

# Gesamtinhaltsverzeichnis

|   |    |
|---|----|
| <b>Vorwort</b> . . . . .  | 3  |
| <b>Die Autoren</b> . . . . .  | 7  |
| <b>1 Einführung und Neuerungen im Überblick</b> . . . . .                           | 19 |
| 1.1 Datenschutz in der EU. . . . .  | 22 |
| 1.1.1 Regelung mit Durchgriffswirkung . . . . .                                     | 23 |
| 1.1.2 Bedeutung der englischen Fassung für die Auslegung . . . . .                  | 23 |
| 1.1.3 Grundsätzliches zur DSGVO . . . . .   | 24 |
| 1.2 Öffnungsklauseln für nationale Umsetzung . . . . .                              | 27 |
| 1.3 Aufsichtsbehörden . . . . .   | 30 |
| 1.3.1 Allgemeines zu den Aufsichtsbehörden . . . . .                                | 30 |
| 1.3.2 Datenschutzkonferenz (DSK) . . . . .  | 31 |
| 1.3.3 Der Europäische Datenschutzausschuss (EDSA) . . . . .                         | 32 |
| 1.4 Aufbau der DSGVO. . . . .   | 34 |
| 1.4.1 Überblick . . . . .   | 34 |
| 1.4.2 Anwendungsbereich . . . . .   | 34 |
| 1.4.3 Struktur . . . . .  | 36 |
| 1.5 Begrifflichkeiten . . . . .   | 42 |
| 1.6 Verbotsgebot mit Erlaubnisvorbehalt . . . . .                                   | 44 |
| 1.7 Grundsätze des Datenschutzes . . . . .  | 48 |
| 1.8 Neuerungen der DSGVO . . . . .  | 51 |
| 1.8.1 Betroffenenrechte im Überblick . . . . .                                      | 51 |
| 1.8.2 Recht auf Datenübertragbarkeit (Datenportabilität) . . . . .                  | 56 |
| 1.8.3 Recht auf Löschung . . . . .  | 58 |
| 1.8.4 Direkterhebung . . . . .  | 60 |
| 1.8.5 Markortprinzip . . . . .  | 61 |
| 1.8.6 „Privacy by Design“ und „Privacy by Default“ . . . . .                        | 61 |
| 1.8.7 Datenschutz-Folgenabschätzung . . . . .                                       | 63 |
| 1.8.8 Sanktionen . . . . .  | 65 |
| 1.9 Drittländer . . . . .   | 69 |
| 1.9.1 Drittländer mit angemessenem Datenschutzniveau . . . . .                      | 70 |
| 1.9.2 Was ist bei einer internationalen Datenübermittlung zu beachten? . . . . .    | 71 |
| 1.9.3 Welche Grundsätze gelten für eine Datenübermittlung in Drittländer? . . . . . | 72 |

|  |           |
|--|-----------|
| 1.9.4 Was müssen Anbieter mit Sitz außerhalb der EU beachten? . . . . .  | 73        |
| 1.9.5 Exkurs EWR: Liechtenstein . . . . .                                | 75        |
| 1.10 Allgemeine Bewertung . . . . .                                      | 77        |
| <b>2 Beschäftigtendatenschutz . . . . .</b>                              | <b>81</b> |
| 2.1 Kurzüberblick . . . . .  | 81        |
| 2.2 Persönlicher Anwendungsbereich . . . . .                             | 86        |
| 2.3 Sachlicher Anwendungsbereich . . . . .                               | 87        |
| 2.4 Datenschutz im Individualarbeitsrecht . . . . .                      | 88        |
| 2.4.1 Sensible Daten . . . . .   | 88        |
| 2.4.2 Anbahnung von Arbeitsverhältnissen . . . . .                       | 88        |
| 2.4.3 Durchführung und Beendigung von Arbeitsverhältnissen               | 90        |
| 2.4.4 Personalakte und Verpflichtungserklärung . . . . .                 | 91        |
| 2.4.5 Datenschutz und freie Mitarbeiter . . . . .                        | 92        |
| 2.5 Datenschutz im Kollektivarbeitsrecht . . . . .                       | 94        |
| 2.5.1 Tarifverträge . . . . .  | 94        |
| 2.5.2 Betriebsvereinbarungen . . . . .                                   | 94        |
| 2.5.3 Exkurs: Kirchliches Datenschutzrecht . . . . .                     | 95        |
| 2.5.4 Datenschutz und Betriebsrat . . . . .                              | 96        |
| 2.6 Praktisches . . . . .  | 99        |
| 2.6.1 Datenschutz im Konzern . . . . .                                   | 99        |
| 2.6.2 Datenschutz und BEM . . . . .                                      | 100       |
| 2.6.3 Datenschutz und Unternehmensnachfolge . . . . .                    | 100       |
| 2.6.4 Das Recht auf Datenübertragbarkeit im Arbeitsverhältnis .          | 101       |
| 2.6.5 Datenschutz und Industrie 4.0 . . . . .                            | 102       |
| 2.7 Informations-, Auskunfts- und Meldepflichten . . . . .               | 111       |
| 2.7.1 Informationspflichten . . . . .                                    | 111       |
| 2.7.2 Auskunftsrecht . . . . .   | 111       |
| 2.7.3 Meldepflicht . . . . .   | 112       |
| 2.8 Prozessuale . . . . .  | 113       |
| 2.8.1 Rechtswidrigkeit von Überwachungs- und Kontrollmaßnahmen . . . . . | 113       |
| 2.8.2 Verwertungsverbote . . . . .                                       | 113       |
| 2.8.3 Rechtsprechung des BAG . . . . .                                   | 114       |
| 2.9 Folgen der Zuwiderhandlung . . . . .                                 | 116       |
| 2.9.1 Sanktionen . . . . .   | 116       |

|          |  |            |
|----------|--|------------|
| 2.9.2    | Schadensersatz . . . . .   | 116        |
| <b>3</b> | <b>Der Datenschutzbeauftragte . . . . .</b>  | <b>119</b> |
| 3.1      | Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten . . . . .               | 121        |
| 3.2      | Einordnung in die Organisation . . . . .   | 125        |
| 3.2.1    | Direktes Vortragsrecht . . . . .   | 125        |
| 3.2.2    | Weisungsungebundenheit . . . . .   | 125        |
| 3.2.3    | Vermeidung von Interessenkonflikten . . . . .                                      | 126        |
| 3.2.4    | Abberufungsschutz bzw. Sonderkündigungsschutz . . . . .                            | 127        |
| 3.3      | Benennung des Datenschutzbeauftragten . . . . .                                    | 130        |
| 3.3.1    | Begrifflichkeiten und Formvorschriften . . . . .                                   | 130        |
| 3.3.2    | Voraussetzungen zur Ausübung der Tätigkeit . . . . .                               | 131        |
| 3.3.3    | Wann ist ein Datenschutzbeauftragter zu benennen? . . . . .                        | 133        |
| 3.3.4    | Interne und externe Datenschutzbeauftragte . . . . .                               | 138        |
| 3.4      | Bekanntmachung des Datenschutzbeauftragten . . . . .                               | 141        |
| 3.5      | Pflichten der Organisation . . . . .   | 144        |
| 3.5.1    | Ordnungsgemäße und frühzeitige Einbindung in datenschutzrelevante Themen . . . . . | 144        |
| 3.5.2    | Unterstützung des Datenschutzbeauftragten . . . . .                                | 145        |
| 3.6      | Haftung des Datenschutzbeauftragten . . . . .                                      | 147        |
| 3.6.1    | Generelle Haftung des DSB . . . . .  | 147        |
| 3.6.2    | Haftung des internen Datenschutzbeauftragten . . . . .                             | 148        |
| 3.6.3    | Haftung des externen Datenschutzbeauftragten . . . . .                             | 150        |
| 3.7      | Umsetzungsmöglichkeiten im Konzern und für öffentliche Stellen . . . . .           | 152        |
| 3.8      | Besonderheiten des kirchlichen Datenschutzbeauftragten . . . . .                   | 154        |
| 3.9      | Datenschutzbeauftragter und Betriebsrat . . . . .                                  | 156        |
| 3.10     | Arbeitshilfen . . . . .  | 157        |
| 3.10.1   | Muster: Benennung zum betrieblichen Datenschutzbeauftragten . . . . .              | 157        |
| <b>4</b> | <b>IT-Sicherheit und Datenschutz . . . . .</b>                                     | <b>161</b> |
| 4.1      | Einleitung . . . . .   | 161        |
| 4.2      | Anforderungen an die IT-Sicherheit . . . . .                                       | 163        |
| 4.2.1    | Gesetzliche Anforderungen an die IT-Sicherheit . . . . .                           | 163        |
| 4.2.2    | Untergesetzliche Normen zur IT-Sicherheit . . . . .                                | 169        |
| 4.2.3    | Schutzziele der IT-Sicherheit . . . . .  | 171        |
| 4.2.4    | Managementsystem zur Umsetzung der IT-Sicherheit . . . . .                         | 172        |

|       |   |     |
|-------|---|-----|
| 4.3   | Anforderungen an die Sicherheit bei der Verarbeitung personenbezogener Daten nach Art. 32 DSGVO . . . . . | 175 |
| 4.3.1 | Schutzziele des Datenschutzes . . . . .   | 175 |
| 4.3.2 | Anforderungen an den Schutz personenbezogener Daten . . . . .   | 177 |
| 4.3.3 | Vorgehen zur Umsetzung der Anforderungen . . . . .  | 178 |
| 4.4   | Gemeinsame Sicherheitsstrategie von IT-Sicherheit und Datenschutz . . . . .                               | 185 |
| 4.4.1 | Konfliktpotenziale bei den Schutzz Zielen . . . . .   | 185 |
| 4.4.2 | Auseinanderfallender Schutzbedarf . . . . .   | 186 |
| 4.4.3 | Fazit . . . . .   | 187 |
| 4.5   | Dokumentationserfordernis: Verzeichnis von Verarbeitungstätigkeiten . . . . .                             | 188 |
| 4.5.1 | Inhaltliche Anforderungen beim Verantwortlichen . . . . .   | 190 |
| 4.5.2 | Inhaltliche Anforderungen bei Auftragsverarbeitern . . . . .  | 194 |
| 4.6   | Datenschutz-Folgenabschätzung . . . . .   | 196 |
| 4.6.1 | Verpflichtung . . . . .   | 196 |
| 4.6.2 | Inhaltliche Anforderungen . . . . .   | 199 |
| 4.6.3 | Konsultationspflicht mit der Datenschutzaufsichtsbehörde  | 200 |
| 4.7   | Besondere Anforderungen bei Cloud-Lösungen . . . . .  | 202 |
| 4.7.1 | Auswahl geeigneter Daten und Datenverarbeitungen . . . . .  | 203 |
| 4.7.2 | Auswahl des Anbieters . . . . .   | 204 |
| 4.7.3 | Vertragliche Sicherstellung von Kontrollmöglichkeiten . . . . .   | 204 |
| 4.7.4 | Transfer der Daten in ein Drittland . . . . .   | 205 |
| 4.8   | Besondere Anforderungen bei der Bereitstellung von WLAN . . . . .   | 206 |
| 4.8.1 | Zugang nur für Betriebsangehörige . . . . .   | 206 |
| 4.8.2 | Zugang auch für Externe . . . . .   | 207 |
| 5     | <b>Umgang mit personenbezogenen Daten in der Praxis</b> . . . . .   | 211 |
| 5.1   | Zentrale abteilungsübergreifende Datenverarbeitungsaspekte . . . . .                                      | 211 |
| 5.1.1 | Datenschutz und IT-Prozesse – ein Interessenkonflikt? . . . . .   | 211 |
| 5.1.2 | Personenbezogene Daten und Kriterien zu deren Ermittlung . . . . .  | 213 |
| 5.1.3 | „Erleichternde“ Datenverarbeitungsumstände . . . . .  | 216 |
| 5.1.4 | Datensicherheitsaspekte . . . . .   | 218 |
| 5.1.5 | Bedeutung des Standard-Datenschutzmodells . . . . .   | 223 |
| 5.1.6 | Datenschutz und Künstliche Intelligenz . . . . .  | 227 |
| 5.1.7 | Tracking und Datenschutz . . . . .  | 232 |

|        |   |     |
|--------|---|-----|
| 5.1.8  | Der Administrator . . . . .   | 234 |
| 5.2    | Personalabteilung . . . . .   | 236 |
| 5.2.1  | Bewerbungsverfahren . . . . .   | 236 |
| 5.2.2  | Durchführung des Beschäftigungsverhältnisses . . . . .  | 240 |
| 5.2.3  | Offboarding . . . . .   | 244 |
| 5.3    | Marketing und Kommunikation . . . . .   | 246 |
| 5.3.1  | Anforderungen an die Verarbeitung personenbezogener Daten zu Werbe- und Marketingzwecken nach DSGVO . . . . .                   | 247 |
| 5.3.2  | Werbeansprachen unter Beachtung wettbewerbsrechtlicher Anforderungen . . . . .  | 261 |
| 5.3.3  | Social-Media-Marketing . . . . .  | 264 |
| 5.3.4  | Einsatz von Trackingmechanismen zu Marketingzwecken . . . . .   | 268 |
| 5.4    | Arbeitshilfen . . . . .   | 270 |
| 5.4.1  | Checkliste: Einwilligungserklärungen und Widerruf im Marketing . . . . .  | 270 |
| 5.4.2  | Checkliste: Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis . . . . .  | 272 |
| 5.4.3  | Checkliste: Umgang mit personenbezogenen Daten im Bewerbungsverfahren . . . . .   | 275 |
| 6      | <b>Rechte der betroffenen Person – Rechts-, Haftungs- und Zahlungsfolgen bei Verstößen . . . . .</b>                            | 279 |
| 6.1    | Rechte der betroffenen Person . . . . .   | 279 |
| 6.1.1  | Einleitung . . . . .  | 279 |
| 6.1.2  | Recht auf transparente Information, Kommunikation und Modalitäten der Ausübung von Betroffenenrechten (Art. 12 DSGVO) . . . . . | 280 |
| 6.1.3  | Recht auf Information (Artt. 13, 14 DSGVO) . . . . .  | 285 |
| 6.1.4  | Recht auf Auskunft (Art. 15 DSGVO) . . . . .  | 291 |
| 6.1.5  | Recht auf Berichtigung (Art. 16 DSGVO) . . . . .  | 299 |
| 6.1.6  | Recht auf Löschung und Recht auf Vergessenwerden (Art. 17 DSGVO) . . . . .  | 304 |
| 6.1.7  | Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) . . . . .  | 313 |
| 6.1.8  | „Recht auf Datenübertragbarkeit“ (Art. 20 DSGVO) . . . . .  | 316 |
| 6.1.9  | Recht auf Widerspruch (Art. 21 DSGVO) . . . . .   | 319 |
| 6.1.10 | Recht auf nicht ausschließlich automatisierte Entscheidungen im Einzelfall inkl. Profiling (Art. 22 DSGVO) . . . . .            | 323 |

|  |            |
|--|------------|
| 6.1.11 Sonderfall: Recht am eigenen Bild (DSGVO vs. KUG) . . . . . | 328        |
| <b>6.2 Folgen bei Verstößen . . . . .</b>                          | <b>337</b> |
| 6.2.1 Potenzielle (Rechts-)Folgen . . . . .                        | 337        |
| 6.2.2 Rechte von Betroffenen . . . . .                             | 337        |
| 6.2.3 Rechte von Aufsichtsbehörden . . . . .                       | 340        |
| 6.2.4 Erfahrungen mit Bußgeldern . . . . .                         | 343        |
| 6.2.5 Sonstige (Rechts-)Folgen . . . . .                           | 348        |
| <b>Adressen der Aufsichtsbehörden . . . . .</b>                    | <b>351</b> |
| <b>Gesetzesgrundlagen . . . . .</b>                                | <b>357</b> |
| <b>Abkürzungsverzeichnis . . . . .</b>                             | <b>359</b> |
| <b>Stichwortverzeichnis . . . . .</b>                              | <b>361</b> |