

# Inhaltsverzeichnis

|   |      |
|---|------|
| Vorwort des Herausgebers zur 2. Auflage .....         | V    |
| Abkürzungsverzeichnis .....                           | XIII |
| Verzeichnis der (abgekürzt) zitierten Literatur ..... | XVII |

## § 1. Einleitung

|  |   |
|--|---|
| A. Zielsetzung und Handhabung der Checklisten .....              | 1 |
| I. Ziele und Genese der DS-GVO .....                             | 1 |
| II. Die DS-GVO als EU-Verordnung .....                           | 3 |
| III. Öffnungsklauseln – Nationales Datenschutzrecht (BDSG) ..... | 3 |
| IV. ePrivacy-Richtlinie .....                                    | 4 |
| B. Die Auslegung der DS-GVO .....                                | 4 |
| C. Anwendbarkeit der DS-GVO .....                                | 5 |

## § 2. Accountability: die Rechenschaftspflicht

|  |    |
|--|----|
| A. Einführung .....  | 7  |
| B. Erläuterungen zur Checkliste .....  | 7  |
| I. Das Prinzip der Accountability .....  | 7  |
| 1. Explizite Verpflichtung zu Rechenschaft und Nachweis in Art. 5 DS-GVO<br>und Art. 24 DS-GVO .....           | 7  |
| 2. Accountability als übergreifendes Prinzip der DS-GVO im Kontext von<br>Managementprozessen .....            | 8  |
| 3. Accountability bezüglich der einzelnen Datenschutzgrundsätze gem. Art. 5<br>DS-GVO .....                    | 10 |
| II. Sicherstellung der Einhaltung der DS-GVO .....   | 12 |
| 1. Grundlagen der Sicherstellung .....   | 12 |
| 2. Vornahme geeigneter technischer und organisatorischer Maßnahmen<br>(TOMs) und Datenschutzvorkehrungen ..... | 13 |
| 3. Risikobasierter Ansatz: Angemessenheit der Maßnahme .....   | 14 |
| 4. Komponenten der Konzeptionierung („Plan“) .....   | 15 |
| 5. Komponenten der Umsetzung („Do“) .....  | 19 |
| III. Nachweis der Sicherstellung der Einhaltung der DS-GVO .....   | 21 |
| 1. Grundlagen zur Nachweispflicht .....  | 21 |
| 2. Risikobasierter Ansatz: Umfang der Nachweispflicht .....  | 22 |
| 3. Komponenten des Nachweises .....  | 23 |
| IV. Überprüfungspflicht und Anpassung .....  | 25 |
| 1. Grundlagen der kontinuierlichen Verbesserung .....  | 25 |
| 2. Komponenten von Überprüfungspflicht und Anpassung („Check“ und<br>„Act“) .....                              | 27 |
| V. Datenschutzmanagement und Datenschutzorganisation .....   | 30 |
| 1. Pflicht, ein Datenschutzmanagement zu etablieren und zu unterhalten .....                                   | 30 |
| 2. Elemente eines Datenschutzmanagements und die<br>Datenschutzorganisation .....                              | 32 |
| 3. Komponenten entlang der 7 Elemente des Datenschutzmanagements nach<br>IDW PS 980 .....                      | 33 |
| VI. Die Bestellung eines Datenschutzbeauftragten .....   | 36 |
| 1. Element der Accountability .....  | 36 |

VII

|   |    |
|---|----|
| 2. Pflicht zur Bestellung des DSB .....   | 36 |
| 3. Materielle Anforderungen an die Bestellung des DSB .....   | 38 |
| 4. Anforderungen an den Status des DSB gem. Art. 38 DS-GVO .....  | 39 |
| 5. Die Aufgaben des DSB .....   | 40 |
| <br>  |    |
| <b>§ 3. Der Kernprozess des Datenschutzes – neue Verarbeitungen erfassen,<br/>bewerten und überwachen</b>   |    |
| A. Einführung .....   | 43 |
| B. Erläuterungen zur Checkliste .....   | 43 |
| I. Rechenschaftspflicht (Accountability) und Datenschutz-Kernprozess .....  | 43 |
| 1. Die allgemeinen Anforderungen an die Implementierung .....   | 43 |
| 2. Anforderungen an einen Prozess, der sicherstellt, dass neue<br>datenschutzrelevante Verarbeitungen und Projekte erfasst und bewertet<br>werden .....   | 44 |
| II. Das Verarbeitungsverzeichnis als Kernstück der Datenschutz-Compliance .....   | 45 |
| 1. Die Funktion des Verarbeitungsverzeichnisses .....   | 45 |
| 2. Das Verarbeitungsverzeichnis des Verantwortlichen .....  | 46 |
| 3. Das Verarbeitungsverzeichnis des Auftragsverarbeiters (Art. 32 Abs. 2<br>DS-GVO) .....   | 51 |
| 4. Weitere Anforderungen an das Verarbeitungsverzeichnis .....  | 53 |
| III. Die Datenschutz-Folgenabschätzung .....  | 53 |
| 1. Hohes Risiko als Voraussetzung für eine<br>Datenschutz-Folgenabschätzung .....   | 54 |
| 2. Durchführung, Dokumentation und Methodik der<br>Datenschutz-Folgenabschätzung .....  | 61 |
| 3. Einbindung von weiteren Akteuren und betroffenen Personen .....  | 63 |
| 4. Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO .....  | 64 |
| 5. Auditierung und Wirksamkeitsprüfung (Art. 35 Abs. 9 DS-GVO) .....  | 65 |
| IV. Privacy by Design and by Default – Datenschutz durch Technikgestaltung<br>und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) .....  | 65 |
| 1. Grundlagen von Privacy by Design and Default .....   | 66 |
| 2. Privacy by Design (Art. 25 Abs. 1 DS-GVO) .....  | 66 |
| 3. Privacy by Default (Art. 25 Abs. 2 DS-GVO) .....   | 71 |
| 4. Zertifizierung von Privacy by Design und by Default .....  | 72 |
| <br>  |    |
| <b>§ 4. Rechtfertigung und Rechtmäßigkeit der Verarbeitung<br/>personenbezogener Daten</b>  |    |
| A. Einführung .....   | 75 |
| B. Erläuterungen zur Checkliste .....   | 76 |
| I. Rechtfertigung einer Verarbeitung personenbezogener Daten .....  | 76 |
| 1. Rechtfertigung durch Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO) .....   | 76 |
| 2. Rechtfertigung durch Vertragsabschluss und Erfüllung vorvertraglicher<br>Maßnahmen (Art. 6 Abs. 1 Buchst. b DS-GVO) .....  | 87 |
| 3. Rechtfertigung durch Erfüllung einer rechtlichen Verpflichtung (Art. 6<br>Abs. 1 Buchst. c DS-GVO) .....   | 88 |
| 4. Rechtfertigung bei Verarbeitung personenbezogener Daten zum Schutz<br>lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d DS-GVO) .....  | 89 |
| 5. Rechtfertigung bei Verarbeitung personenbezogener Daten zur<br>Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung<br>öffentlicher Gewalt (Art. 6 Abs. 1 Buchst. e DS-GVO) ..... | 89 |

|   |    |
|---|----|
| 6. Rechtfertigung aufgrund von berechtigten Interessen (Art. 6 Abs. 1 Buchst. f DS-GVO) .....       | 89 |
| 7. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) .....          | 92 |
| 8. Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) ..... | 93 |
| II. Weitere Anforderungen an eine Verarbeitung personenbezogener Daten .....                        | 95 |
| 1. Accountability im Rahmen der konkreten Verarbeitung (Rechenschaftspflicht) .....                 | 95 |
| 2. Die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) .....         | 96 |

## **§ 5. Die Information der betroffenen Personen**

|  |     |
|--|-----|
| A. Einführung .....  | 103 |
| B. Erläuterungen zur Checkliste .....  | 104 |
| I. Vorüberlegungen .....   | 104 |
| 1. Gesetzliche Verantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO .....                    | 104 |
| 2. Durchführungsverantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO im konkreten Fall ..... | 105 |
| 3. Ausnahmen von der Verpflichtung zur (konkreten) Informationserteilung an die betroffene Person .....                                    | 106 |
| II. Ausgestaltung der Information der betroffenen Personen .....   | 116 |
| 1. Pflichtinhalte .....  | 116 |
| 2. Anforderungen an die Formulierung und Strukturierung der Pflichtinhalte .....   | 134 |
| III. Anforderungen an die Implementierung .....  | 139 |
| 1. Zeitpunkt der Erteilung der Datenschutzinformationen .....  | 139 |
| 2. Darreichungsform der Datenschutzinformationen .....   | 142 |

## **§ 6. Auskunft**

|   |     |
|---|-----|
| A. Einführung .....   | 145 |
| B. Erläuterungen zur Checkliste .....   | 146 |
| I. Organisatorische Anforderungen für die Auskunft .....                      | 146 |
| II. Formelle Anforderungen an die Antwort auf einen Antrag auf Auskunft ..... | 150 |
| 1. Form der Beantwortung .....  | 152 |
| 2. Kosten der Auskunft .....  | 153 |
| III. Materielle Anforderungen an die Auskunft .....                           | 153 |
| 1. Erste Stufe des Auskunftersuchens – Positiv oder Negativtest .....         | 153 |
| 2. Zweite Stufe – Beantwortung des Auskunftersuchens .....                    | 154 |
| IV. Grenzen der Auskunft .....  | 160 |

## **§ 7. Sonstige Betroffenenrechte**

|  |     |
|--|-----|
| A. Einführung .....                      | 163 |
| B. Erläuterungen zur Checkliste .....    | 163 |
| I. Recht auf Berichtigung .....          | 163 |
| II. Recht auf Datenübertragbarkeit ..... | 169 |

## **§ 8. Löschen von Daten**

|  |     |
|--|-----|
| A. Einführung .....  | 179 |
| B. Erläuterungen zur Checkliste .....  | 180 |
| I. Speicherbegrenzung – Regelmäßiges Löschen .....                           | 180 |
| II. Das Betroffenenrecht auf Löschen und das Recht auf Vergessenwerden ..... | 188 |

## **§ 9. Die Sicherheit der Verarbeitung sowie technische und organisatorische Maßnahmen**

|  |     |
|--|-----|
| A. Einführung .....  | 195 |
| B. Erläuterungen zur Checkliste .....                        | 196 |
| I. Die Sicherheit der Verarbeitung nach Art. 32 DS-GVO ..... | 196 |
| 1. Allgemeines .....   | 196 |
| 2. Würde ein Datensicherheitskonzept entwickelt? .....       | 208 |
| 3. Berechtigung – „Need-to-Know-Prinzip“ .....               | 210 |
| II. Praxishinweise für die Umsetzung .....                   | 212 |

## **§ 10. Meldungen und Benachrichtigung von Sicherheitsvorfällen**

|  |     |
|--|-----|
| A. Einführung .....  | 215 |
| B. Erläuterungen zur Checkliste .....  | 215 |
| I. Organisationspflichten des Verantwortlichen (Rechenschaftspflicht und Implementierung) .....            | 215 |
| 1. Allgemeine Anforderungen an die Implementierung .....   | 216 |
| 2. Risikoprognose .....  | 219 |
| 3. Besondere Anforderungen an die Implementierung .....  | 222 |
| 4. Dokumentationspflichten des Verantwortlichen nach Art. 33 Abs. 5 DS-GVO .....                           | 225 |
| II. Ausschlussstatbestände für die Benachrichtigung von betroffenen Personen (Art. 34 Abs. 3 DS-GVO) ..... | 227 |

## **§ 11. Auftragsverarbeitung und gemeinsame Verantwortlichkeit**

|   |     |
|---|-----|
| A. Einführung .....   | 229 |
| B. Erläuterungen zur Checkliste .....   | 230 |
| I. Auftragsverarbeitung .....   | 230 |
| 1. Vorliegen einer Auftragsverarbeitung .....   | 231 |
| 2. (Vertrags-)Rechtliche Bindung des Auftragsverarbeiters in Bezug auf den Verantwortlichen ..... | 233 |
| 3. Implementierung von Kontroll- und Steuerungsmechanismen .....                                  | 248 |
| II. Gemeinsame Verantwortlichkeit .....   | 252 |
| 1. Vorliegen einer gemeinsamen Verantwortlichkeit .....   | 253 |
| 2. Vereinbarung über die gemeinsame Verantwortlichkeit .....                                      | 256 |
| 3. Anforderungen an die Implementierung .....   | 263 |

## **§ 12. Drittlandtransfers**

|   |     |
|---|-----|
| A. Einführung .....                             | 265 |
| B. Erläuterungen zur Checkliste .....           | 266 |
| I. Vorliegen eines Drittlandtransfers .....     | 266 |
| II. Zulässigkeit eines Drittlandtransfers ..... | 268 |

## § 13 Künstliche Intelligenz und Datenschutz

|  |     |
|--|-----|
| A. Einführung .....  | 285 |
| B. Erläuterungen zur Checkliste .....                                    | 286 |
| I. Automatisierte Entscheidungen im Einzelfall nach Art. 22 DS-GVO ..... | 286 |
| 1. Allgemeines .....   | 286 |
| 2. Ausschließliche automatisierte Entscheidung im Einzelfall .....       | 286 |
| 3. Rechtliche Wirkung oder erhebliche Beeinträchtigung .....             | 288 |
| 4. Zulässigkeit automatisierter Entscheidungen .....                     | 288 |
| 5. Angemessene Maßnahmen .....   | 290 |
| 6. Informationspflichten .....   | 291 |
| 7. DSFA .....  | 292 |
| 8. Sonderfall: Besondere Kategorien personenbezogener Daten .....        | 293 |
| II. Sonstiger Einsatz von KI .....                                       | 294 |
| III. Weitere Hinweise und aktuelle Entwicklungen .....                   | 294 |
| Anhang: Zusammengefasste Checklisten .....                               | 297 |
| Sachverzeichnis .....  | 329 |