

Inhaltsübersicht

Kapitel 1: Grundlagen des Umgangs mit der DSGVO

| | | |
|------|---|---|
| I. | Die Anwendung der DSGVO und der nationalen Begleitgesetze | 1 |
| II. | Parallelität von DSGVO und „Altgesetzen“ | 6 |
| III. | Auslegung der DSGVO und der Begleitgesetze | 7 |

Kapitel 2: Grundlagen des Datenschutzrechts

| | | |
|------|--|----|
| I. | Datenschutz im Anwendungsbereich des EU-Rechts | 17 |
| II. | Schutzgut des Datenschutzrechts | 18 |
| III. | Grundbegriffe des Datenschutzrechts | 20 |
| IV. | Zusammenspiel mit anderen Rechtsmaterien | 23 |

Kapitel 3: Anwendungsbereich des Datenschutzrechts

| | | |
|------|---|----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO | 33 |
| II. | Sachlicher Anwendungsbereich | 35 |
| III. | Räumlicher Anwendungsbereich, Art. 3 DSGVO | 43 |
| IV. | Anwendungsbereich mitgliedstaatlicher Regelungen | 56 |
| V. | Anwendungsbereich sonstiger ausfüllender Normen | 60 |

Kapitel 4: Datenschutzrechtliche Grundsätze

| | | |
|------|--|----|
| I. | Bedeutung und Funktion der Datenschutzgrundsätze | 61 |
| II. | Die Grundsätze im Einzelnen | 62 |
| III. | Die Rechenschaftspflicht | 70 |

Kapitel 5: Zulässigkeit der Verarbeitung personenbezogener Daten

| | | |
|------|---|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO | 74 |
| II. | Gesetzliche Erlaubnisvorschriften | 76 |
| III. | Einwilligung der Betroffenen | 173 |

Kapitel 6: Umgang mit Betroffenen

| | | |
|------|--|-----|
| I. | Einführung | 211 |
| II. | Systematischer Überblick über die Betroffenenrechte gem. Art. 12–23 DSGVO und Art. 77 ff. DSGVO | 212 |
| III. | Informationspflichten (Art. 13 und 14 DSGVO) | 214 |
| IV. | Recht auf Auskunft (Art. 15 DSGVO) | 277 |
| V. | Recht auf Berichtigung (Art. 16 DSGVO) | 358 |

XI

| | | |
|-------|---|-----|
| VI. | Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO) . | 367 |
| VII. | Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO).. | 410 |
| VIII. | Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO) | 420 |
| IX. | Recht auf Datenübertragbarkeit (Art. 20 DSGVO)..... | 429 |
| X. | Widerspruchsrecht (Art. 21 DSGVO)..... | 447 |
| XI. | Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO) | 462 |
| XII. | Sanktionierung..... | 487 |

Kapitel 7: Auftragsverarbeitung

| | | |
|-------|---|-----|
| I. | Begriff und Gegenstand der Auftragsverarbeitung | 490 |
| II. | Abgrenzung zum Verantwortlichen und zur gemeinsamen Verantwortlichkeit | 493 |
| III. | Rechtsnatur der Auftragsverarbeitung | 498 |
| IV. | Typische Fallkonstellationen einer Auftragsverarbeitung | 500 |
| V. | Rechte und Pflichten aus einer Auftragsverarbeitung..... | 502 |
| VI. | Begründung einer Auftragsverarbeitung | 506 |
| VII. | Auftragsverarbeitung innerhalb von Unternehmensgruppen..... | 517 |
| VIII. | Unterbeauftragungen..... | 518 |
| IX. | Haftung von Auftragsverarbeitern..... | 522 |
| X. | Kontrolle von Auftragsverarbeitern..... | 526 |
| XI. | Dokumentation der Kontrollen | 529 |
| XII. | Kontrollergebnis | 529 |

Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger Verantwortlichkeit

| | | |
|------|--|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO..... | 532 |
| II. | Gemeinsam für die Verarbeitung Verantwortliche | 532 |
| III. | Getrennte Verantwortlichkeiten..... | 552 |
| IV. | Niederlassungsübergreifende Verarbeitungen..... | 557 |

Kapitel 9: Internationale Datenübermittlungen

| | | |
|------|--|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO..... | 565 |
| II. | Einführung in den Regelungsbereich | 565 |
| III. | Länder mit angemessenem Schutzniveau..... | 575 |
| IV. | Geeignete Garantien für Drittlandtransfers | 582 |
| V. | Ausnahmen für bestimmte Fälle | 614 |

Kapitel 10: Datenschutzmanagement

| | | |
|------|--|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO..... | 627 |
| II. | Terminologie..... | 628 |
| III. | Anforderungen an das Datenschutzmanagement..... | 629 |
| IV. | Risikoadäquates Datenschutzmanagement..... | 630 |
| V. | Konkrete Maßnahmen hängen vom Einzelfall ab..... | 633 |
| VI. | Grundlegende Maßnahmen des Datenschutzmanagements..... | 634 |
| VII. | Datenschutzmanagementsystem..... | 640 |

Kapitel 11: Datenschutzorganisation

| | | |
|------|---|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO..... | 647 |
| II. | Ergänzende Regelungen des BDSG..... | 648 |
| III. | Terminologie..... | 648 |
| IV. | Datenschutzorganisation als Voraussetzung von Datenschutzcompliance..... | 648 |
| V. | Pflicht zur Errichtung einer Datenschutzorganisation..... | 649 |
| VI. | Gestaltung einer Datenschutzorganisation..... | 655 |
| VII. | Beispiele..... | 698 |

Kapitel 12: Datenschutzprozesse

| | | |
|------|--|-----|
| I. | Prozessuale Umsetzung datenschutzrechtlicher Vorgaben..... | 705 |
| II. | Privacy by Design und by Default, Art. 25 DSGVO..... | 707 |
| III. | Datenlöschung..... | 718 |
| IV. | Verzeichnis von Verarbeitungstätigkeiten..... | 727 |
| V. | Datenschutz-Folgenabschätzung..... | 739 |
| VI. | Umgang mit Datenlecks..... | 758 |
| VII. | Integration des Datenschutzes in allgemeine Unternehmensprozesse..... | 780 |

Kapitel 13: Technischer Datenschutz und Risikomanagement

| | | |
|------|--|-----|
| I. | Überblick über die einschlägigen Regelungen..... | 794 |
| II. | Allgemeine Grundlagen des technischen Datenschutzrisiko- managements..... | 797 |
| III. | Nutzung der Standards und Vorgehen der Informationssicherheit.... | 806 |
| IV. | Technische Maßnahmen zur datenschutzkonformen Verarbeitung.... | 826 |
| V. | Privacy by Design und Privacy by Default..... | 871 |
| VI. | Ausblick..... | 876 |

Kapitel 14: Verhaltensregeln und Zertifizierungen

| | | |
|------|---|-----|
| I. | Einleitung | 879 |
| II. | Grundsätzliche Unterscheidung und Komplementarität | 882 |
| III. | Mehrwert für Unternehmen | 883 |
| IV. | Genehmigung von Verhaltensregeln | 889 |
| V. | Überwachung genehmigter Verhaltensregeln/Sanktionen im Falle von Verstößen | 898 |
| VI. | Inhalte und Gestaltung von Verhaltensregeln | 900 |
| VII. | Zertifizierungsverfahren | 903 |

Kapitel 15: Beschäftigtendatenschutz

| | | |
|------|---|-----|
| I. | Überblick über die einschlägigen Regelungen der DSGVO | 908 |
| II. | Handlungsoptionen des Gesetzgebers | 909 |
| III. | Datenschutzrechtliche Erlaubnistatbestände | 918 |
| IV. | Informationspflichten und Betroffenenrechte | 935 |
| V. | Überwachungsmaßnahmen – Rechtslage in Deutschland | 940 |
| VI. | Handlungsempfehlung | 946 |

Kapitel 16: Behördliche und gerichtliche Verfahren

| | | |
|------|------------------------------------|------|
| I. | Aufsichtsbehörden | 950 |
| II. | Aufsichtsverfahren | 965 |
| III. | Umgang mit Aufsichtsbehörden | 977 |
| IV. | Bußgelder | 986 |
| V. | Gerichtlicher Rechtsschutz | 1012 |
| VI. | Verbandsklage | 1025 |

Kapitel 17: Besondere Themenkomplexe

| | | |
|-----------|--|------|
| A. | Web Tracking und Online Advertising | |
| I. | Technische Abläufe | 1039 |
| II. | Zulässigkeit des Web Tracking und des Online Advertising | 1045 |
| III. | Verantwortlichkeit für Web Tracking und Online Advertising | 1095 |
| IV. | Zusätzliche Pflichten | 1098 |
| V. | Bußgeldrahmen bei Verstößen | 1100 |
| B. | Customer-Relationship-Management | |
| I. | Überblick über die einschlägigen Regelungen | 1103 |
| II. | Datenquellen | 1104 |
| III. | Profiling zu Werbezwecken | 1106 |
| IV. | Werbliche Kommunikation mit Kunden | 1113 |

| | |
|--|------|
| C. E-Discovery | |
| I. Ausgewählte Rahmenbedingungen | 1121 |
| II. Kollision mit dem Datenschutz im Beweissicherungsprozess | 1124 |
| III. Fazit | 1134 |
| D. Cloud Computing | |
| I. Eigenschaften und Terminologie | 1136 |
| II. Cloud-spezifische Problemfelder | 1138 |
| E. Big Data | |
| I. Eigenschaften und Terminologie | 1141 |
| II. Big Data-spezifische Problemfelder | 1142 |
| F. Gesundheitsdatenschutz | |
| I. Definition „Gesundheitsdaten“ | 1148 |
| II. Systematik der datenschutzrechtlichen Regelungen im Gesundheitsbereich | 1151 |
| III. Zulässigkeit der Verarbeitung von Gesundheitsdaten auf Basis von Vorschriften aus der DSGVO/dem BDSG | 1159 |
| IV. Weitere Besonderheiten nach der DSGVO/dem BDSG bei der Verarbeitung von Gesundheitsdaten | 1178 |
| V. (Berufsrechtliche) Schweigepflicht | 1181 |
| VI. Verarbeitung zu wissenschaftlichen Forschungszwecken | 1189 |

Kapitel 18: Österreichisches Datenschutzrecht

| | |
|---|------|
| I. Gesetzliche Grundlagen | 1204 |
| II. Nutzung von Öffnungsklauseln | 1205 |
| III. Grundrecht auf Datenschutz | 1209 |
| IV. Marketing und Kontaktaufnahme zu Werbezwecken | 1212 |
| V. Österreichische Spezialregelungen | 1215 |
| VI. Arbeitnehmer-Datenschutz | 1229 |
| VII. Österreichische Entscheidungen | 1235 |
| VIII. Rechtsdurchsetzung und Verfahrensrecht | 1250 |

Kapitel 19: Leitentscheidungen des EuGH zur DSGVO

| | |
|---------------------------------------|------|
| I. Einleitung | 1264 |
| II. Leitentscheidungen des EuGH | 1265 |

Kapitel 20: Vorgehensweise zur Umsetzung von DSGVO-Anforderungen im Unternehmen

| | | |
|------|---|------|
| I. | Anpassungsbedarf im Unternehmen | 1303 |
| II. | Leitbild zur Umsetzung der DSGVO im Unternehmen | 1305 |
| III. | Ausgestaltung eines Umsetzungsprojekts | 1305 |
| IV. | Erste Erfahrungen aus der Umsetzungspraxis | 1319 |
| V. | Fazit | 1321 |

Kapitel 21: Weitere rechtliche Entwicklungen und Ausblick

| | | |
|------|---|------|
| I. | Datenschutzrecht als dynamisches Rechtsgebiet | 1323 |
| II. | Gesetzgeber | 1324 |
| III. | Datenschutzbehörden | 1330 |
| IV. | Rechtsprechung | 1334 |
| V. | Entwicklung der Datenschutzpraxis | 1334 |
| VI. | Ausblick | 1335 |

Inhaltsverzeichnis

| | |
|---|-----------|
| Vorwort | V |
| Autorenverzeichnis | VII |
| Inhaltsübersicht | XI |
| Abkürzungsverzeichnis..... | XLVII |
| Literaturverzeichnis..... | LIII |
| Kapitel 1: Grundlagen des Umgangs mit der DSGVO (Moos/Schefzig) . | 1 |
| I. Die Anwendung der DSGVO und der nationalen Begleitgesetze | 1 |
| 1. Stand der Umsetzung in den Unternehmen | 2 |
| 2. Zeitliche Geltung | 2 |
| 3. Unmittelbare Geltung | 3 |
| 4. Zusammenspiel mit anderen Regelwerken..... | 3 |
| a) Begleitgesetze auf Basis von Öffnungsklauseln..... | 3 |
| b) Spezialgesetzliche Datenschutzregelungen in Richtlinien und Gesetzen..... | 4 |
| c) Datenschutzregelungen außerhalb des Anwendungsbereichs der DSGVO..... | 5 |
| d) Zwischenergebnis..... | 5 |
| II. Parallelität von DSGVO und „Altgesetzen“ | 6 |
| III. Auslegung der DSGVO und der Begleitgesetze..... | 7 |
| 1. Auslegung der DSGVO..... | 8 |
| a) Autonome Auslegung des Unionsrechts | 8 |
| b) Auslegungsmethoden..... | 8 |
| c) Relevanz existierender Rechtsprechung | 14 |
| 2. Auslegung der Begleitgesetze | 15 |
| a) Auslegungsmethoden..... | 15 |
| b) Relevanz existierender Rechtsprechung | 16 |
| Kapitel 2: Grundlagen des Datenschutzrechts (Moos) | 17 |
| I. Datenschutz im Anwendungsbereich des EU-Rechts | 17 |
| II. Schutzgut des Datenschutzrechts | 18 |
| 1. Schutz der natürlichen Personen | 18 |
| 2. Schutz des freien Datenverkehrs | 19 |

| | |
|--|-----------|
| III. Grundbegriffe des Datenschutzrechts | 20 |
| 1. Personenbezug | 20 |
| 2. Datenverarbeitung | 21 |
| 3. Verantwortlicher | 22 |
| IV. Zusammenspiel mit anderen Rechtsmaterien | 23 |
| 1. Wettbewerbsrecht | 23 |
| 2. Kartellrecht | 24 |
| a) Missbräuchliche Nutzung von Kundendaten | 24 |
| b) Missbräuchliche Zugangsverweigerung zu Daten | 25 |
| c) AGB-Recht | 26 |
| 3. Besonderer Geheimnisschutz | 27 |
| a) Berufsrechtliche Schweigepflichten | 27 |
| b) Strafrechtliche Schweigepflichten | 28 |
| c) Fernmeldegeheimnis | 28 |
| d) Schutz von Geschäftsgeheimnissen | 29 |
| 4. Arbeits- und Mitbestimmungsrecht | 30 |
| a) Umfang von Datenerhebungen im Bewerbungsgespräch | 30 |
| b) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisvorschrift | 31 |
| c) Einsicht in Personalakten | 31 |
| d) Kündigungsschutz für Datenschutzbeauftragte | 32 |
| Kapitel 3: Anwendungsbereich des Datenschutzrechts (Meyerdierks) .. | 33 |
| I. Überblick über die einschlägigen Regelungen der DSGVO | 33 |
| II. Sachlicher Anwendungsbereich | 35 |
| 1. Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO | 35 |
| 2. Ausnahmetatbestände, Art. 2 Abs. 2 bis 4 DSGVO | 37 |
| III. Räumlicher Anwendungsbereich, Art. 3 DSGVO | 43 |
| 1. Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO | 43 |
| a) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Verantwortlichen | 44 |
| b) Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Auftragsverarbeiters | 45 |
| 2. Marktortprinzip, Art. 3 Abs. 2 DSGVO | 46 |
| a) Anbieten von Waren oder Dienstleistungen, Art. 3 Abs. 2 lit. a DSGVO | 47 |
| b) Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO | 51 |
| c) Betroffene Person in der EU | 53 |

| | |
|--|-----------|
| 3. Räumlicher Anwendungsbereich bei mehreren Beteiligten..... | 54 |
| 4. Räumliche Reichweite der Betroffenenrechte | 56 |
| 5. Geltung der DSGVO im EWR | 56 |
| IV. Anwendungsbereich mitgliedstaatlicher Regelungen..... | 56 |
| V. Anwendungsbereich sonstiger ausfüllender Normen | 60 |
| Kapitel 4: Datenschutzrechtliche Grundsätze (Moos)..... | 61 |
| I. Bedeutung und Funktion der Datenschutzgrundsätze..... | 61 |
| II. Die Grundsätze im Einzelnen | 62 |
| 1. Rechtmäßigkeit und Verarbeitung nach Treu und Glauben | 62 |
| 2. Transparenz | 64 |
| 3. Zweckbindung | 64 |
| 4. Datenminimierung..... | 66 |
| 5. Datenrichtigkeit | 66 |
| 6. Speicherbegrenzung | 68 |
| 7. Integrität und Vertraulichkeit | 69 |
| III. Die Rechenschaftspflicht | 70 |
| Kapitel 5: Zulässigkeit der Verarbeitung personenbezogener Daten <i>(Arning/Rohwedder)</i> | 73 |
| I. Überblick über die einschlägigen Regelungen der DSGVO..... | 74 |
| II. Gesetzliche Erlaubnisvorschriften..... | 76 |
| 1. Verarbeitung personenbezogener Daten zu Zwecken der Vertrags- erfüllung oder zur Durchführung vorvertraglicher Maßnahmen... .. | 77 |
| a) Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung | 78 |
| b) Verarbeitung personenbezogener Daten zu Zwecken der Durchführung vorvertraglicher Maßnahmen | 84 |
| c) Erforderlichkeit der Datenverarbeitung für die genannten Zwecke..... | 85 |
| 2. Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung..... | 98 |
| 3. Verarbeitung personenbezogener Daten auf Basis einer Interessenabwägung | 101 |
| a) Berechtigte Interessen des Verantwortlichen oder eines Dritten | 102 |
| b) Erforderlichkeit einer Datenverarbeitung zur Wahrung der berechtigten Interessen | 104 |

| | |
|--|-----|
| c) Keine überwiegenden Interessen/Rechte der betroffenen Person am Ausschluss der Datenverarbeitung | 105 |
| 4. Verarbeitung personenbezogener Daten zu Zwecken der Werbung | 111 |
| 5. Verhältnis der Alternativen des Art. 6 Abs. 1 DSGVO zueinander. | 116 |
| 6. Verhältnis zwischen besonders praxisrelevanten nationalen Vorschriften und der DSGVO | 118 |
| a) Videoüberwachung öffentlich zugänglicher Räume gem. § 4 BDSG | 119 |
| b) Scoring und Bonitätsauskünfte gem. § 31 BDSG | 122 |
| c) Verhältnis zwischen dem Kunsturhebergesetz und der DSGVO | 125 |
| 7. Zweckänderung – Verarbeitung personenbezogener Daten zu einem anderen Zweck | 129 |
| a) Zweckänderung auf Basis einer Rechtsvorschrift | 129 |
| b) Zweckänderung auf Basis einer Einwilligung | 133 |
| c) Zweckänderung auf Basis des Kompatibilitätstests gem. Art. 6 Abs. 4 DSGVO | 133 |
| d) Weitere datenschutzrechtliche Pflichten im Fall der Zweckänderung | 135 |
| 8. Verarbeitung besonderer Kategorien personenbezogener Daten .. | 136 |
| a) Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) | 136 |
| b) Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten | 142 |
| c) Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 DSGVO) | 144 |
| 9. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten – Art. 10 DSGVO | 160 |
| 10. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist – Art. 11 DSGVO | 163 |
| a) Keine Pflicht zur Verarbeitung von identifizierenden Merkmalen | 163 |
| b) Pflichten und Privilegierung des Verantwortlichen gem. Art. 11 Abs. 2 DSGVO | 165 |
| 11. Besondere Verarbeitungssituationen | 172 |
| 12. Zulässigkeit der Verarbeitung personenbezogener Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 173 |
| 13. Sanktionierung | 173 |
| III. Einwilligung der Betroffenen | 173 |
| 1. Überblick über die einschlägigen Regelungen | 174 |

| | |
|---|-----|
| 2. Allgemeine Voraussetzungen der Einwilligung | 176 |
| a) Form der Willensbekundung | 176 |
| b) Freiwilligkeit | 182 |
| c) Erteilung für den bestimmten Fall | 189 |
| d) Transparenzgebot | 189 |
| e) Einwilligungen als Gegenstand von AGB | 192 |
| f) Widerruflichkeit | 195 |
| g) Nachweisbarkeit | 197 |
| h) Gültigkeitsdauer | 200 |
| 3. Einwilligung von Kindern | 201 |
| a) Voraussetzungen bei direkten Angeboten von Fernabsatzdiensten | 201 |
| b) Vergewisserungspflicht des Verantwortlichen | 203 |
| 4. Einwilligung bei sensiblen Datenkategorien | 204 |
| 5. Wirksamkeit von Alt-Einwilligungen | 205 |
| Kapitel 6: Umgang mit Betroffenen (Arning) | 207 |
| I. Einführung | 211 |
| II. Systematischer Überblick über die Betroffenenrechte gem. Art. 12–23 DSGVO und Art. 77 ff. DSGVO | 212 |
| III. Informationspflichten (Art. 13 und 14 DSGVO) | 214 |
| 1. Informationspflichten bei der Direkterhebung von Daten von der betroffenen Person (Art. 13 DSGVO) | 216 |
| a) Voraussetzungen der Informationspflicht nach Art. 13 DSGVO | 216 |
| b) Systematik von Art. 13 DSGVO | 216 |
| c) Inhalte der Informationspflichten nach Art. 13 Abs. 1 DSGVO | 218 |
| d) Inhalte der Informationspflichten nach Art. 13 Abs. 2 DSGVO | 224 |
| e) Zeitpunkt der Information | 234 |
| f) Information im Fall der Zweckänderung (Art. 13 Abs. 3 DSGVO) | 235 |
| g) Information im Fall der Änderung der Datenverarbeitung | 238 |
| h) Ausnahmen von der Informationspflicht (Art. 13 Abs. 4 DSGVO) | 241 |
| i) Keine Pflicht zur „Nachinformation“ im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 244 |
| j) Erfüllung der Informationspflichten als Zulässigkeits- voraussetzung? | 244 |
| 2. Informationspflichten bei der Erhebung von Daten aus anderen Quellen als von der betroffenen Person (Art. 14) | 246 |
| a) Voraussetzungen der Informationspflicht nach Art. 14 DSGVO | 246 |

| | |
|--|-----|
| b) Inhalte der Informationspflichten nach Art. 14 Abs. 1 DSGVO | 246 |
| c) Inhalte der Informationspflichten nach Art. 14 Abs. 2 DSGVO | 247 |
| d) Weitere Informationen, die nicht in Art. 14 Abs. 1 und Abs. 2 DSGVO genannt werden | 248 |
| e) Zeitpunkt der Informationserteilung nach Art. 14 Abs. 3 DSGVO | 249 |
| f) Information im Fall der Zweckänderung (Art. 14 Abs. 4 DSGVO) und im Fall der Änderung der Datenverarbeitung | 250 |
| g) Ausnahmen von der Informationspflicht nach Art. 14 DSGVO | 250 |
| h) „Nachinformation“ und keine Zulässigkeitsvoraussetzung | 259 |
| 3. Modalitäten der Information der betroffenen Personen (Art. 12 DSGVO) | 259 |
| a) Formulierung der Information | 259 |
| b) Information in leicht zugänglicher Form | 262 |
| c) Form | 262 |
| d) Unentgeltlichkeit | 267 |
| e) Kombination mit standardisierten Bildsymbolen | 268 |
| 4. Rechenschaftspflicht | 269 |
| 5. Beispiele für Möglichkeiten zur Darstellung der Informationen | 269 |
| a) Gestaltung als Checkliste | 270 |
| b) Gruppierung von Informationen | 271 |
| c) Gestaltung als „Story“/nach dem geschichtlichen Ablauf der Datenverarbeitung | 271 |
| d) Gestaltung unter Einsatz von Tabellen | 272 |
| e) Multilayered notice/Mehrebenenansatz | 274 |
| IV. Recht auf Auskunft (Art. 15 DSGVO) | 277 |
| 1. Auskunftsrecht nach Art. 15 Abs. 1 und 2 DSGVO | 279 |
| a) Voraussetzungen des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO | 279 |
| b) Inhalte des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO | 279 |
| c) Umfang des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO | 287 |
| 2. Ausnahmen vom Auskunftsrecht | 289 |
| a) Ausnahmen vom Auskunftsrecht gem. Art. 15 Abs. 1 und Abs. 2 DSGVO in der DSGVO | 293 |
| b) Ausnahmen vom Auskunftsrecht gem. Art. 15 Abs. 1 und Abs. 2 DSGVO im nationalen Recht | 303 |
| 3. Modalitäten der Auskunftserteilung (Art. 12 DSGVO) | 309 |
| a) Antragserfordernis | 309 |
| b) Erleichterung der Rechtsausübung (Art. 12 Abs. 2 S. 1 DSGVO) | 311 |

| | |
|--|-----|
| c) Identifizierung des Antragstellers (Art. 12 Abs. 6 DSGVO) ... | 312 |
| d) Formulierung der Auskunft (Art. 12 Abs. 1 DSGVO)..... | 319 |
| e) Form der Auskunft | 320 |
| f) Unentgeltlichkeit (Art. 12 Abs. 5 S. 2 lit. a DSGVO)..... | 321 |
| g) Frist zur Erteilung der Auskunft sowie von Informationen über das Auskunftsverlangen und ggf. über dessen Ablehnung (Art. 12 Abs. 3 und Abs. 4 DSGVO) | 323 |
| h) Zweckbindung von Daten im Zusammenhang mit der Auskunftserteilung..... | 330 |
| 4. Recht der betroffenen Person, eine Kopie ihrer Daten zu erhalten (Art. 15 Abs. 3 und 4 DSGVO)..... | 330 |
| a) Inhalte und Umfang der Kopie nach Art. 15 Abs. 3 DSGVO ... | 330 |
| b) Ausnahmen vom Recht auf Erhalt einer Kopie in der DSGVO.. | 341 |
| c) Modalitäten im Hinblick auf die Aushändigung der Kopie gem. Art. 15 Abs. 3 DSGVO | 349 |
| d) Praktischer Umgang mit Anträgen auf Erhalt einer Kopie | 353 |
| 5. Auskunft im Hinblick auf Daten bzw. Erhalt von Kopien von Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden .. | 358 |
| V. Recht auf Berichtigung (Art. 16 DSGVO) | 358 |
| 1. Inhalte des Berichtigungsrechts nach Art. 16 DSGVO..... | 358 |
| a) Berichtigung unrichtiger personenbezogener Daten (S. 1)..... | 359 |
| b) Vervollständigung unvollständiger personenbezogener Daten (S. 2)..... | 359 |
| c) Darlegungs- und Beweislast | 360 |
| 2. Ausnahmen vom Berichtigungsrecht | 364 |
| 3. Modalitäten des Berichtigungs- bzw. Vervollständigungs- anspruchs (Art. 12 DSGVO)..... | 365 |
| 4. Mitteilungspflicht nach Art. 19 DSGVO | 367 |
| 5. Berichtigung/Vervollständigung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 367 |
| VI. Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO).. | 367 |
| 1. Voraussetzungen des Rechts der betroffenen Person auf Löschung sowie der Löschpflicht des Verantwortlichen (Art. 17 Abs. 1 DSGVO)..... | 368 |
| a) Recht der betroffenen Person auf Löschung ihrer Daten..... | 368 |
| b) Pflicht des Verantwortlichen zur Datenlöschung | 369 |
| c) Löschungsgründe: Tatbestandsalternativen des Art. 17 Abs. 1 DSGVO | 376 |
| 2. Rechtsfolge: Löschen i. S. d. Art. 17 Abs. 1 DSGVO | 383 |

| | |
|---|-----|
| 3. Informationspflichten im Fall der Öffentlichmachung der Daten (Art. 17 Abs. 2 DSGVO) | 389 |
| a) Voraussetzungen des Rechts auf Vergessenwerden | 390 |
| b) Vom Verantwortlichen zur Erfüllung des Rechts auf Vergessenwerden zu ergreifende Maßnahmen | 391 |
| 4. Ausnahmen vom Recht auf Löschung gem. Art. 17 Abs. 1 DSGVO und von den Informationspflichten gem. Art. 17 Abs. 2 DSGVO (Art. 17 Abs. 3, Art. 12 DSGVO) | 393 |
| a) Ausnahmen nach Art. 17 Abs. 3 DSGVO | 393 |
| b) Weitere Ausnahmen in der DSGVO | 396 |
| c) Ausnahmen im nationalen Recht | 397 |
| 5. Modalitäten des Lösungsanspruchs (Art. 12 DSGVO) | 402 |
| a) Frist bei Löschung aufgrund der in Art. 17 Abs. 1 DSGVO enthaltenen Löschungsfrist | 403 |
| b) Frist bei Löschung gem. Art. 17 Abs. 1 DSGVO infolge eines Antrags der betroffenen Person | 406 |
| c) Frist für die Information nach Art. 17 Abs. 2 DSGVO | 408 |
| 6. Mitteilungspflicht nach Art. 19 DSGVO/Verhältnis zu Art. 17 Abs. 2 DSGVO | 409 |
| 7. Recht auf Löschung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 410 |
| VII. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO) .. | 410 |
| 1. Inhalte des Rechts auf Einschränkung der Datenverarbeitung | 411 |
| a) Voraussetzungen (Art. 18 Abs. 1 DSGVO) | 411 |
| b) Rechtsfolge: Einschränkung der Datenverarbeitung | 416 |
| c) Bedingungen für die Weiterverarbeitung der Daten (Art. 18 Abs. 2 DSGVO, Erwägungsgrund 67 DSGVO) | 416 |
| d) Informationspflichten für den Fall, dass die Daten wieder uneingeschränkt verarbeitet werden (Art. 18 Abs. 3 DSGVO) .. | 417 |
| 2. Ausnahmen vom Recht auf Einschränkung der Datenverarbeitung | 418 |
| 3. Modalitäten des Rechts auf Einschränkung der Datenverarbeitung (Art. 12 DSGVO) | 419 |
| 4. Mitteilungspflicht nach Art. 19 DSGVO | 420 |
| 5. Recht auf Einschränkung der Datenverarbeitung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden .. | 420 |
| VIII. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO) | 420 |
| 1. Voraussetzungen der Mitteilungspflicht | 421 |

| | |
|---|-----|
| 2. Mitteilung der Berichtigung, Löschung oder Einschränkung der Verarbeitung | 424 |
| 3. Unterrichtungspflicht gegenüber der betroffenen Person (Art. 19 S. 2 DSGVO) | 425 |
| 4. Weitere Ausnahmen von der Mitteilungspflicht | 427 |
| 5. Modalitäten der Mitteilungspflicht (Art. 12 DSGVO) | 428 |
| 6. Mitteilungspflicht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 429 |
| IX. Recht auf Datenübertragbarkeit (Art. 20 DSGVO) | 429 |
| 1. Inhalte des Rechts auf Datenübertragbarkeit | 431 |
| a) Voraussetzungen des Rechts auf Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO) | 431 |
| b) Rechtsfolgen: Bereitstellung (Abs. 1) bzw. Übermittlung (Abs. 2) von Daten durch den Verantwortlichen | 434 |
| c) Verhältnis zu Art. 17 DSGVO (Art. 20 Abs. 3 S. 1 DSGVO) ... | 438 |
| 2. Ausnahmen vom Recht auf Datenübertragbarkeit (Art. 20 Abs. 4, Art. 12 DSGVO) | 439 |
| a) Beeinträchtigung von Rechten und Freiheiten anderer Personen (Art. 20 Abs. 4 DSGVO) | 439 |
| b) Weitere Ausnahmen | 445 |
| 3. Modalitäten des Rechts auf Datenübertragbarkeit | 445 |
| 4. Recht auf Datenübertragbarkeit im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 447 |
| X. Widerspruchsrecht (Art. 21 DSGVO) | 447 |
| 1. Inhalte des Widerspruchsrechts | 448 |
| a) Allgemeines Widerspruchsrecht gem. Art. 21 Abs. 1 DSGVO .. | 448 |
| b) Widerspruchsrecht bei der Datenverarbeitung zu Zwecken der Direktwerbung gem. Art. 21 Abs. 2 und 3 DSGVO | 453 |
| c) Informationspflichten nach Art. 21 Abs. 4 DSGVO | 456 |
| 2. Weitere Ausnahmen vom Widerspruchsrecht | 459 |
| 3. Modalitäten des Widerspruchsrechts | 460 |
| 4. Widerspruchsrecht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 462 |
| XI. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO) | 462 |
| 1. Inhalte des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden | 464 |
| a) Voraussetzungen des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden | 464 |

| | |
|--|------------|
| b) Rechtsfolgen aus Art. 22 Abs. 1 DSGVO | 475 |
| c) Ausnahmen vom Recht, keinen automatisierten Einzelfall- entscheidungen unterworfen zu werden (Art. 22 Abs. 2 und 3 DSGVO) | 475 |
| d) Sonderfall: Verarbeitung besonderer Kategorien personen- bezogener Daten | 485 |
| 2. Modalitäten des Rechts, keinen automatisierten Einzelfall- entscheidungen unterworfen zu werden | 486 |
| 3. Das Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden, im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden | 486 |
| XII. Sanktionierung | 487 |
| Kapitel 7: Auftragsverarbeitung (Moos/Cornelius) | 489 |
| I. Begriff und Gegenstand der Auftragsverarbeitung | 490 |
| II. Abgrenzung zum Verantwortlichen und zur gemeinsamen Verantwortlichkeit | 493 |
| 1. Abgrenzung zum Verantwortlichen | 493 |
| a) Entscheidungsbefugnis über Zwecke | 494 |
| b) Entscheidungsbefugnis über Mittel | 495 |
| 2. Abgrenzung zur gemeinsamen Verantwortlichkeit | 497 |
| III. Rechtsnatur der Auftragsverarbeitung | 498 |
| IV. Typische Fallkonstellationen einer Auftragsverarbeitung | 500 |
| V. Rechte und Pflichten aus einer Auftragsverarbeitung | 502 |
| 1. Pflichten des Auftragsverarbeiters | 502 |
| 2. Rechte und Pflichten des Verantwortlichen | 504 |
| a) Erteilung von Weisungen | 505 |
| b) Dokumentation der Weisungen | 506 |
| VI. Begründung einer Auftragsverarbeitung | 506 |
| 1. Auswahl des Auftragsverarbeiters | 506 |
| 2. Abschluss eines Auftragsverarbeitungsvertrages | 508 |
| a) Form des Auftragsverarbeitungsvertrages | 509 |
| b) Inhalt des Auftragsverarbeitungsvertrages | 510 |
| c) Umstellung von alten Auftragsverarbeitungsverträgen auf die DSGVO | 514 |
| VII. Auftragsverarbeitung innerhalb von Unternehmensgruppen | 517 |

| | |
|--|-----|
| VIII. Unterbeauftragungen | 518 |
| 1. Zustimmungspflicht des Verantwortlichen. | 518 |
| a) Art der Erteilung | 519 |
| b) Einspruchsrecht bei Allgemeinzustimmung | 520 |
| 2. Begründung des Unterauftragsverhältnisses | 521 |
| IX. Haftung von Auftragsverarbeitern | 522 |
| 1. Haftung auf Schadensersatz | 522 |
| a) Haftung für eigenes Verschulden | 523 |
| b) Haftung von Unterauftragsverarbeitern | 523 |
| c) Beweislastumkehr. | 523 |
| d) Gesamtschuldnerische Haftung | 524 |
| 2. Sanktionen gegen Auftragsverarbeiter | 524 |
| X. Kontrolle von Auftragsverarbeitern | 526 |
| 1. Recht zur Kontrolle | 526 |
| 2. Pflicht zur Kontrolle | 527 |
| 3. Art und Häufigkeit der Kontrolle. | 527 |
| a) Art der Kontrolle. | 528 |
| b) Häufigkeit der Kontrolle | 529 |
| XI. Dokumentation der Kontrollen. | 529 |
| XII. Kontrollergebnis. | 529 |

**Kapitel 8: Verarbeitungen in gemeinsamer, getrennter und alleiniger
Verantwortlichkeit (Moos)**

| | |
|---|-----|
| | 531 |
| I. Überblick über die einschlägigen Regelungen der DSGVO. | 532 |
| II. Gemeinsam für die Verarbeitung Verantwortliche. | 532 |
| 1. Der Begriff der gemeinsamen Verantwortlichkeit (Art. 4 Nr. 7 DSGVO) | 533 |
| a) Gemeinsame Entscheidung mehrerer Stellen | 535 |
| b) Entscheidung über Zwecke und Mittel der Verarbeitung | 536 |
| c) Entscheidungshilfen für die Unternehmenspraxis | 538 |
| d) Abgrenzung von der Auftragsverarbeitung. | 541 |
| 2. Reichweite der gemeinsamen Verantwortlichkeit | 541 |
| 3. Zulässigkeit der Verarbeitungen durch gemeinsam Verantwortliche | 542 |
| 4. Rechte und Pflichten der gemeinsam Verantwortlichen | 543 |
| a) Abschluss einer Vereinbarung über die gemeinsame Verantwortlichkeit | 544 |
| b) Geltendmachung der Rechte der Betroffenen. | 548 |

| | |
|--|------------|
| c) Zurverfügungstellung der wesentlichen Teile der Vereinbarung | 549 |
| d) Mitteilung der erforderlichen Informationen nach Art. 13 und Art. 14 DSGVO | 550 |
| 5. Haftung und Sanktionen | 551 |
| III. Getrennte Verantwortlichkeiten | 552 |
| 1. Begriff der Übermittlung | 553 |
| 2. Zulässigkeit von Datenübermittlungen an Dritte | 554 |
| 3. Typische Fallkonstellationen getrennter Verantwortlichkeiten | 554 |
| 4. Besondere Aspekte von Datenübermittlungen im Konzern | 554 |
| a) Fehlendes Konzernprivileg | 555 |
| b) Erlaubnis durch Interessenabwägung | 555 |
| c) Öffnungsklausel für nationale Sonderregelungen | 557 |
| d) Internationale Datenübermittlungen | 557 |
| IV. Niederlassungsübergreifende Verarbeitungen | 557 |
| 1. Die Bestimmung einer Hauptniederlassung für eine niederlassungsübergreifende Verantwortlichkeit | 558 |
| 2. Die Spezifizierung der Verarbeitungsverfahren | 561 |
| Kapitel 9: Internationale Datenübermittlungen (Moos/Zeiter) | 563 |
| I. Überblick über die einschlägigen Regelungen der DSGVO | 565 |
| II. Einführung in den Regelungsbereich | 565 |
| 1. Sonderregelungen für „Drittlands-Übermittlungen“ | 565 |
| a) Begriff des Drittlands | 565 |
| b) Geltung auch für internationale Organisationen | 569 |
| c) Begriff der „Übermittlung“ | 570 |
| d) Geltung auch für Weiterübermittlungen | 571 |
| 2. Anforderungen an Drittlands-Übermittlungen | 571 |
| a) Einhaltung der allgemeinen DSGVO-Anforderungen | 572 |
| b) Gewährleistung eines angemessenen Schutzniveaus | 572 |
| c) Verantwortlicher und Auftragsverarbeiter als Regelungsadressat | 574 |
| 3. Fortgeltung etablierter Sicherungsinstrumente | 574 |
| III. Länder mit angemessenem Schutzniveau | 575 |
| 1. Bestehende Angemessenheitsbeschlüsse | 576 |
| a) Einschränkungen bei Datentransfers nach Kanada | 577 |
| b) Einschränkungen bei Datentransfers nach Israel | 578 |
| c) Der Sonderfall USA: Ungültigkeit des EU-US Privacy Shield .. | 578 |

| | |
|--|-----|
| 2. Neue Angemessenheitsentscheidungen unter der DSGVO | 579 |
| a) Anforderungen an Angemessenheitsfeststellungen der Kommission | 581 |
| b) Das Verfahren der Angemessenheitsfeststellung | 581 |
| 3. Fortlaufende Überwachung der Angemessenheit | 581 |
| IV. Geeignete Garantien für Drittlandtransfers | 582 |
| 1. Standarddatenschutzklauseln | 584 |
| a) Existierende Standardvertragsklauseln nach Maßgabe der RL 95/46/EG | 584 |
| b) Neue Standarddatenschutzklauseln nach DSGVO | 587 |
| c) Standarddatenschutzklauseln einer Aufsichtsbehörde | 587 |
| d) Verwendung der Standarddatenschutzklauseln | 587 |
| 2. Verbindliche interne Datenschutzvorschriften (BCRs) | 596 |
| a) Anforderungen an BCRs | 598 |
| b) Arbeitsdokumente der Artikel-29-Datenschutzgruppe | 600 |
| c) Existierende BCR | 604 |
| d) Genehmigungsverfahren für BCR | 605 |
| e) Integration von BCR in ein Datenschutz-Managementsystem nach DSGVO | 609 |
| 3. Genehmigte Verhaltensregeln | 612 |
| 4. Zertifizierungen | 613 |
| 5. Sonstige behördlich genehmigte Vertragsklauseln | 613 |
| V. Ausnahmen für bestimmte Fälle | 614 |
| 1. Einwilligung der Betroffenen | 615 |
| a) Ausdrückliche Erteilung der Einwilligung | 615 |
| b) Notwendigkeit gesonderter Erteilung | 616 |
| c) Informiertheit der Einwilligung | 616 |
| 2. Erforderlichkeit für die Vertragserfüllung | 618 |
| 3. Sonstige Ausnahmefälle | 618 |
| a) Im Interesse der betroffenen Person geschlossener Vertrag | 618 |
| b) Wichtige Gründe des öffentlichen Interesses | 619 |
| c) Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen | 620 |
| d) Schutz lebenswichtiger Interessen | 622 |
| e) Übermittlungen aus einem Register | 622 |
| 4. Auffangregelung für Einzelübermittlungen | 623 |
| a) Keine wiederholte Übermittlung | 624 |
| b) Begrenzte Zahl betroffener Personen | 624 |
| c) Zwingende berechnete Interessen | 624 |
| d) Keine überwiegenden Interessen der betroffenen Person | 625 |

| | |
|---|------------|
| e) Umfassende Beurteilung und angemessene Garantien | 625 |
| f) Information der Aufsichtsbehörde | 625 |
| Kapitel 10: Datenschutzmanagement (Schefzig)..... | 627 |
| I. Überblick über die einschlägigen Regelungen der DSGVO..... | 627 |
| II. Terminologie | 628 |
| III. Anforderungen an das Datenschutzmanagement | 629 |
| IV. Risikoadäquates Datenschutzmanagement | 630 |
| 1. Risikobewertung grundlegend..... | 630 |
| 2. Risikoprofil eines Unternehmens | 631 |
| 3. Konkrete Maßnahmen hängen vom Einzelfall ab | 632 |
| V. Konkrete Maßnahmen hängen vom Einzelfall ab | 633 |
| VI. Grundlegende Maßnahmen des Datenschutzmanagements | 634 |
| 1. Einführung | 634 |
| 2. Unternehmensrichtlinie zum Datenschutz..... | 634 |
| 3. Datenschutzorganisation | 637 |
| 4. Datenschutzstrategie..... | 637 |
| 5. Meldewege und Whistleblowing | 637 |
| 6. Auditierungen | 638 |
| 7. Einzelfallprüfungen und -beratung..... | 638 |
| 8. Schulungen..... | 638 |
| 9. Sonstige Maßnahmen | 639 |
| VII. Datenschutzmanagementsystem | 640 |
| 1. Sinn eines Datenschutzmanagementsystems..... | 640 |
| 2. Gestaltung eines Datenschutzmanagementsystems | 640 |
| a) Orientierung an ähnlichen Systemen bzw. Standards | 640 |
| b) Drei Säulen | 641 |
| c) Schematische Darstellung eines Datenschutzmanagement- systems | 642 |
| 3. Aufbau eines Datenschutzmanagementsystems | 643 |
| 4. Messung des Erfolgs eines Datenschutzmanagementsystems | 643 |
| Kapitel 11: Datenschutzorganisation (Schefzig) | 647 |
| I. Überblick über die einschlägigen Regelungen der DSGVO..... | 647 |
| II. Ergänzende Regelungen des BDSG | 648 |

| | |
|--|------------|
| III. Terminologie..... | 648 |
| IV. Datenschutzorganisation als Voraussetzung von Datenschutzcompliance | 648 |
| V. Pflicht zur Errichtung einer Datenschutzorganisation..... | 649 |
| 1. Datenschutz-Grundverordnung | 649 |
| a) Gesetzliche Vorgaben..... | 649 |
| b) Konkrete Wertung..... | 650 |
| 2. Gesellschaftsrechtliche Verpflichtung in Deutschland..... | 652 |
| 3. Ordnungswidrigkeitenrecht | 653 |
| 4. Fazit | 654 |
| VI. Gestaltung einer Datenschutzorganisation | 655 |
| 1. Der Zweck einer Datenschutzorganisation..... | 655 |
| 2. Aufgaben einer Datenschutzorganisation..... | 655 |
| a) Vier grundlegende Aufgaben | 655 |
| b) Beachtung und Anwendung des Datenschutzrechts im operativen Geschäft | 655 |
| c) Beratung..... | 656 |
| d) Richtlinienkompetenz | 656 |
| e) Auditierung und Überwachung..... | 656 |
| 3. Elemente einer Datenschutzorganisation | 656 |
| a) Einführung | 656 |
| b) Die Geschäftsleitung | 657 |
| c) Der Datenschutzbeauftragte | 657 |
| d) Datenschutzberater..... | 694 |
| e) Datenschutzmanager | 694 |
| f) Datenschutzexperten | 695 |
| g) Datenschutzkoordinatoren | 696 |
| h) Sonstige Mitarbeiter des Unternehmens | 696 |
| i) (Inländischer) Vertreter | 696 |
| 4. Entwicklung einer Datenschutzorganisation | 697 |
| VII. Beispiele | 698 |
| 1. Verwendung der Beispiele | 698 |
| 2. Datenschutzorganisation in kleinen Unternehmen | 698 |
| 3. Datenschutzorganisation in mittleren Unternehmen..... | 699 |
| 4. Datenschutzorganisation im Großkonzern..... | 700 |
| Kapitel 12: Datenschutzprozesse (Gardyan-Eisenlohr/Cornelius) | 703 |
| I. Prozessuale Umsetzung datenschutzrechtlicher Vorgaben | 705 |

| | |
|---|-----|
| II. Privacy by Design und by Default, Art. 25 DSGVO | 707 |
| 1. Überblick über die einschlägigen Regelungen der DSGVO | 708 |
| 2. Wer ist für Privacy by Design und by Default verantwortlich? | 708 |
| 3. Was bedeutet Privacy by Design und by Default? | 710 |
| a) Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DSGVO. | 711 |
| b) Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DSGVO | 715 |
| c) Genehmigte Zertifizierungsverfahren, Art. 25 Abs. 3 DSGVO. | 718 |
| III. Datenlöschung | 718 |
| 1. Allgemeines | 718 |
| 2. Geschäftliche Relevanz | 721 |
| 3. Löschkonzept | 722 |
| 4. Praktische Hinweise für die Implementierung | 726 |
| IV. Verzeichnis von Verarbeitungstätigkeiten | 727 |
| 1. Überblick über die einschlägigen Regelungen der DSGVO | 728 |
| 2. Aufzeichnungspflichten statt Meldepflicht und Verfahrensverzeichnis | 729 |
| 3. Verarbeitungsverzeichnis des Verantwortlichen | 729 |
| a) Wer ist zur Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO verpflichtet? | 729 |
| b) Inhalt des Verarbeitungsverzeichnisses | 731 |
| c) Form des Verarbeitungsverzeichnisses | 735 |
| 4. Verarbeitungsverzeichnis des Auftragsverarbeiters | 737 |
| 5. Praktische Hinweise zur Implementierung | 738 |
| V. Datenschutz-Folgenabschätzung | 739 |
| 1. Überblick über die einschlägigen Regelungen der DSGVO | 741 |
| 2. Wer ist für eine Datenschutz-Folgenabschätzung verantwortlich? .. | 741 |
| 3. Wann muss eine Datenschutz-Folgenabschätzung erfolgen? | 742 |
| a) Voraussichtlich hohes Risiko (Art. 35 Abs. 1 S. 1 DSGVO) | 744 |
| b) Regelbeispiele (Art. 35 Abs. 3 DSGVO) | 747 |
| c) Positivliste der Aufsichtsbehörden (Art. 35 Abs. 4 DSGVO) .. | 748 |
| d) Mögliche Befreiung von der Folgenabschätzung aufgrund bestimmter Verarbeitungszwecke (Art. 35 Abs. 10 DSGVO) .. | 749 |
| 4. Was muss im Rahmen der Folgenabschätzung passieren? | 750 |
| a) Welche hohen Risiken sind zu adressieren (Art. 35 Abs. 1 DSGVO)? | 750 |
| b) Welche technischen und organisatorischen Maßnahmen sind geeignet, um das Risiko zu minimieren? | 750 |

| | |
|---|-----|
| c) Welche Dokumentation der Folgenabschätzung ist erforderlich (Art. 35 Abs. 7 DSGVO)? | 751 |
| d) Bedarf es der Beratung durch den Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO)? | 752 |
| e) Müssen betroffene Personen oder Vertreter (Art. 35 Abs. 9 DSGVO) eingebunden werden? | 753 |
| f) Wann bedarf es der erneuten Überprüfung? | 754 |
| g) Welche Rolle spielt die Aufsichtsbehörde bei der Folgenabschätzung (Art. 36 Abs. 2 DSGVO)? | 754 |
| 5. Praktische Hinweise zur Implementierung..... | 755 |
| VI. Umgang mit Datenlecks | 758 |
| 1. Überblick über die einschlägigen Regelungen der DSGVO..... | 758 |
| 2. Meldepflichten (Art. 33 DSGVO)..... | 760 |
| a) Was muss gemeldet werden? (Art. 33 Abs. 1 DSGVO)..... | 760 |
| b) Bis wann muss gemeldet werden? (Art. 33 Abs. 1 S. 1 und 2 DSGVO) | 765 |
| c) Wie muss gemeldet werden? (Art. 33 Abs. 3 DSGVO) | 767 |
| d) Was tun bei Verzögerung? (Art. 33 Abs. 4 DSGVO) | 769 |
| e) Was muss in jedem Fall dokumentiert werden? (Art. 33 Abs. 5 DSGVO) | 770 |
| f) Welche Pflichten treffen den Auftragsverarbeiter? (Art. 33 Abs. 2 DSGVO) | 771 |
| 3. Benachrichtigungspflichten (Art. 34 DSGVO) | 772 |
| a) Wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) | 772 |
| b) Bis wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) | 774 |
| c) Was muss die Benachrichtigung beinhalten und wie muss sie erfolgen? (Art. 34 Abs. 2 DSGVO) | 775 |
| d) Wann kann auf eine Benachrichtigung verzichtet werden? (Art. 34 Abs. 3 DSGVO) | 776 |
| 4. Praktische Hinweise zur Implementierung..... | 778 |
| VII. Integration des Datenschutzes in allgemeine Unternehmensprozesse | 780 |
| 1. Aufgaben der Datenschutzorganisation – eine Chance für vielfältige Integration in die Unternehmensprozesse | 780 |
| a) Governance | 780 |
| b) Hinwirken auf den Datenschutz | 781 |
| c) Überwachung und Auditierung..... | 782 |

| | |
|--|-----|
| 2. Definition von Unternehmensprozessen, in denen Datenschutzprozesse integriert werden | 783 |
| a) Datenschutzprozesse | 783 |
| b) Risikobetrachtung | 785 |
| c) Typische Hüter der Anforderungen des Datenschutzes..... | 787 |
| 3. Praktische Hinweise zur Implementierung | 791 |
| Kapitel 13: Technischer Datenschutz und Risikomanagement <i>(Heinemann)</i> | 793 |
| I. Überblick über die einschlägigen Regelungen..... | 794 |
| 1. Art. 24, 32 DSGVO und Erwägungsgrund 83 | 795 |
| 2. Art. 24, 25 DSGVO und Erwägungsgrund 78 | 795 |
| 3. §§ 64, 65, 76 BDSG..... | 796 |
| II. Allgemeine Grundlagen des technischen Datenschutz- risikomanagements | 797 |
| 1. Auswahl eines Vorgehensmodells..... | 800 |
| 2. Anwendung etablierter Methoden und Verfahren..... | 803 |
| a) Anwendung PDCA und Eingliederung in Managementsysteme | 803 |
| b) Anwendung eines risikobasierten Verfahrens..... | 805 |
| III. Nutzung der Standards und Vorgehen der Informationssicherheit ... | 806 |
| 1. Grundlegende Begriffe und Standards der Informationssicherheit | 806 |
| a) Terminologie..... | 807 |
| b) Zentrale Standards der Informationssicherheit | 809 |
| 2. Risikobasiertes Verfahren zur Herstellung der Informationssicherheit | 812 |
| a) Schutzbedarfsfeststellung | 814 |
| b) Soll-Ist-Vergleich/Risiko-Assessment | 816 |
| c) Schutzmaßnahmen..... | 823 |
| d) Dokumentation und Nachweis | 824 |
| e) Kontrolle und Prüfung..... | 824 |
| f) Behandlung von Sicherheitsvorfällen | 825 |
| g) Zertifizierung | 825 |
| 3. Zusammenfassung und Fazit | 825 |
| IV. Technische Maßnahmen zur datenschutzkonformen Verarbeitung... .. | 826 |
| 1. Datenschutzziele | 827 |
| a) Schutzziele der Datensicherheit nach der DSGVO | 827 |
| b) Weitere Schutzziele des Datenschutzes..... | 831 |

| | |
|---|------------|
| 2. Risikobasiertes Verfahren für den Datenschutz | 833 |
| a) Schutzbedarfsfeststellung des Datenschutzes | 835 |
| b) Soll-Ist-Vergleich des Datenschutzes | 838 |
| c) Risiko-Assessment des Datenschutzes | 840 |
| d) Auswahl von Datenschutzmaßnahmen | 844 |
| 3. Dokumentation und Nachweis | 867 |
| 4. Kontrolle und Prüfung | 867 |
| 5. Behandlung von Datenschutzvorfällen | 868 |
| 6. Zertifizierung | 868 |
| 7. Zusammenfassung und Fazit | 869 |
| V. Privacy by Design und Privacy by Default | 871 |
| 1. Privacy Enhancing Technologies | 872 |
| 2. Privacy by Design/Privacy by Default als Ergänzung des IT-Sicherheits- und IT-Risikomanagements | 874 |
| VI. Ausblick | 876 |
| 1. Anpassung des risikobasierten Verfahrens mit Auditierung/ Zertifizierung | 876 |
| 2. Entwicklung von Verhaltensregeln | 876 |
| 3. Datenschutzzeignung von Software | 876 |
| 4. Datenschutzkonformes Design von Datenbeständen | 877 |
| Kapitel 14: Verhaltensregeln und Zertifizierungen (Rothkegel) | 879 |
| I. Einleitung | 879 |
| II. Grundsätzliche Unterscheidung und Komplementarität | 882 |
| III. Mehrwert für Unternehmen | 883 |
| 1. Einhaltung und Nachweis datenschutzkonformen Handelns | 884 |
| 2. Rechtskonkretisierungsfunktion | 885 |
| 3. Absicherung von Drittlandübermittlungen | 886 |
| 4. Berücksichtigung bei der Bemessung von Sanktionen | 888 |
| IV. Genehmigung von Verhaltensregeln | 889 |
| 1. Vorlageberechtigte Stellen | 889 |
| 2. Verhaltensregeln mit rein nationaler Wirkung | 890 |
| 3. Verhaltensregeln mit landesübergreifender Wirkung | 891 |
| 4. Allgemeingültigkeitserklärung | 893 |
| 5. Gültigkeitsdauer | 893 |

| | |
|---|------------|
| 6. Bindungswirkung genehmigter Verhaltensregeln..... | 894 |
| a) Bindungswirkung gegenüber Aufsichtsbehörden | 895 |
| b) Bindungswirkung gegenüber Gerichten | 896 |
| c) Bindungswirkung gegenüber Unternehmen | 897 |
| V. Überwachung genehmigter Verhaltensregeln/ Sanktionen im Falle von Verstößen..... | 898 |
| VI. Inhalte und Gestaltung von Verhaltensregeln | 900 |
| 1. Regelungsinhalte von Verhaltensregeln | 900 |
| 2. Gestaltungsprozess in der Praxis | 901 |
| a) Bedarfs- und Maßnahmenermittlung..... | 902 |
| b) Ausarbeitung unter Beteiligung betroffener Interessenträger .. | 902 |
| VII. Zertifizierungsverfahren | 903 |
| 1. Ablauf des Zertifizierungsverfahrens/ Beteiligte Stellen | 903 |
| 2. Regelungsinhalte und Prüfmaßstab | 904 |
| 3. Bindungswirkung | 905 |
| Kapitel 15: Beschäftigtendatenschutz (Baumgartner/Gausling) | 907 |
| I. Überblick über die einschlägigen Regelungen der DSGVO..... | 908 |
| II. Handlungsoptionen des Gesetzgebers..... | 909 |
| 1. Reichweite des Art. 88 Abs. 1 DSGVO | 909 |
| a) Spezifischere Vorschriften | 909 |
| b) Personenbezogene Beschäftigtendaten | 910 |
| c) Zwecke der Datenverarbeitung..... | 910 |
| 2. Mindestanforderungen gem. Art. 88 Abs. 2 DSGVO | 911 |
| a) Transparenz der Verarbeitung..... | 912 |
| b) Datenübermittlung innerhalb einer Unternehmensgruppe | 913 |
| c) Überwachungssysteme am Arbeitsplatz | 913 |
| 3. Mitteilung gem. Art. 88 Abs. 3 DSGVO | 913 |
| 4. Nationale Regelungen in Deutschland..... | 914 |
| a) Zentrale Vorschrift zum Beschäftigtendatenschutz..... | 914 |
| b) Verhältnis zu den Vorgaben des Art. 88 DSGVO | 917 |
| III. Datenschutzrechtliche Erlaubnistatbestände | 918 |
| 1. Einwilligung im Beschäftigungsverhältnis | 918 |
| a) Allgemeine Voraussetzungen einer wirksamen Einwilligung .. | 918 |
| b) Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis .. | 919 |
| c) Form der Einwilligung im Beschäftigungsverhältnis | 924 |
| 2. Gesetzliche Erlaubnistatbestände | 925 |
| a) Vertragsdurchführung (Art. 6 Abs. 1 lit. b DSGVO)..... | 926 |

| | |
|--|-----|
| b) Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO) | 926 |
| c) Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) .. | 928 |
| d) Besondere Kategorien von personenbezogenen Daten (Art. 9 Abs. 2 lit. b DSGVO) | 928 |
| 3. Betriebsvereinbarungen | 929 |
| a) Angemessene und besondere Schutzmaßnahmen | 929 |
| b) Betriebsvereinbarung als Erlaubnistatbestand | 931 |
| c) Weitere Regelungen in Betriebsvereinbarungen | 932 |
| d) Bereits abgeschlossene Betriebsvereinbarungen | 933 |
| 4. Datenaustausch in Matrixorganisationen | 934 |
| a) Erlaubnistatbestände | 934 |
| b) Gemeinsame Verantwortlichkeit | 935 |
| IV. Informationspflichten und Betroffenenrechte | 935 |
| 1. Informationspflichten des Arbeitgebers | 935 |
| 2. Betroffenenrechte | 936 |
| 3. Automatisierte Entscheidungen einschließlich Profiling | 939 |
| V. Überwachungsmaßnahmen – Rechtslage in Deutschland. | 940 |
| 1. Kontrolle der Internet- und E-Mail-Nutzung | 940 |
| a) Erlaubnistatbestand | 940 |
| b) Kontrolle der dienstlichen Internet- und E-Mail-Nutzung | 941 |
| c) Arbeitgeber als Diensteanbieter | 941 |
| d) Beweisverwertungsverbote | 944 |
| 2. Videoüberwachung | 944 |
| VI. Handlungsempfehlung | 946 |
| Kapitel 16: Behördliche und gerichtliche Verfahren | |
| <i>(Scheffzig/Rothkegel/Cornelius)</i> | 949 |
| I. Aufsichtsbehörden | 950 |
| 1. Überblick über die einschlägigen Normen | 950 |
| 2. Einleitung | 951 |
| 3. Zuständigkeit innerhalb der Europäischen Union | 952 |
| 4. Zuständigkeit innerhalb Deutschlands | 954 |
| 5. Europäischer Datenschutzausschuss | 955 |
| 6. Aufgaben und Befugnisse | 956 |
| a) Aufgaben der Aufsichtsbehörden | 956 |
| b) Befugnisse der Aufsichtsbehörden | 958 |

| | |
|--|------|
| II. Aufsichtsverfahren | 965 |
| 1. Aufsichtsverfahren in Deutschland | 965 |
| 2. Zusammenarbeit der Aufsichtsbehörden auf europäischer Ebene . | 969 |
| a) Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden | 970 |
| b) Kohärenzverfahren im Falle von Unstimmigkeiten | 971 |
| 3. Öffentliche Äußerungen von Behörden/Mediale Aufmerksamkeit | 974 |
| a) Die namentliche Nennung des sanktionierten Unternehmens . | 974 |
| b) Pressemitteilungen und Stellungnahmen zu aktuellen Geschehnissen | 975 |
| III. Umgang mit Aufsichtsbehörden | 977 |
| 1. Gründe für den Kontakt mit Aufsichtsbehörden | 977 |
| a) Kontrolldichte | 977 |
| b) Anfragen durch Aufsichtsbehörden | 978 |
| 2. Bedeutung von Rechtspositionen der Datenschutzbehörden | 979 |
| 3. Erste Maßnahmen nach Anfrage einer Aufsichtsbehörde | 980 |
| 4. Sofortige Korrektur von festgestellten Rechtsverstößen | 981 |
| 5. Generelle Hinweise zur Interaktion mit Aufsichtsbehörden | 982 |
| 6. Kooperation und Selbstbelastung | 983 |
| IV. Bußgelder | 986 |
| 1. Überblick über die einschlägigen Normen | 986 |
| 2. Bußgeldvorschriften der DSGVO | 987 |
| a) Kategorisierung der Bußgelder und Strafvorschriften | 987 |
| b) Referenztechnik | 988 |
| c) Einzelne Tatbestände | 988 |
| d) Bisher bekannte und nennenswerte Bußgelder | 990 |
| 3. Bemessung des Bußgeldes | 995 |
| a) Allgemeine Vorgaben nach der DSGVO | 995 |
| b) Das Bußgeldmodell der Datenschutzkonferenz in Deutschland | 998 |
| 4. Straf- und Bußgeldvorschriften des BDSG | 1004 |
| a) Strafvorschriften | 1004 |
| b) Bußgeldvorschriften | 1008 |
| 5. Adressat des Bußgeldes | 1008 |
| a) Verantwortliche Stelle, Auftragsverarbeiter und spezielle Stellen | 1008 |
| b) Bußgelder gegenüber einzelnen Personen innerhalb eines Unternehmens | 1010 |
| c) Bußgelder gegenüber Behörden | 1011 |

| | |
|---|-------------|
| V. Gerichtlicher Rechtsschutz | 1012 |
| 1. Überblick über die einschlägigen Normen | 1012 |
| 2. Verhältnis Betroffener – Verantwortlicher bzw. Auftragsverarbeiter | 1012 |
| a) Auskunftsanspruch und weitere subjektive Rechte | 1013 |
| b) Unterlassungsanspruch | 1014 |
| c) Schadensersatzanspruch | 1015 |
| 3. Verhältnis Verantwortlicher bzw. Auftragsverarbeiter – Aufsichtsbehörde | 1019 |
| a) Rechtsschutzgarantie unter der DSGVO | 1019 |
| b) Konkreter Rechtsschutz nach deutschem Verfahrensrecht | 1020 |
| 4. Sonderfall: Beschlüsse des Europäischen Datenschutzausschusses | 1023 |
| 5. Vorgehen gegen öffentliche Äußerungen der Datenschutzbehörden | 1023 |
| VI. Verbandsklage | 1025 |
| 1. Überblick über die einschlägigen Normen | 1025 |
| 2. Verbandsklagen auf Grundlage der DSGVO (Art. 80 DSGVO) ... | 1026 |
| a) Unter Mitwirkung des Betroffenen (Art. 80 Abs. 1 DSGVO) ... | 1026 |
| b) Ohne Mitwirkung des Betroffenen (Art. 80 Abs. 2 DSGVO) ... | 1028 |
| 3. Möglichkeiten zur Verbandsklage nach deutschem Recht | 1029 |
| a) UKlaG | 1029 |
| b) Anwendbarkeit des UWG und AGB-Rechts seit Einführung der DSGVO | 1032 |
| Kapitel 17: Besondere Themenkomplexe | 1035 |
| A. Web Tracking und Online Advertising <i>(Arning/Hansen-Oest/Strassemeyer)</i> | 1037 |
| I. Technische Abläufe | 1039 |
| 1. Der Einsatz von Cookies zum Web Tracking | 1040 |
| 2. Das Ausspielen von Werbung (Online Advertising) | 1041 |
| 3. Weitere Methoden zum Web Tracking | 1042 |
| a) Tracking Pixel | 1042 |
| b) Social Plugins | 1043 |
| c) Andere dynamische Websiteinhalte Dritter | 1044 |
| d) Fingerprinting | 1044 |
| e) Server to Server Tracking | 1045 |

| | |
|---|-------------|
| II. Zulässigkeit des Web Tracking und des Online Advertising | 1045 |
| 1. Anwendbare Regelungen auf das Web Tracking und Online Advertising. | 1046 |
| a) Rechtsunklarheit aufgrund fehlender ePrivacy-Verordnung . . . | 1046 |
| b) Das Zusammenspiel zwischen der DSGVO und der ePrivacy-Richtlinie | 1048 |
| c) Das einschlägige Regelungsregime für einzelne Trackingmethoden | 1053 |
| d) Anwendbarkeit der DSGVO für die (weitere) Verarbeitung. . . | 1056 |
| 2. Zulässigkeit des Web Tracking für einzelne Zwecke | 1060 |
| a) Zulässigkeit zu Zwecken des Online Advertising | 1061 |
| b) Zulässigkeit der Datenverarbeitung zu anderen Zwecken als dem Online Advertising | 1087 |
| III. Verantwortlichkeit für Web Tracking und Online Advertising | 1095 |
| 1. Verpflichteter nach Art. 5 Abs. 3 ePrivacy-Richtlinie | 1095 |
| 2. Datenschutzrechtlich Verantwortlicher nach Art. 4 Nr. 7 DSGVO. | 1096 |
| IV. Zusätzliche Pflichten. | 1098 |
| V. Bußgeldrahmen bei Verstößen | 1100 |
| B. Customer-Relationship-Management (Rohwedder). | 1103 |
| I. Überblick über die einschlägigen Regelungen. | 1103 |
| II. Datenquellen | 1104 |
| III. Profiling zu Werbezwecken | 1106 |
| 1. Interessenabwägung | 1106 |
| 2. Zweckändernde Verarbeitung | 1110 |
| 3. Keine Anwendung von Art. 22 DSGVO. | 1111 |
| 4. Einwilligung | 1112 |
| IV. Werbliche Kommunikation mit Kunden. | 1113 |
| 1. Briefwerbung | 1113 |
| a) Interessenabwägung/Zweckänderung. | 1113 |
| b) Einwilligung | 1114 |
| 2. Direktwerbung über elektronische Post, Anrufautomaten und Fax. | 1115 |
| 3. Persönliche Telefonwerbung | 1116 |
| 4. Vorrang der ePrivacy-Bestimmungen. | 1118 |
| 5. Zusammenfassung. | 1118 |

| | |
|---|------|
| C. E-Discovery (<i>Heinemann</i>) | 1120 |
| I. Ausgewählte Rahmenbedingungen | 1121 |
| 1. Federal Rule of Civil Procedure der Vereinigten Staaten | 1121 |
| 2. Sedona Konferenzen, Frameworks und Arbeitsgruppen | 1123 |
| 3. Leitlinien der Artikel-29-Datenschutzgruppe | 1124 |
| II. Kollision mit dem Datenschutz im Beweissicherungsprozess | 1124 |
| 1. Grundlage: Das e-Discovery Referenzmodell (EDRM) | 1125 |
| 2. Grundlage: Information Management und Governance | 1125 |
| 3. Durchführung des e-Discovery-Prozesses mit dem Referenzmodell | 1126 |
| a) Identifikationsphase (Identification) | 1126 |
| b) Phase der Extraktion und Sicherung (Collection and Preservation) | 1127 |
| c) Phase der Bearbeitung (Processing, Review and Analysis) | 1132 |
| d) Phase der Weitergabe und Nutzung (Production and Presentation) | 1132 |
| III. Fazit | 1134 |
| D. Cloud Computing (<i>Meyerdierks</i>) | 1136 |
| I. Eigenschaften und Terminologie | 1136 |
| II. Cloud-spezifische Problemfelder | 1138 |
| E. Big Data (<i>Meyerdierks</i>) | 1141 |
| I. Eigenschaften und Terminologie | 1141 |
| II. Big Data-spezifische Problemfelder | 1142 |
| 1. Personenbezug | 1142 |
| 2. Zweckbindung | 1143 |
| 3. Datenminimierung | 1144 |
| 4. Betroffenenrechte | 1144 |
| a) Informationspflichten | 1145 |
| b) Auskunftsrecht | 1145 |
| F. Gesundheitsdatenschutz (<i>Arning</i>) | 1147 |
| I. Definition „Gesundheitsdaten“ | 1148 |
| II. Systematik der datenschutzrechtlichen Regelungen im Gesundheitsbereich | 1151 |

| | |
|---|-------------|
| III. Zulässigkeit der Verarbeitung von Gesundheitsdaten auf Basis von Vorschriften aus der DSGVO/dem BDSG | 1159 |
| 1. Verarbeitung von Gesundheitsdaten auf Basis einer Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) | 1161 |
| a) Allgemeine Anforderungen an die Einwilligung | 1161 |
| b) Freiwilligkeit der Einwilligung gem. Art. 4 Nr. 11 und Art. 7 Abs. 4 DSGVO | 1163 |
| c) Ausschluss der Einwilligung gem. Art. 9 Abs. 2 lit. a DSGVO .. | 1165 |
| 2. Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung (Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b, Abs. 2 BDSG) | 1166 |
| a) Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung gem. Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 22 Abs. 1 lit. b BDSG | 1170 |
| b) Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gem. Art. 9 Abs. 4 DSGVO i.V.m. § 22 Abs. 2 BDSG | 1175 |
| 3. Verarbeitung von Gesundheitsdaten im Beschäftigungskontext (Art. 9 Abs. 2 lit. b DSGVO, § 26 Abs. 3 und 4 BDSG) | 1178 |
| IV. Weitere Besonderheiten nach der DSGVO/dem BDSG bei der Verarbeitung von Gesundheitsdaten | 1178 |
| V. (Berufsrechtliche) Schweigepflicht | 1181 |
| VI. Verarbeitung zu wissenschaftlichen Forschungszwecken | 1189 |
| 1. Zulässigkeit der Verarbeitung von Gesundheitsdaten zu Zwecken der wissenschaftlichen Forschung | 1191 |
| a) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken gem. Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 Abs. 1 BDSG | 1191 |
| b) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken auf Basis einer Einwilligung | 1195 |
| 2. Weitere Besonderheiten bei der Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken | 1199 |
| Kapitel 18: Österreichisches Datenschutzrecht (Braun) | 1203 |
| I. Gesetzliche Grundlagen | 1204 |
| II. Nutzung von Öffnungsklauseln | 1205 |
| III. Grundrecht auf Datenschutz | 1209 |
| IV. Marketing und Kontaktaufnahme zu Werbezwecken | 1212 |

| | |
|--|------|
| V. Österreichische Spezialregelungen | 1215 |
| 1. Verarbeitung von Bilddaten (Bildaufnahmen) | 1215 |
| 2. Verarbeitung von Strafdaten | 1220 |
| 3. Back-Up-Privileg | 1222 |
| 4. Verwarnung durch die Datenschutzbehörde | 1222 |
| 5. Datengeheimnis | 1223 |
| 6. Datenschutz-Folgenabschätzungen | 1226 |
| 7. Regelungen in Materiengesetzen | 1228 |
| VI. Arbeitnehmer-Datenschutz | 1229 |
| 1. Einwilligungen im Arbeitsverhältnis, Tracking von Mitarbeitern .. | 1229 |
| 2. Betriebsverfassungsrecht und DSGVO | 1231 |
| 3. Betriebsrat | 1235 |
| VII. Österreichische Entscheidungen | 1235 |
| 1. Anwendbarkeit der DSGVO | 1235 |
| 2. Sensible Daten | 1236 |
| 3. Verwendung öffentlich zugänglicher Registerdaten | 1237 |
| 4. Automatische Erfassung von Daten | 1238 |
| 5. Speicherung von Daten | 1238 |
| 6. Datenschutzbeauftragter | 1240 |
| 7. Einwilligung | 1240 |
| 8. Informationsrecht | 1243 |
| 9. Auskunftsrecht | 1244 |
| 10. Löschung | 1245 |
| 11. Kreditauskunft | 1247 |
| 12. Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO | 1249 |
| VIII. Rechtsdurchsetzung und Verfahrensrecht | 1250 |
| 1. Verwaltungsverfahren | 1250 |
| a) Beschwerde an die Datenschutzbehörde | 1250 |
| b) Amtswegiges Prüfungsverfahren der Datenschutzbehörde | 1253 |
| c) Rechtsmittel und Rechtsbehelfe gegen Entscheidungen der Datenschutzbehörde | 1253 |
| d) Vollstreckung von Entscheidungen im Verwaltungsverfahren .. | 1254 |
| 2. Verwaltungsstrafverfahren | 1254 |
| 3. Verfahren vor ordentlichen Gerichten und parallele Verfahrensführung | 1258 |

Kapitel 19: Leitentscheidungen des EuGH zur DSGVO

| | |
|--|------|
| <i>(Strassemeyer/Schefzig/Moos)</i> | 1263 |
| I. Einleitung | 1264 |
| II. Leitentscheidungen des EuGH. | 1265 |
| 1. Anwendungsbereich des europäischen Datenschutzrechts (EuGH, Urt. v. 13.5.2014 – C-131/12 – <i>Google Spain</i>) | 1265 |
| a) Sachverhalt | 1265 |
| b) Entscheidungsgründe | 1265 |
| c) Implikationen für die Unternehmenspraxis | 1267 |
| 2. Personenbezug von Daten (EuGH, Urt. v. 6.12.2016 – C-582/14 – <i>Breyer</i>) | 1271 |
| a) Sachverhalt | 1271 |
| b) Entscheidungsgründe – der Personenbezug dynamischer IP-Adressen. | 1272 |
| c) Implikationen für die Unternehmenspraxis | 1273 |
| 3. Gemeinsame Verantwortlichkeit I (EuGH, Urt. v. 5.6.2018 – C-210/16 – <i>Facebook Fanpages</i>) | 1274 |
| a) Sachverhalt | 1274 |
| b) Entscheidungsgründe | 1275 |
| c) Implikationen für die Unternehmenspraxis | 1276 |
| 4. Gemeinsame Verantwortlichkeit II (EuGH, Urt. v. 10.7.2018 – C-25/17 – <i>Zeugen Jehovas</i>) | 1277 |
| a) Sachverhalt | 1277 |
| b) Entscheidungsgründe | 1278 |
| c) Implikationen für die Unternehmenspraxis | 1279 |
| 5. Gemeinsame Verantwortlichkeit III (EuGH, Urt. v. 29.7.2019 – C-40/17 – <i>Fashion ID</i>) | 1280 |
| a) Sachverhalt | 1280 |
| b) Entscheidungsgründe | 1281 |
| c) Implikationen für die Unternehmenspraxis | 1282 |
| 6. Verlinkung auf besondere personenbezogene Daten (EuGH, Urt. v. 14.9.2019 – C-136/17) | 1284 |
| a) Sachverhalt | 1285 |
| b) Entscheidungsgründe | 1285 |
| c) Implikationen für die Unternehmenspraxis | 1286 |
| 7. Keine extraterritoriale Auslistung (EuGH, Urt. v. 14.9.2019 – C-507/17) | 1287 |
| a) Sachverhalt | 1287 |
| b) Entscheidungsgründe | 1287 |
| c) Implikationen für die Unternehmenspraxis | 1288 |

| | |
|--|------|
| 8. Anforderungen an eine wirksame Einwilligung (EuGH, Urt. v. 1.10.2019 – C-673/17 – <i>Planet49</i>)..... | 1288 |
| a) Sachverhalt | 1289 |
| b) Entscheidungsgründe..... | 1289 |
| c) Implikationen für die Unternehmenspraxis..... | 1290 |
| 9. Die Rechtfertigung von Drittlandtransfers (EuGH, Urt. v 16.7.2020 – C-311/18 – <i>Schrems II</i>)..... | 1295 |
| a) Sachverhalt | 1295 |
| b) Entscheidungsgründe..... | 1295 |
| c) Implikationen für die Unternehmenspraxis..... | 1297 |

| | |
|---|-------------|
| Kapitel 20: Vorgehensweise zur Umsetzung von DSGVO-Anforderungen im Unternehmen (Zeiter/Moos) .. | 1303 |
| I. Anpassungsbedarf im Unternehmen | 1303 |
| II. Leitbild zur Umsetzung der DSGVO im Unternehmen..... | 1305 |
| III. Ausgestaltung eines Umsetzungsprojekts..... | 1305 |
| 1. Vorbereitung..... | 1305 |
| a) Welche Abteilung bzw. welche Person ist unternehmensintern für die Umstellung auf die DSGVO verantwortlich? | 1306 |
| b) Welche datenschutzrechtlichen Vorschriften sollen konkret umgesetzt werden? | 1306 |
| c) Auf welche verantwortlichen Stellen bezieht sich das Umsetzungsprojekt genau? | 1307 |
| d) Sollte die DSGVO im Unternehmen global umgesetzt werden? | 1308 |
| e) Welche Ressourcen stehen zur Verfügung?..... | 1308 |
| f) Soll die Implementierung durch interne oder externe Ressourcen erfolgen? | 1309 |
| g) Welche Abteilungen sollten involviert bzw. informiert werden? | 1309 |
| h) Bis wann sollte die DSGVO im Unternehmen umgesetzt sein? . | 1309 |
| i) Kann die Umsetzung der DSGVO im Unternehmen auch als Chance wahrgenommen werden?..... | 1310 |
| 2. Anforderungsspezifizierung | 1311 |
| 3. Gap-Analyse..... | 1312 |
| a) Vorbereitung der Gap-Analyse | 1312 |
| b) Durchführung der Gap-Analyse | 1312 |
| c) Ergebnis der Gap-Analyse..... | 1314 |
| 4. Planung von Ressourcen | 1314 |
| a) Planung von Budget | 1314 |
| b) Planung von Mitarbeitern | 1315 |
| c) Zeitplan | 1315 |

| | |
|--|------|
| 5. Implementierung | 1315 |
| a) Definition von Unterprojekten | 1316 |
| b) Bestimmung von Meilensteinen und Abhängigkeiten | 1316 |
| c) Durchführung der Unterprojekte | 1317 |
| 6. Testing und Monitoring | 1317 |
| 7. Kommunikation und Training | 1318 |
| a) Interne Unternehmenskommunikation | 1319 |
| b) Mitarbeiterschulungen | 1319 |
| IV. Erste Erfahrungen aus der Umsetzungspraxis | 1319 |
| V. Fazit | 1321 |
| | |
| Kapitel 21: Weitere rechtliche Entwicklungen und Ausblick | |
| <i>(Moos/Schefzig)</i> | 1323 |
| I. Datenschutzrecht als dynamisches Rechtsgebiet | 1323 |
| II. Gesetzgeber | 1324 |
| 1. Rechtsakte der Europäischen Kommission | 1324 |
| a) Delegierte Rechtsakte | 1325 |
| b) Durchführungsrechtsakte | 1325 |
| 2. Begleitgesetze der Mitgliedstaaten | 1328 |
| 3. ePrivacy | 1328 |
| III. Datenschutzbehörden | 1330 |
| 1. Europäischer Datenschutzausschuss | 1330 |
| 2. Black- und Whitelists für Datenschutz-Folgenabschätzung | 1331 |
| 3. Musterverträge | 1331 |
| 4. Konkretisierung von Pflichten nach der DSGVO | 1332 |
| IV. Rechtsprechung | 1334 |
| V. Entwicklung der Datenschutzpraxis | 1334 |
| VI. Ausblick | 1335 |
| | |
| Sachregister | 1337 |