Inhaltsverzeichnis

§ 1: Einleitung 33
I. Einige praktische Probleme 33
1. Das verdächtige Personalratsmitglied 33
2. Lidl, Telekom, Deutsche Bahn u. a. 33
3. Neuere technische Entwicklungen 37
4. Staatlicher Zugriff 41
II. Technische Entwicklung und Recht 42
III. Informationstechnologien und Recht 44
IV. Technikbewältigung im Arbeitsrecht? 47

§ 2: Datenverarbeitung im Betrieb und ihre grundsätzlichen rechtlichen Schranken 50
I. Der Tatbestand 50
1. Traditionelle Erscheinungsformen, insbesondere Personalinformationssysteme und Betriebsdatenerfassung 50
2. Aktuelle Entwicklungen 53
3. Technikspezifische Risiken 55
II. Datenschutzrecht auf nationaler und auf EU-Ebene 58
1. Datenschutz im deutschen Recht 58
2. Die Rechtsprechung des EuGH 59
3. Grundrechtecharta und AEUV 63
4. Die EU-Datenschutz-Grundverordnung (DSGVO) 64
a) Entstehungsgeschichte 64
b) Wirkung einer Verordnung 65
c) Auslegungsprobleme vielsprachiger Texte 66
5. Die Öffnungsklausel des Art. 88 DSGVO und das neue BDSG 67
6. Sonderregelungen 68
III. Grundbegriffe im BDSG und in der DSGVO 70
1. Datenschutz als Querschnittsmaterie 70
2. Verbot mit Erlaubnisvorbehalt 72
3. Zweckbindung 73
4. Betroffenenrechte und Implementationsmechanismen . . 74
5. Subsidiarität oder Vorrang? 75

IV. Arbeitsrechtliche Spezialbestimmungen 76
1. Der bisherige § 32 BDSG 76
2. Weitere arbeitsrechtliche Vorschriften 76
3. Mitbestimmungsrechte 77
4. Datenschutz im Telekommunikationsrecht 77
5. Datenschutz im Beamtenrecht 78
6. Ausnahmen vom Datenschutzrecht 79
V. Datenschutzrechtliche Regelungen auf internationaler Ebene 80
1. Europarat 80
2. OECD 81
3. ILO 81
4. UN 82
VI. Offene Fragen und Überblick über den Gang der Darstellung 82

§ 3: Informationelle Selbstbestimmung und EU-Grundrecht auf Datenschutz 86
I. Das Grundrecht auf informationelle Selbstbestimmung – von der Volkszählungsentscheidung bis zur Gegenwart 86
II. Normative Vorgaben für Einschränkungen 90
III. Bedeutung unter der DSGVO 94
IV. Das unionsrechtliche Grundrecht auf Datenschutz 95
V. Die Übertragung des informationellen Selbstbestimmungsrechts ins Arbeits- und Beamtenrecht 97
1. Rechtsprechung 97
a) Bundesverfassungsgericht 97
b) Bundesarbeitsgericht 98
c) Landesarbeitsgerichte 104
d) Verwaltungsgerichte 105
2. Literatur 105
3. Ergebnis und offene Fragen 107
VI. Eingriffe in das informationelle Selbstbestimmungsrecht des Arbeitnehmers und ihre Schranken 108
1. Rechtfertigung durch ein »überwiegendes Allgemeininteresse« 109
2. Rechtfertigung durch ein »überwiegendes Arbeitgeberinteresse«? 110
a) Informationsfreiheit nach Art. 5 Abs. 1 Satz 1 GG? . . 110
b) Unternehmerische Betätigungsfreiheit 111
c) Substanzieller Persönlichkeitsschutz als Grenze? . . . 113
3. Die Zweckbindung der Daten 115
a) Weiter oder enger Zweck 115
b) Grundsätzliches Verbot der Zweckentfremdung . . . 117
4. Verfahrensmäßige Konsequenzen 118
a) Datentransparenz 118

b) Unabhängige Kontrollinstanzen 118
c) Datensicherung 119
VII. Die neuen unionsrechtlichen Rahmenbedingungen – Auswirkungen im Arbeits- und Beamtenrecht 120
1. Art. 7 und 8 Grundrechte-Charta im Arbeitsverhältnis . . 120
2. Die Datenschutz-Grundverordnung 121
a) Persönlichkeitsprofile 121
b) Zweckbindung 122
c) Begleitende Verfahrensbestimmungen 123

§ 4: Voraussetzungen einer wirksamen Einwilligung 124
I. Die Problematik 124
1. Anwendungsbereich 124
2. Die gesetzliche Regelung und der mit ihr verfolgte Zweck. 124
3. Einwilligung und andere Rechtsgrundlagen für die Datenverarbeitung 126
4. Gang der Darstellung 127
II. Formale Erfordernisse 127
1. Zeitpunkt 127
2. Einsichtsfähigkeit des Betroffenen 128
3. Vorherige Information des Betroffenen 129
4. Schriftform? 130
III. Inhaltliche Anforderungen 132
IV. Das Erfordernis der Freiwilligkeit 132
1. Die Ausgangssituation 132
a) Normative Grundlage 132
b) Stellungnahmen in Bezug auf das Arbeitsverhältnis nach bisherigem Recht 134
2. Notwendige Differenzierungen 135
a) Nur Fehlen von Willensmängeln 135
b) Keine Einwilligung im Arbeitsverhältnis? 135
c) Das Koppelungsverbot 136
d) Druck bei Verhandlungen und einseitige Beratung . . 136
e) Angedrohte oder erwartbare Nachteile 137
f) Versprechen hoher Vorteile 138
g) Zusammenfassung: Voraussetzungen einer wirksamen Einwilligung 138
V. Inhaltsschranken der Einwilligung 139
1. Zwingendes Recht: Einstellungsgrundsätze und Grenzen im Arbeitsverhältnis 139
2. Angemessenheitskontrolle 140
VI. Widerruf der Einwilligung 143
VII. Einwilligung in die Verarbeitung sensitiver Daten 145
VIII. Telekommunikation 145

§ 5: Datenerhebung gegenüber Bewerbern 147
I. Die Vorgaben der DSGVO und des BDSG n. F. 147
1. § 26 Abs. 1 BDSG als Rechtsgrundlage 147
a) Der erfasste Personenkreis 147
b) Verzicht auf das Dateierfordernis 151
c) Ausklammerung des persönlichen Nahbereichs 151
2. Erforderlichkeit der Datenverarbeitung 152
3. Verhältnis von § 26 BDSG n. F. zu anderen Vorschriften . 153
4. Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO. 155
5. Die Sonderregeln über sog. sensitive Daten 156
a) Die einzelnen Fälle 156
b) Inhaltliche Voraussetzungen für die Erhebung sensitiver Daten 158
6. Das Gebot der Direkterhebung 160
II. Das Fragerecht des Arbeitgebers 161
1. Die Ausgangssituation 161
2. Die überkommene Rechtsprechung: Rückgriff auf das allgemeine Persönlichkeitsrecht 162
3. Die datenschutzrechtliche Begrenzung: »Erforderlichkeit« nach § 26 Abs. 1 Satz 1 BDSG n. F. 162
4. Zulässigkeit einzelner Fragen 163
a) Privatsphäre 163
b) »Diskriminierungsverdächtige« Tatsachen 164
c) Schwangerschaft und Wehrdienst 165
d) Gesundheitszustand und Eigenschaft als schwerbehinderter Mensch 166
e) Vorstrafen 167
f) Vermögensverhältnisse 168
g) Berufliche Fähigkeiten und Laufbahn 169
5. Hinweis auf den Erhebungszweck 169
6. Das sog. Recht zur Lüge und andere Sanktionen 170
7. Informationspflichten des Arbeitgebers und des Bewerbers 171
III. Ärztliche Untersuchungen und Eignungstests 171
IV. Gentechnische Untersuchungen nach dem Gendiagnostikgesetz 173
V. Datenerhebung bei Dritten und allgemein zugängliche Beschäftigtendaten 176
1. Entsprechende Anwendung der Grundsätze über das Fragerecht 176
2. Einschaltung Dritter als Ausnahmetatbestand 177
3. Einschaltung der Verfassungsschutzbehörden? 179
4. Informationen aus allgemein zugänglichen Quellen, insbesondere aus dem Internet? 179

VI. Digitalisierte Vorauswahl 181
1. Videogestütztes Interview 181
2. Stimmanalyse beim ersten Anruf 181
3. Einsatz von Algorithmen 182
VII. Besonderheiten im öffentlichen Dienst 182
1. Die normative Ausgangslage 182
2. Auslegungsprobleme 184
VIII. Datenerhebung durch private Arbeitsvermittler 185

§ 6: Datenerhebung gegenüber Beschäftigten 186
I. Gesetzliche Vorgaben 186
II. Privatsphäre und Konsumverhalten 188
III. Durchführung des Beschäftigungsverhältnisses 188
1. Entgeltabrechnung 188
2. Arbeitszeit und Arbeitsverhalten 189
3. Torkontrolle 190
4. Weiterförderung 191
5. Erhebung zahlreicher persönlicher Umstände im Hinblick auf eine mögliche »soziale Auswahl«? 191
6. Umfragen im Betrieb 193
7. Übergang zur elektronischen Personalakte 194
IV. Gesundheitsdaten und gentechnische Untersuchungen 195
1. Traditionelle Gesundheitsdaten 195
a) Die Sonderregeln über sensitive Daten 195
b) Informationspflichten des Arbeitnehmers und ihre Grenzen 196
c) Pflicht des Arbeitnehmers, sich untersuchen zu lassen? 198
d) Weitere Datenerhebung durch den Betriebsarzt 200
e) Untersuchungen bei Änderungen der Tätigkeit 200
f) Beschäftigte im Krankenhaus als Patienten 200
2. Zulässigkeit von Gentests? 201
V. Erfassung biometrischer Merkmale 201
1. Anerkennung als sensitives Datum 201
2. Zulässigkeit 202
3. Überschießende Informationen 203
VI. Überwachung des Arbeitsverhaltens: Insbesondere Privatdetektive als verdeckte Ermittler 204
1. Kontrollrecht des Arbeitgebers 204
2. Einsatz von Privatdetektiven 204
3. Die Parallele zum verdeckten Ermittler 205
4. Anwendungsfälle 206
5. Stellen einer »Falle« 206
6. Heimliches Mithören und Verdacht strafbarer Handlungen 207

VII. Überwachung des Arbeitsverhaltens: Videokontrolle 207
1. Praktische Bedeutung und rechtliche Regelung 207
2. Videokontrolle in öffentlich zugänglichen Räumen. . . . 209
a) Der erfasste Bereich 209
b) Die eingesetzte Technik 209
c) Die Voraussetzungen im Einzelnen 210
d) Die schutzwürdigen Interessen der Betroffenen. . . . 210
e) Transparenz 212
f) Umgang mit den erhobenen Daten 213
g) Verhältnis zur DSGVO 214
3. Videoüberwachung in nicht öffentlich zugänglichen Räumen 214
a) Rechtsgrundlage 214
b) Rechtsprechung zur heimlichen und offenen Videoüberwachung. 215
c) Sanktionen bei unerlaubter Videoüberwachung . . . 217
4. Mitbestimmung 218
5. Exkurs: Mitwirkung in Filmen. 218
VIII. Spezielle Überwachungsprogramme 219
1. Beispiele 219
2. Strafsanktionen 220
3. Rechtfertigung durch Einwilligung des Betroffenen? . . . 220
4. Data Loss Prevention 220
5. Social Graph 221
IX. Ortungssysteme und Erstellung eines Bewegungsprofils . . . 221
1. Ortungssysteme 221
a) Die Ausgangssituation 221
b) Das Strafprozessrecht als Vorreiter. 223
c) Zulässigkeitsschranken im Arbeitsrecht 224
2. Erstellung von Bewegungsprofilen im Betrieb 225
3. Mitbestimmung 226
X. Kontrolle durch andere technische Mittel 226
1. RFID 226
2. Einsatz von Drohnen 228
3. Beurteilung durch Dritte auf der Webseite des Arbeitgebers. 229
4. Smart factory. 229
XI. Überwachung der Telekommunikation 229
1. Rechtliche Grundlagen. 229
a) TKG, TMG, BGB 230
b) Vorschriften zum Datenschutz. 231
c) Anwendung der §§ 88 ff. TKG im Arbeitsverhältnis? . 232
aa) Differenzierung zwischen dienstlicher und privater Nutzung 232
bb) Einwände 233

cc) Rechtsfolgen 234
dd) Technische Trennung. 235
d) Anwendbarkeit der §§ 11 ff. TMG im Arbeitsverhältnis? 236
e) Allgemeiner Beschäftigtendatenschutz für die Inhalte . 237
2. Kontrolle der dienstlichen Nutzung von Einrichtungen der Telekommunikation 237
a) Der grundsätzliche Ausgangspunkt 237
b) Mithören von Telefongesprächen. 238
aa) Der Persönlichkeitsschutz und seine Grenzen . . . 238
bb) Äußere Telefondaten 239
cc) Zugriff auf Inhalte: Abwägung der Interessen . . . 239
c) Sonstige Telekommunikationsdienste: E-Mails 240
aa) Die grundsätzliche Behandlung: Zugriff auf die Inhalte? 240
bb) Verschlüsselung 241
cc) Äußere Daten 241
dd) Ausgeschiedene und abwesende Mitarbeiter . . . 242
d) Sonstige Telekommunikationsdienste: Intranet 242
e) Sonstige Telekommunikationsdienste: Internet 243
3. Kontrolle der privaten Nutzung von Einrichtungen der Telekommunikation 245
a) Anforderungen des TKG 245
aa) Wahrung des Fernmeldegeheimnisses nach § 88 TKG 245
bb) Technische Schutzmaßnahmen nach § 109 TKG . 246
4. Anforderungen des TMG. 247
5. Anforderungen bei »Mischtatbeständen« 249
6. Spamfilter. 250
7. Die Mithörerproblematik 251
8. Vorratsdatenspeicherung nach § 113a TKG a. F.? 251
9. Verpflichtung zur Mitteilung der privaten Mobilfunknummer an den Arbeitgeber? 252
XII. Kumulierte Überwachung – die Arbeit im Call Center. 252
XIII. Datenermittlung gegenüber »Verdächtigen« 254
1. Die Ermächtigung des Arbeitgebers durch § 26 Abs. 1 Satz 2 BDSG 254
2. Die Rechtsfolgen 257
3. Das Problem des »Zufallsfunds« 259
4. Mitbestimmung und verdächtiges Betriebsratsmitglied . . 259
5. Einsatz anderer Mittel als der versteckten Videokamera . . 260
6. Einschaltung staatlicher Behörden 261
7. Information der betroffenen Person 261
8. Verbot der Zweckentfremdung. 261
XIV. Arbeitnehmer mit Sonderstatus 261

1. Träger von Berufsgeheimnissen 261
2. Beschäftigte mit fachlicher Unabhängigkeit 263
3. Wissenschaftler 263
XV. Einschaltung Dritter 264
XVI. Besonderheiten im öffentlichen Dienst 264
XVII. Keine Verwertung rechtswidrig erlangter Informationen im Prozess? 265
1. Die Problematik 265
2. Verwertungsverbot bei Verstößen gegen das Persönlichkeitsrecht 265
3. Verwertungsverbot bei Verstößen gegen Betriebsverfassungsrecht 268
XVIII. Sonderregeln für Homeoffice und mobiles Arbeiten? 270

§ 7: Auswertung der erhobenen und gespeicherten Daten und von Big-Data-Erkenntnissen 272
I. Überblick 272
1. Die Entwicklung bis 2009 272
2. Die Regelung des § 32 Abs. 1 Satz 1 BDSG 2009 274
3. DSGVO und § 26 BDSG n. F. 275
4. Überblick über den Gang der Darstellung 276
II. Auswertungen unter Wahrung des Zweckbindungsgrundsatzes: Informationelle Gewaltenteilung 277
1. Festlegung des Zwecks 277
2. Das Beispiel der arbeitsmedizinischen Daten 277
3. Das Beispiel: Betriebliches Eingliederungsmanagement (BEM) 280
a) Der Grundsatz 280
b) Einwilligungen der betroffenen Person 281
c) Verarbeitung von Daten Dritter 282
d) Datenminimierung und Löschung 282
4. Das Beispiel der Daten zur sozialen Auswahl 283
5. Das Beispiel der Daten zur Entgeltabrechnung 283
6. Das Beispiel der Betriebsdaten 284
7. Der große Rest: Personaldaten im engeren Sinn 285
8. Die Separierung einzelner Datenbestände – ein lästiges Novum? 286
III. Die ausnahmsweise zulässige Zweckentfremdung 289
1. Verwendung für andere Zwecke 289
2. Sonderfälle: verbotene Zweckentfremdung 290
a) Schutz der professionellen Datenverarbeiter 290
b) Wissenschaftliche Forschung 290
c) Durch Videoaufnahmen, heimliche Erhebungen und bei der Telekommunikation gewonnene Daten 291
d) Statistische Erhebungen 291

IV. Screening und Rasterfahndung im Betrieb? 292
1. Anschauungsmaterial. 292
2. Bewertung auf der Grundlage des geltenden Rechts 293
a) Die Suche nach Informationsgebern 293
b) Korruptionsbekämpfung: Die Rekonstruktion von Kontobewegungen 293
c) Handlungsmöglichkeiten? 294
V. Compliance als Rechtfertigung? 295
1. Was bedeutet »Compliance«? 295
2. Datenschutz und Compliance 295
3. Allgemeine datenschutzrechtliche Vorgaben 296
4. Die Zulässigkeit einzelner Maßnahmen 296
a) Überblick 296
b) Auskunftspflicht des Arbeitnehmers – aber keine Selbstbezichtigung 297
c) Auskunftspflicht des Arbeitnehmers – Belastung Dritter? 298
d) Gewährung und Annahme von Vorteilen 299
VI. Verbot von Persönlichkeitsprofilen? 299
VII. Einsatz von Erkenntnissen aus der Auswertung von Big Data . 301
VIII. Umgang mit datenschutzwidrig erlangten Informationen . . . 304
IX. Automatisierte Entscheidungen nach Art. 22 DSGVO 305
1. Die Grundentscheidung des Art. 22 DSGVO 305
2. Anwendung im Arbeitsrecht 305
X. Verwendung von Chipkarten 306
XI. Besonderheiten im öffentlichen Dienst? 306

§ 8: Auftragsdatenverarbeitung und Übermittlung von Beschäftigtendaten im Inland 308
I. Die scheinbare Übermittlung: Auftragsdatenverarbeitung . . . 308
1. Die Abgrenzung zur Funktionsübertragung 308
2. Die vertraglichen Beziehungen zum Auftragsverarbeiter . 310
3. Die Einschaltung von Unterauftragnehmern 311
4. Verantwortung des Auftragsverarbeiters 312
5. Auslandsbezüge 312
6. Erleichterungen 313
II. Die Zulässigkeit der Übermittlung im Allgemeinen 314
1. Der Begriff »Übermittlung« 314
a) Eine gesetzliche Definition? 314
b) Übermittlung innerhalb der verantwortlichen Stelle? . 315
c) Veröffentlichung 315
d) Die Problematik des Abrufverfahrens 315
2. Zulässigkeit nach Art. 5 und 6 DSGVO und nach § 26 Abs.1 Satz 1 BDSG n.F. 316
III. Anwendungsfälle 316

1. Übermittlung von Betriebsdaten 317
2. Überlassung von Arbeitskräften 317
3. Konzerndatenverarbeitung 318
4. Übermittlung von Arbeitnehmerdaten an einen Branchenauskunftsdienst 321
5. Weitergabe von Beschäftigtendaten an Koalitionen 322
6. Übermittlung an einen anderen Arbeitgeber beim Arbeitsplatzwechsel 322
7. Weitergabe von Arbeitnehmerdaten zu Zwecken der Werbung und der Markt- und Meinungsforschung? . . . 323
8. Unzulässige Übermittlung per E-Mail 324
9. Datenübermittlung durch Whistleblower 325
10. Sonstige Fälle 325
IV. Zweckbindung beim Empfänger 327
V. Veröffentlichung von Arbeitnehmerdaten am Beispiel des Internet 327
1. Die bewusste Verwendung im Internet 327
2. Der Sonderfall: Fotos im Internet 331
3. Sonstige Arbeitnehmerdaten im Internet 332
4. Die Facebookseite 333
VI. Unternehmensinterne Weitergabe von Arbeitnehmerdaten . . 334
1. Der rechtliche Rahmen 334
2. Inhalt der Personalakte 335
3. Personalgespräche 336
4. Unternehmensinterne Veröffentlichung des Leistungsverhaltens 337
5. Betriebszeitung 338
6. Mitteilungen an den Betriebsrat 339
VII. Besonderheiten im öffentlichen Dienst? 340
1. Die allgemeinen Regeln 340
2. Sonderregeln für Beamte 340
VIII. Umstrukturierung von Unternehmen und Betrieben 341
1. Das datenschutzrechtliche Problem 341
2. Art. 6 Abs. 1 Buchst. f DSGVO als Rechtsgrundlage . . . 342
3. Die Behandlung sensitiver Daten 343
4. Auflösung des Unternehmens 343

§ 9: Drittlandsbezüge, insbesondere Übermittlung von Beschäftigtendaten ins Ausland 345
I. Die Ausgangssituation 345
II. Das Kollisionsrecht der DSGVO 346
1. Die Grundentscheidungen 346
2. Das Niederlassungsprinzip 347
3. Das Marktortprinzip 348
4. Rechtsfolgen 349

5. Nationale Sonderregeln 351
III. Die Übermittlung in EU- und EWR-Mitgliedstaaten 352
IV. Übermittlung in Drittstaaten – allgemeine Grundsätze 353
V. Übermittlung in Drittstaaten mit angemessenem Datenschutzniveau 354
1. Was ist »angemessenes Datenschutzniveau«? 354
2. Lösung über das Verfahren 355
VI. Übermittlung in Drittstaaten ohne angemessenes Datenschutzniveau 357
1. Der Sonderfall USA 357
a) Von Safe Harbor zu Privacy Shield 357
b) Weitere Transferprobleme 360
2. Andere Drittstaaten 361
a) Das notwendige Minimum an Datenübermittlung nach Art. 49 DSGVO 361
b) »Geeignete Garantien« 362
c) Vertragslösungen 363
(1) Individuelle Verträge 363
(2) Musterverträge der EU-Kommission 364
d) Selbstverpflichtungen von Unternehmen – Binding Corporate Rules 366
e) Daten im Internet 367
f) Insbesondere: Cloud Computing 368
VII. Datenimport 369

§ 10: Das Recht des Beschäftigten auf Datentransparenz 370
I. Normative Vorgaben 370
1. Volkszählungsentscheidung 370
2. Datentransparenz im Unionsrecht 371
3. Konkrete Erscheinungsformen 371
II. Die Informationspflicht bei Direkterhebung nach Art. 13 DSGVO 372
1. Der Grundsatz 372
2. Ausnahmen 374
3. Sanktionen 376
III. Informationspflichten bei Nicht-Direkterhebung nach Art. 14 DSGVO 377
IV. Der Auskunftsanspruch nach Art. 15 DSGVO 378
1. Gegenstand der Auskunft 378
2. Praktische Umsetzung 380
3. Ausnahmen 382
4. Zwingender Charakter und Sanktionen bei Verstößen . . 383
5. Gerichtliche Durchsetzung 384
V. Einsicht in die Personalakte nach § 83 BetrVG 384
1. Verhältnis zu Art. 15 DSGVO 384

2. Der Begriff »Personalakte«. 385
3. Was bedeutet »Einsichtnahme«? 385
4. Verbleibender Anwendungsbereich des Art. 15 DSGVO . 385
5. Sonderfall: Betriebsärztlicher Befundbogen 386
VI. Sonderregeln im Beamtenrecht 387
VII. Recht auf Datenübertragbarkeit 388

§ 11: Das Recht des Beschäftigten auf Intervention, insbesondere auf Datenkorrektur 390
I. Einleitung 390
II. Berichtigung nach Art. 16 DSGVO 390
1. Wann ist ein Datum »unrichtig«? 391
2. Wer trägt die Beweislast? 391
3. Wie wird die Berichtigung durchgeführt? 392
4. Berichtigung bei vorheriger Übermittlung an Dritte . . . 392
5. Konkurrenz mit arbeitsvertraglichen Ansprüchen 393
III. Anspruch auf Löschung 393
1. Unrechtmäßige Speicherung 393
2. Wegfall des Speicherungszwecks 394
3. Ausnahmen 396
4. Was bedeutet »Löschung«? 396
IV. Das Recht auf Vergessenwerden 397
V. Anspruch auf Einschränkung der Verarbeitung 400
VI. Widerspruchsrecht nach Art. 21 DSGVO 401
1. Grundsatz 401
2. Anwendungsfälle 402
3. Rechtsfolgen 403
VII. Zwingender Charakter 403
VIII. Gegendarstellung 403
IX. Anspruch auf Schadensersatz 404
X. Besonderheiten im öffentlichen Dienst? 404

§ 12: Mechanismen, um das Datenschutzrecht wirksam werden zu lassen 406
I. Die Schwäche der Individualrechte 406
II. Kompensatorische Mechanismen in der DSGVO 407
III. Verhaltensregeln und Zertifizierung 408
1. Verhaltensregeln 408
2. Zertifizierungen 410
IV. Dokumentationspflichten des Verantwortlichen 411
1. Die allgemeine Verpflichtung nach Art. 5 Abs. 2 DSGVO. 411
2. Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten 411
3. Weitere Dokumentationspflichten 412
V. Datenschutz-Folgenabschätzung 413

VI. Datensicherung und Informationspflicht bei Datenpannen . . 415
1. Datensicherung 415
2. Informationspflicht bei Datenpannen 415
VII. Der »betriebliche« Datenschutzbeauftragte 417
1. Pflicht zur Benennung 418
a) Überschreitung bestimmter Schwellenwerte 418
b) Notwendige Benennung auch bei geringerer Beschäftigtenzahl 419
c) Behördlicher Datenschutzbeauftragter 420
d) Freiwillige Bestellung 420
e) Sanktionen 420
2. Die Benennung einer geeigneten Person 420
a) Allgemeine Voraussetzungen 420
b) Fachkunde und Fehlen von Interessenkollisionen . . . 422
c) Beteiligung des Betriebsrats 423
d) Mitteilung und Bestellung einer ungeeigneten Person . 424
3. Aufgaben des Datenschutzbeauftragten 425
a) Beratung 425
b) Kontrolle 425
c) Zusammenarbeit mit der Aufsichtsbehörde 426
d) Fortbildung 426
e) Weitere Aufgaben 426
f) Anordnungsbefugnisse? 426
4. Die Absicherung der Aufgabenerfüllung 427
a) Zeit und Hilfspersonal 427
b) Teilnahme an Fort- und Weiterbildungsveranstaltungen 428
c) Stellung in der Hierarchie 429
d) Weisungsfreiheit und Geheimhaltungspflicht 429
e) Benachteiligungsverbot 430
5. Abberufung des Datenschutzbeauftragten 431
a) Verlangen der Aufsichtsbehörde? 431
b) Widerruf der Benennung aus wichtigem Grund 432
c) Erstreckung des Schutzes auf das Arbeitsverhältnis . . 433
d) Befristung 434
e) Externe Datenschutzbeauftragte 435
f) Freiwillig bestellte Datenschutzbeauftragte 435
6. Verbleibende Defizite in der Rechtsstellung 435
VIII. Die unabhängige Aufsichtsbehörde 436
1. Überblick 436
2. Aufgaben 437
3. Befugnisse 437
4. Zuständigkeiten 438
5. Unabhängigkeit der Aufsichtsbehörde 439
6. Grenzüberschreitende Zusammenarbeit 440

d) Veränderung der technischen Einrichtung 527
e) Alt-Einrichtungen 528
f) Einsatz fremder Systeme 529
7. Gesetzes- und Tarifvorbehalt 530
8. Besonderheiten im Tendenzbetrieb? 532
III. Rechtliche Schranken für eine Regelung durch Betriebsrat und Arbeitgeber 532
1. Allgemeine Grenzen 533
a) Zwingendes Recht 533
b) Grundrechtsbindung 533
c) Kann durch Betriebsvereinbarung und Einigungsstellenspruch von der DSGVO zu Lasten oder zu Gunsten der Beschäftigten abgewichen werden? . . . 534
d) »Billiger« Ausgleich der Interessen 535
e) Einbeziehung aller »Beschäftigten«? 536
2. Insbesondere: Persönlichkeitsschutz des Arbeitnehmers . 536
3. Insbesondere: Telefondatenerfassung 538
4. Billige Abwägung der beiderseitigen Interessen 540
a) Versuche zur Beschränkung des Regelungsspielraums 540
b) Die abzuwägenden Interessen 541
c) Was ist »billiger« Ausgleich? 542
5. Überwachung des Betriebsrats 545
IV. Ausübung und Durchsetzung des Mitbestimmungsrechts – Abschluss von Betriebsvereinbarungen 546
1. Einzelbetriebsrat, Gesamtbetriebsrat oder Konzernbetriebsrat? 546
2. Initiativrechte des Betriebsrats 548
3. Betriebsvereinbarungen 550
4. Rahmenbetriebsvereinbarungen 551
5. Ausübung des Mitbestimmungsrechts durch Regelungsabrede? 552
6. Durchsetzung des Mitbestimmungsrechts 553
7. Anpassung bestehender Betriebsvereinbarungen 554
8. Sprecherausschussvereinbarungen 554
V. Anwendung des § 87 Abs. 1 Nr. 6 BetrVG auf einzelne Problembereiche 555
1. Probleme um den PC 557
a) Das isolierte Gerät 557
b) Das vernetzte Gerät 558
2. Anwendung auf E-Mail und Internet 559
3. Integration sozialer Netzwerke in den Arbeitsprozess . . . 560
4. Videoüberwachung 561
5. Weitere Problemfälle: Erfassung biometrischer Merkmale, Bestimmung des Aufenthaltsorts, elektronische Personalakte, Nutzung mobiler Geräte 561

6. Arbeit 4.0: Wearables und Datenbrillen als Erscheinungsform . . . 562
7. Änderungen des technischen Systems . . . 563
8. Maßnahmen auf Veranlassung einer ausländischen Konzernspitze . . . 563
VI. Sanktionen bei Verletzung des Mitbestimmungsrechts . . . 564
VII. Verwertungsverbot? . . . 565
1. Allgemeiner Grundsatz . . . 565
2. Ablehnung des Verwertungsverbots durch die Rechtsprechung . . . 565
3. Gegenargumente . . . 566
4. Erkenntnisse über Dritte . . . 567

§ 15: Besonderheiten der Personalvertretung . . . 568
I. Überblick . . . 568
II. Die Rechtmäßigkeitskontrolle durch den Personalrat nach § 68 Abs. 1 Nr. 2 BPersVG . . . 570
1. Worauf bezieht sich die Kontrollfunktion des Personalrats? 570
2. Formen der Umsetzung . . . 571
a) Information des Personalrats durch den Dienststellenleiter . . . 571
b) Eigene Ermittlungen des Personalrats . . . 573
c) Zuziehung eines Sachverständigen . . . 574
d) Schulung und Fortbildung . . . 574
e) Einleitung eines Beschlussverfahrens . . . 575
f) Einschaltung des Datenschutzbeauftragten . . . 576
g) Verschwiegenheitspflicht . . . 576
3. Umgang des Personalrats mit Beschäftigtendaten . . . 577
III. Präventiver Persönlichkeitsschutz durch Ausübung von Beteiligungsrechten . . . 577
1. Überblick . . . 577
2. Zweck der Beteiligungsrechte . . . 579
3. Inhalt von Personalfragebogen nach § 75 Abs. 3 Nr. 8 und § 76 Abs. 2 Nr. 2 BPersVG . . . 580
4. Beurteilungsrichtlinien nach § 75 Abs. 3 Nr. 9 bzw. § 76 Abs. 2 Nr. 3 BPersVG . . . 581
5. Auswahlrichtlinien nach § 76 Abs. 2 Nr. 8 BPersVG . . . 582
6. Mitbestimmung nach § 75 Abs. 3 Nr. 17 BPersVG . . . 582
7. Konkurrenz von Beteiligungsrechten . . . 585
8. Stufenvertretung . . . 586

§ 16: Staatlicher Zugriff auf Beschäftigtendaten . . . 587
I. Überblick . . . 587
II. Beschäftigtendaten als Gegenstand der Rasterfahndung . . . 588
1. Rechtsgrundlagen . . . 588

2. Datenschutzrechtliche und arbeitsrechtliche Konsequenzen . . . 590
a) Recht des Arbeitgebers zur Datenübermittlung 590
b) Information des Betroffenen . . . 590
c) Verdachtskündigung? . . . 590
d) Verdachtsversetzung? . . . 591
III. Überwachung der Telekommunikation . . . 591
IV. Behördlich angeordnete Maßnahmen im Betrieb . . . 592
V. Sicherheitsüberprüfung . . . 593
1. Das Verfahren der Sicherheitsüberprüfung . . . 594
a) Erfasster Personenkreis . . . 594
b) Zuständige Behörde . . . 594
c) Sicherheitserklärung . . . 594
d) Kriterien für die Sicherheitsüberprüfung . . . 594
e) Anhörung des Betroffenen . . . 595
f) Entscheidung . . . 595
g) Wiederholung des Verfahrens . . . 596
h) Behandlung der angefallenen Daten . . . 596
2. Handhabung der Zuverlässigkeitskriterien durch die Rechtsprechung . . . 596
3. Erfasste Bereiche . . . 598
4. Arbeitsrechtliche Folgen . . . 600
a) Personenbedingte Kündigung . . . 600
b) Ausdehnung auf nicht vom SÜG erfasste Bereiche? . . . 600
5. Rechtsschutzmöglichkeiten bei verweigertem Zugang zu sicherheitsempfindlichen Bereichen . . . 601
VI. Abgleichung mit Antiterrorlisten . . . 602
VII. ECHELON und NSA . . . 604
1. Echelon . . . 604
2. NSA . . . 605

§ 17: Einige Perspektiven . . . 606
I. Die permanente Reformdiskussion . . . 606
II. Die DSGVO als Paukenschlag . . . 608
III. Datenschutz als Wettbewerbsfaktor . . . 609
IV. Transparenz des Datenschutzrechts . . . 611
V. Die nicht (voll) bewältigten Probleme . . . 612
1. Cloud Computing . . . 612
2. Big Data . . . 613
3. Datenschutz im Internet . . . 614