Inhaltsübersicht

Vorwort	5
Abkürzungsverzeichnis	27
§ 1: Einleitung	33
§ 2: Datenverarbeitung im Betrieb und ihre grundsätzlichen rechtlichen Schranken	49
§ 3: Informationelle Selbstbestimmung und EU-Grundrecht auf Datenschutz	84
§ 4: Voraussetzungen einer wirksamen Einwilligung	121
§ 5: Datenerhebung gegenüber Bewerbern	142
§ 6: Datenerhebung gegenüber Beschäftigten	177
§ 7: Auswertung der erhobenen und gespeicherten Daten und von Big-Data-Erkenntnissen	256
§ 8: Auftragsdatenverarbeitung und Übermittlung von Beschäftigten- daten im Inland	291
§ 9: Drittlandsbezüge, insbesondere Übermittlung von Beschäftigten- daten ins Ausland	325
§ 10: Das Recht des Beschäftigten auf Datentransparenz	349
§ 11: Das Recht des Beschäftigten auf Intervention, insbesondere auf Datenkorrektur	368
§ 12: Mechanismen, um das Datenschutzrecht wirksam werden zu lassen	383
§ 13: Kontrolle durch den Betriebsrat	429
§ 14: Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG und Abschluss von Betriebsvereinbarungen	460
§ 15: Besonderheiten der Personalvertretung	538
§ 16: Staatlicher Zugriff auf Beschäftigtendaten	556
§ 17: Einige Perspektiven	574
Literaturverzeichnis	583
Stichwortverzeichnis	639

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	40
II. Technische Entwicklung und Recht	42
III. Informationstechnologien und Recht	43
IV. Technikbewältigung im Arbeitsrecht?	46
§ 2: Datenverarbeitung im Betrieb und ihre grundsätzlichen rechtlichen Schranken	49
I. Der Tatbestand	49
1. Traditionelle Erscheinungsformen, insbesondere Personalinformationssysteme und Betriebsdatenerfassung	49
2. Aktuelle Entwicklungen	52
3. Technikspezifische Risiken	54
II. Datenschutzrecht auf nationaler und auf EU-Ebene	57
1. Datenschutz im deutschen Recht	57
2. Die Rechtsprechung des EuGH	58
3. Grundrechtecharta und AEUV	62
4. Die EU-Datenschutz-Grundverordnung (DSGVO)	63
a) Entstehungsgeschichte	63
b) Wirkung einer Verordnung	64
c) Auslegungsprobleme vielsprachiger Texte	64
5. Die Öffnungsklausel des Art. 88 DSGVO und das neue BDSG	65
6. Sonderregelungen	67
III. Grundbegriffe im BDSG und in der DSGVO	68
1. Datenschutz als Querschnittsmaterie	68
2. Verbot mit Erlaubnisvorbehalt	70
3. Zweckbindung	72
4. Betroffenenrechte und Implementationsmechanismen	73
5. Subsidiarität oder Vorrang?	73
IV. Arbeitsrechtliche Spezialbestimmungen	74

Inhaltsverzeichnis

1.	Der bisherige § 32 BDSG	74
2.	Weitere arbeitsrechtliche Vorschriften	75
3.	Mitbestimmungsrechte	75
4.	Datenschutz im Telekommunikationsrecht	76
5.	Datenschutz im Beamtenrecht	76
6.	Ausnahmen vom Datenschutzrecht	77
V.	Datenschutzrechtliche Regelungen auf internationaler Ebene	79
1.	Europarat	79
2.	OECD	80
3.	ILO	80
4.	UN	80
VI.	Offene Fragen und Überblick über den Gang der Darstellung	81
§ 3:	Informationelle Selbstbestimmung und EU-Grundrecht auf Datenschutz	84
I.	Das Grundrecht auf informationelle Selbstbestimmung – von der Volkszählungsentscheidung bis zur Gegenwart	84
II.	Normative Vorgaben für Einschränkungen	88
III.	Bedeutung unter der DSGVO	92
IV.	Das unionsrechtliche Grundrecht auf Datenschutz	93
V.	Die Übertragung des informationellen Selbstbestimmungs- rechts ins Arbeits- und Beamtenrecht	95
1.	Rechtsprechung	95
a)	Bundesverfassungsgericht	95
b)	Bundesarbeitsgericht	96
c)	Landesarbeitsgerichte	101
d)	Verwaltungsgerichte	102
2.	Literatur	103
3.	Ergebnis und offene Fragen	105
VI.	Eingriffe in das informationelle Selbstbestimmungsrecht des Arbeitnehmers und ihre Schranken	106
1.	Rechtfertigung durch ein »überwiegendes Allgemein- interesse«	106
2.	Rechtfertigung durch ein »überwiegendes Arbeitgeber- interesse«?	107
a)	Informationsfreiheit nach Art. 5 Abs. 1 Satz 1 GG?	107
b)	Unternehmerische Betätigungsfreiheit	108
c)	Substanzieller Persönlichkeitsschutz als Grenze?	110
3.	Die Zweckbindung der Daten	112
a)	Weiter oder enger Zweck	112
b)	Grundsätzliches Verbot der Zweckentfremdung	114
4.	Verfahrensmäßige Konsequenzen	115
a)	Datentransparenz	115
b)	Unabhängige Kontrollinstanzen	116
c)	Datensicherung	116

VII.	Die neuen unionsrechtlichen Rahmenbedingungen –	
	Auswirkungen im Arbeits- und Beamtenrecht	117
	1. Art. 7 und 8 Grundrechte-Charta im Arbeitsverhältnis	117
	2. Die Datenschutz-Grundverordnung	118
	a) Persönlichkeitsprofile	118
	b) Zweckbindung	119
	c) Begleitende Verfahrensbestimmungen	120
§ 4:	Voraussetzungen einer wirksamen Einwilligung	121
I.	Die Problematik	121
	1. Anwendungsbereich	121
	2. Die gesetzliche Regelung und der mit ihr verfolgte Zweck	121
	3. Einwilligung und andere Rechtsgrundlagen für die Datenverarbeitung	123
	4. Gang der Darstellung	123
II.	Formale Erfordernisse	124
	1. Zeitpunkt	124
	2. Einsichtsfähigkeit des Betroffenen	124
	3. Vorherige Information des Betroffenen	125
	4. Schriftform?	126
III.	Inhaltliche Anforderungen	128
IV.	Das Erfordernis der Freiwilligkeit	128
	1. Die Ausgangssituation	128
	a) Normative Grundlage	128
	b) Stellungnahmen in Bezug auf das Arbeitsverhältnis nach bisherigem Recht	130
	2. Notwendige Differenzierungen	131
	a) Nur Fehlen von Willensmängeln?	131
	b) Keine Einwilligung im Arbeitsverhältnis?	131
	c) Das Koppelungsverbot	132
	d) Druck bei Verhandlungen und einseitige Beratung	132
	e) Angedrohte oder erwartbare Nachteile	133
	f) Versprechen hoher Vorteile	133
	g) Zusammenfassung: Voraussetzungen einer wirksamen Einwilligung	134
V.	Inhaltsschranken der Einwilligung	134
	1. Zwingendes Recht: Einstellungsgrundsätze und Grenzen im Arbeitsverhältnis	134
	2. Angemessenheitskontrolle	136
VI.	Widerruf der Einwilligung	139
VII.	Einwilligung in die Verarbeitung sensibler Daten	140
VIII.	Telekommunikation	141

Inhaltsverzeichnis

§ 5: Datenerhebung gegenüber Bewerbern	142
I. Die Vorgaben der DSGVO	142
1. § 26 Abs. 1 BDSG als Rechtsgrundlage	142
a) Der erfasste Personenkreis	142
b) Verzicht auf das Dateierfordernis	145
c) Ausklammerung des persönlichen Nahbereichs	146
2. Verhältnis von § 26 BDSG n.F. zu anderen Vorschriften	147
3. Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO	148
4. Die Sonderregeln über sog. sensitive Daten	149
a) Die einzelnen Fälle	150
b) Inhaltliche Voraussetzungen für die Erhebung sensitiver Daten	151
5. Das Gebot der Direkterhebung	153
II. Das Fragerecht des Arbeitgebers	154
1. Die Ausgangssituation	154
2. Die überkommene Rechtsprechung: Rückgriff auf das allgemeine Persönlichkeitsrecht	155
3. Die datenschutzrechtliche Begrenzung: »Erforderlichkeit« nach § 26 Abs. 1 Satz 1 BDSG n.F.	155
4. Zulässigkeit einzelner Fragen	156
a) Privatsphäre	156
b) »Diskriminierungsverdächtige« Tatsachen	157
c) Schwangerschaft und Wehrdienst	157
d) Gesundheitszustand und Eigenschaft als schwer- behinderter Mensch	158
e) Vorstrafen	160
f) Vermögensverhältnisse	161
g) Berufliche Fähigkeiten und Laufbahn	161
5. Hinweis auf den Erhebungszweck	162
6. Das sog. Recht zur Lüge und andere Sanktionen	163
7. Informationspflichten des Arbeitgebers und des Bewerbers	164
III. Ärztliche Untersuchungen und Eignungstests	164
IV. Gentechnische Untersuchungen nach dem Gendiagnostik- gesetz	166
V. Datenerhebung bei Dritten und allgemein zugängliche Beschäftigtendaten	169
1. Entsprechende Anwendung der Grundsätze über das Fragerecht	169
2. Einschaltung Dritter als Ausnahmetatbestand	170
3. Einschaltung der Verfassungsschutzbehörden?	171
4. Informationen aus allgemein zugänglichen Quellen, insbesondere aus dem Internet?	172
VI. Besonderheiten im öffentlichen Dienst	173
1. Die normative Ausgangslage	173

2.	Auslegungsprobleme	174
VII.	Datenerhebung durch private Arbeitsvermittler	176
§ 6:	Datenerhebung gegenüber Beschäftigten	177
I.	Gesetzliche Vorgaben	177
II.	Privatsphäre und Konsumverhalten	178
III.	Durchführung des Beschäftigungsverhältnisses	179
1.	Entgeltabrechnung	179
2.	Arbeitszeit und Arbeitsverhalten	180
3.	Torkontrolle	180
4.	Weiterförderung	181
5.	Erhebung zahlreicher persönlicher Umstände im Hinblick auf eine mögliche »soziale Auswahl«?	181
6.	Umfragen im Betrieb	182
7.	Übergang zur elektronischen Personalakte	184
IV.	Gesundheitsdaten und gentechnische Untersuchungen	184
1.	Traditionelle Gesundheitsdaten	184
a)	Die Sonderregeln über sensitive Daten	184
b)	Informationspflichten des Arbeitnehmers und ihre Grenzen	186
c)	Pflicht des Arbeitnehmers, sich untersuchen zu lassen?	187
d)	Weitere Datenerhebung durch den Betriebsarzt	189
e)	Untersuchungen bei Änderungen der Tätigkeit	189
f)	Beschäftigte im Krankenhaus als Patienten	190
2.	Zulässigkeit von Gentests?	190
V.	Erfassung biometrischer Merkmale	191
1.	Anerkennung als sensibles Datum	191
2.	Zulässigkeit	191
3.	Überschießende Informationen	193
VI.	Überwachung des Arbeitsverhaltens: Insbesondere Privatdetektive als verdeckte Ermittler	193
1.	Kontrollrecht des Arbeitgebers	193
2.	Einsatz von Privatdetektiven	194
3.	Die Parallele zum verdeckten Ermittler	194
4.	Anwendungsfälle	195
5.	Stellen einer »Falle«	196
6.	Heimliches Mithören und Verdacht strafbarer Handlungen	196
VII.	Überwachung des Arbeitsverhaltens: Videokontrolle	197
1.	Praktische Bedeutung und rechtliche Regelung	197
2.	Videokontrolle in öffentlich zugänglichen Räumen	198
a)	Der erfasste Bereich	198
b)	Die eingesetzte Technik	198
c)	Die Voraussetzungen im Einzelnen	199
d)	Die schutzwürdigen Interessen der Betroffenen	199

Inhaltsverzeichnis

e)	Transparenz	201
f)	Umgang mit den erhobenen Daten	202
g)	Verhältnis zur DSGVO	202
3.	Videouberwachung in nicht öffentlich zugänglichen Räumen	203
a)	Rechtsgrundlage	203
b)	Rechtsprechung – heimliche und offene Videoüber- wachung	203
c)	Sanktionen bei unerlaubter Videoüberwachung	205
4.	Mitbestimmung	206
5.	Exkurs: Mitwirkung in Filmen	206
VIII.	Spezielle Überwachungsprogramme	207
1.	Beispiele	207
2.	Strafsanktionen	207
3.	Rechtfertigung durch Einwilligung des Betroffenen?	208
4.	Data Loss Prevention	208
IX.	Ortungssysteme und Erstellung eines Bewegungsprofils	209
1.	Ortungssysteme	209
a)	Die Ausgangssituation	209
b)	Das Strafprozessrecht als Vorreiter	210
c)	Zulässigkeitsschranken im Arbeitsrecht	211
2.	Erstellung von Bewegungsprofilen im Betrieb	212
3.	Mitbestimmung	213
X.	Kontrolle durch andere technische Mittel	213
1.	RFID	213
2.	Einsatz von Drohnen	215
XI.	Überwachung der Telekommunikation	216
1.	Rechtliche Grundlagen	216
a)	TKG, TMG, BGB	216
b)	Vorschriften zum Datenschutz	217
c)	Anwendung der §§ 88 ff. TKG im Arbeitsverhältnis?	218
aa)	Differenzierung zwischen dienstlicher und privater Nutzung	218
bb)	Einwände	219
cc)	Rechtsfolgen	220
dd)	Technische Trennung	222
d)	Anwendbarkeit der §§ 11 ff. TMG im Arbeits- verhältnis?	222
e)	Allgemeiner Beschäftigtendatenschutz für die Inhalte	223
2.	Kontrolle der dienstlichen Nutzung von Einrichtungen der Telekommunikation	224
a)	Der grundsätzliche Ausgangspunkt	224
b)	Mithören von Telefongesprächen	224
aa)	Der Persönlichkeitsschutz und seine Grenzen	224
bb)	Äußere Telefondaten	225

cc)	Zugriff auf Inhalte: Abwägung der Interessen . . .	225
c)	Sonstige Telekommunikationsdienste: E-Mails . . .	226
aa)	Die grundsätzliche Behandlung: Zugriff auf die Inhalte?	226
bb)	Verschlüsselung	227
cc)	Äußere Daten	227
dd)	Ausgeschiedene und abwesende Mitarbeiter . . .	228
d)	Sonstige Telekommunikationsdienste: Intranet . . .	228
e)	Sonstige Telekommunikationsdienste: Internet . . .	229
3.	Kontrolle der privaten Nutzung von Einrichtungen der Telekommunikation	231
a)	Anforderungen des TKG	231
aa)	Wahrung des Fernmeldegeheimnisses nach § 88 TKG	231
bb)	Technische Schutzmaßnahmen nach § 109 TKG .	232
4.	Anforderungen des TMG	233
5.	Anforderungen bei »Mischtatbeständen«	235
6.	Spamfilter	236
7.	Die Mithörerproblematik	237
8.	Vorratsdatenspeicherung nach § 113a TKG a. F.?	237
XII.	Kumulierte Überwachung – die Arbeit im Call Center	238
XIII.	Datenermittlung gegenüber »Verdächtigen«	240
1.	Die Ermächtigung des Arbeitgebers durch § 26 Abs. 1 Satz 2 BDSG	240
2.	Die Rechtsfolgen	242
XIV.	Arbeitnehmer mit Sonderstatus	246
1.	Träger von Berufsgeheimnissen	246
2.	Beschäftigte mit fachlicher Unabhängigkeit	247
3.	Wissenschaftler	248
XV.	Einschaltung Dritter	249
XVI.	Besonderheiten im öffentlichen Dienst	249
XVII.	Keine Verwertung rechtswidrig erlangter Informationen im Prozess?	249
1.	Die Problematik	249
2.	Verwertungsverbot bei Verstößen gegen das Persönlich- keitsrecht	249
3.	Verwertungsverbot bei Verstößen gegen Betriebs- verfassungsrecht	252
XVIII.	Sonderregeln für Homeoffice und mobiles Arbeiten?	254
§ 7:	Auswertung der erhobenen und gespeicherten Daten und von Big-Data-Erkenntnissen	256
I.	Überblick	256
1.	Die Entwicklung bis 2009	256
2.	Die Regelung des § 32 Abs. 1 Satz 1 BDSG 2009	258

Inhaltsverzeichnis

3.	DSGVO und § 26 BDSG n. F.	259
4.	Überblick über den Gang der Darstellung	260
II.	Auswertungen unter Wahrung des Zweckbindungsgrundsatzes: Informationelle Gewaltenteilung	261
1.	Festlegung des Zwecks	261
2.	Das Beispiel der arbeitsmedizinischen Daten	261
3.	Das Beispiel Eingliederungsmanagement	264
4.	Das Beispiel der Daten zur sozialen Auswahl	266
5.	Das Beispiel der Daten zur Entgeltabrechnung	266
6.	Das Beispiel der Betriebsdaten	267
7.	Der große Rest: Personaldaten im engeren Sinn	268
8.	Die Separierung einzelner Datenbestände – ein lästiges Novum?	269
III.	Die ausnahmsweise zulässige Zweckentfremdung	272
1.	Verwendung für andere Zwecke	272
2.	Sonderfälle: verbotene Zweckentfremdung	273
a)	Schutz der professionellen Datenverarbeiter	273
b)	Wissenschaftliche Forschung	273
c)	Durch Videoaufnahmen, heimliche Erhebungen und bei der Telekommunikation gewonnene Daten	274
d)	Statistische Erhebungen	274
IV.	Screening und Rasterfahndung im Betrieb?	275
1.	Anschauungsmaterial	275
2.	Bewertung auf der Grundlage des geltenden Rechts	276
a)	Die Suche nach Informationsgebern	276
b)	Korruptionsbekämpfung: Die Rekonstruktion von Kontobewegungen	276
c)	Handlungsmöglichkeiten?	277
V.	Compliance als Rechtfertigung?	278
1.	Was bedeutet »Compliance«?	278
2.	Datenschutz und Compliance	278
3.	Allgemeine datenschutzrechtliche Vorgaben	279
4.	Die Zulässigkeit einzelner Maßnahmen	279
a)	Überblick	279
b)	Auskunftspflicht des Arbeitnehmers – aber keine Selbstbeziehung	280
c)	Auskunftspflicht des Arbeitnehmers – Belastung Dritter?	281
d)	Gewährung und Annahme von Vorteilen	282
VI.	Verbot von Persönlichkeitsprofilen?	282
VII.	Einsatz von Erkenntnissen aus der Auswertung von Big Data	284
VIII.	Umgang mit datenschutzwidrig erlangten Informationen	287
IX.	Automatisierte Entscheidungen nach Art. 22 DSGVO	287
1.	Die Grundentscheidung des Art. 22 DSGVO	287
2.	Anwendung im Arbeitsrecht	288

X.	Verwendung von Chipkarten	289
XI.	Besonderheiten im öffentlichen Dienst ?	289
§ 8:	Auftragsdatenverarbeitung und Übermittlung von	
	Beschäftigtendaten im Inland	291
I.	Die scheinbare Übermittlung: Auftragsdatenverarbeitung	291
1.	Die Abgrenzung zur Funktionsübertragung	291
2.	Die vertraglichen Beziehungen zum Auftragsverarbeiter	292
3.	Die Einschaltung von Unterauftragnehmern	294
4.	Verantwortung des Auftragsverarbeiters	295
5.	Auslandsbezüge	295
6.	Erleichterungen	296
II.	Die Zulässigkeit der Übermittlung im Allgemeinen	296
1.	Der Begriff »Übermittlung«	296
a)	Eine gesetzliche Definition?	296
b)	Übermittlung innerhalb der verantwortlichen Stelle?	297
c)	Veröffentlichung	298
d)	Die Problematik des Abrufverfahrens	298
2.	Zulässigkeit nach Art. 5 und 6 DSGVO und nach § 26 Abs. 1 Satz 1 BDSG n.F.	299
III.	Anwendungsfälle	299
1.	Übermittlung von Betriebsdaten	299
2.	Überlassung von Arbeitskräften	300
3.	Konzerndatenverarbeitung	301
4.	Übermittlung von Arbeitnehmerdaten an einen Bran- chenauskunftsdienst	304
5.	Weitergabe von Beschäftigtendaten an Koalitionen	305
6.	Übermittlung an einen anderen Arbeitgeber beim Ar- beitsplatzwechsel	305
7.	Weitergabe von Arbeitnehmerdaten zu Zwecken der Werbung und der Markt- und Meinungsforschung?	306
8.	Unzulässige Übermittlung per E-Mail	306
9.	Datenübermittlung durch Whistleblower	307
10.	Sonstige Fälle	308
IV.	Zweckbindung beim Empfänger	309
V.	Veröffentlichung von Arbeitnehmerdaten am Beispiel des Internet	310
1.	Die bewusste Verwendung im Internet	310
2.	Der Sonderfall: Fotos im Internet	313
3.	Sonstige Arbeitnehmerdaten im Internet	314
VI.	Unternehmensinterne Weitergabe von Arbeitnehmerdaten	315
1.	Der rechtliche Rahmen	315
2.	Inhalt der Personalakte	316
3.	Personalgespräche	317

Inhaltsverzeichnis

4. Unternehmensinterne Veröffentlichung des Leistungsverhaltens	318
5. Betriebszeitung	319
6. Mitteilungen an den Betriebsrat	319
VII. Besonderheiten im öffentlichen Dienst?	320
1. Die allgemeinen Regeln	320
2. Sonderregeln für Beamte	321
VIII. Umstrukturierung von Unternehmen und Betrieben	322
1. Das datenschutzrechtliche Problem	322
2. Art. 6 Abs. 1 Buchst. f DSGVO als Rechtsgrundlage	323
3. Die Behandlung sensibler Daten	324
4. Auflösung des Unternehmens	324

§ 9: Drittlandsbezüge, insbesondere Übermittlung von Beschäftigtendaten ins Ausland	325
I. Die Ausgangssituation	325
II. Das Kollisionsrecht der DSGVO	326
1. Die Grundentscheidungen	326
2. Das Niederlassungsprinzip	327
3. Das Marktortprinzip	328
4. Rechtsfolgen	329
5. Nationale Sonderregeln	330
III. Die Übermittlung in EU- und EWR-Mitgliedstaaten	332
IV. Übermittlung in Drittstaaten – allgemeine Grundsätze	333
V. Übermittlung in Drittstaaten mit angemessenem Datenschutzniveau	334
1. Was ist »angemessenes Datenschutzniveau«?	334
2. Lösung über das Verfahren	335
V. Übermittlung in Drittstaaten ohne angemessenes Datenschutzniveau	337
1. Der Sonderfall USA	337
a) Von Safe Harbor zu Privacy Shield	337
b) Weitere Transferprobleme	339
2. Andere Drittstaaten	341
a) Das notwendige Minimum an Datenübermittlung nach Art. 49 DSGVO	341
b) »Geeignete Garantien«	342
c) Vertragslösungen	343
d) Selbstverpflichtungen von Unternehmen – Binding Corporate Rules	345
e) Daten im Internet	346
f) Insbesondere: Cloud Computing	347
VI. Datenimport	347

§ 10: Das Recht des Beschäftigten auf Datentransparenz	349
I. Normative Vorgaben	349
1. Volkszählungsentscheidung	349
2. Datentransparenz im Unionsrecht	350
3. Konkrete Erscheinungsformen	350
II. Die Informationspflicht bei Direkterhebung nach	
Art. 13 DSGVO	351
1. Der Grundsatz	351
2. Ausnahmen	353
3. Sanktionen	355
III. Informationspflichten bei Nicht-Direkterhebung nach	
Art. 14 DSGVO	356
IV. Der Auskunftsanspruch nach Art. 15 DSGVO	357
1. Gegenstand der Auskunft	357
2. Praktische Umsetzung	358
3. Ausnahmen	360
4. Zwingender Charakter und Sanktionen bei Verstößen	362
5. Gerichtliche Durchsetzung	362
V. Einsicht in die Personalakte nach § 83 BetrVG	363
1. Verhältnis zu Art. 15 DSGVO	363
2. Der Begriff »Personalakte«	363
3. Was bedeutet »Einsichtnahme«?	363
4. Verbleibender Anwendungsbereich des Art. 15 DSGVO	364
5. Sonderfall: Betriebsärztlicher Befundbogen	365
VI. Sonderregeln im Beamtenrecht	365
VII. Recht auf Datenübertragbarkeit	367
§ 11: Das Recht des Beschäftigten auf Intervention, insbesondere auf	
Datenkorrektur	368
I. Einleitung	368
II. Berichtigung nach Art. 16 DSGVO	368
1. Wann ist ein Datum »unrichtig«?	369
2. Wer trägt die Beweislast?	369
3. Wie wird die Berichtigung durchgeführt?	370
4. Berichtigung bei vorheriger Übermittlung an Dritte	370
5. Konkurrenz mit arbeitsvertraglichen Ansprüchen	371
III. Anspruch auf Löschung	371
1. Unrechtmäßige Speicherung	371
2. Wegfall des Speicherungszwecks	372
3. Ausnahmen	373
4. Was bedeutet »Löschung«?	374
IV. Das Recht auf Vergessenwerden	375
V. Anspruch auf Einschränkung der Verarbeitung	377
VI. Widerspruchsrecht nach Art. 21 DSGVO	378
1. Grundsatz	378

Inhaltsverzeichnis

2. Anwendungsfälle	379
3. Rechtsfolgen	380
VII. Zwingender Charakter	380
VIII. Gegendarstellung	380
IX. Anspruch auf Schadensersatz	381
X. Besonderheiten im öffentlichen Dienst?	381

§ 12: Mechanismen, um das Datenschutzrecht wirksam werden zu lassen

I. Die Schwäche der Individualrechte	383
II. Kompensatorische Mechanismen in der DSGVO	384
III. Verhaltensregeln und Zertifizierung	385
1. Verhaltensregeln	385
2. Zertifizierungen	387
IV. Dokumentationspflichten des Verantwortlichen	388
1. Die allgemeine Verpflichtung nach Art. 5 Abs. 2 DSGVO	388
2. Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten	388
3. Weitere Dokumentationspflichten	389
V. Datenschutz-Folgenabschätzung	390
VI. Datensicherung und Informationspflicht bei Datenpannen	391
1. Datensicherung	391
2. Informationspflicht bei Datenpannen	392
VII. Der »betriebliche« Datenschutzbeauftragte	393
1. Pflicht zur Benennung	394
a) Überschreitung bestimmter Schwellenwerte	394
b) Notwendige Benennung auch bei geringerer Beschäftigtenzahl	395
c) Behördlicher Datenschutzbeauftragter	396
d) Freiwillige Bestellung	396
e) Sanktionen	396
2. Die Benennung einer geeigneten Person	396
a) Allgemeine Voraussetzungen	396
b) Fachkunde und Fehlen von Interessenkollisionen	397
c) Beteiligung des Betriebsrats	399
d) Bestellung einer ungeeigneten Person	400
3. Aufgaben des Datenschutzbeauftragten	400
a) Beratung	401
b) Kontrolle	401
c) Zusammenarbeit mit der Aufsichtsbehörde	401
d) Fortbildung	402
e) Weitere Aufgaben	402
f) Anordnungsbefugnisse?	402
4. Die Absicherung der Aufgabenerfüllung	402
a) Zeit und Hilfspersonal	403

b)	Teilnahme an Fort- und Weiterbildungsveranstaltungen	404
c)	Stellung in der Hierarchie	405
d)	Weisungsfreiheit und Geheimhaltungspflicht	405
e)	Benachteiligungsverbot	406
5.	Abberufung des Datenschutzbeauftragten	406
a)	Verlangen der Aufsichtsbehörde?	407
b)	Widerruf der Benennung aus wichtigem Grund	408
c)	Erstreckung des Schutzes auf das Arbeitsverhältnis	408
d)	Befristung	410
e)	Externe Datenschutzbeauftragte	410
f)	Freiwillig bestellte Datenschutzbeauftragte	410
6.	Verbleibende Defizite in der Rechtsstellung	411
VIII.	Die unabhängige Aufsichtsbehörde	412
1.	Überblick	412
2.	Aufgaben	413
3.	Befugnisse	413
4.	Zuständigkeiten	414
5.	Unabhängigkeit der Aufsichtsbehörde	415
6.	Grenzüberschreitende Zusammenarbeit	416
IX.	Rechtsbehelfe	417
1.	Beschwerde	417
2.	Gerichtlicher Rechtsschutz für die betroffene Person und den Verantwortlichen	418
3.	Verbandsklage	418
X.	Haftung auf Schadensersatz	419
1.	Der Grundsatz	419
2.	Anwendungsprobleme im Arbeitsleben	422
3.	Sonstige Haftungsnormen	423
XI.	Bußgelder und strafrechtliche Sanktionen	424
1.	Der allgemeine Rahmen	424
2.	Ordnungswidrigkeiten nach Art. 83 DSGVO	425
3.	Strafbare Verletzung des persönlichen Lebens- und Geheimbereichs	426
4.	Strafbare Beschädigung und Zerstörung	428
§ 13:	Kontrolle durch den Betriebsrat	429
I.	Einleitung	429
II.	Die Rechtmäßigkeitskontrolle durch den Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG	430
1.	Worauf bezieht sich die Kontrollfunktion des Betriebsrats?	430
2.	Formen der Umsetzung	431
a)	Information des Betriebsrats durch den Arbeitgeber	431
b)	Eigene Initiativen des Betriebsrats	435

Inhaltsverzeichnis

c)	Datenschutz im Betriebsratsbüro	437
d)	Beteiligung an Informationssystemen des Arbeitgebers	439
e)	Zuziehung eines Sachverständigen	439
f)	Schulung und Fortbildung	444
g)	Nutzung von SAP	445
h)	Einleitung eines Beschlussverfahrens	445
i)	Einschaltung der Aufsichtsbehörde?	446
III.	Präventiver Persönlichkeitsschutz durch Ausübung von Beteiligungsrechten	447
1.	Überblick	447
2.	Zweck der Beteiligungsrechte	449
3.	Das Beratungsrecht des § 92 BetrVG	451
4.	Mitbestimmung nach § 94 BetrVG	452
a)	Personalfragebogen	452
b)	Formulararbeitsverträge	454
c)	Aufstellung allgemeiner Beurteilungsgrundsätze	454
5.	Mitbestimmung über Auswahlrichtlinien nach § 95 BetrVG	455
6.	Mitbestimmung über berufliche Weiterbildung – E-Learning	456
7.	Konkurrenz von Beteiligungsrechten	457
IV.	Das Verhältnis zum Datenschutzbeauftragten	458
§ 14: Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG und Abschluss von Betriebsvereinbarungen		
I.	Auslegungsgrundsätze zu § 87 Abs. 1 Nr. 6 BetrVG	460
1.	Wortlaut	460
2.	Entstehungsgeschichte	461
3.	Zweck der Vorschrift	462
4.	§ 75 Abs. 2 und Grundcharakter des BetrVG – Rückgriff auf BDSG	464
5.	Stellenwert des § 87 Abs. 1 Nr. 6 BetrVG unter verfas- sungsrechtlichen Aspekten	465
6.	Unterstützende Erwägungen	467
II.	Voraussetzungen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG	467
1.	Überwachung durch »Technik«	468
2.	Was versteht man unter »Überwachung«?	470
a)	Begriffsbestimmungen	470
b)	Stellungnahme	472
c)	Mitbestimmung bei den einzelnen Phasen des Überwachungsprozesses	475
d)	Einzelfragen	478
3.	Der Gegenstand der Überwachung	478

a)	»Verhalten oder Leistung der Arbeitnehmer«	479
b)	Die Qualität der gespeicherten Daten	482
c)	Überwachung einzelner Arbeitnehmer und Gruppenüberwachung	483
d)	Die Bedeutung von Zusatzwissen	486
4.	Definition: Zur Überwachung »bestimmt«	489
a)	Geeignetheit	489
b)	Das Unmittelbarkeitserfordernis	490
c)	Das Programmierfordernis	491
d)	Kritik und Gegenposition: Auch Hardware mitbestimmungspflichtig	493
5.	Das »System« als Gegenstand der Mitbestimmung	494
6.	Die mitbestimmungspflichtigen Arbeitgebermaßnahmen: Einführung und Anwendung	495
a)	Grundsätze	496
b)	Mitbestimmung über die Datenverwendung	496
c)	Auftragsdatenverarbeitung	498
d)	Veränderung der technischen Einrichtung	498
e)	Alt-Einrichtungen	499
f)	Einsatz fremder Systeme	500
7.	Gesetzes- und Tarifvorbehalt	501
8.	Besonderheiten im Tendenzbetrieb?	503
III.	Rechtliche Schranken für eine Regelung durch Betriebsrat und Arbeitgeber	503
1.	Allgemeine Grenzen	504
a)	Zwingendes Recht	504
b)	Grundrechtsbindung	504
c)	Kann durch Betriebsvereinbarung und Einigungsstel- lenspruch von der DSGVO zu Lasten oder zu Gunsten der Beschäftigten abgewichen werden?	506
d)	»Billiger« Ausgleich der Interessen	506
e)	Einbeziehung aller »Beschäftigten«?	507
2.	Insbesondere: Persönlichkeitsschutz des Arbeitnehmers	507
3.	Insbesondere: Telefondatenerfassung	509
4.	Billige Abwägung der beiderseitigen Interessen	511
a)	Versuche zur Beschränkung des Regelungsspielraums	511
b)	Die abzuwägenden Interessen	512
c)	Was ist »billiger« Ausgleich?	513
5.	Überwachung des Betriebsrats	515
IV.	Ausübung und Durchsetzung des Mitbestimmungsrechts – Abschluss von Betriebsvereinbarungen	517
1.	Einzelbetriebsrat, Gesamtbetriebsrat oder Konzern- betriebsrat?	517
2.	Initiativrechte des Betriebsrats	519
3.	Betriebsvereinbarungen	520

Inhaltsverzeichnis

4.	Rahmenbetriebsvereinbarungen	522
5.	Ausübung des Mitbestimmungsrechts durch Regelungs- abrede?	523
6.	Durchsetzung des Mitbestimmungsrechts	523
7.	Bestehende Betriebsvereinbarungen	524
V.	Anwendung des § 87 Abs. 1 Nr. 6 BetrVG auf einzelne Problembereiche	525
1.	Probleme um den PC	526
a)	Das isolierte Gerät	526
b)	Das vernetzte Gerät	528
2.	Anwendung auf E-Mail und Internet	529
3.	Integration sozialer Netzwerke in den Arbeitsprozess	530
4.	Videoüberwachung	530
5.	Weitere Problemfälle: Erfassung biometrischer Merkmale, Bestimmung des Aufenthaltsorts, elektronische Personalakte, Nutzung mobiler Geräte	531
6.	Arbeit 4.0: Wearables und Datenbrillen als Erscheinungs- form	531
7.	Änderungen des technischen Systems	532
8.	Maßnahmen auf Veranlassung einer ausländischen Konzernspitze	533
VI.	Sanktionen bei Verletzung des Mitbestimmungsrechts	533
VII.	Verwertungsverbot?	534
1.	Allgemeiner Grundsatz	534
2.	Ablehnung des Verwertungsverbots durch die Recht- sprechung	535
3.	Gegenargumente	536
4.	Erkenntnisse über Dritte	537
§ 15:	Besonderheiten der Personalvertretung	538
I.	Überblick	538
II.	Die Rechtmäßigkeitskontrolle durch den Personalrat nach § 68 Abs. 1 Nr. 2 BPersVG	540
1.	Worauf bezieht sich die Kontrollfunktion des Personal- rats?	540
2.	Formen der Umsetzung	541
a)	Information des Personalrats durch den Dienststellen- leiter	541
b)	Eigene Ermittlungen des Personalrats	542
c)	Zuziehung eines Sachverständigen	543
d)	Schulung und Fortbildung	544
e)	Einleitung eines Beschlussverfahrens	544
f)	Einschaltung des Datenschutzbeauftragten	545
g)	Verschwiegenheitspflicht	546

III.	Präventiver Persönlichkeitsschutz durch Ausübung von Beteiligungsrechten	546
1.	Überblick	546
2.	Zweck der Beteiligungsrechte	548
3.	Inhalt von Personalfragebogen nach § 75 Abs. 3 Nr. 8 und § 76 Abs. 2 Nr. 2 BPersVG	549
4.	Beurteilungsrichtlinien nach § 75 Abs. 3 Nr. 9 bzw. § 76 Abs. 2 Nr. 3 BPersVG	550
5.	Auswahlrichtlinien nach § 76 Abs. 2 Nr. 8 BPersVG	551
6.	Mitbestimmung nach § 75 Abs. 3 Nr. 17 BPersVG	551
7.	Konkurrenz von Beteiligungsrechten	554
8.	Stufenvertretung	555
§ 16:	Staatlicher Zugriff auf Beschäftigendaten	556
I.	Überblick	556
II.	Beschäftigendaten als Gegenstand der Rasterfahndung	557
1.	Rechtsgrundlagen	557
2.	Datenschutzrechtliche und arbeitsrechtliche Konsequenzen	559
a)	Recht des Arbeitgebers zur Datenübermittlung	559
b)	Information des Betroffenen	559
c)	Verdachtskündigung?	559
d)	Verdachtsversetzung?	560
III.	Überwachung der Telekommunikation	560
IV.	Behördlich angeordnete Maßnahmen im Betrieb	561
V.	Sicherheitsüberprüfung	562
1.	Das Verfahren der Sicherheitsüberprüfung	562
a)	Erfasster Personenkreis	563
b)	Zuständige Behörde	563
c)	Sicherheitserklärung	563
d)	Kriterien für die Sicherheitsüberprüfung	563
e)	Anhörung des Betroffenen	564
f)	Entscheidung	564
g)	Wiederholung des Verfahrens	564
h)	Behandlung der angefallenen Daten	564
2.	Handhabung der Zuverlässigkeitskriterien durch die Rechtsprechung	565
3.	Erfasste Bereiche	566
4.	Arbeitsrechtliche Folgen	568
a)	Personenbedingte Kündigung	568
b)	Ausdehnung auf nicht vom SÜG erfasste Bereiche?	569
5.	Rechtsschutzmöglichkeiten bei verweigertem Zugang zu sicherheitsempfindlichen Bereichen	569
VI.	Abgleichung mit Antiterrorlisten	570
VII.	ECHELON und NSA	572

Inhaltsverzeichnis

1. Echelon	572
2. NSA	573
§ 17: Einige Perspektiven	574
I. Die permanente Reformdiskussion	574
II. Die DSGVO als Paukenschlag	576
III. Datenschutz als Wettbewerbsfaktor	577
IV. Transparenz des Datenschutzrechts	579
V. Die nicht (voll) bewältigten Probleme	580
1. Cloud Computing	580
2. Big Data	581
3. Datenschutz im Internet	582