

Inhaltsübersicht

Abkürzungsverzeichnis — **XXXV**

Literaturverzeichnis — **XLIII**

Bearbeiterverzeichnis — **LI**

Kapitel 1

Datenschutz im Unternehmen – Von lästiger Pflicht zur grundlegenden Organisationsaufgabe des Compliance-Managements

A. Entwicklung — **1**

B. Anforderungen an eine Datenschutzorganisation — **3**

C. Sanktionen — **24**

Kapitel 2

Grundlagen des Datenschutzes im Unternehmen

A. Zur Ausgangslage — **31**

B. Der Schutzanspruch der Betroffenen — **32**

C. Die europarechtlichen Vorgaben — **34**

D. Die datenschutzrechtlichen Grundprinzipien — **35**

E. Bereichsspezifische Regelungen — **37**

F. Datenschutz und unlauterer Wettbewerb — **38**

G. Normadressaten und Verantwortlichkeiten — **40**

H. Die gesetzlichen Kontrollorgane — **41**

I. Vermögensrechtliche Haftung — **42**

J. Ordnungs- und strafrechtliche Sanktionen — **44**

K. Zertifizierung und Vorteil im Wettbewerb — **44**

Kapitel 3

Der betriebliche Datenschutzbeauftragte – Verantwortlichkeiten, Aufgaben und Status

A. Verantwortlichkeiten – Allgemeines — **47**

B. Aufgaben — **58**

C. Status — **82**

Kapitel 4

Outsourcing datenschutzkonform ausgestalten

A. Outsourcing und Datenschutz — **93**

B. Auftragsdatenverarbeitung und Outsourcing — **98**

- C. Bereichsausnahmen, Subsidiarität, Compliance — **117**
- D. Outsourcingnehmer im Ausland — **126**
- E. Auftraggeber im Drittland — **148**
- F. EU Datenschutz-Grundverordnung — **148**
- G. Outsourcing und Cloud Computing — **151**

Kapitel 5

Datenverarbeitung im (internationalen) Konzern

- A. Einwilligung, Rechtsvorschriften und Datenschutzrichtlinien (Betriebsvereinbarungen; BCR) — **181**
- B. Problem der grenzüberschreitenden E-Discovery — **254**

Kapitel 6

Telekommunikation im Unternehmen – Was ist erlaubt, was ist verboten?

- A. Einleitung — **283**
- B. Zugriffsgründe und -arten — **283**
- C. Zulässigkeit von Zugriffen — **285**

Kapitel 7

Die Website – Datenschutzerklärung, Impressum & Co.

- A. Einleitung — **323**
- B. Datenschutzerklärung — **323**
- C. Impressum — **341**

Kapitel 8

Umgang mit Beschäftigtendaten – Von der Bewerbung bis zur Kündigung

- A. Einführung — **353**
- B. Datenschutz im Anbahnungsverhältnis — **359**
- C. Datenschutz im Beschäftigungsverhältnis — **395**
- D. Verarbeitung bei und nach Beendigung des Beschäftigungsverhältnisses — **428**
- E. Datenverarbeitungen durch den Betriebsrat — **435**

Kapitel 9

Unternehmensinterne Ermittlungen datenschutzkonform ausgestalten

- A. Rechtlicher Rahmen und operatives Vorgehen — **441**

- B. Zusammenfassende rechtliche Einordnung von Einzelermittlungsmaßnahmen — 476

Kapitel 10

Nutzung von Kundendaten – Werbung, Kundenbetreuung und CRM on- und offline rechtssicher gestalten

- A. Werbung — 486
- B. Customer Relationship Management — 566

Kapitel 11

Datenschutz im Credit Management

- A. Einleitung — 571
- B. Prozesse vor der Entstehung von Forderungen — 572
- C. Maßnahmen während bestehender Kundenbeziehungen — 590
- D. Datenverwendung nach Vertragsbeendigung — 607
- E. Transparenzpflichten — 610

Kapitel 12

Die technisch-organisatorischen Maßnahmen des Datenschutzes – von der Theorie zur Praxis

- A. Anwendbarkeit des BDSG und Einordnung der technisch-organisatorischen Maßnahmen — 617
- B. Datenschutz und Informationssicherheit — 618
- C. Technisch-organisatorische Maßnahmen — 625
- D. Umsetzung der technisch-organisatorischen Maßnahmen — 657
- E. Zusammenfassung — 670

Kapitel 13

Zertifizierungen – Arten und Nutzen

- A. Motivation und Zielsetzung — 673
- B. Rechtlicher Rahmen — 675
- C. Begriffsklärung — 677
- D. Anforderungen an Zertifikate — 680
- E. Unternehmenszertifizierungen — 682
- F. Produktzertifizierungen — 698
- G. Fazit und Ausblick — 699

Kapitel 14

Ausblick

A. Mögliche gesetzgeberische Entwicklungen — **701**

B. Fazit — **711**

Stichwortverzeichnis — 713

Inhaltsverzeichnis

Abkürzungsverzeichnis — XXXV

Literaturverzeichnis — XLIII

Bearbeiterverzeichnis — LI

Kapitel 1

Datenschutz im Unternehmen – Von lästiger Pflicht zur grundlegenden Organisationsaufgabe des Compliance-Managements

A. Entwicklung — 1

B. Anforderungen an eine Datenschutzorganisation — 3

I. Vorgaben des BDSG — 4

1. Datenschutzbeauftragter und -koordinatoren — 5

2. Vorabkontrolle sowie allgemeine Prüfungs- und Meldeprozesse — 6

3. Melde- und Prüfprozesse für den Fall rechtswidriger Datenabflüsse — 8

4. Auskunft-, Unterrichts- und Benachrichtigungsprozesse — 9

5. Berichtigungs-, Löscho- und Sperrprozesse — 12

6. Schulungen — 14

7. Aufsichtsbehördliche Anforderungen — 15

II. Allgemeine Compliance-Vorgaben — 16

1. Berichterstattung — 16

2. Aufdeckung und Sanktionen — 16

III. Vorgaben mit Blick auf den aktuellen EU-Parlamentsvorschlag für eine Datenschutz-Grundverordnung (DS-GVO-V) — 17

1. „Privacy by design“ und „privacy by default“ — 17

2. Datenschutz-Risikoanalyse, -Folgenabschätzung und -Compliance-Review — 18

3. Recht auf Vergessenwerden — 21

4. Recht auf Datenübertragbarkeit — 23

C. Sanktionen — 24

I. Behördliche Sanktionspraxis — 24

II. Sanktionsrahmen im Einzelnen und sonstige Konsequenzen — 25

1. Zivilrechtliche Haftung — 25

2. Straf- bzw. ordnungswidrigkeitsrechtliche Haftung — 26

3. Wettbewerbsrecht und Verbraucherschutz — 29

Kapitel 2

Grundlagen des Datenschutzes im Unternehmen

A. Zur Ausgangslage — 31

- B. Der Schutzanspruch der Betroffenen — 32**
- C. Die europarechtlichen Vorgaben — 34**
- D. Die datenschutzrechtlichen Grundprinzipien — 35**
- E. Bereichsspezifische Regelungen — 37**
- F. Datenschutz und unlauterer Wettbewerb — 38**
- G. Normadressaten und Verantwortlichkeiten — 40**
- H. Die gesetzlichen Kontrollorgane — 41**
- I. Vermögensrechtliche Haftung — 42**
- J. Ordnungs- und strafrechtliche Sanktionen — 44**
- K. Zertifizierung und Vorteil im Wettbewerb — 44**

Kapitel 3

Der betriebliche Datenschutzbeauftragte – Verantwortlichkeiten, Aufgaben und Status

- A. Verantwortlichkeiten – Allgemeines — 47**
 - I. Wer muss einen Datenschutzbeauftragten bestellen? — 47**
 - 1. Einzelunternehmen — 47**
 - 2. Ausnahmen im nicht-öffentlichen Bereich — 48**
 - a) Private Datenverarbeitung — 48**
 - b) Anzahl der Mitarbeiter — 48**
 - c) Welche Personen zählen? — 48**
 - d) Zeitpunkt — 49**
 - 3. Nationale Konzerne — 49**
 - 4. Internationale Konzerne — 50**
 - II. Auswahl und Bestellung — 52**
 - 1. Notwendige Qualifikation — 52**
 - 2. Formalien der Bestellung — 53**
 - a) Befristung — 54**
 - b) Haupt- oder nebenamtlich — 55**
 - 3. Ausstattung und Größe der Datenschutzabteilung — 56**
 - III. Pflichten der verantwortlichen Stelle — 56**
 - 1. Unterstützung bei den Aufgaben des Datenschutzbeauftragten — 56**
 - 2. Benachteiligungsverbot — 57**
 - 3. Fort- und Weiterbildung — 57**
 - 4. Verfahrensverzeichnis — 58**
- B. Aufgaben — 58**
 - I. Hinwirken auf den Datenschutz — 58**
 - 1. Ansprechpartner für das Unternehmen und die Mitarbeiter — 58**
 - 2. Verpflichtung auf das Datengeheimnis — 60**
 - 3. Datenschutzrechtliche Regelwerke — 60**
 - II. Überwachung der Datenverarbeitungsprogramme — 61**

1.	Vorabkontrollen —	61
2.	Verfahrensmeldung/Verfahrensverzeichnis —	63
3.	Interne Prüfungen —	64
4.	Zusammenarbeit mit dem Betriebsrat und dem Fachbereich IT-Sicherheit —	65
	a) Betriebsrat —	65
	b) Fachbereich IT-Sicherheit —	67
5.	Einbindung von Dritten/Outsourcing —	68
	a) Begründung einer Auftragsdatenverarbeitung —	69
	b) Regelmäßige Kontrollen der Auftragsdatenverarbeiter —	70
III.	Schulung der Mitarbeiter —	71
1.	Schulungsinstrumente —	72
2.	Schulungen für neue Mitarbeiter —	73
3.	Regelmäßigkeit der Schulungen —	73
IV.	Auskunftsersuchen von Betroffenen —	74
V.	Zusammenarbeit mit der Aufsichtsbehörde —	74
1.	Einzelanfragen —	75
	a) Allgemeine Anfragen —	75
	b) Konkrete Anfragen zu bestimmten Datenverarbeitungen —	76
	c) Datenschutzverstöße —	76
2.	Genehmigungsverfahren und Abstimmungen —	77
3.	Betriebsprüfungen —	79
4.	Auskunfts- und Einsichtsrecht —	79
5.	Aussageverweigerungsrecht —	81
6.	Anordnungen der Aufsichtsbehörde —	81
VI.	Erstellung eines Datenschutzberichts —	82
C.	Status —	82
I.	Stellung als interner Datenschutzbeauftragter —	82
II.	Stellung als externer Datenschutzbeauftragter —	83
III.	Organisatorische Stellung im Unternehmen —	84
IV.	Weisungsrechte —	86
V.	Verschwiegenheitspflicht —	86
VI.	Zeugnisverweigerungsrecht/Beschlagnahmeverbot —	87
VII.	Haftung —	87
1.	Arbeits- oder allgemein zivilrechtliche Schadensersatzansprüche —	88
2.	Strafrechtliche Verantwortung —	89
VIII.	Abberufung des Datenschutzbeauftragten —	90

Kapitel 4

Outsourcing datenschutzkonform ausgestalten

A.	Outsourcing und Datenschutz —	93
----	-------------------------------	----

- I. Einleitung — **93**
- II. Verbreitung und Bedeutung — **95**
- B. Auftragsdatenverarbeitung und Outsourcing — **98**
 - I. Einleitung — **98**
 - II. Abgrenzungsfragen — **100**
 - 1. Auftragsdatenverarbeitung vs. Funktionsausgliederung — **100**
 - 2. Datenschutzrechtliche Anforderungen an ein Outsourcing mittels Funktionsausgliederung — **103**
 - 3. Mehrfache oder überschneidende Zweckbestimmung — **106**
 - III. Vertragliche Grundlagen einer Auftragsdatenverarbeitung — **106**
 - 1. Schriftformerfordernis — **107**
 - 2. Vertragliche Anforderungen an eine zulässige und wirksame Auftragsdatenverarbeitung — **107**
 - IV. Pflichten des Auftraggebers — **108**
 - 1. Auswahl- und Kontrollpflichten — **109**
 - 2. Vor-Ort-Kontrolle beim Auftragnehmer — **110**
 - 3. Dokumentation — **111**
 - 4. Verantwortlichkeit und Zuständigkeit — **112**
 - V. Pflichten des Auftragnehmers — **112**
 - VI. Vertragliche Gestaltung — **114**
 - 1. Mindestinhalt — **114**
 - 2. Weitergehende Duldungs- und Mitwirkungspflichten des Auftraggebers — **114**
 - 3. Sonstige zentrale Regelungsgegenstände — **115**
 - VII. Technische und organisatorische Maßnahmen — **115**
 - VIII. Unterbeauftragung — **115**
 - IX. Prüfung und Wartung automatisierter Verfahren — **116**
 - X. Rechtsfolgen — **116**
 - 1. Wirksame Auftragsdatenverarbeitung — **116**
 - 2. Unwirksame Auftragsdatenverarbeitung — **117**
 - XI. Landesrecht — **117**
- C. Bereichsausnahmen, Subsidiarität, Compliance — **117**
 - I. Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, Ärzte — **118**
 - II. Banken, Finanzsektor — **120**
 - III. Öffentlicher Sektor, Gesundheits- und Krankenhauswesen — **121**
 - 1. Kernbereichstheorie — **121**
 - 2. Sonderregelungen — **122**
 - IV. Versicherungen — **124**
 - V. Telekommunikation — **124**
 - VI. Exportbeschränkungen und weitere Compliance-Anforderungen — **125**
- D. Outsourcingnehmer im Ausland — **126**
 - I. Allgemein: EU/EWR contra Drittstaaten — **128**

1. Auftragnehmer mit Sitz in EU/EWR — **129**
2. Auftragnehmer mit Sitz in „sicheren Drittstaaten“ — **129**
 - a) Angemessenheit des Datenschutzniveaus — **129**
 - b) Sonderfall USA: Safe-Harbor-Abkommen und PRISM — **132**
 - c) Erlaubnisvorbehalt — **135**
3. Auftragnehmer mit Sitz in „unsicheren Drittstaaten“ — **135**
 - a) Binding Corporate Rules — **136**
 - aa) Ebene des Auftraggebers — **136**
 - bb) Ebene des Auftragsdatenverarbeiters — **136**
 - b) EU-Standardverträge — **137**
 - aa) Abänderungen der Standardvertragsklauseln — **139**
 - bb) Standardvertragsklauseln „Controller-to-Controller, Set I“ und „Set II“ — **142**
 - cc) Standardvertragsklauseln Controller-to-Processor — **144**
- II. Auftragsdatenverarbeitung im (internationalen) Konzern — **146**
- III. Datenschutzbeauftragter beim Auftragsdatenverarbeiter — **147**
- IV. Cloud Computing — **147**
- E. Auftraggeber im Drittland — **148**
- F. EU Datenschutz-Grundverordnung — **148**
- G. Outsourcing und Cloud Computing — **151**
 - I. Hintergrund, Entwicklung — **153**
 - II. Ebenen und Organisationsformen des Cloud Computings — **155**
 1. Ebenen des Cloud Computings — **155**
 2. Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud — **156**
 - III. Wesentliche Risiken des Cloud Computings — **157**
 - IV. Vertrags- und Zivilrecht — **158**
 1. Vertragstypologie und Vertragsgestaltung — **158**
 2. Anwendbares Recht — **160**
- V. Datenschutzrecht — **160**
 1. Anwendbares Datenschutzrecht — **161**
 2. Reine EU-Clouds — **162**
 3. Clouds (auch) in Drittstaaten — **162**
 4. EU Datenschutz-Grundverordnung — **163**
 5. Datenübermittlung oder Auftragsdatenverarbeitung — **164**
 6. Anforderungen an ein zulässiges Outsourcing in die Cloud — **165**
 7. Outsourcing in Drittländer-Clouds — **168**
 - a) Cloud-Anbieter mit Sitz in EU/EWR — **170**
 - b) Cloud-Anbieter mit Sitz in „sicheren Drittstaaten“ — **170**
 - aa) Safe Harbor-Abkommen — **171**
 - bb) EU-Standardvertragsklauseln — **173**
 - cc) Binding Corporate Rules — **173**
 - (a) Ebene des Cloud-Anwenders — **173**

- (b) Ebene des Cloud-Anbieters — **173**
 - c) Cloud-Anbieter mit Sitz in „unsicheren Drittstaaten“ — **174**
 - d) Rechtfertigung — **174**
 - e) EU Datenschutz-Grundverordnung — **175**
 - f) Datensicherheit — **176**
- 8. Bereichsspezifische Nutzung — **176**
 - a) Nutzung durch die öffentliche Hand — **176**
 - aa) Auslagerung in die Cloud durch Behörden — **176**
 - bb) Gesundheitswesen und Sozialleistungen — **176**
 - cc) Vergaberecht — **176**
 - b) Berufsrecht, elektronische Handakte — **177**
 - c) Finanzsektor, MaRisk — **177**
 - d) Versicherungsbranche — **178**
 - e) Telekommunikation — **178**

Kapitel 5

Datenverarbeitung im (internationalen) Konzern

- A. Einwilligung, Rechtsvorschriften und Datenschutzrichtlinien (Betriebsvereinbarungen; BCR) — **181**
 - I. Einwilligung, Betriebsvereinbarung und Rechtsvorschriften als Grundlage konzerninterner Datentransfers — **181**
 - 1. Konzerninterner Austausch personenbezogener Daten: „Auftragsdatenverarbeitung“ oder „Übermittlung“ — **181**
 - 2. Beispiele und Grenzen der Auftragsdatenverarbeitung im Konzern — **185**
 - a) Konzernweites Rechenzentrum — **185**
 - b) Personalverwaltung, Personalinformationssysteme — **185**
 - c) Lohn- und Gehaltsabrechnung — **187**
 - d) Werkschutz — **187**
 - e) Kundenbetreuung durch konzerneigenes Call-Center — **187**
 - f) Reisemanagement und Reisekostenabrechnung — **188**
 - g) Grenzen der Auftragsdatenverarbeitung im Konzern — **188**
 - 3. Konzerninterne Übermittlungen personenbezogener Daten — **189**
 - a) Einwilligung: Taugliche Rechtsgrundlage für konzerninterne Übermittlungen? — **192**
 - b) Betriebsvereinbarung als Rechtsgrundlage für Übermittlungen — **194**
 - aa) Betriebsvereinbarung als „Rechtsvorschrift“ gem. § 4 Abs. 1 BDSG — **194**
 - bb) Betriebsvereinbarungen: praxistaugliche Rechtsgrundlage für Übermittlungen innerhalb eines Konzerns? — **196**

- c) Übermittlungen auf der Grundlage gesetzlicher Vorschriften bei nicht-sensitiven personenbezogenen Daten — **198**
 - aa) Zentralisierung von Aufgaben der Personalverwaltung — **201**
 - bb) Konzernweites Namens-, Telefon-, E-Mail-Verzeichnis — **204**
 - cc) „Konzernbezogene Beschäftigungsverhältnisse“ und Matrix-Strukturen — **205**
 - dd) „Skill-Datenbanken“ — **207**
 - ee) Konzerninterne Übermittlung von Kundendaten — **207**
 - d) Übermittlungen auf der Grundlage gesetzlicher Vorschriften bei sensitiven personenbezogenen Daten gem. § 3 Abs. 9 BDSG — **208**
- 4. Zusätzliche Anforderungen für Übermittlungen in Drittstaaten — **210**
 - a) Drittstaaten mit angemessenem Datenschutzniveau — **210**
 - b) Sonderfall USA: Safe Harbor — **211**
 - c) Ausnahmetatbestände gem. § 4c Abs. 1 BDSG — **213**
 - d) EU-Standardvertragsklauseln — **214**
 - e) Individuelle Verträge zur Erbringung ausreichender Datenschutzgarantien — **215**
 - f) Binding Corporate Rules — **215**
 - g) Zusammenfassung — **216**
- II. Binding Corporate Rules — **217**
 - 1. Sinn und Zweck von BCR — **217**
 - 2. Vorüberlegungen zur Einführung von BCR in einer Unternehmensgruppe — **220**
 - a) Sind BCR überhaupt das passende Instrument? — **220**
 - b) BCR liefern keine Rechtsgrundlage für die „erste Stufe“ der Datenübermittlung — **221**
 - 3. Anerkennung der BCR als angemessene Datenschutzgarantien sowie Genehmigungserteilung für Datenexporte auf der Grundlage von BCR — **222**
 - a) Schritt 1: Verfahren zur Anerkennung der BCR als ausreichende Garantien — **222**
 - aa) Auswahl der federführenden Behörde; Sprache der BCR — **222**
 - bb) Weiterer Ablauf des BCR-Anerkennungsverfahrens — **225**
 - b) Schritt 2: Einholung von Genehmigungen für die einzelnen Datenexporte — **226**
 - 4. Inhaltliche und weitere Anforderungen an BCR — **228**
 - a) Verbindlichkeit der BCR; Haftung — **230**
 - aa) Interne Verbindlichkeit gegenüber den Gruppenmitgliedern — **230**
 - (1) Vertragliche Regelungen — **231**

- (2) Gestaltung als unternehmensinterne Regelungen (z. B. Konzernrichtlinien) — **232**
 - (3) Einseitige Erklärungen — **233**
 - bb) Interne Verbindlichkeit gegenüber den Mitarbeitern — **234**
 - cc) Externe Verbindlichkeit (rechtliche Durchsetzbarkeit von außen) — **236**
 - dd) Haftung — **238**
 - b) Definition des Anwendungsbereichs — **238**
 - c) Beschreibung der Datenverarbeitungen und -übermittlungen — **240**
 - d) Datenschutzgrundsätze — **241**
 - aa) Transparenz und Fairness gegenüber den Betroffenen — **242**
 - bb) Zweckbeschränkung und Erforderlichkeit — **243**
 - cc) Datenqualität — **243**
 - dd) Datensicherheit — **243**
 - ee) Verhältnis zu Auftragsdatenverarbeitern, die der Unternehmensgruppe angehören — **244**
 - ff) Rechtsgrundlage für die Datenverarbeitung — **244**
 - gg) Rechte auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch — **245**
 - hh) Beschränkung des Datentransfers an gruppenfremde Stellen — **245**
 - e) Nachweis der praktischen Wirksamkeit in der Unternehmensgruppe — **247**
 - aa) Einsetzung eines Mitarbeiterstabs — **247**
 - bb) Schulung — **248**
 - cc) Audit — **248**
 - dd) Beschwerdeverfahren — **249**
 - f) Nachweis der Zusammenarbeit mit den EWR-Datenschutzbehörden — **250**
 - g) Nachweis eines Systems zur Aktualisierung der BCR und des Kreises der an die BCR gebundenen Unternehmen — **250**
 - h) Vorgehen im Falle von in Drittstaaten geltenden Rechtsvorschriften, die der Einhaltung der BCR entgegenstehen — **251**
 - i) Erklärung zum Verhältnis zwischen den BCR und nationalen Rechtsvorschriften — **251**
5. BCR für Auftragsdatenverarbeiter — **251**
- B. Problem der grenzüberschreitenden E-Discovery — 254**
- I. Verfahren der Pre-Trial Discovery — **254**
 - II. Unterschiede zu anderen Rechtsordnungen — **255**
 - 1. Common Law – USA und Großbritannien — **256**
 - 2. Kontinentaleuropa — **256**

- 3. Blocking Statutes — 257
- III. Gegenstand der Pre-Trial Discovery — 258
- IV. Sanktionen bei Nichtvorlage von Daten — 258
- V. Leitlinien der Artikel 29-Datenschutzgruppe — 259
- VI. Rechtmäßigkeit der US e-Discovery nach BDSG — 259
 - 1. Anwendbarkeit des BDSG — 260
 - 2. Datenverarbeitung zum Zweck der e-Discovery — 261
 - a) Unterschiedliche Verarbeitungsphasen — 261
 - b) Zweistufige Prüfung — 261
 - 3. Allgemeine Zulässigkeit der Datenverarbeitung — 262
 - a) Rechtsgrundlage — 262
 - aa) Einwilligung — 262
 - bb) Erlaubnistatbestände des BDSG — 264
 - cc) Schutz berechtigter Unternehmensinteressen — 265
 - dd) Berechtigtes Unternehmensinteresse — 265
 - ee) Abwägung mit schutzwürdigem Interesse der Betroffenen — 266
 - ff) Erforderlichkeit — 266
 - gg) Kein entgegenstehendes Betroffeneninteresse — 269
 - b) Besonderheiten bei Beschäftigtendaten — 270
 - 4. Zulässigkeit der Datenübermittlung in die USA — 271
 - a) Haager Beweisübereinkommen — 272
 - b) Grundsätze des sicheren Hafens („Safe Harbor“) — 273
 - c) EU-Standardvertragsklauseln — 274
 - d) Binding Corporate Rules — 274
 - e) Ausnahmetatbestand des § 4c Abs. 1 Nr. 4 BDSG — 275
 - 5. Beteiligung des Betriebsrats — 276
 - 6. Einbeziehung des Datenschutzbeauftragten — 278
 - 7. Information der Betroffenen — 278
 - 8. Rechte auf Auskunft, Berichtigung und Löschung — 278
 - 9. Einschaltung eines e-Discovery-Dienstleisters — 279
 - 10. Datensicherheit — 281

Kapitel 6

Telekommunikation im Unternehmen – Was ist erlaubt, was ist verboten?

- A. Einleitung — 283
- B. Zugriffsgründe und -arten — 283
 - I. Zugriffsgründe — 283
 - II. Zugriffsarten — 284
- C. Zulässigkeit von Zugriffen — 285

- I. Internationale Anwendbarkeit sowie Abgrenzung von TKG und TMG zu BDSG — **285**
- II. Zulässigkeitsmaßstab bei ausschließlich dienstlicher Nutzung — **287**
 - 1. Folge für Zugriffe im Bereich telefonischer Kommunikation — **287**
 - 2. Folge für Zugriffe in den Bereichen E-Mail, Internet und Intranet — **288**
- III. Zulässigkeit bei Duldung oder Gestattung der auch privaten Nutzung — **289**
 - 1. Erlaubnis durch Duldung? — **289**
 - 2. Zulässigkeitsmaßstab bei gestatteter Privatnutzung — **290**
 - a) Vorliegen eines Telekommunikationsdienstes — **291**
 - b) Übermittlungsvorgang — **292**
 - c) Arbeitgeber als Diensteanbieter — **294**
 - aa) Auffassung der noch herrschenden Meinung im Schrifttum — **295**
 - bb) Im Vordringen befindliche Gegenauffassung — **295**
 - d) Zusammenfassung — **296**
- IV. Zulässigkeit von Einzelmaßnahmen — **297**
 - 1. Welche Daten dürfen erhoben und verarbeitet werden? — **297**
 - 2. Zulässigkeit der Datenverarbeitung im Einzelnen — **298**
 - a) Zugriffe auf E-Mail-Daten — **298**
 - aa) Der Meinungsstand — **298**
 - bb) Zugriffe auf betriebliche Webmailinterfaces — **299**
 - cc) Zugriffe auf E-Mail-Daten im betrieblichen Alltag — **299**
 - dd) E-Mail-Zugriffe zur Verhaltenskontrolle — **301**
 - b) Spamfilter und Antivirenprogramme — **305**
 - aa) Erforderlichkeit risikominimierender Maßnahmen — **305**
 - bb) Einwilligung des Arbeitnehmers — **305**
 - cc) Betriebsvereinbarung — **306**
 - dd) Einwilligung des Kommunikationspartners — **306**
 - ee) Entbehrlichkeit einer Einwilligung — **306**
 - c) E-Mail-Archivierungen — **307**
 - d) Löschen von E-Mail-Konten und -Nachrichten nach Ausscheiden — **310**
 - e) Telefonie einschließlich Mobilfunk — **310**
 - aa) Mit- und Abhören — **311**
 - bb) Zugriff auf Verkehrsdaten — **311**
 - cc) Nutzung von Geo- bzw. Standortdaten — **312**
 - f) TK-Outsourcing/Zentralisierung — **314**
 - aa) Allgemeine Anforderungen — **314**
 - bb) Auftragsdatenverarbeitung — **314**
 - cc) Drittstaatentransfer — **314**
 - dd) Besondere Verpflichtung des Dienstleisters — **315**

- ee) Herausforderungen für Berufsgeheimnisträger — 315
 - g) Social Media — 316
 - h) Intranetspezifischer Datenschutz — 317
 - V. Gestaltungshinweise — 318
 - a) Striktes Verbot der privaten Nutzung — 318
 - b) Qualifiziertes Verbot der privaten Nutzung — 318
 - c) Einholung von Einwilligungen — 319
 - d) Betriebsvereinbarungen als Ausnahme von § 88 Abs. 3 S. 3 TKG — 321

Kapitel 7

Die Website – Datenschutzerklärung, Impressum & Co.

- A. Einleitung — 323
- B. Datenschutzerklärung — 323
 - I. Ausgangslage — 323
 - II. Intention und Rechtsgrundlagen — 324
 - III. Adressaten — 325
 - 1. Diensteanbieter — 325
 - 2. Telemedium — 326
 - IV. Formale Anforderungen — 327
 - V. Inhaltliche Gestaltung — 328
 - 1. Zwingende gesetzliche Anforderungen — 328
 - a) Allgemeine inhaltliche Gestaltungsanforderungen — 328
 - b) Darstellung einzelner Datenverarbeitungen — 330
 - c) Cookies, Web-Bugs und ähnliche Verfahren — 332
 - d) Tracking und Tracing — 334
 - e) Retargeting/Online Behavioural Advertising — 337
 - f) Social Media — 338
 - 2. Fakultative Informationen — 339
 - VI. Haftungsrisiken bei fehlerhafter Datenschutzerklärung — 340
- C. Impressum — 341
 - I. Ausgangslage — 341
 - II. Adressaten — 342
 - 1. Adressaten des § 5 TMG — 342
 - a) Geschäftsmäßigkeit und Entgeltlichkeit — 343
 - b) Bereithalten zur Nutzung — 343
 - 2. Adressaten des § 6 TMG — 344
 - III. Formale Anforderungen — 344
 - 1. Leicht erkennbar — 345
 - 2. Unmittelbar erreichbar — 345
 - 3. Ständig verfügbar — 346
 - IV. Inhalt — 346

1. Anbieterkennzeichnungspflicht für natürliche Personen — **347**
2. Anbieterkennzeichnungspflicht für juristische Personen und Personengesellschaften — **348**
3. Besondere Informationspflichten für bestimmte Diensteanbieter — **350**
- V. Haftungsrisiken — **351**

Kapitel 8

Umgang mit Beschäftigtendaten – Von der Bewerbung bis zur Kündigung

- A. Einführung — **353**
 - I. Die Rechtsquellen — **353**
 1. Das Arbeitsrecht — **353**
 2. Das BDSG — **353**
 3. Keine Ausschließlichkeit — **354**
 4. „Beschäftigungsfremde“ Verarbeitungszwecke — **354**
 - II. Die Rechtspositionen des Beschäftigten — **355**
 1. Einwilligung des Beschäftigten — **355**
 2. Transparenz — **355**
 3. Korrekturrechte — **356**
 - III. Datenschutz im kollektiven Arbeitsrecht — **357**
 1. Die Schutzfunktion der Mitarbeitervertretung — **357**
 2. Betriebsvereinbarungen — **358**
 - IV. Ausblick — **358**
- B. Datenschutz im Anbahnungsverhältnis — **359**
 - I. Rechtliche Grundlagen — **359**
 - II. Das Fragerecht des Arbeitgebers — **360**
 1. Allgemeines — **360**
 - a) Grundlagen — **360**
 - b) Erweiterung des Fragerechts durch Einwilligung, ungefragte Offenbarungen — **361**
 - c) Rechtsfolgen unzulässiger Fragen — **362**
 2. Fallgruppen — **364**
 - a) Stammdaten — **364**
 - b) Familienverhältnisse, Informationen über Angehörige — **364**
 - c) Angaben zur Verfügbarkeit — **365**
 - d) Ausbildung, Qualifikationen und Berufserfahrung — **365**
 - e) Staatsangehörigkeit, Aufenthalts- und Arbeitserlaubnis, Geburtsort — **367**
 - f) Gesundheitsdaten (Krankheiten, Behinderung, Drogen) — **368**
 - g) Schwerbehinderteneigenschaft — **370**
 - h) Schwangerschaft, Kinderwunsch, Familienplanung — **371**

- i) Vorstrafen, Ermittlungsverfahren, gerichtliche Strafverfahren, Haftstrafen — **372**
- j) Eintragungen im Verkehrszentralregister und Erziehungsregister, Disziplinarstrafen, Bußgeldentscheidungen — **372**
- k) Vermögensverhältnisse — **373**
- l) Religion, Konfession und Weltanschauung — **374**
- m) Scientology und Verfassungstreue — **374**
- n) MfS-Mitarbeit, SED-Mitgliedschaft — **375**
- o) Partei- und Gewerkschaftsangehörigkeit, Berufsfachverband — **376**
- p) Nebentätigkeiten, Konkurrenz — **377**
- q) Freizeitbeschäftigungen, Mitgliedschaft in Vereinen, Ehrenamt — **377**
- r) Wehrdienst, Ersatzdienst — **378**
- s) Sonstige diskriminierungsrelevante Merkmale: Alter, Geschlecht, Rasse und ethnische Herkunft, Sexualität — **378**
- t) Fragerecht in der Leiharbeitsbranche — **379**
- III. Offenbarungspflichten des Arbeitnehmers — **379**
- IV. Sonstige Datenerhebungen durch Arbeitgeber — **379**
 - 1. Erhebung allgemein zugänglicher Daten, insbesondere Internetrecherchen — **379**
 - 2. Arbeitgeberauskunft — **383**
 - 3. Ärztliche Untersuchungen — **383**
 - 4. Psychologische Untersuchungen und Persönlichkeitstests, Graphologische Untersuchung — **388**
 - 5. Anforderung sonstiger Unterlagen vom Bewerber — **389**
 - a) Lebenslauf, Zeugnisse, Lichtbild, Aufenthaltstitel — **389**
 - b) Polizeiliches Führungszeugnis, Auskünfte der Polizei oder Nachrichtendienste — **389**
 - c) Bonitätsauskünfte — **391**
 - d) Auszug aus dem Gewerbezentralregister — **391**
 - e) Namensabgleich mit Antiterrorlisten und sonstigen Sanktionslisten — **392**
- V. Nutzung, Speicherung und Übermittlung von Bewerberdaten — **392**
- VI. Einschaltung Dritter in das Bewerbungs- und Auswahlverfahren durch Arbeitgeber — **394**
- C. Datenschutz im Beschäftigungsverhältnis — **395**
 - I. Rechtliche Grundlagen — **395**
 - 1. Verarbeitungsgrundsätze — **395**
 - 2. Technisch-organisatorischer Datenschutz — **396**
 - 3. Folgen rechtswidrigen Verarbeitungshandelns — **396**
 - II. Allgemeine Verarbeitungen — **397**

1. Weitere Verarbeitung der Daten aus dem Anbahnungsverhältnis — **397**
2. Grundlegende Personaldaten — **398**
3. Private Verhältnisse — **399**
4. Private Telefonnummern, E-Mail-Adressen, Soziale Netzwerke — **400**
5. Urlaubsabsichten — **401**
6. Arbeitszeiterfassung — **401**
7. Entgeltabrechnung — **402**
8. Schutz der Betriebsstätte — **402**
9. Identifikation und Legitimation — **403**
10. Gesundheitsdaten — **404**
 - a) Rechtliche Grundlagen — **404**
 - b) Fehlzeiten wegen Erkrankung — **405**
 - c) Betriebliches Eingliederungsmanagement — **406**
 - d) Krankenrückkehrgespräche — **406**
 - e) Arbeitsmedizinische Untersuchungen — **407**
 - f) Schwangerschaft — **408**
11. Innerbetriebliche Aushänge — **409**
12. Verarbeitungsbezogene Rechte des Beschäftigten — **410**
- III. Besondere Verarbeitungen zur Beschäftigtenkontrolle — **410**
 1. Grundsätze zur Kontrolle Beschäftigter — **411**
 2. Aufklärung von Straftaten Beschäftigter — **412**
 3. Personenkontrollen, Testkäufe, Detektive — **413**
 4. Besonderheiten bei Aufenthalts- und Bewegungskontrollen — **413**
 5. Videoüberwachung am Arbeitsplatz — **414**
 - a) Offene Beobachtung öffentlich zugänglicher Bereiche — **416**
 - b) Offene Beobachtung allein betriebsöffentlicher Bereiche — **417**
 - c) Interessenabwägung — **417**
 - d) Heimliche Beobachtung — **418**
 - e) Attrappen — **419**
 6. Kontrolle betrieblicher Kommunikation (Telefon, PC, Internet, Mail) — **419**
 7. Mitarbeiterscreening — **420**
- IV. Sonstiges Verarbeitungsinteresse des Arbeitgebers — **421**
 1. Innerbetriebliche Mitteilungen, Erhebungen, Umfragen und Statistiken — **421**
 2. Außendarstellung und Öffentlichkeitsarbeit — **422**
 3. Fürsorge, Eigen- und Fremdwerbung — **424**
 - a) Freiwillige (soziale) Angebote — **424**
 - b) Versicherungen — **424**
 - c) Eigen- und Fremdwerbung — **425**
 4. Nutzung und Verarbeitung von Beschäftigtendaten durch externe Wirtschaftsprüfer — **425**

- 5. Datenübermittlung an potenzielle Unternehmenskäufer — 426
- 6. (e-)Discovery — 427
- D. Verarbeitung bei und nach Beendigung des Beschäftigungsverhältnisses — 428
 - I. Allgemeines — 428
 - II. Erstellung von Zeugnissen — 430
 - III. Befragung über den Grund des Ausscheidens — 432
 - IV. Betriebsübergang — 432
 - V. Das Verarbeiten nach Beendigung des Arbeitsverhältnisses — 434
- E. Datenverarbeitungen durch den Betriebsrat — 435
 - I. Allgemeines — 435
 - II. Der Betriebsrat als „unabhängiger“ Teil des Betriebs — 436
 - III. Die technische Infrastruktur — 436
 - IV. Personenbezogene Informationsansprüche — 437
 - V. Eigene Personaldateien — 438

Kapitel 9

Unternehmensinterne Ermittlungen datenschutzkonform ausgestalten

- A. Rechtlicher Rahmen und operatives Vorgehen — 441
 - I. Anlass und Ausgangssituation — 441
 - II. Rechtlicher Rahmen im Inland — 442
 - 1. Anwendbares Recht — 442
 - 2. Anwendbarkeit des TKG — 442
 - 3. Unterscheidung unternehmens- und personenbezogener Daten — 443
 - 4. § 32 BDSG als zentrale Erlaubnisnorm — 445
 - 5. Einbindung von Mitarbeitervertretung, Datenschutzbeauftragten und Aufsichtsbehörde — 447
 - a) Betrieblicher Datenschutzbeauftragter oder Datenschutzaufsicht — 447
 - b) Betriebsrat und Sprecherausschuss — 448
 - 6. Fehlen eines Beschäftigungsbezugs und Nicht-Beschäftigte — 449
 - 7. Einwilligung und Widerspruch des Beschäftigten — 450
 - a) Einwilligung — 450
 - b) Widerspruch — 450
 - 8. Auslandsbezug — 451
 - a) Innereuropäische Sachverhalte — 451
 - b) Sachverhalte mit Drittstaatenbezug — 452
 - III. Anlassbezogene unternehmensinterne Ermittlungen — 454
 - 1. Auslösende Momente — 454
 - 2. Situationsbewertung und Zuständigkeiten — 455
 - IV. Ermittlungsdurchführung — 456

1. Zentrale Ermittlungstätigkeiten — **456**
 2. Herausgabe von Daten und Dokumenten — **461**
 3. Durchführung von Hintergrund-Checks — **462**
 4. Durchführung von Interviews — **464**
 - a) Auskunftspflicht im Interview — **464**
 - b) Beteiligung des Betriebsrats am Interview — **465**
 - c) Beteiligung eines Rechtsanwalts am Interview — **465**
 - d) Belehrungspflichten — **466**
 - e) Anfertigung von Aufzeichnungen/Datenerhebung — **467**
 - f) Aushändigung von Aufzeichnungen/Einsichtsrecht des Arbeitnehmers — **468**
 - g) Beweisverwertung im Strafverfahren/Interviews im Beisein staatlicher Ermittler — **468**
 5. Analyse von IT-Ressourcen und Mobile Devices — **469**
 - a) Vorbereitung und Ausgangslage — **469**
 - aa) Einzel-PCs — **469**
 - bb) Mehrere Beteiligte — **470**
 - cc) Sonderfall: E-Discovery — **472**
 - b) Betroffene Datenarten als personenbezogene Daten — **473**
 - c) Sicherstellung und technische Datenaufbereitung — **474**
 - d) Entlöschen von Daten — **475**
- B. Zusammenfassende rechtliche Einordnung von Einzelermittlungsmaßnahmen — 476**
- I. Auswertung von Telefon-Verbindungsdaten (sog. Verkehrsdaten) — **476**
 - II. Abhören/Mitschneiden von Telefonaten und Gesprächen in Büros, Besprechungsräumen und in Firmenwagen — **476**
 - III. Laufende E-Mail- und Netzwerküberwachung zur Erfassung weiterer Tatbestände — **478**
 - IV. Internetüberwachung, bei der aufgerufene Websites gelistet und rekonstruiert werden — **478**
 - V. Nutzung sog. Keylogger auf den Endgeräten von Verdächtigen — **479**
 - VI. Videoüberwachung in nichtöffentlich zugänglichen Räumen — **480**
 - VII. Videoüberwachung in öffentlich zugänglichen Räumen — **481**
 - VIII. Standortüberwachung/Erstellen von Bewegungsprotokollen durch Technologien wie GPS, RFID und Standortdaten — **481**
 - IX. Detektiveinsatz — **482**
 - X. Fahrzeugregistrauskunft — **482**
 - XI. Einsicht in Kontodaten und Kreditkartenabrechnungen — **483**
 - XII. Grundbucheinsicht — **483**
 - XIII. Datenabgleich mit Terror- und Sanktionslisten — **484**

Kapitel 10

Nutzung von Kundendaten – Werbung, Kundenbetreuung und CRM on- und offline rechtssicher gestalten

A. Werbung — 486

I. Grundlagen — 486

II. Widerspruchsrecht und Unterrichtungspflichten — 487

1. Inhalt der Unterrichtung — 488

a) Information über das Widerspruchsrecht und dessen
Ausübung — 488

b) Angabe der verantwortlichen Stelle — 490

c) Weitere Angaben zur Herkunft der Kundendaten — 491

2. Form der Unterrichtung — 491

3. Zeitpunkt der Unterrichtung — 492

4. Pflichten nach Ausübung des Widerspruchsrechts — 493

III. Ohne Einwilligung zulässige Werbung — 496

1. Listendaten — 496

2. Zulässige Werbemaßnahmen — 499

a) Werbung für eigene Angebote — 499

b) Berufsbezogene Werbung — 504

c) Spendenwerbung — 506

3. Werbung für fremde Angebote — 507

4. Berücksichtigung schutzwürdiger Interessen der Betroffenen — 509

5. Freundschaftswerbung — 510

IV. Voraussetzungen wirksamer Einwilligungen — 511

1. Freie Entscheidung des Betroffenen — 511

2. Inhaltliche Anforderungen — 511

3. Opt-in oder Opt-out — 514

4. Vorformulierte Einwilligungserklärungen — 515

5. Formelle Anforderungen — 516

6. Kopplungsverbot — 518

7. Einwilligung Minderjähriger — 519

8. Einwilligung durch Bevollmächtigte oder Vertreter — 520

9. Widerruf der Einwilligung — 521

10. Anfechtbarkeit der Einwilligung — 522

11. Wirkungskdauer einer Einwilligung — 523

V. Online-Shops und andere Telemediendienste — 524

1. Anwendungsbereich des TMG — 524

2. Notwendigkeit einer Einwilligung in die werbliche Verwendung
personenbezogener Daten — 527

3. Voraussetzungen einer elektronischen Einwilligung — 528

a) Bewusst und eindeutig erteilte Einwilligung — 528

- b) Darstellung der Einwilligungserklärung — 529
 - c) Gesonderte Erklärung — 530
 - d) Ausgestaltung als Opt-in — 530
 - e) Protokollierung, jederzeitige Abrufbarkeit und Widerrufbarkeit — 531
- 4. Verhaltensbasierte Online-Werbung — 531
 - a) Zulässige Bildung von Nutzungsprofilen — 532
 - b) Nutzungsprofile ohne Verwendung von Pseudonymen — 535
 - c) Einsatz von Cookies — 535
- VI. Werbung durch die Anbieter von Telekommunikationsdiensten — 536
 - 1. Anwendungsbereich des TKG — 537
 - 2. Werbliche Verwendung von Teilnehmerdaten — 537
 - a) Werbliche Verwendung von Bestandsdaten — 537
 - b) Werbliche Verwendung von Verkehrsdaten — 539
 - 3. Zulässigkeit einer elektronisch erteilten Einwilligung — 539
- VII. Social Media Marketing — 539
 - 1. Unternehmenspräsenz in sozialen Netzwerken — 540
 - 2. Social Plugins — 542
- VIII. Wettbewerbsrechtliche Beschränkungen — 543
 - 1. Briefkasten- und Briefwerbung — 544
 - 2. Werbung mittels elektronischer Fernkommunikation — 546
 - a) Notwendigkeit einer vorherigen ausdrücklichen Einwilligung — 546
 - b) Zufriedenheitsbefragungen — 549
 - c) Empfehlungs-E-Mails — 550
 - d) Wettbewerbswidrige Werbung in sozialen Netzwerken — 551
 - e) Verbot der Rufnummernunterdrückung — 552
 - f) Nachweis der Einwilligung – Double-Opt-in-Verfahren — 552
 - g) Widerruf der Einwilligung — 554
 - h) Wirksamkeitsdauer der Einwilligung — 554
 - 3. Wettbewerbsrechtlich zulässige Werbung ohne (ausdrückliche) Einwilligung — 555
 - a) Telefonwerbung — 555
 - b) Werbung mittels elektronischer Post — 556
 - 4. Reaktionsmöglichkeiten von Wettbewerbern — 560
- IX. Werbung unter Verwendung fremder Daten — 561
 - 1. Nutzung von Kundendaten im Konzern — 561
 - 2. Adresshandel — 562
 - a) Adresshandel mit Listendaten — 563
 - b) Geschäftsmäßiger Adresshandel — 563
 - 3. Melderegisterdaten — 565
- B. Customer Relationship Management — 566

- I. Grundlagen — 567
- II. Gesetzliche Erlaubnis — 567
- III. Notwendigkeit von Einwilligungen der Betroffenen — 569

Kapitel 11

Datenschutz im Credit Management

- A. Einleitung — 571
 - I. Begrifflichkeit — 571
 - II. Bedeutung des Datenschutzes für das Credit Management — 571
 - III. Datensicherheit — 572
- B. Prozesse vor der Entstehung von Forderungen — 572
 - I. Überprüfung der Kreditwürdigkeit zukünftiger Kunden — 572
 - 1. Informationsbeschaffung und -validierung — 572
 - a) Allgemeines — 572
 - b) Direkterhebung — 573
 - c) Verwendung eigener Erkenntnisse — 574
 - aa) Exkurs: Aufbewahrungsfristen für eigene Datenbestände — 574
 - bb) Plausibilitätsprüfung — 575
 - d) Verwendung von Informationen aus externen Quellen — 576
 - aa) Allgemeines — 576
 - bb) Einwilligung — 576
 - cc) Gesetzliche Verarbeitungsgrundlage — 577
 - dd) Bereichsspezifische Normen für die Kreditwirtschaft — 577
 - e) Auskünfte aus dem persönlichen Umfeld und aus dem Internet — 578
 - f) Statistische Erkenntnisse über Geschäftskunden — 579
 - g) Informationen aus besonderen Quellen (Banken, Behörden, Sozialdaten) — 579
 - aa) Banken — 579
 - bb) Behörden — 580
 - cc) Sozialdaten — 581
 - 2. Informationsbewertung — 581
 - a) Scoring — 581
 - aa) Umfang der Anwendbarkeit des § 28b BDSG — 582
 - bb) Zulässigkeit vertragsbezogenen Scorings — 583
 - cc) Für Scoring verwendete Daten — 583
 - dd) Verhältnis zu § 10 Abs. 1 KWG — 585
 - ee) Sanktionen — 587
 - b) Automatisierte Entscheidungssysteme — 587
 - aa) Verfahren und Rechtsfolgen gem. § 6a BDSG — 588

bb) Verhältnis § 28b zu § 6a BDSG — 588

II. Limitsteuerung — 589

C. Maßnahmen während bestehender Kundenbeziehungen — 590

I. Monitoring bei bestehenden Kundenbeziehungen — 590

II. Maßnahmen bei notleidenden Vertragsverhältnissen — 591

1. Forderungsrealisierung — 591

a) Mahnwesen — 591

b) Inkasso — 592

c) Factoring — 593

2. Einmeldung offener Forderungen und vertragswidrigen Handelns — 594

a) In Auskunfteien — 595

aa) Anwendbare Bestimmungen — 595

bb) Feste Tatbestände („Fünferkatalog“) statt Interessenabwägung — 595

cc) Einmeldungsempfänger: Auskunftei — 596

dd) Einmeldebefugnis — 596

ee) Fälligkeit der Forderung — 597

ff) Erforderlichkeit der Einmeldung — 598

gg) Tatbestandsvoraussetzungen für eine Einmeldung offener Forderungen an Auskunfteien („Fünferkatalog“) — 599

(1) Amtlich festgestellte Zahlungsunfähigkeit und Anerkenntnis (Abs. 1 Nr. 1–3) — 599

(a) Übermittlung aufgrund eines Urteils oder eines Titels (Nr. 1) — 600

(b) Übermittlung aufgrund Feststellung im Insolvenzverfahren (Nr. 2) — 601

(c) Übermittlung aufgrund Anerkenntnisses (Nr. 3) — 601

(2) Übermittlung bei sonstigen Forderungen (Nr. 4 und 5) — 601

(a) Forderungen im Mahnstadium (Nr. 4) — 601

(b) Schriftliche Mahnungen — 602

(c) Vier-Wochen-Frist — 602

(d) Unterrichtung über die bevorstehende Einmeldung — 602

(e) Unbestrittene Forderung — 604

(3) Forderungen, die zur fristlosen Kündigung berechtigen (Nr. 5) — 604

hh) Nachmeldepflicht (§ 28a Abs. 3 BDSG) — 605

b) Einmeldung in Warndateien — 605

III. Setzen von Liefersperren/Kündigung — 606

D. Datenverwendung nach Vertragsbeendigung — 607

- I. Ordnungsgemäße Vertragsbeendigung — **607**
- II. Vertragsbeendigung bei Zahlungsstörungen — **609**
 - 1. Beendigung nach Forderungsausgleich — **609**
 - 2. Beendigung nach Zahlungsausfall — **609**
- E. Transparenzpflichten — **610**
 - I. Benachrichtigung — **610**
 - II. Selbstauskunft — **611**
 - 1. Allgemeines — **611**
 - 2. Identitätsprüfung — **611**
 - 3. Missbräuchliches Auskunftsverlangen — **613**
 - 4. Form und Frist der Selbstauskunft — **613**
 - 5. Inhalt der Selbstauskunft — **614**
- III. Mitteilungspflichten bei sog. Datenpannen — **615**

Kapitel 12

Die technisch-organisatorischen Maßnahmen des Datenschutzes – von der Theorie zur Praxis

- A. Anwendbarkeit des BDSG und Einordnung der technisch-organisatorischen Maßnahmen — **617**
- B. Datenschutz und Informationssicherheit — **618**
 - I. Daten und Informationen — **618**
 - II. Datenschutz — **618**
 - III. Informationssicherheit — **619**
 - IV. Technische und organisatorische Anforderungen an Datenschutz und Informationssicherheit — **621**
 - 1. Arten von Anforderungen — **621**
 - 2. Technische und organisatorische Anforderungen an den Datenschutz — **622**
 - 3. Anforderungen an die Informationssicherheit — **622**
 - V. Gemeinsamkeiten und Unterschiede von Datenschutz und Informationssicherheit — **623**
- C. Technisch-organisatorische Maßnahmen — **625**
 - I. Zutrittskontrolle — **627**
 - 1. Allgemeine Beschreibung — **627**
 - 2. Beispiele aus der Praxis — **627**
 - II. Zugangskontrolle — **630**
 - 1. Allgemeine Beschreibung — **630**
 - 2. Beispiele aus der Praxis — **631**
 - III. Zugriffskontrolle — **634**
 - 1. Allgemeine Beschreibung — **634**
 - 2. Beispiele aus der Praxis — **635**

- IV. Weitergabekontrolle — **636**
 - 1. Allgemeine Beschreibung — **636**
 - 2. Beispiele aus der Praxis — **637**
- V. Eingabekontrolle — **643**
 - 1. Allgemeine Beschreibung — **643**
 - 2. Beispiele aus der Praxis — **643**
- VI. Auftragskontrolle — **646**
 - 1. Allgemeine Beschreibung — **646**
 - 2. Beispiele aus der Praxis — **647**
- VII. Verfügbarkeitskontrolle — **650**
 - 1. Allgemeine Beschreibung — **650**
 - 2. Beispiele aus der Praxis — **651**
- VIII. Trennungsgebot — **655**
 - 1. Allgemeine Beschreibung — **655**
 - 2. Beispiele aus der Praxis — **655**
- D. Umsetzung der technisch-organisatorischen Maßnahmen — **657**
 - I. Plan-Phase – Maßnahmenplanung und -umsetzung — **659**
 - 1. Initialisierung der Umsetzung der TOMs — **659**
 - 2. Ermittlung des Status quo und Durchführung einer Gap-Analyse — **661**
 - 3. Maßnahmenplanung und -priorisierung — **666**
 - II. Do-Phase – Umsetzung des priorisierten Maßnahmenplans — **666**
 - III. Check-Phase – Überprüfung des Umsetzungserfolgs — **668**
 - IV. Act-Phase – Verstetigung im Regelbetrieb — **668**
 - V. KVP – kontinuierlicher Verbesserungsprozess — **670**
- E. Zusammenfassung — **670**

Kapitel 13

Zertifizierungen – Arten und Nutzen

- A. Motivation und Zielsetzung — **673**
- B. Rechtlicher Rahmen — **675**
- C. Begriffsklärung — **677**
 - I. Standards und Normen — **677**
 - II. Zertifikate, Prüf-/Gütesiegel und Testate — **678**
 - 1. Zertifikat und Prüfbericht — **678**
 - 2. Testat — **679**
 - 3. Prüf- und Gütesiegel — **679**
- D. Anforderungen an Zertifikate — **680**
- E. Unternehmenszertifizierungen — **682**
 - I. ISO/IEC 29100:2011 und ISO/IEC 29101:2013 — **682**
 - II. ISO/IEC 27001:2013 — **684**
 - III. IT-Grundschutz — **687**

- IV. ISAE 3000 — **691**
- V. Datenschutzaudit beim ULD — **692**
- VI. Datenschutz-Audit der TÜV Rheinland i-sec — **695**
- F. Produktzertifizierungen — **698**
- G. Fazit und Ausblick — **699**

Kapitel 14

Ausblick

- A. Mögliche gesetzgeberische Entwicklungen — **701**
 - I. Auf nationaler Ebene — **701**
 - II. Auf europäischer Ebene — **707**
- B. Fazit — **711**

Stichwortverzeichnis — **713**