Beschäftigtendatenschutz und Compliance

Thüsing

3. Auflage 2021
ISBN 978-3-406-71502-0
C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.
beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Thüsing

Beschäftigtendatenschutz
und Compliance

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Beschäftigtendatenschutz und Compliance

Effektive Compliance im Spannungsfeld von DS-GVO, BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung

von

Dr. Gregor Thüsing, LL.M. (Harvard)
o. Professor und Direktor des Instituts für Arbeitsrecht
und Recht der Sozialen Sicherheit,
Universität Bonn

unter Mitarbeit von

Dr. Gerrit Forst, LL.M. (Cantab.)
Vertreter des Lehrstuhls für Bürgerliches Recht,
Arbeitsrecht, Handels- und Wirtschaftsrecht,
Universität Mannheim

Dr. Stephan Pötters, LL.M. (Cantab.)
Institut für Arbeitsrecht und
Recht der sozialen Sicherheit,
Universität Bonn

Dr. Thomas Granetzny
Rechtsanwalt in Köln

Dr. Johannes Traut
Institut für Arbeitsrecht und
Recht der sozialen Sicherheit,
Universität Bonn

beck-shop.de
DIE FACHBUCHHANDLUNG

3. Auflage 2021

C.H.BECK

Zitiervorschlag:
Thüsing Beschäftigtendatenschutz/*Bearbeiter* § … Rn. …

beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 71502 0

© 2021 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck: Druckerei C.H. Beck Nördlingen
(Adresse wie Verlag)

Satz: 3w+p GmbH, Rimpar
Umschlaggestaltung: Martina Busch, Grafikdesign, Homburg Saar

CO_2 neutral
chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

Die Anforderungen an Unternehmen zur Verhinderung von Straftaten rücken von Jahr zu Jahr mehr ins Bewusstsein nicht nur der Juristen, sondern einer immer breiteren Öffentlichkeit. Werden diese Anforderungen nicht erfüllt, drohen Management und Unternehmen Haftung und Sanktionen. Viele Unternehmen haben daher detaillierte Compliance- und Betrugsbekämpfungsprogramme eingeführt. Gleichzeitig präzisiert der Gesetzgeber die Voraussetzungen für den zulässigen Umgang mit Arbeitnehmerdaten. Die Datenschutz-Grundverordnung hat alles noch einmal neu geordnet. Weitere Schritte werden folgen. Dabei ist Datenschutz im Beschäftigungsverhältnis wichtiger denn je: Prominente Bußgeldverfahren der Aufsichtsbehörden betrafen gerade diesen Bereich. Datenschlamperei kann Millionen kosten. Wirksame Sanktionen sind zu begrüßen, doch gilt auch: Recht lebt von gesellschaftlicher Akzeptanz. Nirgend wann ist das deutlicher geworden als in den jüngsten Wochen, als Freiheitsrechte eingeschränkt werden mussten zum Schutz von Gesundheit und Leben. Gesellschaftliche Akzeptanz aber geht verloren, wo Regel nicht begründet oder absolut gesetzt werden, wo sie nicht absolut sind, wo sich der Blick auf ein Interesse verengt und alles andere beiseitegeschoben wird. Das gilt auch für den Datenschutz. Die gute Sache, der er dient, rechtfertigt nicht den Eifer des Zeloten.

Dies gilt es auch bei Maßnahmen der Compliance zu beachten. Denn Compliance und Datenschutz deuten dabei zuweilen in unterschiedliche Richtungen: Wieviel muss ich wissen, wieviel darf ich wissen? Die divergierenden Interessen müssen in einen angemessenen Ausgleich gebracht werden. Hierbei will diese Darstellung eine Hilfe sein. Sie strebt dabei nicht an, ein umfassendes Handbuch zu sein oder eine Kommentierung des BDSG zu sein. Ziel ist es, an exemplarischen, praxisrelevanten Schwerpunkten deutlich zu machen, was für das Datenschutzrecht allgemein gilt: Die Abwägung des Persönlichkeitsschutzes des Arbeitnehmers mit den Aufklärungsinteressen der verantwortlichen Stelle kann nur im Einzelfall gelingen und bleibt oftmals unscharf; klare Hinweise in der Rechtsprechung mehren sich, aber fehlen allzu oft. Einiges wurde daher weggelassen, um anderes in größerer Breite zu diskutieren. Die ersten Auflagen dieses Buchs sind freundlich aufgenommen worden. Dem Vorschlag des Verlags, eine weitere Auflage in Angriff zu nehmen, habe ich gerne entsprochen. Allen Mitautoren danke ich für anregende Diskussionen und viel Engagement. Mögen die Fehler auch allein von mir zu verantworten sein, so ist jeder hilfreiche Hinweis – sollte er sich in diesem Buch finden – allen Autoren gemeinsam geschuldet.

beck-shop.de
DIE FACHBUCHHANDLUNG

Bonn, im November 2019 *Gregor Thüsing*

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort V
Abkürzungsverzeichnis XIX
Verzeichnis der (abgekürzt zitierten) Literatur XXV

§ 1. Der Beschäftigtendatenschutz als Aufgabe für Gesetzgebung und Rechtsprechung

A. Datenschutz als Persönlichkeitsschutz 1

B. Ein Blick zurück – ein Blick nach vorne 2

C. Der Beschäftigtendatenschutz in der Entwicklung: Die Anfangszeit 3

D. Die Forderung nach einem Beschäftigtendatenschutzgesetz: Die vergangene Dekade 4

E. Das neue Datenschutzrecht im Zusammenspiel von DS-GVO und neuem BDSG 5

§ 2. Compliance als Aufgabe der Unternehmensleitung

A. Begriff und rechtliche Bedeutung 8
I. Begriff 8
II. Rechtliche Bedeutung 9

B. Das Pflichtenheft der Unternehmensleitung 11
I. Legalitätspflicht 11
II. Überwachungspflicht 12
1. Grundzüge der Überwachungspflicht 12
2. Mangelnde Überwachung als Eigenpflichtverletzung des Vorstandes 13
3. Keine Pflicht zur Einführung eines allgemeinen Compliance-Systems 15
III. Sorgfaltspflicht im engeren Sinne 17
IV. Treuepflicht 17

C. Folgen einer Pflichtverletzung der Unternehmensleitung 18
I. Rechtsfolgen 18
1. Folgen für die Gesellschaft 18
2. Folgen für die Unternehmensleitung 20
II. Faktische Folgen 22

D. Bestandteile eines Compliance-Systems 23

E. Pflicht zur Compliance in der Unternehmensgruppe? 24
I. Ausdehnung der in der einzelnen Gesellschaft geltenden Tatbestände? 24
II. Eigenständiger Compliance-Tatbestand in der Unternehmensgruppe? 26

F. Zusammenfassung 27

§ 3. Zum System des Beschäftigtendatenschutzes

A. Unions- und verfassungsrechtkonforme Auslegung des Datenschutzrechts 29

B. „Verbot mit Erlaubnisvorbehalt“ nach Art. 5 Abs. 1 lit. a) iVm Art. 6 DS-GVO 31

C. Das bisherige System nach den §§ 28, 32 BDSG aF 32

beck-shop.de
DIE FACHBUCHHANDLUNG

D. § 26 BDSG als lex regia des Beschäftigtendatenschutzes 33
I. Personaler Schutzbereich: Wer ist „Beschäftigter“? 33
II. § 26 BDSG als Ausgangspunkt jedweder datenschutzrechtlicher Betrachtung im Beschäftigungskontext 34
1. Erforderlichkeit der Datenverarbeitung 34
2. Begrenztheit der Zweckbestimmung 35
a) Entscheidung über die Begründung des Beschäftigungsverhältnisses 35
b) Durchführung des Beschäftigungsverhältnisses 35
c) Beendigung des Beschäftigungsverhältnisses 36
3. Sonderregelung zur Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG 36
4. Möglichkeiten präventiven Vorgehens: Compliance 37
5. Aufdeckung schwerwiegender Vertragsbrüche 37
III. Einwilligung 38
IV. Kollektivvereinbarung 39
V. § 26 Abs. 7 BDSG: Keine automatisierte Verarbeitung erforderlich 39

E. Interessenabwägung 40
I. Grundstruktur der Abwägung 40
II. Kriterien der Abwägung nach der Rechtsprechung des *BVerfG* 41
1. Eine Systematisierung der verfassungsrechtlichen Rechtsprechung 41
2. Grenzen der Übertragbarkeit auf das Datenschutzrecht 43
3. Anhaltspunkte für die Auslegung von § 26 BDSG 43

F. Verhältnis des neuen Datenschutzrechts zum TKG 44
I. Subsidiarität des BDSG im Verhältnis zum auf der DS-GVO beruhenden TKG 45
II. Anwendbarkeit des TKG bei verbotener Privatnutzung 45
1. Merkmale eines Anbieters iSd §§ 88, 91 TKG 46
2. Meinungsstand zum Arbeitgeber als Anbieter – Verbot privater Nutzung 47
III. Anwendbarkeit des TKG bei erlaubter Privatnutzung? 51
1. Der Meinungsstand in Literatur und Rechtsprechung 51
2. Eine Gewichtung der Argumente 53
a) Wortlaut 54
b) Geschichte 55
c) Systematik 56
d) Teleologie 57
3. Fazit: Keine Anwendbarkeit des TKG auch bei erlaubter Privatnutzung 58

beck-shop.de
DIE FACHBUCHHANDLUNG

§ 4. Regelbarkeit durch Kollektivvereinbarungen

A. Betriebsvereinbarung 59
I. Üblichkeit einer Regelung 59
II. Die Betriebsvereinbarung als Mittel zur rechtmäßigen Datenverarbeitung 60
III. Gestaltungsspielraum bei Betriebsvereinbarungen 62
IV. Die Bedeutung von § 26 Abs. 6 BDSG 64
V. Die Betriebsvereinbarung als gesetzliche Vorschrift iSd § 88 Abs. 3 S. 3 Alt. 2 TKG 64
VI. Regelungsgrenzen einer Betriebsvereinbarung 67
VII. Anforderungen an eine Betriebsvereinbarung 67

B. Dienstvereinbarung 68

C. Tarifvertrag 68
I. Abweichung vom Schutzniveau der DS-GVO durch einen Tarifvertrag 69
II. Aussagegehalt des § 26 Abs. 6 BDSG 69
III. Sprecherausschussvereinbarung 70

§ 5. Die Einwilligung des Beschäftigten

A. Datenschutzrechtliche Anforderungen 71
I. Zusammenspiel von DS-GVO und § 26 Abs. 2 BDSG 71
II. Zeitpunkt der Einwilligung 72
III. Die informierte und bestimmte Einwilligung 72
IV. Freiwilligkeit 75
V. Unmissverständlichlichkeit/eindeutig bestätigende Handlung 77
VI. Form (§ 26 Abs. 2 S. 3 BDSG) 79
VII. Grenzen der Einwilligung 80

B. AGB-rechtliche Anforderungen? 80
I. Verbot überraschender Klauseln 80
II. Inhaltskontrolle 81

C. Zusätzliche Aufklärungspflicht (§ 26 Abs. 2 S. 4 BDSG) 81

D. Rechtsnatur/Verhältnis zum nationalen Zivilrecht 82

E. Zwingender Charakter 83

F. Mustereinwilligung 83

§ 6. Whistleblowing

A. Begriff und Herkunft 85
I. Begriff 86
II. Herkunft 86
III. Zweck 87
1. Kontinentaleuropa 87
2. Vereinigtes Königreich 88
3. Recht der Europäischen Union 88

B. Fallgruppen des Whistleblowing 93
I. Anonymes und offenes Whistleblowing 94
II. Internes und externes Whistleblowing 95
III. Zentrales und dezentrales Whistleblowing 96

C. Wer darf melden? 96

D. Was darf gemeldet werden? 99

E. Wie darf gemeldet werden? 101

F. Vertragliche Verpflichtung zum Whistleblowing 105

G. Folgen des berechtigten Whistleblowing 106
I. Retrospektiver Schutz 106
II. Präventiver Schutz 108

H. Zum Schutz des Angezeigten 109

§ 7. Informationserhebung bei der Einstellung und beim beruflichen Aufstieg

A. Grundlagen 111

beck-shop.de
DIE FACHBUCHHANDLUNG

B. Datenschutzrechtliche Vorgaben 112
I. Grundregel: Datenverarbeitung nur bei Erforderlichkeit 112
II. Sonderfall: Besondere Kategorien personenbezogener Daten 112

C. Zusammenspiel von Datenschutzrecht und Antidiskriminierungsrecht 114

D. Fallgruppen 115
I. Schwangerschaft 115
II. Behinderung/Schwerbehinderteneigenschaft 115
III. Religion, Weltanschauung und sexuelle Identität 117
IV. Gewerkschaftszugehörigkeit 117
V. Gesundheitszustand, medizinische und psychologische Untersuchungen 118
VI. Genetische Merkmale 119
VII. Vorstrafen und Ermittlungsverfahren, Führungszeugnis 120
VIII. Weitere Fallgruppen 121

E. Datenerhebung bei Dritten 122

§ 8. Der elektronische Datenabgleich

A. Geeignetheit 126

B. Erforderlichkeit 126
I. Generalverdacht vs. Einschränkung auf eine bestimmte Personengruppe 126
II. Notwendigkeit einer Unterrichtung oder Pseudonymisierung/Anonymisierung? 128

C. Angemessenheit 129
I. Üblichkeit 129
1. Gebrauch durch staatliche Stellen 129
a) Sozialversicherungsrecht 129
b) Steuerrecht 130
c) BAföG 131
d) Bundesrechnungshof 132
2. Gebrauch im privaten Bereich 132
3. Bewertung der Üblichkeit in der Literatur 134
4. Ein Seitenblick auf das Europarecht 138
II. Das Interesse der verantwortlichen Stelle 139
III. Das Interesse der betroffenen Arbeitnehmer 140
IV. Angemessenheit im engeren Sinne 141

§ 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles

A. Grundlagen 144
I. Zwecke der Speicherung und Sichtung des E-Mail-Verkehrs 144
II. Objekte des Zugriffs: Logfiles und E-Mails 145
III. Verantwortlicher, Betroffene 145
IV. Prüfungsrahmen: DS-GVO und BDSG oder TKG und StGB? 146

B. Erfordernis einer Rechtfertigung (Art. 5 Abs. 1 lit. a, 6 Abs. 1 DS-GVO, § 26 BDSG) 146
I. E-Mail-Logfiles als personenbezogene Daten 146
II. E-Mails 147

C. Rechtfertigung (§ 26 BDSG) 148
I. Leitlinien für die Verhältnismäßigkeitsprüfung 148
1. Zugriff auf Logfiles vs. Zugriff auf E-Mails 149

beck-shop.de
DIE FACHBUCHHANDLUNG

2. Vergleichbarkeit mit Brief oder Telefonat? 149
3. Privatnutzung erlaubt vs. Privatnutzung verboten 151
4. Leitlinien für gute Praxis 153
5. Kriterien der Interessenabwägung im Einzelfall 154
II. Aufklärung von Straftaten (§ 26 Abs. 1 S. 2 BDSG)/schwerwiegenden Pflichtverletzungen (§ 26 Abs. 1 S. 1 BDSG) 155
III. Zwecke des Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 Var. 1 BDSG) 157
1. Compliance (präventiv/repressiv) 157
2. Zugriff auf dienstliche Informationen 159
3. Leistungskontrolle 160

D. Strafrechtliche Risiken? 160

§ 10. Überwachung von Telefonverbindungsdaten

A. Rechtmäßigkeit nach DS-GVO und BDSG 161
I. Rechtsprechung und Literatur zur generellen Erfassung 161
II. Vollständige Nummernerfassung 162

B. Rechtmäßigkeit nach dem TKG 163

§ 11. Videoüberwachung

A. Begriff und rechtliche Bedeutung 165
I. Begriff der Videoüberwachung 166
1. Videoüberwachung iSd § 4 Abs. 1 BDSG 166
2. Videoüberwachung nach der Definition des BAG 167
II. Rechtliche Bedeutung 168

B. Prüfungsrahmen 168
I. Datenschutz-Grundverordnung 168
II. Grundgesetz und EU-Grundrechtecharta 169
III. BDSG 170
1. § 4 BDSG 170
2. § 26 BDSG 171
IV. Sonstige Rechtsvorschriften 172
1. Verhältnis zum TKG 172
2. § 22 KUG 172
3. Notwehr und Notstand 173

C. Voraussetzungen der Videoüberwachung 173
I. § 26 BDSG als einheitlicher Prüfungsmaßstab der Videoüberwachung im Beschäftigungsverhältnis 173
1. Fortführung der Differenzierung nach dem BDSG aF 173
2. Unionsrechtswidrigkeit des § 4 BDSG und systematischer Vorrang des § 26 BDSG im Beschäftigungsverhältnis 173
3. Anwendungsbereich von § 4 BDSG bzw. Art. 6 Abs. 1 S. 1 Buchst. f DS-GVO 175
II. Der Zweck der Videoüberwachung als vorentscheidendes Kriterium 175
III. § 26 Abs. 1 S. 1 BDSG 176
IV. § 26 Abs. 1 S. 2 BDSG 180
1. Voraussetzungen 180
2. Insbesondere: Zulässigkeit heimlicher Überwachung? 183
V. Einwilligung (§ 26 Abs. 2 BDSG) 185

beck-shop.de
DIE FACHBUCHHANDLUNG

D. (Weiter-)Verarbeitung und Nutzung erhobener Daten 185
I. Der Verarbeitungsbegriff als Ausgangspunkt 185
II. Zweckbindung und Datenminimierung: Begrenzte Auswertung des aufgezeichneten Materials 186

E. Löschpflichten 186

F. Prozessuales: Beweisverwertungsverbot 188

G. Videoüberwachung auf Grundlage einer Betriebsvereinbarung 191
I. Regelbarkeit durch Betriebsvereinbarung 191
II. Muster-Betriebsvereinbarung 192
III. Muster-Hinweisschild nach Art. 13 DS-GVO bei Videoüberwachung 196
IV. Muster-Datenschutzerklärung 198

§ 12. Überwachung mobiler Arbeitnehmer

A. Einleitung 201

B. Technische Möglichkeiten 202
I. Überwachung mittels Satellitenortung 202
II. Überwachung mittels RFID 203
III. Ortung mittels der Telekommunikationsnetze 203

C. Rechtliche Zulässigkeit 204
I. Überwachung mittels Satellitenortung 204
1. Prüfungsmaßstab 204
2. Personenbezogene Daten 205
3. Informationspflicht 206
4. Erlaubnistatbestände 206
5. Sanktionen bei rechtswidriger Nutzung 208
II. Überwachung mittels RFID 208
1. Prüfungsmaßstab 208
2. Personenbezogene Daten 209
3. Informationspflicht 209
4. Erlaubnistatbestände 209
5. Sanktionen bei rechtswidriger Nutzung 210
III. Ortung mittels der Telekommunikationsnetze 210
1. Prüfungsmaßstab 210
2. Personenbezogene Daten 211
3. Informationspflicht 211
4. Erlaubnistatbestände 211
5. Sanktionen bei rechtswidriger Nutzung 212
6. *Disputandi causa:* Zulässigkeit nach dem TKG und dem TMG 212

§ 13. Personengebundene Merkmale

A. Biometrische Daten 215

B. Umgang mit biometrischen Daten 216

C. Rechtfertigung im Beschäftigtenkontext 217
I. Legitime Zwecksetzung 218
II. Erforderlichkeit 218
III. Kein Entgegenstehen schutzwürdiger Interessen des Beschäftigten – Verhältnismäßigkeit im engeren Sinne 219

beck-shop.de
DIE FACHBUCHHANDLUNG

D. Exkurs: Ärztliche Untersuchungen 220
I. Datenerhebung im Wege einer ärztlichen Untersuchung 220
II. Rechtfertigung nach § 26 Abs. 1 BDSG 221
1. Notwendigkeit der ärztlichen Untersuchung 221
2. Berechtigtes Interesse 222
III. Einwilligung 222
IV. Rechtsfolgen einer angeordneten Untersuchung 223
1. Zulässige Anordnung 223
2. Unzulässige Anordnung 224
V. Auswahl des Arztes und Kommunikation des Untersuchungsergebnisses 224

§ 14. Social Media in Betrieb und Unternehmen

A. Social Media als auch betriebliches Phänomen 227

B. Zugriff des Arbeitgebers auf Informationen in Internet und Social Media 228
I. Die Positionen in der Literatur 228
II. Abwägung, kein absolutes Gebot der Direkterhebung 230
III. Leitlinien für die Abwägung 231
1. Öffentlich zugänglich: Vorbelastung für Zulässigkeit 231
2. (Sonstige) Veranlassung durch Betroffenen 234
3. Aufgaben und berufliche Stellung des Bewerbers 234
4. Verarbeitung von Zufallsfunde 235
5. Eingesetzte Suchwerkzeuge, „Big-Data“ 236
IV. Zugriff für Zwecke des Beschäftigungsverhältnisses (§ 26 Abs. 1 BDSG) 237
1. Rechtsgrundlagen und Zwecke 237
2. Bewerbungsphase 237
3. Laufendes Arbeitsverhältnis 238
V. Nutzung von Social Media für eigene und private Zwecke 240
VI. Transparenz nach Art. 14 DS-GVO 240
VII. Abgrenzung zum Abhören 240

C. *Social Media Guidelines* auf Grundlage des Weisungsrechts (§ 315 Abs. 1 BGB, § 106 GewO) 241
I. Beschränkung der Privatnutzung 241
1. Einschränkungen des Gebrauchs von Betriebsmitteln für die private Social Media Nutzung 241
2. Vorgaben für die Nutzung von Social Media im privaten Bereich (§ 241 Abs. 2 BGB) 243
II. *Social Media* als Arbeitsmittel 243
1. Anordnung der Nutzung interner *Social Media* 243
2. Anordnung der Nutzung externer *Social Media* 245
3. Allgemeine Leitlinien für den dienstlichen Umgang 246

D. Social Media Guidelines und Mitbestimmung 247
I. Mitbestimmung bei Einführung unternehmenseigener Social Media 247
II. Mitbestimmung bei der Anordnung der dienstlichen Nutzung externer Social Media 247
III. Mitbestimmung bei Social Media Guidelines 247
IV. Social Media Guidelines auf Grundlage von Betriebsvereinbarungen 248
1. Persönlicher Regelungsbereich 250
2. Räumlicher Regelungsbereich 250
3. Sachlicher Regelungsbereich 251
4. Zeitlicher Regelungsbereich 251
5. Option: Rechtsgrundlage für Datenverarbeitung 252

beck-shop.de
DIE FACHBUCHHANDLUNG

E. Beispiel: Social Media Anwendungsrichtline Pfefferminzia AG 252

§ 15. Nutzung von Cloud-Technologien im Arbeitsverhältnis

A. Cloud Computing: Begriff und Bedeutung 255
I. Cloud Computing – Fehlen einer einheitlichen Definition 255
II. Trend der Arbeitswelt: Bring Your Own Device 256
III. Gemeinsame Kernmerkmale und Risiken von Cloud-Technologien 256

B. Datenschutzrechtliche Besonderheiten beim Cloud Computing 257
I. Anwendbares Datenschutzrecht 257
1. Anwendbarkeit von DS-GVO und BDSG 257
2. Übertragung auf den Einsatz von Cloud-Services im Beschäftigungsverhältnis 259
II. Datenschutzrechtliche Verantwortlichkeit 260
1. Datenschutzrechtliche „Rollen“ nach der DS-GVO 260
2. Übertragung auf den Einsatz von Cloud-Services im Beschäftigungsverhältnis 261
III. Anforderungen an die Auftragsverarbeitung 262
IV. Probleme bei der Nutzung privater IT (Bring Your Own Device) 263
V. Mitbestimmung 264

§ 16. Datentransfer im Konzern und Zulässigkeit der Datenweitergabe an Dritte

A. Praktische Relevanz und rechtliche Bedeutung 265
I. Praktische Relevanz 265
II. Rechtliche Einordnung und Bedeutung 265

B. Klärung der Begrifflichkeiten 267
I. „Datenübermittlung“ 267
II. „Verantwortlicher“ (Art. 4 Nr. 7 DS-GVO) 267
III. „Dritter“ (Art. 4 Nr. 10 DS-GVO) 268

C. Auftragsverarbeitung – Eigenverarbeitung – Gemeinsam Verantwortliche (Joint Control) 268
I. Auftragsverarbeitung 268
II. Eigenverarbeitung 269
III. Gemeinsam Verantwortliche (Joint Control) 269
IV. Auftragswidrige Nutzung der Daten durch den Auftragsverarbeiter 270

D. Voraussetzungen für die Rechtmäßigkeit einer Auftragsverarbeitung 271
I. Schriftlichkeit der Auftragserteilung 271
1. Form der Auftragserteilung 271
2. Umfang der Dokumentationspflicht 271
II. Auswahl des Auftragnehmers 272

§ 17. Internationale Datenübermittlung

A. Einführung 275

B. Anzuwendendes Recht 276

C. Zweistufige Rechtmäßigkeitsprüfung bei einer Übermittlung in Drittstaaten 277

D. Rechtfertigung einer Datenübermittlung in Drittstaaten 278
I. Allgemeine Grundsätze 278
II. Angemessenes Schutzniveau 279

beck-shop.de
DIE FACHBUCHHANDLUNG

III. Geeignete Garantien 279
1. Standardvertragsklauseln I und II 281
2. Standardvertragsklauseln für Auftragsverarbeiter 282
IV. Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) ... 282
1. Empirie 283
2. Notwendiger Inhalt 283
3. Verbindlichkeit 285
4. Haftung 287
V. Ausnahmen für bestimmte Fälle 289

E. Sonderfall: Datenübermittlung in die USA 290

§ 18. Absicherung des materiellen Datenschutzes durch Transparenz, Organisationspflichten und Dokumentation

A. Transparenz, Organisationspflichten und Dokumentation als tragende Säulen des EU-Datenschutzrechts 293

B. Organisatorische Maßnahmen 294
I. Data Governance als Baustein der Unternehmensorganisation 294
II. Verpflichtung von Beschäftigten auf die Einhaltung des Datenschutzrechts 295
1. Fehlen einer ausdrücklichen Regelung, vergleichbar § 5 BDSG aF 295
2. Muster 295
III. Unternehmensinterne Regelwerke und Prozesse 297

C. Dokumentation, Rechenschaftspflicht 298

D. Transparenz (Informationspflichten, Auskunftsrecht) 299
I. Überblick 299
II. Informationspflichten gegenüber Beschäftigten nach Art. 13, 14 DS-GVO 300
1. Inhalt der Informationspflichten 300
2. Muster 302
III. Auskunftsrecht (Art. 15 DS-GVO) 309
1. Voraussetzungen 309
2. Inhalt und Reichweite der Auskunft 309
3. Einschränkungen und Grenzen des Auskunftsanspruches 312
4. Praktische Umsetzung/Prozess für die Erteilung von Auskünften 313
IV. Benachrichtigung bei Data Breaches (Art. 34 DS-GVO) 314
1. Voraussetzungen 314
2. Rechtzeitigkeit der Benachrichtigung 315
3. Form und Inhalt der Benachrichtigung der Betroffenen (Art. 34 DS-GVO) 316

§ 19. Die Einbindung des betrieblichen Datenschutzbeauftragten – Partner in der Compliance

A. Der Datenschutzbeauftragte im Betrieb 317

B. Pflicht zur Bestellung eines Datenschutzbeauftragten 317

C. Qualifikationsanforderungen 320

D. Bestellung, zugrunde liegendes Rechtsverhältnis und Widerruf 321

E. Die Aufgaben des Datenschutzbeauftragten 323

beck-shop.de
DIE FACHBUCHHANDLUNG

F. Sicherung der Aufgabenerfüllung 324

G. Die strafrechtliche Verantwortung des Datenschutzbeauftragten 328

§ 20. Betriebsverfassungsrechtliche Zulässigkeit einer Datenverarbeitung

A. Allgemeine Fragen des § 87 BetrVG 329
I. Persönlicher Anwendungsbereich 329
II. Erfordernis kollektiver Maßnahmen 330
III. Keine gesetzliche Regelung – Sperre des § 87 Abs. 1 Einleitungssatz BetrVG 330

B. Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG 332
I. Zweck des Mitbestimmungsrechts 332
II. Umfang des Mitbestimmungsrechts 333
1. Technische Einrichtung 333
2. Zur Überwachung 334
a) Überwachung als Erhebung, Verarbeitung und Auswertung 334
b) Selbständige Kontrollwirkung 339
c) Überwachung vs. Kontrolle? 340
d) Durchführung der Überwachung durch Dritte 340
e) Natur der einbezogenen Daten 341
f) Von Verhalten und Leistung der Arbeitnehmer 342
g) Bestimmung zur Überwachung 343
h) Fazit 343
III. Rechtsfolgen 344
1. Individualrechtliche Folgen 344
2. Beweisrechtliche Folgen 345
3. Unterlassungsansprüche 346
4. Straf- und Bußgeldvorschriften des BetrVG: § 119 BetrVG 347
a) Störung oder Behinderung der Tätigkeit der Betriebsverfassungsorgane 347
b) Tauglicher Täter 348
c) Subjektiver Tatbestand 348
d) Verschulden 349
e) Antragsdelikt 349
f) Verjährung 349
IV. Zuständigkeit 350

C. Weitere Mitbestimmungs- und Beteiligungsrechte 351
I. Anwendungsbereich 351
II. Rechtsfolgen 353

D. Informationsrechte des Betriebsrats beim Beschäftigtendatenschutz gemäß § 80 Abs. 2 BetrVG 353
I. Wahrscheinlichkeit des Aufgabenbezugs 354
II. Erforderlichkeit 356
III. Anforderungen an die Geltendmachung des Informationsanspruchs 357
IV. Insbesondere: Informationen bei Internal Investigations 358
1. Bedeutung 358
2. Ablauf einer Internal Investigation 358
3. Informations- und Mitbestimmungsrechte des Betriebsrats 359
a) Informationsbeschaffung 359
b) Bewertung und Auswertung von Informationen 359
c) Investigation Report 359

beck-shop.de
DIE FACHBUCHHANDLUNG

d) Regelung durch Betriebsvereinbarung 360

E. Übersicht: Datenschutzkompetenzen des Betriebsrat zum BetrVG 361

F. Datenschutz gegenüber dem Betriebsrat 361
I. Der Betriebsrat als Adressat des BDSG? 361
II. Datenschutzrechtliche Rechtfertigungstatbestände 362
III. Das Betriebsverfassungsrecht als Grenze von Datenerhebung, -verarbeitung oder -nutzung 364
IV. Kontrolle des Betriebsrats durch den Arbeitgeber? 364

G. Parallele Regelungen des Personalvertretungsrechts 365
I. § 75 Abs. 3 Nr. 17 BPersVG 365
II. Negative Abweichung vom BDSG durch Dienstvereinbarung? 366

§ 21. Haftung bei Datenschutzverstößen

A. Unionsrechtlicher Hintergrund und das anwendbare Recht 367

B. Zivilrechtliche Folgen 368
I. Zurückbehaltungsrecht des Beschäftigten 368
II. Schadensersatzansprüche 370
1. Art. 82 DS-GVO 370
a) Tatbestandliche Voraussetzungen und Beweislast 370
b) Rechtsfolge: Materieller und immaterieller Schadensersatz 373
2. § 280 Abs. 1 S. 1 BGB iVm § 241 Abs. 2 BGB/§ 311 Abs. 2 BGB 375
3. §§ 823 Abs. 1 und 2, 824, 826 BGB 376
4. Hilfspersonen 378
a) Haftung für Hilfspersonen 378
b) Haftung der Hilfsperson 379
5. Konkurrenzen 380
6. Haftung im kirchlichen Datenschutzrecht 381
III. Unterlassungs-, Beseitigungs- und Gegendarstellungsansprüche 381
IV. Herausgabeansprüche und Gewinnabschöpfung 382

C. Straf- und ordnungswidrigkeitenrechtliche Folgen 382

D. Beweisverwertungsverbot? 383

Stichwortverzeichnis 387

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG