

# Inhaltsverzeichnis

Vorwort — V

Inhaltsübersicht — VII

Literaturverzeichnis — XLV

Autorenverzeichnis — LIII

## Kapitel 1

### Grundlagen des Umgangs mit dem neuen Datenschutzrecht

- A. Der Übergang vom Gesetz zur Verordnung — 1
  - I. Zeitliche Geltung — 1
  - II. Unmittelbare Geltung — 2
  - III. Zusammenspiel mit anderen Regelwerken — 2
    - 1. Begleitgesetze auf Basis von Öffnungsklauseln — 2
    - 2. Spezialgesetzliche Datenschutzregelungen in Richtlinien und Gesetzen — 3
    - 3. Datenschutzregelungen außerhalb des Anwendungsbereichs der DSGVO — 3
    - 4. Zwischenergebnis — 4
- B. Parallelität von DSGVO und „Altgesetzen“ — 4
- C. Auslegung der DSGVO und der Begleitgesetze — 5
  - I. Auslegung der DSGVO — 6
    - 1. Auslegungsmethoden — 6
      - a) Wortlaut — 6
      - b) Teleologische Auslegung — 7
      - c) Systematische Auslegung — 8
      - d) Historische Auslegung — 8
      - e) Effet-utile-Prinzip — 9
      - f) Mischung verschiedener Auslegungsmethoden — 9
    - 2. Relevanz existierender Rechtsprechung — 10
  - II. Auslegung der Begleitgesetze — 11
    - 1. Auslegungsmethoden — 11
      - a) Klassische Auslegungsmethoden — 11
      - b) Europarechtskonforme Auslegung — 11
    - 2. Relevanz existierender Rechtsprechung — 11

## **Kapitel 2**

### **Grundlagen des Datenschutzrechts**

- A. Historie — 13**
  - I. Historie des Datenschutzes und der Gesetzesentwicklung — 13**
    - 1. Von der Antike bis zum Mittelalter — 13**
    - 2. Datenschutz im Zeitalter der industriellen Revolution — 13**
    - 3. Von der Mitte des 20. Jahrhunderts bis 2012 — 15**
    - 4. Die Datenschutzgrundverordnung — 18**
  - II. Harmonisierung des Datenschutzrechts — 18**
- B. Grundbegriffe — 20**
  - I. Grundrecht auf Schutz personenbezogener Daten — 20**
  - II. Personenbezogenes Datum — 21**
    - 1. Informationen — 21**
    - 2. Personenbezug — 22**
      - a) Personenbezogene Daten vs. Sachdaten — 22**
      - b) Betroffene Person — 23**
      - c) Identifizierte bzw. identifizierbare betroffene Person — 24**
        - aa) Identifizierte betroffene Person — 24**
        - bb) Identifizierbare betroffene Person — 24**
      - d) Anonyme Informationen — 28**
      - e) Pseudonyme Informationen — 29**
  - III. Datenverarbeitung — 30**
  - IV. Akteure — 31**
    - 1. Verantwortlicher — 31**
    - 2. Dritter — 32**
    - 3. Auftragsverarbeiter — 33**
    - 4. Joint-Controller — 34**
  - V. Besondere Kategorien personenbezogener Daten — 35**

## **Kapitel 3**

### **Anwendungsbereich des Datenschutzrechts**

- A. Überblick über die einschlägigen Regelungen der DSGVO — 37**
- B. Sachlicher Anwendungsbereich — 38**
  - I. Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO — 38**
  - II. Ausnahmetatbestände, Art. 2 Abs. 2 bis 4 DSGVO — 39**
- C. Räumlicher Anwendungsbereich — 43**
  - I. Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO — 43**
    - 1. Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Verantwortlichen — 44**

- 2. Verarbeitung im Rahmen der Tätigkeiten der Niederlassung eines Auftragsverarbeiters — **45**
- II. Marktortprinzip, Art. 3 Abs. 2 DSGVO — **46**
  - 1. Anbieten von Waren oder Dienstleistungen, Art. 3 Abs. 2 lit. a DSGVO — **47**
  - 2. Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO — **50**
  - 3. Betroffene Person in der EU — **52**
- III. Auseinanderfallen bei mehreren Beteiligten — **53**
- D. Anwendungsbereich mitgliedstaatlicher Regelungen — **54**
  - I. Anwendungsbereich des BDSG (2018) für nicht-öffentliche Stellen — **54**
    - 1. Sachlicher Anwendungsbereich, § 1 Abs. 1 S. 2 BDSG (2018) — **54**
    - 2. Räumlicher Anwendungsbereich, § 1 Abs. 4 S. 2 BDSG (2018) — **55**
      - a) Deutsches Territorialitätsprinzip, § 1 Abs. 4 S. 2 Nr. 1 BDSG (2018) — **55**
      - b) Deutsches Niederlassungsprinzip, § 1 Abs. 4 S. 2 Nr. 2 BDSG (2018) — **55**
      - c) Europäisches Marktortprinzip, § 1 Abs. 4 S. 2 Nr. 3 BDSG (2018) — **56**
    - 3. Unmittelbare Geltung der Verordnung, § 1 Abs. 5 BDSG (2018) — **56**
    - 4. Umgang mit Anwendungsproblemen — **57**
      - a) Kollision mit Regelungen anderer Mitgliedstaaten — **57**
      - b) Anwendbarkeit des BDSG (2018) außerhalb der Verordnung — **58**
  - II. Anwendungsbereich sonstiger ausfüllender Normen — **59**

## **Kapitel 4**

### **Datenschutzrechtliche Grundsätze**

- A. Bedeutung der Grundsätze — **61**
- B. Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DSGVO) — **63**
- C. Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO) — **64**
- D. Transparenz (Art. 5 Abs. 1 lit. a DSGVO) — **65**
- E. Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) — **66**
- F. Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) — **68**
- G. Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) — **68**
- H. Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) — **70**
- I. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) — **72**
- J. Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) — **73**

## **Kapitel 5**

### **Zulässigkeit der Verarbeitung personenbezogener Daten**

- A. Überblick über die einschlägigen Regelungen der DSGVO — 77**
- B. Gesetzliche Erlaubnisvorschriften — 78**
  - I. Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen — 79**
    - 1. Verarbeitung personenbezogener Daten zu Zwecken der Vertragserfüllung — 79**
    - 2. Verarbeitung personenbezogener Daten zu Zwecken der Durchführung vorvertraglicher Maßnahmen — 81**
    - 3. Erforderlichkeit der Datenverarbeitung für die genannten Zwecke — 82**
      - a) „Erforderlichkeit“ einer Datenverarbeitung — 82**
      - b) Erforderlichkeit einer Datenverarbeitung für die in Art. 6 Abs. 1 lit. b DSGVO genannten Zwecke — 84**
  - II. Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung — 85**
  - III. Verarbeitung personenbezogener Daten auf Basis einer Interessenabwägung — 87**
    - 1. Berechtigte Interessen des Verantwortlichen oder eines Dritten — 88**
    - 2. Erforderlichkeit einer Datenverarbeitung zur Wahrung der berechtigten Interessen — 90**
    - 3. Keine überwiegenden Interessen/Rechte der betroffenen Person am Ausschluss der Datenverarbeitung — 90**
  - IV. Verarbeitung personenbezogener Daten zu Zwecken der Werbung — 94**
  - V. Verhältnis der Alternativen des Art. 6 Abs. 1 DSGVO zueinander — 96**
  - VI. Zweckänderung – Verarbeitung personenbezogener Daten zu einem anderen Zweck — 97**
  - VII. Verarbeitung besonderer Kategorien personenbezogener Daten — 100**
    - 1. Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) — 101**
    - 2. Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 DSGVO) — 103**
      - a) Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) — 103**
      - b) Beschäftigungs- und Sozialschutzkontext (Art. 9 Abs. 2 lit. b DSGVO) — 104**
      - c) Offenkundig öffentliche Daten (Art. 9 Abs. 2 lit. e DSGVO) — 105**
      - d) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte (Art. 9 Abs. 2 lit. f DSGVO) — 105**

- e) Erlaubnis durch das Recht der Union oder des Mitgliedstaates aus Gründen eines erheblichen öffentlichen Interesses (Art. 9 Abs. 2 lit. g DSGVO) — **106**
- f) Verarbeitung für die Gesundheitsversorgung (Art. 9 Abs. 2 lit. h DSGVO) — **106**
- g) Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO) — **107**
- h) Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (Art. 9 Abs. 2 lit. j DSGVO) — **108**
- i) Erforderlichkeit der Datenverarbeitung — **109**
- j) Besondere Anforderungen für die Verarbeitung genetischer oder biometrischer Daten und Gesundheitsdaten — **109**
- k) Zweckänderung bei der Verarbeitung besonderer Kategorien personenbezogener Daten — **110**
- VIII. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten – Art. 10 DSGVO — **111**
- IX. Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist – Art. 11 DSGVO — **112**
- X. Besondere Verarbeitungssituationen — **115**
- XI. Zulässigkeit der Verarbeitung personenbezogener Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — **116**
- XII. Sanktionierung — **116**
- C. Einwilligung der Betroffenen — **116**
  - I. Überblick über die einschlägigen Regelungen — **117**
  - II. Allgemeine Voraussetzungen der Einwilligung — **118**
    - 1. Form der Willensbekundung — **118**
      - a) Opt-out vs. Opt-in — **119**
      - b) Besondere Formerfordernisse bei elektronischer Einholung — **120**
      - c) Besondere Formerfordernisse im Beschäftigungskontext — **121**
    - 2. Freiwilligkeit — **122**
      - a) Koppelungsverbot — **122**
      - b) Trennungsgebot — **124**
      - c) Klares Ungleichgewicht — **125**
    - 3. Erteilung für den bestimmten Fall — **127**
    - 4. Transparenzgebot — **127**
      - a) Notwendige Inhalte der Information — **127**
      - b) Art und Weise der Informationserteilung — **128**
    - 5. Einwilligungen als Gegenstand von AGB — **128**
      - a) Inhaltskontrolle — **129**
      - b) Einwilligung zusammen mit anderen Erklärungen — **130**
      - c) Unverbindlichkeit/Blue-Pencil-Test — **130**

- 6. **Widerruflichkeit — 131**
- 7. **Nachweisbarkeit — 133**
- 8. **Gültigkeitsdauer — 134**
- III. **Einwilligung von Kindern — 135**
  - 1. **Voraussetzungen bei direkten Angeboten von Fernabsatzdiensten — 136**
  - 2. **Vergewisserungspflicht des Verantwortlichen — 136**
- IV. **Einwilligung bei sensiblen Datenkategorien — 138**
- V. **Wirksamkeit von Alt-Einwilligungen — 138**

## **Kapitel 6**

### **Umgang mit Betroffenen**

- A. **Überblick über die einschlägigen Regelungen der DSGVO — 141**
  - I. **Einführung — 141**
  - II. **Systematischer Überblick über die Betroffenenrechte gem. Art. 12–23 DSGVO und Art. 77 ff. DSGVO — 142**
- B. **Rechte der von der Datenverarbeitung betroffenen Personen — 143**
  - I. **Informationspflichten (Art. 13 und 14 DSGVO) — 143**
    - 1. **Informationspflichten bei der Direkterhebung von Daten von der betroffenen Person (Art. 13) — 144**
      - a) **Voraussetzungen der Informationspflicht nach Art. 13 DSGVO — 144**
      - b) **Systematik von Art. 13 DSGVO — 144**
      - c) **Inhalte der Informationspflichten nach Art. 13 Abs. 1 DSGVO — 145**
        - aa) **Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters (§ 13 Abs. 1 lit. a DSGVO) — 145**
        - bb) **Kontaktdaten des Datenschutzbeauftragten (§ 13 Abs. 1 lit. b DSGVO) — 146**
        - cc) **Zwecke und Rechtsgrundlage der Datenverarbeitung (§ 13 Abs. 1 lit. c DSGVO) — 146**
        - dd) **Information über die berechtigten Interessen i.S.d. Art. 6 Abs. 1 lit. f DSGVO (§ 13 Abs. 1 lit. d DSGVO) — 147**
        - ee) **Empfänger bzw. Kategorien von Empfängern der personenbezogenen Daten (§ 13 Abs. 1 lit. e DSGVO) — 147**
        - ff) **Übermittlung in ein Drittland oder an eine internationale Organisation (§ 13 Abs. 1 lit. f DSGVO) — 148**
      - d) **Inhalte der Informationspflichten nach Art. 13 Abs. 2 DSGVO — 149**
        - aa) **Dauer der Speicherung (Art. 13 Abs. 2 lit. a DSGVO) — 149**

- bb) Bestehen von Betroffenenrechten  
(Art. 13 Abs. 2 lit. b DSGVO) — **150**
- cc) Widerrufbarkeit der Einwilligung  
(Art. 13 Abs. 2 lit. c DSGVO) — **150**
- dd) Beschwerderecht bei einer Aufsichtsbehörde  
(Art. 13 Abs. 2 lit. d DSGVO) — **151**
- ee) Verpflichtung zur Bereitstellung von Daten, Erforderlichkeit  
der Bereitstellung von Daten für den Vertragsschluss und Fol-  
gen der Nichtbereitstellung (Art. 13 Abs. 2 lit. e DSGVO) — **151**
- ff) Automatisierte Entscheidungsfindung (Art. 13 Abs. 2 lit. f  
DSGVO) — **151**
- e) Zeitpunkt der Information — **153**
- f) Information im Fall der Zweckänderung (Art. 13 Abs. 3  
DSGVO) — **153**
- g) Ausnahmen von der Informationspflicht (Art. 13 Abs. 4  
DSGVO) — **154**
- h) Keine Pflicht zur „Nachinformation“ im Hinblick auf Daten, die  
vor der Anwendbarkeit der DSGVO erhoben wurden — **156**
- i) Keine Zulässigkeitsvoraussetzung — **156**
- 2. Informationspflichten bei der Erhebung von Daten aus anderen  
Quellen als von der betroffenen Person (Art. 14) — **157**
  - a) Voraussetzungen der Informationspflicht nach Art. 14  
DSGVO — **157**
  - b) Inhalte der Informationspflichten nach Art. 14 Abs. 1  
DSGVO — **157**
  - c) Inhalte der Informationspflichten nach Art. 14 Abs. 2  
DSGVO — **158**
  - d) Zeitpunkt der Informationserteilung nach Art. 14 Abs. 3  
DSGVO — **159**
  - e) Information im Fall der Zweckänderung (Art. 14 Abs. 4  
DSGVO) — **159**
  - f) Ausnahmen (Art. 14 Abs. 5 DSGVO) — **160**
    - aa) Betroffene Person verfügt bereits über die Information  
(Art. 14 Abs. 5 lit. a DSGVO) — **160**
    - bb) Unmöglichkeit bzw. unverhältnismäßiger Aufwand  
(Art. 14 Abs. 5 lit. b DSGVO) — **160**
    - cc) Rechtsvorschriften der EU oder der Mitgliedstaaten  
(Art. 14 Abs. 5 lit. c DSGVO) — **162**
    - dd) Berufsgeheimnis (Art. 14 Abs. 5 lit. d DSGVO) — **162**
    - ee) Umfang der Ausnahme von der Informationspflicht — **162**
    - ff) Weitere Ausnahmen — **163**
  - g) „Nachinformation“ und keine Zulässigkeitsvoraussetzung — **164**

3. Modalitäten der Information der betroffenen Personen (Art. 12 DSGVO) — **165**
  - a) Formulierung der Information — **165**
  - b) Information in leicht zugänglicher Form — **166**
  - c) Form — **166**
  - d) Unentgeltlichkeit — **168**
  - e) Kombination mit standardisierten Bildsymbolen — **168**
- II. Recht auf Auskunft (Art. 15 DSGVO) — **169**
  1. Auskunftsrecht nach Art. 15 Abs. 1 und 2 DSGVO — **170**
    - a) Voraussetzungen des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO — **170**
    - b) Inhalte des Auskunftsrechts nach Art. 15 Abs. 1 und 2 DSGVO — **170**
      - aa) Empfänger oder Kategorien von Empfängern (Art. 15 Abs. 1 lit. c DSGVO) — **172**
      - bb) Herkunft der Daten (Art. 15 Abs. 1 lit. g DSGVO) — **172**
      - cc) Übermittlungen in ein Drittland (Art. 15 Abs. 2 DSGVO) — **173**
  2. Ausnahmen vom Auskunftsrecht — **173**
  3. Modalitäten der Auskunftserteilung (Art. 12, Art. 15 Abs. 3 und 4 DSGVO) — **177**
    - a) Antragserfordernis — **177**
    - b) Identifizierung des Antragstellers (Art. 12 Abs. 6 DSGVO) — **177**
    - c) Erleichterung der Rechtsausübung (Art. 12 Abs. 2 S. 1 DSGVO) — **179**
    - d) Formulierung der Auskunft (Art. 12 Abs. 1 DSGVO) — **179**
    - e) Form der Auskunft — **180**
    - f) Unentgeltlichkeit (Art. 12 Abs. 5 DSGVO) — **180**
    - g) Frist zur Erteilung der Auskunft (Art. 12 Abs. 3 und 4 DSGVO) — **181**
  4. Recht der betroffenen Person, eine Kopie ihrer Daten zu erhalten (Art. 15 Abs. 3 und 4 DSGVO) — **182**
    - a) Inhalte der Kopie nach Art. 15 Abs. 3 DSGVO — **182**
    - b) Ausnahmen vom Recht auf Erhalt einer Kopie gem. Art. 15 Abs. 3 DSGVO — **183**
    - c) Modalitäten im Hinblick auf die Aushändigung der Kopie gem. Art. 15 Abs. 3 DSGVO — **184**
      - aa) Antrag — **184**
      - bb) Unentgeltlichkeit der Erstkopie — **184**
      - cc) Form der Kopie — **184**
      - dd) Weitere Modalitäten — **185**
  5. Auskunft im Hinblick auf Daten bzw. Erhalt von Kopien von Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — **185**



- III. Recht auf Berichtigung (Art. 16 DSGVO) — **186**
  - 1. Inhalte des Berichtigungsrechts nach Art. 16 DSGVO — **186**
    - a) Berichtigung unrichtiger personenbezogener Daten (S. 1) — **186**
    - b) Vervollständigung unvollständiger personenbezogener Daten (S. 2) — **187**
    - c) Darlegungs- und Beweislast — **187**
  - 2. Ausnahmen vom Berichtigungsrecht — **187**
  - 3. Modalitäten des Berichtigungs- bzw. Vervollständigungsanspruchs (Art. 12 DSGVO) — **188**
  - 4. Mitteilungspflicht nach Art. 19 DSGVO — **188**
  - 5. Berichtigung/Vervollständigung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — **189**
- IV. Recht auf Löschung/Recht auf Vergessenwerden (Art. 17 DSGVO) — **189**
  - 1. Voraussetzungen des Rechts auf Löschung (Art. 17 Abs. 1 DSGVO) — **189**
    - a) Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig (Art. 17 Abs. 1 lit. a DSGVO) — **190**
    - b) Widerruf der Einwilligung (Art. 17 Abs. 1 lit. b DSGVO) — **191**
    - c) Widerspruch gegen die Verarbeitung gem. Art. 21 DSGVO (Art. 17 Abs. 1 lit. c DSGVO) — **191**
    - d) Unrechtmäßige Verarbeitung (Art. 17 Abs. 1 lit. d DSGVO) — **192**
    - e) Erfüllung einer rechtlichen Verpflichtung (Art. 17 Abs. 1 lit. e DSGVO) — **193**
    - f) Erhebung der Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gem. Art. 8 Abs. 1 DSGVO — **193**
  - 2. Rechtsfolge: Löschen i.S.d. Art. 17 Abs. 1 DSGVO — **194**
  - 3. Mitteilungspflichten im Fall der Öffentlichmachung der Daten (Art. 17 Abs. 2 DSGVO) — **195**
    - a) Voraussetzungen des Rechts auf Vergessenwerden — **195**
    - b) Vom Verantwortlichen zur Erfüllung des Rechts auf Vergessenwerden zu ergreifende Maßnahmen — **196**
  - 4. Ausnahmen vom Recht auf Löschung (Art. 17 Abs. 3, Art. 12 DSGVO) — **197**
    - a) Ausnahmen nach Art. 17 Abs. 3 DSGVO — **197**
    - b) Weitere Ausnahmen/Informationspflicht nach Art. 12 Abs. 4 DSGVO — **197**
  - 5. Modalitäten des Löschungsanspruchs (Art. 12 DSGVO) — **200**
  - 6. Mitteilungspflicht nach Art. 19 DSGVO — **200**
  - 7. Recht auf Löschung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — **202**

- V. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO) — 202**
  - 1. Inhalte des Rechts auf Einschränkung der Datenverarbeitung — 202**
    - a) Voraussetzungen (Art. 18 Abs. 1 DSGVO) — 202**
      - aa) Bestreiten der Richtigkeit der Daten durch die betroffene Person (Art. 18 Abs. 1 lit. a DSGVO) — 203**
      - bb) Die betroffene Person benötigt die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen — 204**
    - b) Rechtsfolge: Einschränkung der Datenverarbeitung — 204**
    - c) Bedingungen für die Weiterverarbeitung der Daten (Art. 18 Abs. 2 DSGVO, Erwägungsgrund 67 DSGVO) — 205**
    - d) Informationspflichten für den Fall, dass die Daten wieder uneingeschränkt verarbeitet werden (Art. 18 Abs. 3 DSGVO) — 205**
  - 2. Ausnahmen vom Recht auf Einschränkung der Datenverarbeitung — 205**
  - 3. Modalitäten des Rechts auf Einschränkung der Datenverarbeitung (Art. 12 DSGVO) — 206**
  - 4. Mitteilungspflicht nach Art. 19 DSGVO — 206**
  - 5. Recht auf Einschränkung der Datenverarbeitung im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — 207**
- VI. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO) — 207**
  - 1. Voraussetzungen der Mitteilungspflicht — 207**
  - 2. Mitteilung der Berichtigung, Löschung oder Einschränkung der Verarbeitung — 209**
  - 3. Unterrichtungspflicht gegenüber der betroffenen Person — 209**
  - 4. Ausnahmen von der Mitteilungspflicht — 210**
  - 5. Modalitäten der Mitteilungspflicht (Art. 12 DSGVO) — 210**
  - 6. Mitteilungspflicht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — 210**
- VII. Recht auf Datenübertragbarkeit (Art. 20 DSGVO) — 210**
  - 1. Inhalte des Rechts auf Datenübertragbarkeit — 211**
    - a) Voraussetzungen des Rechts auf Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO) — 211**
      - aa) Daten, die den Anspruchsteller selbst betreffen — 211**
      - bb) Bereitstellen von Daten — 212**
      - cc) Verarbeitung auf Basis einer Einwilligung oder zur Erfüllung eines Vertrages — 213**
      - dd) Verarbeitung mithilfe automatisierter Verfahren — 213**

- b) Rechtsfolgen: Bereitstellung (Abs. 1) bzw. Übermittlung (Abs. 2) von Daten durch den Verantwortlichen — 213
      - aa) Bereitstellung von Daten durch den Verantwortlichen (Abs. 1) — 214
      - bb) Übermittlung durch den Verantwortlichen (Abs. 2) — 215
    - c) Verhältnis zu Art. 17 DSGVO (Abs. 3 S. 1) — 215
  - 2. Ausnahmen vom Recht auf Datenübertragbarkeit (Abs. 4, Art. 12 DSGVO) — 216
  - 3. Modalitäten des Rechts auf Datenübertragbarkeit — 218
  - 4. Recht auf Datenübertragbarkeit im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — 218
- VIII. Widerspruchsrecht (Art. 21 DSGVO) — 219
  - 1. Inhalte des Widerspruchsrechts — 219
    - a) Allgemeines Widerspruchsrecht gem. Art. 21 Abs. 1 DSGVO — 219
      - aa) Voraussetzungen des allgemeinen Widerspruchsrechts — 219
      - bb) Rechtsfolgen des allgemeinen Widerspruchsrechts — 220
    - b) Widerspruchsrecht bei der Datenverarbeitung zu Zwecken des Direktmarketings gem. Art. 21 Abs. 2 und 3 DSGVO — 221
      - aa) Voraussetzungen für das Widerspruchsrecht bei der Verarbeitung von Daten zu Zwecken des Direktmarketings — 221
      - bb) Rechtsfolgen des Widerspruchsrechts bei der Verarbeitung von Daten zu Zwecken des Direktmarketings — 223
    - c) Informationspflichten nach Art. 21 Abs. 4 DSGVO — 223
  - 2. Ausnahmen vom Widerspruchsrecht — 225
  - 3. Modalitäten des Widerspruchsrechts — 225
  - 4. Widerspruchsrecht im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — 226
- IX. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO) — 226
  - 1. Inhalte des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden — 228
    - a) Voraussetzungen des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden — 228
      - aa) Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht — 228
      - bb) Entscheidung, die rechtliche Wirkung gegenüber der betroffenen Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt — 231
    - b) Rechtsfolgen aus Art. 22 Abs. 1 DSGVO — 232

- c) Ausnahmen vom Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden (Art. 22 Abs. 2 und 3 DSGVO) — **232**
    - aa) Voraussetzungen (Abs. 2) — **233**
    - bb) Vorhaltung von Schutzmaßnahmen (Abs. 3) — **235**
    - cc) Weitere Ausnahmen vom Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden — **236**
  - d) Sonderfall: Verarbeitung besonderer Kategorien personenbezogener Daten — **237**
- 2. Modalitäten des Rechts, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden — **237**
- 3. Das Recht, keinen automatisierten Einzelfallentscheidungen unterworfen zu werden, im Hinblick auf Daten, die vor der Anwendbarkeit der DSGVO erhoben wurden — **238**
- X. Sanktionierung — **238**

## **Kapitel 7**

### **Auftragsverarbeitung**

- A. Begriff und Gegenstand der Auftragsverarbeitung — **239**
- B. Abgrenzung zum Verantwortlichen und zur gemeinsamen Verantwortlichkeit — **241**
  - I. Abgrenzung zum Verantwortlichen — **241**
    - 1. Entscheidung über Zwecke und Mittel der Verarbeitung — **241**
      - a) Entscheidungsbefugnis über Zwecke — **241**
      - b) Entscheidungsbefugnis über Mittel — **242**
  - II. Abgrenzung zur gemeinsamen Verantwortlichkeit — **243**
- C. Rechtsnatur der Auftragsverarbeitung — **244**
- D. Typische Fallkonstellationen einer Auftragsverarbeitung — **246**
- E. Rechte und Pflichten aus einer Auftragsverarbeitung — **247**
  - I. Pflichten des Auftragsverarbeiters — **247**
  - II. Rechte und Pflichten des Verantwortlichen — **248**
    - 1. Erteilung von Weisungen — **249**
    - 2. Dokumentation der Weisungen — **249**
- F. Begründung einer Auftragsverarbeitung — **250**
  - I. Auswahl des Auftragsverarbeiters — **250**
  - II. Abschluss eines Auftragsverarbeitungsvertrages — **251**
    - 1. Form des Auftragsverarbeitungsvertrages — **251**
    - 2. Inhalt des Auftragsverarbeitungsvertrages — **252**
    - 3. Umstellung von Auftragsverarbeitungsverträgen auf die DSGVO — **253**

- a) Überarbeitung der BDSG (bis 2018)-Muster zur Anpassung an die DSGVO-Anforderungen — 254
  - b) Neuabschluss von Verträgen im Übergangszeitraum — 255
  - c) Anpassung von bestehenden Altverträgen — 255
- G. Auftragsverarbeitung innerhalb von Unternehmensgruppen — 256
- H. Unterbeauftragungen — 257
  - I. Zustimmungspflicht des Verantwortlichen — 257
    - 1. Art der Erteilung — 257
    - 2. Einspruchsrecht bei Allgemeinzustimmung — 258
  - II. Begründung des Unterauftragsverhältnisses — 260
- I. Haftung von Auftragsverarbeitern — 260
  - I. Haftung auf Schadensersatz — 261
    - 1. Haftung für eigenes Verschulden — 261
    - 2. Haftung von Unterauftragsverarbeitern — 261
    - 3. Beweislastumkehr — 261
    - 4. Gesamtschuldnerische Haftung — 262
  - II. Sanktionen gegen Auftragsverarbeiter — 262
- J. Kontrolle von Auftragsverarbeitern — 264
  - I. Recht zur Kontrolle — 264
  - II. Pflicht zur Kontrolle — 264
  - III. Art und Häufigkeit der Kontrolle — 264
    - 1. Art der Kontrolle — 265
    - 2. Häufigkeit der Kontrolle — 266
  - IV. Dokumentation der Kontrollen — 266
  - V. Kontrollergebnis — 266

## Kapitel 8

### Zusammenarbeit mit Dritten

- A. Überblick über die einschlägigen Regelungen der DSGVO — 267
- B. Gemeinsam für die Verarbeitung Verantwortliche — 267
  - I. Der Begriff der gemeinsamen Verantwortlichkeit (Art. 4 Nr. 7 DSGVO) — 268
    - 1. Gemeinsame Entscheidung mehrerer Stellen — 269
    - 2. Entscheidung über Zwecke und Mittel der Verarbeitung — 269
    - 3. Entscheidungshilfen für die Unternehmenspraxis — 269
    - 4. Abgrenzung von der Auftragsverarbeitung — 271
  - II. Rechte und Pflichten der gemeinsam Verantwortlichen — 271
    - 1. Abschluss einer Vereinbarung über die gemeinsame Verantwortlichkeit — 272
      - a) Inhalt der Vereinbarung — 272

- aa) Gesetzliche Mindestinhalte — 272
    - bb) Sinnvolle Zusatzregelungen — 273
  - b) Transparenz der Vereinbarung — 275
  - c) Form der Vereinbarung — 275
- 2. Geltendmachung der Rechte der Betroffenen — 276
- 3. Zurverfügungstellung der wesentlichen Teile der Vereinbarung — 276
- III. Zulässigkeit der Verarbeitungen durch gemeinsam Verantwortliche — 277
- C. Getrennte Verantwortlichkeiten — 277
  - I. Begriff der Übermittlung — 278
  - II. Zulässigkeit von Datenübermittlungen an Dritte — 278
  - III. Typische Fallkonstellationen getrennter Verantwortlichkeiten — 279
  - IV. Besondere Aspekte von Datenübermittlungen im Konzern — 279
    - 1. Fehlendes Konzernprivileg — 280
    - 2. Erlaubnis durch Interessenabwägung — 280
    - 3. Öffnungsklausel für nationale Sonderregelungen — 282
    - 4. Internationale Datenübermittlungen — 282
- D. Niederlassungsübergreifende Verarbeitungen — 282
  - I. Der Begriff der Niederlassung — 283
  - II. Niederlassungsübergreifende Verarbeitung — 284
    - 1. Die Bestimmung der Hauptniederlassung (Art. 4 Nr. 16 DSGVO) — 285
    - 2. Die Spezifizierung der Verarbeitungsverfahren — 287

## **Kapitel 9**

### **Internationale Datenübermittlungen**

- A. Überblick über die einschlägigen Regelungen der DSGVO — 289
- B. Einführung in den Regelungsbereich — 290
  - I. Sonderregelungen für „Drittlands-Übermittlungen“ — 290
    - 1. Begriff des Drittlands — 290
    - 2. Geltung auch für internationale Organisationen — 291
    - 3. Begriff der „Übermittlung“ — 291
    - 4. Geltung auch für Weiterübermittlungen — 292
  - II. Anforderungen an Drittlands-Übermittlungen — 293
    - 1. Einhaltung der allgemeinen DSGVO-Anforderungen — 293
    - 2. Gewährleistung eines angemessenen Schutzniveaus — 294
    - 3. Verantwortlicher und Auftragsverarbeiter als Regelungsadressat — 294
  - III. Fortgeltung etablierter Sicherungsinstrumente — 295
- C. Länder mit angemessenem Schutzniveau — 296
  - I. Bestehende Angemessenheitsbeschlüsse — 296
    - 1. Einschränkungen bei Datentransfers nach Kanada — 298

2. Einschränkungen bei Datentransfers nach Israel — 298
3. Der Sonderfall USA: Die Zusatzanforderungen des EU-US Privacy Shield — 299
  - a) Hintergrund des Selbstzertifizierungsansatzes — 299
  - b) Von Safe Harbor zu EU-U.S. Privacy Shield — 299
  - c) Gegenstand und Anforderungen des EU-U.S. Privacy Shields — 300
  - d) Aktuelle Prüfpunkte bei Datentransfers in die USA — 301
  - e) Die Zukunft des EU-U.S. Privacy Shield — 303
- II. Neu zu treffende Angemessenheitsentscheidungen — 303
  1. Anforderungen an Angemessenheitsfeststellungen der Kommission — 304
  2. Das Verfahren der Angemessenheitsfeststellung — 304
- III. Fortlaufende Überwachung der Angemessenheit — 304
- D. Geeignete Garantien für Drittlandtransfers — 305
  - I. Standarddatenschutzklauseln — 305
    1. Existierende Standardvertragsklauseln — 306
      - a) EU-Standardvertragsklauseln für Übermittlungen an Verantwortliche — 306
      - b) EU-Standardvertragsklauseln für Übermittlungen an Auftragsverarbeiter — 307
    2. Standarddatenschutzklauseln einer Aufsichtsbehörde — 308
    3. Verwendung der Standarddatenschutzklauseln — 308
      - a) Änderungsverbot — 308
      - b) Ergänzungen und Einbettung in andere Vertragswerke — 309
      - c) Vertragsparteien — 310
      - d) Entbehrlichkeit behördlicher Genehmigung — 310
  - II. Verbindliche interne Datenschutzvorschriften (BCRs) — 311
    1. Anforderungen an BCRs — 313
      - a) Verbindlichkeit — 313
      - b) Drittbegünstigung — 313
      - c) Regelungsinhalte — 313
    2. Arbeitsdokumente der Art. 29-Datenschutzgruppe — 315
    3. Existierende BCR — 317
    4. Genehmigungsverfahren für BCR — 317
      - a) Abstimmung der BCR mit der zuständigen Aufsichtsbehörde — 317
      - b) Durchführung des Kohärenzverfahrens — 318
    5. Integration von BCR in ein Datenschutz-Managementsystem nach DSGVO — 319
      - a) Parallelen zu DSGVO-Anforderungen — 319
      - b) Nutzung von Ergebnissen aus der DSGVO-Umstellung — 321

- III. Genehmigte Verhaltensregeln — **322**
- IV. Zertifizierungen — **323**
- V. Sonstige behördlich genehmigte Vertragsklauseln — **324**
- E. Ausnahmen für bestimmte Fälle — **324**
  - I. Einwilligung der Betroffenen — **325**
    - 1. Ausdrückliche Erteilung der Einwilligung — **326**
    - 2. Notwendigkeit gesonderter Erteilung — **326**
    - 3. Informiertheit der Einwilligung — **326**
  - II. Erforderlichkeit für die Vertragserfüllung — **327**
  - III. Sonstige Ausnahmefälle — **328**
    - 1. Im Interesse der betroffenen Person geschlossener Vertrag — **328**
    - 2. Wichtige Gründe des öffentlichen Interesses — **328**
    - 3. Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen — **329**
    - 4. Schutz lebenswichtiger Interessen — **330**
    - 5. Übermittlungen aus einem Register — **330**
  - IV. Auffangregelung für Einzelübermittlungen — **331**
    - 1. Keine wiederholte Übermittlung — **331**
    - 2. Begrenzte Zahl betroffener Personen — **331**
    - 3. Zwingende berechnigte Interessen — **332**
    - 4. Keine überwiegenden Interessen der betroffenen Person — **332**
    - 5. Umfassende Beurteilung und angemessene Garantien — **332**
    - 6. Information der Aufsichtsbehörde — **332**

## **Kapitel 10**

### **Datenschutzmanagement**

- A. Überblick über die einschlägigen Regelungen der DSGVO — **335**
- B. Terminologie — **335**
- C. Anforderungen an das Datenschutzmanagement — **337**
- D. Risikoadäquates Datenschutzmanagement — **337**
  - I. Risikobewertung grundlegend — **337**
  - II. Kritikalität einer Datenverarbeitung — **337**
  - III. Konkrete Maßnahmen hängen vom Einzelfall ab — **339**
- E. Grundlegende Maßnahmen des Datenschutzmanagements — **340**
  - I. Einführung — **340**
  - II. Unternehmensrichtlinie zum Datenschutz — **340**
  - III. Datenschutzorganisation — **342**
  - IV. Datenschutzstrategie — **342**
  - V. Meldewege und Whistleblowing — **342**
  - VI. Auditierungen — **343**



- VII. Einzelfallprüfungen und -beratung — 343
- VIII. Schulungen — 343
- IX. Sonstige Maßnahmen — 344
- F. Datenschutzmanagementsystem — 344
  - I. Sinn eines Datenschutzmanagementsystems — 344
  - II. Gestaltung eines Datenschutzmanagementsystems — 345
    - 1. Orientierung an ähnlichen Systemen — 345
    - 2. Drei Säulen — 345
      - a) Vermeidung von Datenschutzverstößen — 346
      - b) Überwachung — 346
      - c) Verbessern des Datenschutzmanagementsystems — 346
    - 3. Schematische Darstellung eines Datenschutzmanagementsystems — 346
  - III. Aufbau eines Datenschutzmanagementsystems — 347

## Kapitel 11

### Datenschutzorganisation

- A. Überblick über die einschlägigen Regelungen der DSGVO — 349
- B. Ergänzende Regelungen des BDSG (2018) — 349
- C. Terminologie — 349
- D. Datenschutzorganisation als Voraussetzung von Datenschutzcompliance — 350
- E. Pflicht zur Errichtung einer Datenschutzorganisation — 350
  - I. Datenschutz-Grundverordnung — 350
    - 1. Gesetzliche Vorgaben — 350
    - 2. Konkrete Wertung — 352
      - a) Modifizierte Verhältnismäßigkeitsprüfung — 352
      - b) Senkung des Risikos von Datenschutzverstößen — 352
      - c) Implementierung gleich geeigneter Maßnahmen — 352
      - d) Angemessenheit der Datenschutzorganisation — 352
        - aa) Relevante Faktoren — 352
        - bb) Kritikalität der Datenverarbeitung — 353
        - cc) Wahrscheinlichkeit von Datenschutzverstößen — 353
        - dd) Aufwand der Etablierung einer Datenschutzorganisation — 353
  - II. Gesellschaftsrechtliche Verpflichtung in Deutschland — 354
  - III. Ordnungswidrigkeitenrecht — 354
  - IV. Fazit — 355
- F. Gestaltung einer Datenschutzorganisation — 356
  - I. Der Zweck einer Datenschutzorganisation — 356

- II. Aufgaben einer Datenschutzorganisation — 356**
  - 1. Vier grundlegende Aufgaben — 356**
  - 2. Beachtung und Anwendung des Datenschutzrechts im operativen Geschäft — 356**
  - 3. Beratung — 357**
  - 4. Richtlinienkompetenz — 357**
  - 5. Auditierung und Überwachung — 357**
- III. Elemente einer Datenschutzorganisation — 357**
  - 1. Einführung — 357**
  - 2. Die Geschäftsleitung — 358**
  - 3. Der Datenschutzbeauftragte — 358**
    - a) Die Funktion des Datenschutzbeauftragten — 358**
    - b) Pflicht zur Benennung eines Datenschutzbeauftragten — 358**
      - aa) Art. 37 Abs. 1 DSGVO und § 38 Abs. 1 BDSG (2018) im Überblick — 358**
      - bb) Kerntätigkeit — 360**
      - cc) Umfangreiche Datenverarbeitung — 361**
      - dd) Regelmäßige und systematische Überwachung — 362**
      - ee) Umfangreiche Verarbeitung besonders geschützter Daten — 363**
      - ff) Optionale Benennung eines Datenschutzbeauftragten, Art. 37 Abs. 4 DSGVO — 363**
      - gg) § 38 Abs. 1 BDSG (2018) — 364**
        - Mit der Datenverarbeitung beschäftigte Personen — 364**
        - Datenschutz-Folgenabschätzung — 365**
        - Geschäftsmäßige Verarbeitung — 365**
      - hh) Umgang mit bereits existierenden Datenschutzbeauftragten — 365**
    - c) Art und Weise der Bestellung und Veröffentlichung der Kontaktdaten — 366**
    - d) Gemeinsamer Konzernschutzbeauftragter, Art. 37 Abs. 2 DSGVO — 367**
    - e) Eigenschaften des Datenschutzbeauftragten — 369**
      - aa) Allgemeines — 369**
      - bb) Berufliche Qualifikation — 370**
      - cc) Fähigkeit zur Erfüllung seiner Aufgaben — 370**
      - dd) Interne und externe Datenschutzbeauftragte — 371**
    - f) Stellung des Datenschutzbeauftragten — 372**
      - aa) Unabhängigkeit grundlegend — 372**
      - bb) Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen — 372**

- cc) Verschaffung von Ressourcen und Zugang zur Datenverarbeitung — **375**
- dd) Welsungsfreiheit — **377**
- ee) Benachteiligung und Abberufung — **378**
- ff) Direkte Berichtslinie an oberste Managementebene — **380**
- gg) Ansprechpartner für alle Betroffenen — **381**
- hh) Pflicht zur Wahrung der Geheimhaltung und der Vertraulichkeit — **382**
- ii) Wahrnehmung anderer Aufgaben — **383**
- jj) Vermeidung von Interessenskonflikten — **383**
- g) Aufgaben des Datenschutzbeauftragten — **384**
  - aa) Überblick — **384**
  - bb) Unterrichtung und Beratung — **385**
  - cc) Überwachung — **385**
  - dd) Beratung bei Datenschutz-Folgenabschätzung — **387**
  - ee) Zusammenarbeit mit und Anlaufstelle der Aufsichtsbehörde — **387**
  - ff) Risikobasiertes Arbeiten — **388**
  - gg) Aufgabenallokation — **389**
  - h) Datenschutzbeauftragter als „Datenschutzzentrale“ — **390**
- 4. Datenschutzberater — **391**
- 5. Datenschutzmanager — **391**
- 6. Datenschutzexperten — **392**
- 7. Datenschutzkoordinatoren — **392**
- 8. Sonstige Mitarbeiter des Unternehmens — **393**
- 9. (Inländischer) Vertreter — **393**
- IV. Entwicklung einer Datenschutzorganisation — **394**
- G. Beispiele — **395**
  - I. Verwendung der Beispiele — **395**
  - II. Datenschutzorganisation in kleinen Unternehmen — **395**
  - III. Datenschutzorganisation in mittleren Unternehmen — **396**
  - IV. Datenschutzorganisation im Großkonzern — **397**

## **Kapitel 12**

### **Datenschutzprozesse**

- A. Überblick über die einschlägigen Regelungen — **401**
- B. Privacy by Design und by Default, Art. 25 DSGVO — **401**
  - I. Überblick über die einschlägigen Regelungen der DSGVO — **401**
  - II. Wer ist für Privacy by Design und by Default verantwortlich? — **402**
  - III. Was bedeutet Privacy by Design und by Default? — **403**

1. Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DSGVO — **403**
2. Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DSGVO — **404**
- IV. Praktische Hinweise zur Implementierung — **405**
- C. Datenlöschung — **406**
  - I. Geschäftliche Relevanz — **407**
  - II. Löschkonzept — **408**
  - III. Praktische Hinweise für die Implementierung — **410**
- D. Verzeichnis von Verarbeitungstätigkeiten — **411**
  - I. Überblick über die einschlägigen Regelungen der DSGVO — **412**
  - II. Aufzeichnungspflichten statt Meldepflicht und Verfahrensverzeichnis — **412**
  - III. Verarbeitungsverzeichnis des Verantwortlichen — **413**
    1. Wer ist zur Führung eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO verpflichtet? — **413**
    2. Inhalt des Verarbeitungsverzeichnisses — **415**
    3. Form des Verarbeitungsverzeichnisses — **418**
  - IV. Verarbeitungsverzeichnis des Auftragsverarbeiters — **419**
  - V. Praktische Hinweise zur Implementierung — **420**
- E. Datenschutz-Folgenabschätzung — **421**
  - I. Überblick über die einschlägigen Regelungen der DSGVO — **423**
  - II. Wer ist für eine Datenschutz-Folgenabschätzung verantwortlich? — **423**
  - III. Wann muss eine Datenschutz-Folgenabschätzung erfolgen? — **424**
    1. Voraussichtlich hohes Risiko (Art. 35 Abs. 1 S. 1 DSGVO) — **426**
      - a) Regelbeispiele (Art. 35 Abs. 3 DSGVO) — **427**
      - b) Positivliste der Aufsichtsbehörden (Art. 35 Abs. 4) — **428**
    2. Mögliche Befreiung von der Folgenabschätzung aufgrund bestimmter Verarbeitungszwecke (Art. 35 Abs. 10) — **429**
  - IV. Was muss im Rahmen der Folgenabschätzung passieren? — **429**
    1. Welche hohen Risiken sind zu adressieren (Art. 35 Abs. 1 DSGVO)? — **429**
    2. Welche technischen und organisatorischen Maßnahmen sind geeignet, um das Risiko zu minimieren? — **430**
    3. Welche Dokumentation der Folgenabschätzung ist erforderlich (Art. 35 Abs. 7 DSGVO)? — **431**
    4. Bedarf es der Beratung durch den Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO)? — **431**
    5. Müssen betroffene Person oder Vertreter (Art. 35 Abs. 9 DSGVO) eingebunden werden? — **432**
    6. Wann bedarf es der erneuten Überprüfung? — **433**

- 7. Welche Rolle spielt die Aufsichtsbehörde bei der Folgenabschätzung (Art. 36 Abs. 2 DSGVO)? — 433
- V. Praktische Hinweise zur Implementierung — 434
- F. Umgang mit Datenlecks — 436
  - I. Überblick über die einschlägigen Regelungen der DSGVO — 437
  - II. Meldepflichten (Art. 33 DSGVO) — 438
    - 1. Was muss gemeldet werden? (Art. 33 Abs. 1 DSGVO) — 439
    - 2. Bis wann muss gemeldet werden? (Art. 33 Abs. 1 S. 1 und 2 DSGVO) — 440
    - 3. Wie muss gemeldet werden? (Art. 33 Abs. 3 DSGVO) — 441
    - 4. Was tun bei Verzögerung? (Art. 33 Abs. 4 DSGVO) — 442
    - 5. Was muss in jedem Fall dokumentiert werden? (Art. 33 Abs. 5 DSGVO) — 443
    - 6. Welche Pflichten treffen den Auftragsverarbeiter? (Art. 33 Abs. 2 DSGVO) — 444
  - III. Benachrichtigungspflichten (Art. 34 DSGVO) — 444
    - 1. Wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) — 445
      - a) Hohes Risiko für die persönlichen Rechte und Freiheit der betroffenen Personen — 445
      - b) Voraussichtliches Risiko — 445
    - 2. Bis wann müssen betroffene Personen benachrichtigt werden? (Art. 34 Abs. 1 DSGVO) — 445
    - 3. Was muss die Benachrichtigung beinhalten und wie muss sie erfolgen? (Art. 34 Abs. 2 DSGVO) — 446
    - 4. Wann kann auf eine Benachrichtigung verzichtet werden? (Art. 34 Abs. 3 DSGVO) — 447
  - IV. Praktische Hinweise zur Implementierung — 448
- G. Integration des Datenschutzes in allgemeine Unternehmensprozesse — 449
  - I. Aufgaben der Datenschutzorganisation – eine Chance für vielfältige Integration in die Unternehmensprozesse — 449
    - 1. Governance — 449
    - 2. Hinwirken auf den Datenschutz — 450
      - a) Geschäftsberatung — 450
      - b) Datenschutz-Netzwerk — 450
      - c) Training und Ausbildung — 451
    - 3. Überwachung und Auditierung — 451
  - II. Definition von Unternehmensprozessen, in denen Datenschutzprozesse integriert werden — 452
    - 1. Definierte Datenschutzprozesse — 452
      - a) Zentrale Integration — 453

- b) Dezentrale Integration — 453
    - c) Auswahl des Integrationsansatzes — 453
  - 2. Risikobetrachtung — 454
    - a) Risikofelder — 454
    - b) In welchen Geschäftsprozessen spielen diese Risiken eine Rolle und können adressiert werden? — 455
  - 3. Typische Hüter der Anforderungen des Datenschutzes — 456
    - a) Einkauf — 456
    - b) IT und IT-Entwicklung — 457
    - c) Personalabteilung — 458
- III. Praktische Hinweise zur Implementierung — 460

## **Kapitel 13**

### **Technischer Datenschutz**

- A. Überblick über die einschlägigen Regelungen — 463
  - I. Art. 24, 32 DSGVO und Erwägungsgrund 83 — 464
  - II. ART. 24, 25 DSGVO und Erwägungsgrund 78 — 467
  - III. §§ 64, 65, 76 BDSG (2018) — 468
- B. Datenschutzkonforme sichere Datenverarbeitung — 469
  - I. Grundlegende Begriffe und Standards der Informationssicherheit — 470
    - 1. Terminologie — 470
    - 2. Zentrale Standards der Informationssicherheit — 472
  - II. Risikobasiertes Verfahren zur Herstellung der Informationssicherheit — 475
    - 1. Überblick — 476
    - 2. Gestaltung des risikobasierten Verfahrens — 476
      - a) Schutzbedarfsfeststellung — 478
      - b) Soll-Ist-Vergleich/Risiko-Assessment — 481
    - 3. Schutzmaßnahmen — 488
    - 4. Kontrolle und Prüfung — 488
    - 5. Behandlung von Sicherheitsvorfällen — 488
- III. Anpassung des risikobasierten Verfahrens zur Herstellung der datenschutzkonformen und sicheren Datenverarbeitung — 489
  - 1. Datenschutzziele — 490
    - a) Schutzziele der Datensicherheit nach der DSGVO — 490
      - aa) Schutzziel Vertraulichkeit — 490
      - bb) Schutzziel Integrität — 492
      - cc) Schutzziel Verfügbarkeit — 493
      - dd) Schutzziel Belastbarkeit der Systeme — 493
    - b) Weitere Schutzziele des Datenschutzes — 494

- 2. Anpassung des risikobasierten Verfahrens — 495
  - a) Anpassung der Schutzbedarfsfeststellung — 496
  - b) Anpassung des Soll-Ist-Vergleichs und Risiko-Assessments — 500
- 3. Ausgewählte Datenschutzmaßnahmen — 503
  - a) Anonymisierung — 504
  - b) Pseudonymisierung — 507
  - c) Kryptographische Verfahren – Verschlüsselung und Hash Funktionen — 511
  - d) Identitäts- und Berechtigungsmanagement — 515
  - e) Enterprise Information Management (EIM) — 516
  - f) Organisatorische Datenschutzmaßnahmen — 517
- 4. Ergänzung der Kontrolle und Prüfung — 517
- 5. Ergänzung der Behandlung von Sicherheitsvorfällen — 518
- IV. Einbeziehung von Privacy by Design und Privacy by Default (PbD) — 518
  - 1. Privacy Enhancing Technologies — 519
  - 2. PbD als Ergänzung des IT-Sicherheits- und IT-Risikomanagements — 520
  - 3. Integration von PbD in den Soll-/Ist Vergleich und in ein Risiko-Assessment — 520
- V. Ausblick — 521
  - 1. Anpassung des risikobasierenden Verfahrens mit Auditierung — 522
  - 2. Entwicklung von Verhaltensregeln — 522
  - 3. Datenschutzzeignung von Software und Zertifizierungen — 522

## Kapitel 14

### Verhaltensregeln und Zertifizierungen

- A. Einleitung — 523
- B. Grundsätzliche Unterscheidung und Komplementarität — 524
- C. Mehrwert für Unternehmen — 525
  - I. Einhaltung und Nachweis datenschutzkonformen Handelns — 526
  - II. Rechtskonkretisierungsfunktion — 527
  - III. Absicherung von Drittlandübermittlungen — 528
  - IV. Berücksichtigung bei der Bemessung von Sanktionen — 529
- D. Genehmigung von Verhaltensregeln — 530
  - I. Vorlageberechtigte Stellen — 530
  - II. Verhaltensregeln mit rein nationaler Wirkung — 530
  - III. Verhaltensregeln mit landesübergreifender Wirkung — 531
  - IV. Allgemeingültigkeitserklärung — 532
  - V. Gültigkeitsdauer — 532

- VI. Bindungswirkung genehmigter Verhaltensregeln — 532**
  - 1. Bindungswirkung gegenüber Aufsichtsbehörden — 533**
  - 2. Bindungswirkung gegenüber Gerichten — 534**
  - 3. Bindungswirkung gegenüber Unternehmen — 535**
- E. Überwachung genehmigter Verhaltensregeln/Sanktionen im Falle von Verstößen — 535**
- F. Inhalte und Gestaltung von Verhaltensregeln — 536**
  - I. Regelungsinhalte von Verhaltensregeln — 536**
  - II. Gestaltungsprozess in der Praxis — 538**
    - 1. Bedarfs- und Maßnahmenermittlung — 538**
    - 2. Ausarbeitung unter Beteiligung betroffener Interessenträger — 538**
- G. Zertifizierungsverfahren — 539**
  - I. Ablauf des Zertifizierungsverfahrens/Beteiligte Stellen — 539**
  - II. Regelungsinhalte und Prüfmaßstab — 540**
  - III. Bindungswirkung — 541**

## **Kapitel 15**

### **Beschäftigtendatenschutz**

- A. Überblick über die einschlägigen Regelungen der DSGVO — 543**
- B. Handlungsoptionen des Gesetzgebers — 544**
  - I. Reichweite des Art. 88 Abs. 1 DSGVO — 544**
    - 1. Spezifischere Vorschriften — 544**
    - 2. Personenbezogene Beschäftigtendaten — 544**
    - 3. Zwecke der Datenverarbeitung — 545**
  - II. Mindestanforderungen gem. Art. 88 Abs. 2 DSGVO — 546**
    - 1. Transparenz der Verarbeitung — 546**
    - 2. Datenübermittlung innerhalb einer Unternehmensgruppe — 547**
    - 3. Überwachungssysteme am Arbeitsplatz — 548**
  - III. Mitteilung gem. Art. 88 Abs. 3 DSGVO — 548**
  - IV. BDSG (2018) im Überblick — 548**
    - 1. Zentrale Vorschrift zum Beschäftigtendatenschutz — 549**
      - a) Beschäftigungsverhältnis und Aufklärung von Straftaten — 549**
      - b) Rechtausübung und Pflichterfüllung durch die Interessenvertretung — 549**
      - c) Datenschutzgrundsätze — 550**
      - d) Einwilligungen im Beschäftigungskontext — 550**
      - e) Besondere Kategorien personenbezogener Daten — 550**
      - f) Nicht-automatisierte Datenverarbeitung — 550**
      - g) Definition von „Beschäftigten“ — 551**
    - 2. Verhältnis zu den Vorgaben des Art. 88 DSGVO — 551**



- C. Datenschutzrechtliche Erlaubnistatbestände — 552
  - I. Einwilligung im Beschäftigungsverhältnis — 552
    - 1. Allgemeine Voraussetzungen einer wirksamen Einwilligung — 553
    - 2. Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis — 553
      - a) Gesetzgebungshistorie — 554
      - b) Freiwilligkeit in der DSGVO — 554
        - aa) Voraussetzungen für die Freiwilligkeit der Arbeitnehmereinwilligung — 555
        - bb) Indikatoren für eine freiwillige Entscheidung — 556
        - cc) Indikatoren für eine unfreiwillige Entscheidung — 556
      - c) Freiwilligkeit der Einwilligung unter dem neuen BDSG — 557
    - 3. Form der Einwilligung im Beschäftigungsverhältnis — 558
      - a) Anforderungen der DSGVO — 558
      - b) Schriftform der Einwilligung gem. BDSG (2018) — 558
  - II. Gesetzliche Erlaubnistatbestände — 559
    - 1. Vertragsdurchführung (Art. 6 Abs. 1 lit. b DSGVO) — 559
    - 2. Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO) — 560
    - 3. Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) — 561
    - 4. Besondere Kategorien von personenbezogenen Daten (Art. 9 Abs. 2 lit. b DSGVO) — 562
  - III. Betriebsvereinbarungen — 562
    - 1. Angemessene und besondere Schutzmaßnahmen — 562
      - a) Transparenz der Verarbeitung — 563
      - b) Datenübermittlung innerhalb einer Unternehmensgruppe — 564
      - c) Überwachungssysteme am Arbeitsplatz — 564
    - 2. Betriebsvereinbarung als Erlaubnistatbestand — 564
    - 3. Weitere Regelungen in Betriebsvereinbarungen — 565
    - 4. Bereits abgeschlossene Betriebsvereinbarungen — 566
  - IV. Datenaustausch in Matrixorganisationen — 566
    - 1. Erlaubnistatbestände — 567
    - 2. Gemeinsame Verantwortlichkeit — 568
- D. Informationspflichten und Betroffenenrechte — 568
  - I. Informationspflichten des Arbeitgebers — 568
  - II. Betroffenenrechte — 569
  - III. Profiling — 570
- E. Überwachungsmaßnahmen — 571
  - I. Kontrolle der Internet- und E-Mail-Nutzung — 571
    - 1. Erlaubnistatbestand — 571
    - 2. Kontrolle der dienstlichen Internet- und E-Mail-Nutzung — 571
    - 3. Arbeitgeber als Dienstanbieter — 572

- a) Keine Kontrollbefugnis bei erlaubter Privatnutzung — **572**
  - b) Keine Unterscheidung zwischen privater und dienstlicher Nutzung — **573**
- 4. Beweisverwertungsverbote — **574**
- II. Videoüberwachung — **575**
- F. Handlungsempfehlung — **576**

## **Kapitel 16**

### **Behördliche und gerichtliche Verfahren**

- A. Überblick über die einschlägigen Regelungen der DSGVO — **579**
- B. Aufsichtsbehörden — **579**
  - I. Überblick über die einschlägigen Normen — **579**
    - 1. DSGVO — **579**
    - 2. BDSG (2018) — **579**
  - II. Einleitung — **580**
  - III. Zuständigkeit innerhalb der Europäischen Union — **580**
  - IV. Zuständigkeit innerhalb Deutschlands — **581**
  - V. Europäischer Datenschutzausschuss — **582**
  - VI. Aufgaben und Befugnisse — **583**
    - 1. Aufgaben der Aufsichtsbehörden — **583**
    - 2. Befugnisse der Aufsichtsbehörden — **584**
      - a) Untersuchungsbefugnisse, Art. 58 Abs. 1 DSGVO — **586**
      - b) Abhilfebefugnisse, Art. 58 Abs. 2 DSGVO — **587**
      - c) Genehmigungs- und Beratungsbefugnisse, Art. 58 Abs. 3 DSGVO — **589**
      - d) Befugnisse nach dem BDSG (2018) — **589**
- C. Aufsichtsverfahren — **590**
  - I. Aufsichtsverfahren in Deutschland — **590**
  - II. Zusammenarbeit der Aufsichtsbehörden auf europäischer Ebene — **593**
    - 1. Grundsätzliche Zusammenarbeit zwischen federführender Aufsichtsbehörde und übrigen nationalen Aufsichtsbehörden — **594**
    - 2. Kohärenzverfahren im Falle von Unstimmigkeiten — **595**
  - III. Öffentliche Äußerungen von Behörden/Mediale Aufmerksamkeit — **597**
- D. Umgang mit Aufsichtsbehörden — **598**
  - I. Gründe für den Kontakt mit Aufsichtsbehörden — **598**
    - 1. Kontrolldichte — **598**
    - 2. Anfragen durch Aufsichtsbehörden — **599**
  - II. Bedeutung von Rechtspositionen der Datenschutzbehörden — **599**
  - III. Erste Maßnahmen nach Anfrage einer Aufsichtsbehörde — **601**

- IV. Sofortige Korrektur von festgestellten Rechtsverstößen — **601**
- V. Generelle Hinweise zur Interaktion mit Aufsichtsbehörden — **602**
- E. Bußgelder — **602**
  - I. Überblick über die einschlägigen Normen — **602**
    - 1. DSGVO — **602**
    - 2. BDSG (2018) — **603**
    - 3. OWiG und StPO — **603**
  - II. Bußgeldvorschriften der DSGVO — **603**
    - 1. Kategorisierung der Bußgelder und Strafvorschriften — **603**
    - 2. Referenztechnik — **604**
    - 3. Einzelne Tatbestände — **605**
  - III. Bemessung des Bußgeldes — **606**
  - IV. Straf- und Bußgeldvorschriften des BDSG (2018) — **608**
    - 1. Strafvorschriften — **608**
      - a) § 42 Abs. 1 BDSG (2018) — **609**
      - b) § 42 Abs. 2 BDSG (2018) — **611**
      - c) Antragsdelikte — **612**
    - 2. Bußgeldvorschriften — **612**
  - V. Adressat des Bußgeldes — **612**
    - 1. Verantwortliche Stelle, Auftragsverarbeiter und spezielle Stellen — **612**
    - 2. Bußgelder gegenüber einzelnen Personen innerhalb eines Unternehmens — **614**
    - 3. Bußgelder gegenüber Behörden — **614**
- F. Gerichtlicher Rechtsschutz — **615**
  - I. Überblick über die einschlägigen Normen — **615**
  - II. Verhältnis Betroffener – Verantwortlicher bzw. Auftragsverarbeiter — **615**
    - 1. Auskunftsanspruch und andere Betroffenenrechte — **616**
    - 2. Unterlassungsanspruch — **616**
    - 3. Schadensersatzanspruch — **617**
  - III. Verhältnis Verantwortlicher bzw. Auftragsverarbeiter – Aufsichtsbehörde — **619**
    - 1. Rechtsschutzgarantie unter der DSGVO — **619**
    - 2. Konkreter Rechtsschutz nach deutschem Verfahrensrecht — **620**
  - IV. Sonderfall: Beschlüsse des Europäischen Datenschutzausschusses — **623**
  - V. Vorgehen gegen öffentliche Äußerungen der Datenschutzbehörden — **623**
- G. Verbandsklage — **625**
  - I. Überblick über die einschlägigen Normen — **625**
  - II. Art. 80 DSGVO — **626**

1. Art. 80 Abs. 1 DSGVO — **626**
  - a) Grundgedanke der Norm — **626**
  - b) Erfasste Rechte — **626**
  - c) Durchsetzungsberechtigte Stellen — **627**
2. Art. 80 Abs. 2 DSGVO — **628**
- III. § 2 Abs. 2 S. 1 Nr. 11 UKlaG — **628**

## **Kapitel 17**

### **Besondere Themenkomplexe**

- A. Web Tracking und Online Advertising — **631**
  - I. Technische Abläufe — **632**
  - II. Datenschutzrechtliche Zulässigkeit des Web Tracking und des Online Advertising — **634**
    1. Verarbeitung personenbezogener Daten/anonymer Daten — **635**
    2. Anwendbare datenschutzrechtliche Regelungen — **637**
    3. Zulässigkeit des Web Tracking zu Zwecken des Online Advertising nach § 15 Abs. 3 TMG bzw. Art. 6 Abs. 1 lit. f DSGVO — **638**
    4. Zulässigkeit des Web Tracking zu Zwecken des Online Advertising auf Basis einer Einwilligung — **643**
      - a) Form der Einwilligung — **643**
      - b) Informiertheit der Einwilligung — **645**
      - c) Kopplung der Nutzung einer Webseite an die Erteilung der Einwilligung — **646**
      - d) Freiwilligkeit der Einwilligungserteilung vs. klares Ungleichgewicht — **647**
    5. Zulässigkeit des Web Tracking zu Zwecken der Erbringung/ bedarfsgerechten Gestaltung des Dienstes — **648**
      - a) Web Tracking zu Zwecken der Erbringung des Dienstes — **648**
      - b) Web Tracking zu Zwecken der bedarfsgerechten Gestaltung des Dienstes — **649**
- B. Customer Relationship Management — **650**
  - I. Überblick über die einschlägigen Regelungen — **650**
  - II. Datenquellen — **651**
  - III. Profiling zu Werbezwecken — **653**
    1. Interessenabwägung — **654**
    2. Zweckändernde Verarbeitung — **656**
    3. Keine Anwendung von Art. 22 DSGVO — **657**
    4. Einwilligung — **657**

- IV. Werbliche Kommunikation mit Kunden — 658**
  - 1. Briefwerbung — 658**
    - a) Interessenabwägung/Zweckänderung — 658
    - b) Einwilligung — 659
  - 2. Direktwerbung über elektronische Post, Anrufautomaten und Fax — 660**
  - 3. Persönliche Telefonwerbung — 661**
  - 4. Zusammenfassung — 662**
- C. E-Discovery — 664**
  - I. Ausgewählte Rahmenbedingungen — 665**
    - 1. Federal Rule of Civil Procedure der Vereinigten Staaten — 665**
    - 2. Sedona Konferenzen, Frameworks und Arbeitsgruppen — 667**
    - 3. Leitlinien der Artikel-29-Datenschutzgruppe — 668**
  - II. Kollision mit dem Datenschutz bei Umsetzung des Beweissicherungsprozesses — 668**
    - 1. Grundlage: Das e-Discovery Referenzmodell (EDRM) — 669**
    - 2. Grundlage: Information Management und Governance — 669**
    - 3. Durchführung des e-Discovery Prozesses mit dem Referenzmodell — 670**
      - a) Identifikationsphase (Identification) — 670
      - b) Phase der Extraktion und Sicherung (Collection and Preservation) — 671
        - aa) Identifikation der Risiken und der risikobehafteten Daten — 671
        - bb) Entwicklung der Suchstrategie, Suche, Prüfung, Qualitätskontrolle und Aussonderung — 674
        - cc) Überprüfung der Verletzung von Löschverpflichtungen — 675
      - c) Phase der Bearbeitung (Processing, Review and Analysis) — 675
      - d) Phase der Weitergabe und Nutzung (Production and Presentation) — 675
  - III. Fazit — 678**
- D. Cloud Computing — 678**
  - I. Eigenschaften und Terminologie — 678**
  - II. Cloud-spezifische Problemfelder — 680**
- E. Big Data — 683**
  - I. Eigenschaften und Terminologie — 683**
  - II. Big Data-spezifische Problemfelder — 684**
    - 1. Personenbezug — 684**
    - 2. Zweckbindung — 685**

- 3. Datenminimierung — **686**
- 4. Betroffenenrechte — **686**
  - a) Informationspflichten — **686**
  - b) Auskunftsrecht — **687**
- F. Gesundheitsdatenschutz — **688**
  - I. Definition „Gesundheitsdaten“ — **688**
  - II. Systematik der datenschutzrechtlichen Regelungen im Gesundheitsbereich — **690**
  - III. Zulässigkeit der Verarbeitung von Gesundheitsdaten auf Basis von Vorschriften aus der DSGVO — **693**
    - 1. Verarbeitung von Gesundheitsdaten auf Basis einer Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) — **694**
      - a) Allgemeine Anforderungen an die Einwilligung — **694**
      - b) Freiwilligkeit der Einwilligung gem. Art. 4 Nr. 11 und Art. 7 Abs. 4 DSGVO — **695**
      - c) Ausschluss der Einwilligung gem. Art. 9 Abs. 2 lit. a DSGVO — **697**
    - 2. Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung (Art. 9 Abs. 2 lit. b, Abs. 3 DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b, Abs. 2 BDSG (2018)) — **698**
      - a) Zwecke nach § 22 Abs. 1 lit. b BDSG (2018) — **698**
        - aa) Vertrag mit einem Angehörigen eines Gesundheitsberufs — **698**
        - bb) Gesundheitsvorsorge — **700**
        - cc) Medizinische Diagnostik — **700**
        - dd) Versorgung oder Behandlung im Gesundheits- oder Sozialbereich — **700**
        - ee) Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich — **700**
      - b) Verarbeitung durch ärztliches Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung — **701**
      - c) Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gem. § 22 Abs. 2 BDSG (2018) — **702**
    - 3. Verarbeitung von Gesundheitsdaten im Beschäftigungskontext (Art. 9 Abs. 2 lit. b DSGVO, § 26 Abs. 3 und 4 BDSG (2018)) — **703**
  - IV. Weitere Besonderheiten nach der DSGVO bei der Verarbeitung von Gesundheitsdaten — **704**
  - V. (Berufsrechtliche) Schweigepflicht — **705**
  - VI. Verarbeitung zu wissenschaftlichen Forschungszwecken — **708**

1. Zulässigkeit der Verarbeitung von Gesundheitsdaten zu Zwecken der wissenschaftlichen Forschung — **709**
  - a) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken gem. Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 Abs. 1 BDSG (2018) — **709**
  - b) Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken auf Basis einer Einwilligung — **711**
2. Weitere Besonderheiten bei der Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken — **712**

## Kapitel 18

### Vorgehensweise zur Umsetzung der DSGVO im Unternehmen

- A. Anpassungsbedarf im Unternehmen — **715**
- B. Leitbild zur Umsetzung der DSGVO im Unternehmen — **715**
- C. Ausgestaltung eines Umsetzungsprojekts — **716**
  - I. Vorbereitung — **716**
    1. Welche Abteilung bzw. welche Person ist unternehmensintern für die Einführung der DSGVO verantwortlich? — **716**
    2. Welche datenschutzrechtlichen Vorschriften sollen konkret umgesetzt werden? — **717**
    3. Auf welche verantwortlichen Stellen bezieht sich das Umsetzungsprojekt genau? — **717**
    4. Sollte die DSGVO im Unternehmen global umgesetzt werden? — **718**
    5. Welche Ressourcen stehen zur Verfügung? — **718**
    6. Soll die Implementierung durch interne oder externe Ressourcen erfolgen? — **719**
    7. Welche Abteilungen sollten involviert bzw. informiert werden? — **719**
    8. Bis wann sollte die DSGVO im Unternehmen umgesetzt sein? — **719**
    9. Kann die Umsetzung der DSGVO im Unternehmen auch als Chance wahrgenommen werden? — **720**
  - II. Anforderungsspezifizierung — **721**
  - III. Gap-Analyse — **722**
    1. Vorbereitung der Gap-Analyse — **722**
    2. Durchführung der Gap-Analyse — **722**
    3. Ergebnis der Gap-Analyse — **723**
  - IV. Planung von Ressourcen — **724**
    1. Planung von Budget — **724**
    2. Planung von Mitarbeitern — **724**
    3. Zeitplan — **725**

- V. Implementierung — 725**
  - 1. Definition von Unterprojekten — 725**
  - 2. Bestimmung von Meilensteinen und Abhängigkeiten — 726**
  - 3. Durchführung der Unterprojekte — 726**
- VI. Testing und Monitoring — 727**
- VII. Kommunikation und Training — 728**
  - 1. Interne Unternehmenskommunikation — 728**
  - 2. Mitarbeiterschulungen — 728**
- D. Fazit — 729**

## **Kapitel 19**

### **Weitere rechtliche Entwicklungen und Ausblick**

- A. Datenschutzrecht als dynamisches Rechtsgebiet — 731**
- B. Gesetzgeber — 731**
  - I. Rechtsakte der Europäischen Kommission — 732**
    - 1. Delegierte Rechtsakte — 732**
    - 2. Durchführungsrechtsakte — 732**
  - II. Begleitgesetze der Mitgliedsstaaten — 734**
  - III. E-Privacy Verordnung — 734**
- C. Datenschutzbehörden — 735**
  - 1. Europäischer Datenschutzausschuss — 735**
  - 2. Black- und Whitelists für Datenschutzfolgenabschätzung — 736**
  - 3. Musterverträge — 736**
  - 4. Konkretisierung von Pflichten nach der DSGVO — 736**
- D. Rechtsprechung — 737**
- E. Entwicklung der Datenschutzpraxis — 738**
- F. Ausblick — 738**

### **Sachregister — 741**