.3.5 | Zulässigkeit der Verarbeitung..... | 221 |
| 15.3.6 | Transparenzpflichten | 226 |
| 15.3.7 | Korrekturrechte | 229 |
| 15.4 | Fazit | 230 |
| 16 | Maßgeschneiderte Lösungen durch Kollektivvereinbarung? – Möglichkeiten und Risiken des Art. 88 Abs. 1 DS-GVO..... | 231 |
| 16.1 | Verhältnis von DS-GVO, BetrVG und TVG | 231 |
| 16.2 | Erste Schranke: Art. 88 Abs. 1 DS-GVO..... | 232 |
| 16.2.1 | Sachliche und persönliche Reichweite des Art. 88 DS-GVO..... | 233 |
| 16.2.2 | „Spezifischere Vorschriften...“ | 234 |
| 16.2.3 | „...zur Gewährleistung des Schutzes der Rechte und Freiheiten“ | 236 |
| 16.2.4 | Gestaltungsdirektiven für Spezifizierungsakte..... | 238 |
| 16.2.5 | Partielle Regelung durch Spezifizierungsrechtsakte und Weitergeltung der DS-GVO | 241 |
| 16.2.6 | Einschätzungsprärogative auch der Betriebspartner?..... | 242 |
| 16.3 | Zweite Schranke: Nationales Recht (insb. BetrVG) | 243 |
| 16.4 | Was geschieht am 25.05.2018?..... | 244 |
| 16.5 | Risiken und Nebenwirkungen: Verstoß gegen die Schranken, Sanktionen | 245 |
| 16.6 | Fazit | 246 |
| 17 | Personalrecruiting (bald) ein risikoreiches Geschäft? Auswirkungen der DS-GVO im Bereich des Personalrecruitings | 247 |
| 17.1 | Zwei Jahre bis zum Vollzug – eine knappe Zeitspanne | 247 |
| 17.2 | Insolvenz durch Recruiting? | 248 |
| 17.3 | Informationspflichten im Bewerbungsprozess | 248 |
| 17.4 | Informationspflichten bei neuen Zwecken | 253 |
| 17.5 | Sicherheitsüberprüfungen und polizeiliche Führungszeugnisse | 253 |
| 17.6 | Automatisierte Entscheidungen und Profiling | 254 |
| 17.7 | Neue Rechte für Bewerber („Betroffenenrechte“) | 254 |
| 17.7.1 | Recht auf Vervollständigung | 256 |
| 17.7.2 | Recht auf Beschränkung der Verarbeitung | 256 |
| 17.7.3 | Recht auf Datenportabilität..... | 258 |
| 17.8 | Fazit | 259 |

| | |
|--|------------|
| 18 E-Learning in der Cloud – der Datenschutzcheck | 261 |
| 18.1 Glossar | 262 |
| | |
| Teil VII Auswirkungen auf die IT-Administration und IT-Sicherheit | 265 |
| | |
| 19 Mehr gesetzliche Pflichten für IT-Verantwortliche – Auswirkungen auf die IT-Sicherheitsorganisation/IT-Sicherheitsmanagement | 267 |
| 19.1 Gesetzliche Vorgaben zur Sicherheitsorganisation..... | 267 |
| 19.2 Sicherheitskonzeption | 268 |
| 19.3 Wirksamkeitstest | 270 |
| 19.4 Melde- und Dokumentationspflichten bei Sicherheitsvorfällen..... | 270 |
| 19.5 Dokumentation von Sicherheitsvorfällen | 271 |
| 19.6 Meldepflicht als Auftragnehmer..... | 272 |
| 19.7 Meldepflicht gegenüber der Datenschutzaufsichtsbehörde | 272 |
| 19.8 Information betroffener Personen..... | 274 |
| 19.9 Gesetzliche Erlaubnis zur Datenverarbeitung | 276 |
| 19.10 Informationspflichten über Datenverarbeitung | 277 |
| 19.11 Gesetzliche Einkaufshilfe | 278 |
| 19.12 Gesetzliche Konfigurationshilfe | 279 |
| 19.13 Zertifizierung und Standards | 279 |
| 19.14 Erste Schritte zur Umsetzung..... | 280 |
| 19.15 Fazit | 281 |
| | |
| 20 Neue Dokumentationspflichten in der IT | 283 |
| 20.1 Einleitung..... | 283 |
| 20.2 Anforderungen an eine Dokumentation..... | 284 |
| 20.3 Inhalte der Dokumentation | 285 |
| 20.4 Phase Planung | 286 |
| 20.5 Sicherheitskonzept | 286 |
| 20.6 Beschreibung der Unternehmensprozesse | 286 |
| 20.7 Phase Umsetzung | 288 |
| 20.8 Phase Kontrolle | 289 |
| 20.9 Phase Mängelbeseitigung | 290 |
| 20.10 Fazit | 290 |
| | |
| 21 Am Anfang steht das Sicherheitskonzept | 291 |
| 21.1 Einleitung..... | 291 |
| 21.2 Neue Datenschutzerfordernungen an ein Sicherheitskonzept – in vier Schritten zum Sicherheitskonzept | 292 |
| 21.2.1 Auswahl einer Methode | 292 |
| 21.2.2 Strukturanalyse | 292 |
| 21.2.3 Risikoanalyse | 293 |
| 21.2.4 Auswahl geeigneter Maßnahmen..... | 294 |

| | | |
|---|---|------------|
| 21.3 | Diese Prozesse dürfen nicht fehlen..... | 297 |
| 21.4 | Neue Pflicht: Wirksamkeitstest..... | 297 |
| 21.5 | Fazit | 298 |
| 22 | Biometrische Zutrittskontrollen: ein Auslaufmodell? | 299 |
| 22.1 | Einleitung..... | 299 |
| 22.2 | Zulässiger Einsatz | 300 |
| 22.3 | Gestaltung des Zutrittskontrollsystems | 303 |
| 22.4 | Sicherheit | 304 |
| 22.5 | Informationspflichten | 305 |
| 22.6 | Fazit | 306 |
| Teil VIII Auftragsdatenverarbeitung und Softwareanbieter | | 307 |
| 23 | ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in | |
| | Deutschland | 309 |
| 23.1 | Zur Auftragsverarbeitung..... | 309 |
| 23.1.1 | Vergleich der Definitionen | 310 |
| 23.1.2 | Anforderungen an den Auftraggeber..... | 312 |
| 23.2 | Anforderungen an den Auftragnehmer..... | 316 |
| 23.2.1 | Haftung..... | 316 |
| 23.2.2 | Organisationsregeln | 318 |
| 23.2.3 | Technische und organisatorische Maßnahmen (TOM)/Sicherheit der Verarbeitung | 321 |
| 23.2.4 | Dokumentationspflicht | 324 |
| 23.3 | Unterauftragnehmer | 325 |
| 23.4 | Wartung/Fernwartung (§ 11 Abs. 5 BDSG)..... | 328 |
| 23.5 | Auftragsdatenverarbeitung in Drittländern..... | 328 |
| 23.6 | Funktionsübertragung | 329 |
| 23.7 | Aufsichtsbehörden..... | 332 |
| 23.8 | Umsetzung von Standards | 333 |
| 23.9 | Zertifizierung | 334 |
| 23.10 | Fazit | 334 |
| 24 | (Fehlende) Privilegierung der Auftragsverarbeitung unter der | |
| | Datenschutz-Grundverordnung? | 337 |
| 24.1 | Einleitung..... | 337 |
| 24.2 | Privilegierungswirkung der Auftragsdatenverarbeitung nach Datenschutzrichtlinie und BDSG | 338 |
| 24.3 | Datenweitergabe vom Auftraggeber an den Auftragnehmer nach der Datenschutz-Grundverordnung | 339 |
| 24.3.1 | Rückgriff auf die allgemeinen Erlaubnistatbestände | 341 |

| | | |
|---|---|------------|
| 24.3.2 | Art. 28 DS-GVO als Rechtfertigung für die Datenverarbeitung im Rahmen der Auftragsverarbeitung..... | 343 |
| 24.3.3 | Einheitliche Bewertung des Vorgangs der Datenverarbeitung bei der Auftragsverarbeitung | 344 |
| 24.4 | Fazit | 347 |
| 25 | Datenschutz-Compliance bei der Auswahl von Dienstleistern..... | 349 |
| 25.1 | Einleitung..... | 349 |
| 25.2 | Gesetzliche Mindestinhalte des Vertrags | 350 |
| 25.3 | Formerfordernisse des Vertrags..... | 352 |
| 25.4 | Beauftragung von Unterauftragnehmern..... | 352 |
| 25.5 | Garantien zur Einhaltung von geeigneten technischen und organisatorischen Maßnahmen..... | 353 |
| 25.6 | Ort der Datenverarbeitung..... | 354 |
| 25.7 | Fazit | 355 |
| 26 | 2017 das Jahr der Entscheidung für Softwareanbieter? | 357 |
| 26.1 | Einleitung..... | 357 |
| 26.2 | Steckbrief der gesetzlichen Anforderungen | 357 |
| 26.3 | HCM: Vorteile integrierter Produkte | 362 |
| 26.4 | Besonderheiten Cloud..... | 362 |
| 26.5 | Zertifizierungen als Compliance-Nachweise | 364 |
| 26.6 | Fazit | 364 |
| Teil IX Compliance-Kosten vs. Nutzen | | 365 |
| 27 | Wann kostet ein Personenbezug zu viel? | 367 |
| 27.1 | Einleitung..... | 367 |
| 27.2 | Welche Daten dürfen verarbeitet werden?..... | 368 |
| 27.3 | Compliance-Kosten vs. Nutzen | 368 |
| 27.4 | Fazit | 370 |
| Index | | 371 |
| Mitwirkende an diesem Buch | | 375 |