

Inhaltsverzeichnis

Vorwort	5
Inhaltsübersicht	7
Abkürzungsverzeichnis	29
§ 1: Einleitung	35
I. Einige praktische Probleme	35
1. Das verdächtige Personalratsmitglied	35
2. Lidl, Telekom, Deutsche Bahn u. a.	36
3. Neuere technische Entwicklungen	40
4. Staatlicher Zugriff	43
II. Technische Entwicklung und Recht	44
III. Informationstechnologien und Recht	47
IV. Technikbewältigung im Arbeitsrecht?	50
§ 2: Datenverarbeitung im Betrieb und ihre grundsätzlichen rechtlichen Schranken	53
I. Der Tatbestand	53
1. Erscheinungsformen, insbesondere Personalinformationssysteme und Betriebsdatenerfassung	53
2. Technikspezifische Risiken	58
II. Datenschutzrechtliche Regelungen auf nationaler Ebene	61
1. Das BDSG als Querschnittsgesetz	61
2. Arbeitsrechtliche Spezialbestimmungen	64
3. Anwendungsvoraussetzungen des BDSG	67
III. Datenschutzrechtliche Regelungen auf EU-Ebene	69
1. EG-Datenschutzrichtlinie	69
2. EU-Grundrechtecharta und AEUV	69
3. Rechtsprechung des EuGH	71
4. Der Entwurf einer Datenschutz-Grundverordnung	75

IV.	Datenschutzrechtliche Regelungen auf internationaler Ebene	78
1.	Europarat	78
2.	OECD	79
3.	ILO	79
4.	UN	80
V.	Offene Fragen und Überblick über den Gang der Darstellung.	80
 § 3: Die Volkszählungentscheidung und ihre Auswirkungen auf das Arbeitsrecht.		85
I.	Das informationelle Selbstbestimmungsrecht und seine Weiterentwicklung	85
II.	Normative Vorgaben für Einschränkungen	89
IIa.	Das unionsrechtliche Grundrecht auf Datenschutz	95
III.	Die Übertragung ins Arbeits- und Beamtenrecht	96
1.	Rechtsprechung	96
a)	Bundesverfassungsgericht	96
b)	Bundesarbeitsgericht	98
c)	Landesarbeitsgerichte	103
d)	Verwaltungsgerichte	105
2.	Literatur	105
3.	Ergebnis und offene Fragen	108
IV.	Eingriffe in das informationelle Selbstbestimmungsrecht des Arbeitnehmers und ihre Schranken	109
1.	Rechtfertigung durch ein »überwiegendes Allgemeininteresse«	110
2.	Rechtfertigung durch ein »überwiegendes Arbeitgeberinteresse«?	111
a)	Art. 5 Abs. 1 Satz 1 GG.	111
b)	Unternehmerische Betätigungsfreiheit	112
c)	Substanzieller Persönlichkeitsschutz als Grenze?	114
3.	Die Zweckbindung der Daten	117
a)	Weiter oder enger Zweck	117
b)	Grundsätzliches Verbot der Zweckentfremdung	119
4.	Verfahrensmäßige Konsequenzen	120
a)	Datentransparenz	121
b)	Unabhängige Kontrollinstanzen	121

c) Datensicherung	122
IVa. Unionsrechtliche Rahmenbedingungen	123
§ 4: Voraussetzungen einer wirksamen Einwilligung	125
I. Die Problematik	125
II. Formale Erfordernisse	127
1. Zeitpunkt	127
2. Einsichtsfähigkeit des Betroffenen	127
3. Vorherige Information des Betroffenen	128
4. Schriftform	129
5. Eindeutigkeit der Erklärung	131
6. Änderungen durch die EU-Verordnung?	132
III. Inhaltliche Anforderungen	133
IV. Das Erfordernis der Freiwilligkeit	134
1. Die Ausgangssituation	134
a) Normative Grundlage	134
b) Stellungnahmen in Bezug auf das Arbeits- verhältnis	135
2. Notwendige Differenzierungen	135
a) Nur Fehlen von Willensmängeln?	135
b) Keine Einwilligung im Arbeitsverhältnis?	136
c) Das Koppelungsverbot	136
d) Druck bei Verhandlungen und einseitige Beratung	137
e) Angedrohte oder erwartbare Nachteile	138
f) Versprechen hoher Vorteile	139
g) Zusammenfassung: Voraussetzungen einer wirksamen Einwilligung	139
3. Änderungen durch die EU-Verordnung?	140
V. Inhaltsschranken der Einwilligung	140
1. Zwingendes Recht: Einstellungsgrundsätze und Grenzen im Arbeitsverhältnis	140
2. Angemessenheitskontrolle	142
VI. Widerruf der Einwilligung	145
VII. Einwilligung in die Verarbeitung sensibler Daten	147
VIII. Telekommunikation	148

§ 5: Datenerhebung gegenüber Bewerbern	150
I. Die Vorgaben des BDSG	150
1. § 32 Abs. 1 BDSG als Rechtsgrundlage	150
a) Der erfasste Personenkreis	151
b) Verzicht auf das Dateierfordernis	153
c) Ausklammerung des persönlichen Nahbereichs	153
d) Anwendungsvoraussetzungen nach dem Entwurf der EU-Datenschutzverordnung	154
2. Verhältnis von § 32 BDSG zu anderen Vorschriften	155
3. Die Bestimmung des konkreten Zwecks nach § 28 Abs. 1 Satz 2 BDSG	157
4. Datenvermeidung und Datensparsamkeit nach § 3a BDSG	158
5. Die Sonderregeln über sog. sensitive Daten	158
a) Die einzelnen Fälle	159
b) Inhaltliche Voraussetzungen für die Erhebung sensitiver Daten	161
6. Das Gebot der Direkterhebung	163
II. Das Fragerrecht des Arbeitgebers	164
1. Die Ausgangssituation	164
2. Die Reaktion der Rechtsprechung	165
3. Die »Erforderlichkeit« nach § 32 Abs. 1 Satz 1 BDSG	166
4. Zulässigkeit einzelner Fragen	167
a) Privatsphäre	167
b) »Diskriminierungsverdächtige« Tatsachen	168
c) Schwangerschaft und Wehrdienst	168
d) Gesundheitszustand und Eigenschaft als schwer-behinderter Mensch	169
e) Vorstrafen	171
f) Vermögensverhältnisse	172
g) Berufliche Fähigkeiten und Laufbahn	173
5. Hinweis auf den Erhebungszweck	174
6. Das sog. Recht zur Lüge und andere Sanktionen	174
7. Informationspflichten des Arbeitgebers und des Arbeitnehmers	175
III. Ärztliche Untersuchungen und Eignungstests	176
IV. Gentechnische Untersuchungen nach dem Gendiagnostikgesetz	178

V.	Datenerhebung bei Dritten und allgemein zugängliche Beschäftigtendaten	182
1.	Entsprechende Anwendung der Grundsätze über das Fragerrecht	182
2.	Einschaltung Dritter als Ausnahmetatbestand (§ 4 Abs. 2 Satz 2 BDSG)	183
3.	Einschaltung der Verfassungsschutzbehörden	185
4.	Informationen aus allgemein zugänglichen Quellen, insbesondere aus dem Internet?	185
VI.	Besonderheiten im öffentlichen Dienst	187
1.	Die gesetzliche Ausgangslage	187
2.	Auslegungsprobleme	188
VII.	Datenerhebung durch private Arbeitsvermittler	190
§ 6:	Datenerhebung gegenüber Beschäftigten	192
I.	Gesetzliche Vorgaben	192
II.	Privatsphäre und Konsumverhalten	193
III.	Durchführung des Beschäftigungsverhältnisses	194
1.	Entgeltabrechnung	194
2.	Arbeitszeit und Arbeitsverhalten	195
3.	Torkontrolle	196
4.	Weiterförderung	196
5.	Erhebung zahlreicher persönlicher Umstände im Hinblick auf eine mögliche »soziale Auswahl«?	197
6.	Umfragen im Betrieb	199
7.	Übergang zur elektronischen Personalakte	200
IV.	Gesundheitsdaten und gentechnische Untersuchungen	201
1.	Traditionelle Gesundheitsdaten	201
a)	Die Sonderregeln über sensitive Daten	201
b)	Informationspflichten des Arbeitnehmers und ihre Grenzen	202
c)	Pflicht des Arbeitnehmers, sich untersuchen zu lassen?	204
d)	Weitere Datenerhebung durch den Betriebsarzt	206
e)	Untersuchungen bei Änderungen der Tätigkeit	207
f)	Beschäftigte im Krankenhaus als Patienten	207
2.	Zulässigkeit von Gentests?	208
V.	Erfassung biometrischer Merkmale	208

VI. Überwachung des Arbeitsverhaltens:	
Insbesondere Privatdetektive als verdeckte Ermittler	211
1. Kontrollrecht des Arbeitgebers	211
2. Einsatz von Privatdetektiven	212
3. Die Parallele zum verdeckten Ermittler.	212
4. Anwendungsfälle	213
5. Stellen einer »Falle«.	214
6. Heimliches Mithören und Verdacht strafbarer Handlungen	214
VII. Überwachung des Arbeitsverhaltens: Videokontrolle	215
1. Praktische Bedeutung und rechtliche Regelung	215
2. Videokontrolle in öffentlich zugänglichen Räumen	216
a) Der erfasste Bereich.	216
b) Die eingesetzte Technik.	217
c) Die Voraussetzungen im Einzelnen	217
d) Die schutzwürdigen Interessen der Betroffenen. .	218
e) Transparenz	220
f) Umgang mit den erhobenen Daten.	221
3. Videoüberwachung in nicht öffentlich zugänglichen Räumen	221
a) Rechtsgrundlage	221
b) Rechtsprechung – heimliche und offene Videoüberwachung	222
c) Sanktionen bei unerlaubter Videoüberwachung .	224
4. Mitbestimmung.	225
5. Exkurs: Mitwirkung in Filmen	225
VIII. Spezielle Überwachungsprogramme	226
1. Beispiele	226
2. Strafsanktionen	226
3. Rechtfertigung durch Einwilligung des Betroffenen? .	227
4. Data Loss Prevention	227
IX. Ortungssysteme und Erstellung eines Bewegungsprofils	228
1. Ortungssysteme.	228
a) Die Ausgangssituation	228
b) Das Strafprozessrecht als Vorreiter.	230
c) Zulässigkeitsschranken im Arbeitsrecht	231
2. Erstellung von Bewegungsprofilen im Betrieb	232
3. Mitbestimmung.	233

X.	Kontrolle durch andere technische Mittel	233
1.	RFID	233
2.	Einsatz von Drohnen	235
XI.	Überwachung der Telekommunikation	235
1.	Rechtliche Grundlagen	235
a)	TKG, TMG, BGB	236
b)	Vorschriften zum Datenschutz	237
c)	Anwendung der §§ 88ff. TKG im Arbeitsverhältnis?	238
aa)	Differenzierung zwischen dienstlicher und privater Nutzung	238
bb)	Einwände	240
cc)	Rechtsfolgen	241
dd)	Technische Trennung	243
d)	Anwendbarkeit der §§ 11ff. TMG im Arbeitsverhältnis?	243
e)	Allgemeiner Beschäftigtendatenschutz für die Inhalte	245
2.	Kontrolle der dienstlichen Nutzung von Einrichtungen der Telekommunikation	245
a)	Der grundsätzliche Ausgangspunkt	245
b)	Mithören von Telefongesprächen	245
aa)	Der Persönlichkeitsschutz und seine Grenzen	245
bb)	Äußere Telefondaten	247
cc)	Zugriff auf Inhalte: Abwägung der Interessen	247
c)	Sonstige Telekommunikationsdienste: E-Mails	248
aa)	Die grundsätzliche Behandlung: Zugriff auf die Inhalte?	248
bb)	Verschlüsselung	249
cc)	Äußere Daten	250
dd)	Ausgeschiedene und abwesende Mitarbeiter	250
d)	Sonstige Telekommunikationsdienste: Intranet	251
e)	Sonstige Telekommunikationsdienste: Internet	252
3.	Kontrolle der privaten Nutzung von Einrichtungen der Telekommunikation	255
a)	Anforderungen des TKG	255

aa) Wahrung des Fernmeldegeheimnisses nach § 88 TKG	255
bb) Technische Schutzmaßnahmen nach § 109 TKG	256
4. Anforderungen des TMG.	257
5. Anforderungen bei »Mischtatbeständen«	259
6. Spamfilter.	261
7. Die Mithörerproblematik.	261
8. Vorratsdatenspeicherung nach § 113a TKG?	262
XII. Kumulierte Überwachung – die Arbeit im Call Center	263
XIII. Datenermittlung gegenüber »Verdächtigen«	265
1. Die Ermächtigung des Arbeitgebers durch § 32 Abs. 1 Satz 2 BDSG.	265
2. Die Rechtsfolgen.	267
XIV. Arbeitnehmer mit Sonderstatus.	271
1. Träger von Berufsgeheimnissen.	271
2. Beschäftigte mit fachlicher Unabhängigkeit	273
3. Wissenschaftler	273
XV. Einschaltung Dritter	274
XVI. Besonderheiten im öffentlichen Dienst	275
XVII. Keine Verwertung rechtswidrig erlangter Informationen im Prozess?	275
1. Die Problematik	275
2. Verwertungsverbot bei Verstößen gegen das Persönlichkeitsrecht	275
3. Verwertungsverbot bei Verstößen gegen Betriebsverfassungsrecht	278
§ 7: Auswertung der erhobenen und gespeicherten Daten	280
I. Überblick	280
1. Die Entwicklung bis 2009	280
2. Die Regelung des § 32 Abs. 1 Satz 1 BDSG 2009	282
3. Überblick über den Gang der Darstellung.	284
II. Auswertungen unter Wahrung des Zweckbindungs- grundsatzes: Informationelle Gewaltenteilung	284
1. Festlegung des Zwecks.	284
2. Das Beispiel der arbeitsmedizinischen Daten	285
3. Das Beispiel Eingliederungsmanagement	288

4. Das Beispiel der Daten zur sozialen Auswahl	291
5. Das Beispiel der Daten zur Entgeltabrechnung	291
6. Das Beispiel der Betriebsdaten	292
7. Der große Rest: Personaldaten im engeren Sinn	293
8. Die Separierung einzelner Datenbestände – ein lästiges Novum?	295
III. Die ausnahmsweise zulässige Zweckentfremdung	298
1. Nutzung und Übermittlung für andere Zwecke	298
2. Rechtfertigung der Zweckentfremdung auf der Grundlage des § 28 Abs. 2 Nr. 1 BDSG	300
3. Rechtfertigung der Zweckentfremdung auf der Grundlage des § 28 Abs. 2 Nr. 2 BDSG	301
4. Sonderfälle: verbotene Zweckentfremdung	302
a) Schutz der professionellen Datenverarbeiter	302
b) Wissenschaftliche Forschung	302
c) Durch Videoaufnahmen, heimliche Erhebungen und bei der Telekommunikation gewonnene Daten	303
d) Statistische Erhebungen	303
IV. Screening und Rasterfahndung im Betrieb?	304
1. Anschauungsmaterial	304
2. Bewertung auf der Grundlage des geltenden Rechts	305
a) Die Suche nach Informationsgebern	305
b) Korruptionsbekämpfung: Die Rekonstruktion von Kontobewegungen	306
c) Handlungsmöglichkeiten?	307
V. Compliance als Rechtfertigung?	308
1. Was bedeutet »Compliance«?	308
2. Datenschutz und Compliance	308
3. Allgemeine datenschutzrechtliche Vorgaben	309
4. Die Zulässigkeit einzelner Maßnahmen	310
a) Überblick	310
b) Auskunftspflicht des Arbeitnehmers – aber keine Selbstbeziehtigung	310
c) Auskunftspflicht des Arbeitnehmers – Belastung Dritter?	312
d) Gewährung und Annahme von Vorteilen	313
VI. Verbot von Persönlichkeitsprofilen	313

VII.	Umgang mit datenschutzwidrig erlangten Informationen	315
VIII.	Automatisierte Entscheidungen nach § 6a BDSG	315
1.	Die Grundentscheidung des § 6a BDSG	315
2.	Anwendung im Arbeitsrecht	316
VIII.	Verwendung von Chipkarten	317
IX.	Besonderheiten im öffentlichen Dienst	317
§ 8:	Übermittlung von Beschäftigtendaten im Inland	319
I.	Die scheinbare Übermittlung: Auftragsdaten- verarbeitung	319
II.	Die Zulässigkeit der Übermittlung im Allgemeinen	322
1.	Der Begriff »Übermittlung«	322
a)	Die gesetzliche Definition	322
b)	Übermittlung innerhalb der verantwortlichen Stelle?	323
c)	Veröffentlichung	324
d)	Die Problematik des Abrufverfahrens	324
2.	Zulässigkeit nach § 28 Abs. 1 BDSG und nach § 32 Abs.1 Satz 1 BDSG	325
III.	Anwendungsfälle	326
1.	Übermittlung von Betriebsdaten	326
2.	Überlassung von Arbeitskräften	327
3.	Konzerndatenverarbeitung	328
4.	Übermittlung von Arbeitnehmerdaten an einen Branchenaukunftsdiest	331
5.	Weitergabe von Beschäftigtendaten an Koalitionen	332
6.	Übermittlung an einen anderen Arbeitgeber beim Arbeitsplatzwechsel	332
7.	Weitergabe von Arbeitnehmerdaten zu Zwecken der Werbung und der Markt- und Meinungsforschung?	333
8.	Unzulässige Übermittlung per E-Mail	334
9.	Datenübermittlung durch Whistleblower	335
10.	Sonstige Fälle	336
IV.	Zweckbindung beim Empfänger	337
V.	Veröffentlichung von Arbeitnehmerdaten am Beispiel des Internet	338
1.	Die bewusste Verwendung im Internet	338

2. Der Sonderfall: Fotos im Internet	342
3. Sonstige Arbeitnehmerdaten im Internet.	343
VI. Unternehmensinterne Weitergabe von Arbeit- nehmerdaten.	344
1. Der rechtliche Rahmen	344
2. Inhalt der Personalakte	345
3. Personalgespräche	346
4. Unternehmensinterne Veröffentlichung des Leistungsverhaltens	347
5. Betriebszeitung.	348
6. Mitteilungen an den Betriebsrat	349
VII. Besonderheiten im öffentlichen Dienst?	350
1. Die allgemeinen Regeln	350
2. Sonderregeln für Beamte	351
VIII. Umstrukturierung von Unternehmen und Betrieben	352
1. Das datenschutzrechtliche Problem.	352
2. § 28 Abs. 1 Satz 1 Nr. 2 BDSG als Rechtsgrundlage. .	353
3. Die Behandlung sensibler Daten.	354
4. Auflösung des Unternehmens	354
 § 9: Übermittlung von Beschäftigtendaten ins Ausland	355
I. Die Ausgangssituation	355
II. Das Kollisionsrecht des BDSG.	356
III. Die Übermittlung in EU- und EWR-Mitglied- staaten	360
1. Der Grundsatz	360
2. Praktische Konsequenzen	361
IV. Übermittlung in Drittstaaten mit angemessenem Datenschutzniveau.	361
1. Was ist »angemessenes Datenschutzniveau?	362
2. Lösung über das Verfahren	362
V. Übermittlung in Drittstaaten ohne angemessenes Datenschutzniveau.	363
1. Der Sonderfall USA	363
2. Andere Drittstaaten.	367
a) Unproblematische Fälle.	367
b) Vertragslösungen	367
c) Selbstverpflichtungen von Unternehmen.	371

d) Daten im Internet	374
e) Insbesondere: Cloud Computing	375
VI. Datenimport	375
§ 10: Das Recht des Beschäftigten auf Datentransparenz	377
I. Die Vorgaben der Volkszählungentscheidung und die Regelung des BDSG	377
1. Volkszählungentscheidung	377
2. Datentransparenz im BDSG	378
II. Die Benachrichtigung des Arbeitnehmers nach § 33 BDSG	379
1. Der Grundsatz	379
2. Ausnahmen	381
3. Sanktionen	385
4. Sonderregelung des § 6c BDSG	386
III. Der Auskunftsanspruch nach § 34 BDSG	386
1. Gegenstand der Auskunft	387
2. Praktische Umsetzung und Ausnahmen	388
3. Zwingender Charakter und Sanktionen bei Verstößen	391
4. Gerichtliche Durchsetzung	391
IV. Vorrangiges Recht nach § 83 BetrVG	392
1. Verhältnis zu § 34 BDSG	392
2. Der Begriff »Personalakte«	392
3. Was bedeutet »Einsichtnahme«?	393
4. Verbleibender Anwendungsbereich des § 34 BDSG .	394
5. Sonderfall: Betriebsärztlicher Befundbogen	395
V. Sonderregeln im Beamtenrecht	395
§ 11: Das Recht des Beschäftigten auf Datenkorrektur und Schadensersatz	398
I. Einleitung	398
II. Berichtigung nach § 35 Abs. 1 BDSG	398
1. Wann ist ein Datum »unrichtig«?	399
2. Wer trägt die Beweislast?	399
3. Wie wird die Berichtigung durchgeführt?	400
4. Berichtigung bei vorheriger Übermittlung an Dritte .	400
5. Konkurrenz mit arbeitsvertraglichen Ansprüchen .	401

III.	Anspruch auf Löschung	402
1.	Unzulässige Speicherung	402
2.	Besonders sensible Daten	402
3.	Wegfall des Speicherungszwecks	403
4.	Ausnahmen	404
5.	Was bedeutet »Lösung«?	405
IV.	Das Recht auf Vergessenwerden	406
1.	Stand im Unionsrecht	406
2.	Vergleich mit dem deutschen Recht	407
V.	Anspruch auf Sperrung	409
VI.	Widerspruchsrecht nach § 35 Abs. 5 BDSG	410
1.	Grundsatz	410
2.	Anwendungsfälle	411
3.	Rechtsfolgen	411
VII.	Zwingender Charakter	412
VIII.	Gegendarstellung	412
IX.	Anspruch auf Schadensersatz	413
1.	Der Grundsatz	413
2.	Anwendungsprobleme	414
X.	Sonstige Rechte des Arbeitnehmers	416
XI.	Probleme im Internet	417
XII.	Besonderheiten im öffentlichen Dienst?	417
 § 12: Institutionalisierte Kontrolle durch den Datenschutzbeauftragten und die Aufsichtsbehörde – Sanktionen bei Verstößen – Datenpannen		419
I.	Die Schwäche der Individualrechte	419
II.	Der »betriebliche« Datenschutzbeauftragte	420
1.	Pflicht zur Bestellung	420
a)	Überschreitung bestimmter Schwellenwerte	420
b)	Notwendigkeit einer Vorabkontrolle	423
c)	Behördlicher Datenschutzbeauftragter	423
d)	Freiwillige Bestellung	424
e)	Sanktionen	424
2.	Die Bestellung einer geeigneten Person	425
a)	Allgemeine Voraussetzungen	425
b)	Fachkunde und Zuverlässigkeit; Fehlen von Interessenkollisionen	426

c)	Beteiligung des Betriebsrats	427
d)	Bestellung einer ungeeigneten Person.	429
3.	Aufgaben des »betrieblichen« Datenschutzbeauftragten.	429
a)	Kontrolle	430
b)	Fortbildung	430
c)	Führung des Verfahrensverzeichnisses und Herstellung von Publizität	431
d)	Anordnungsbefugnisse?	432
4.	Die Absicherung der Aufgabenerfüllung	432
a)	Zeit und Hilfspersonal	432
b)	Teilnahme an Fort- und Weiterbildungsveranstaltungen	433
c)	Stellung in der Hierarchie.	435
d)	Weisungsfreiheit und Geheimhaltungspflicht . . .	436
e)	Benachteiligungsverbot	437
5.	Abberufung des »betrieblichen« Datenschutzbeauftragten.	437
a)	Abberufungsverlangen der Aufsichtsbehörde . . .	437
b)	Widerruf der Bestellung aus wichtigem Grund . .	438
c)	Erstreckung des Schutzes auf das Arbeitsverhältnis	439
d)	Befristung	440
e)	Externe Datenschutzbeauftragte	441
f)	Freiwillig bestellte Datenschutzbeauftragte . . .	442
6.	Verbleibende Defizite in der Rechtsstellung	442
7.	Rechtsentwicklung in der EU	444
III.	Die Stellung der Aufsichtsbehörde	444
1.	Die Zuständigkeit.	444
2.	Die Beschaffung von Informationen	446
3.	Möglichkeiten der Abhilfe bei Rechtsverstößen .	447
4.	Unabhängigkeit der Aufsichtsbehörde	449
5.	Informelle Einflussnahmen	450
IV.	Ordnungswidrigkeiten und strafrechtliche Sanktionen	450
1.	Der allgemeine Rahmen	450
2.	Ordnungswidrigkeiten nach § 43 BDSG und Straftaten nach § 44 BDSG	451

3. Strafbare Verletzung des persönlichen Lebens- und Geheimbereichs	453
4. Strafbare Beschädigung und Zerstörung	454
V. Informationspflicht bei Datenpannen.	455
§ 13: Institutionalisierte Kontrolle durch den Betriebsrat	457
I. Einleitung	457
II. Die Rechtmäßigkeitskontrolle durch den Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG	458
1. Worauf bezieht sich die Kontrollfunktion des Betriebsrats?	458
2. Formen der Umsetzung	459
a) Information des Betriebsrats durch den Arbeitgeber	459
b) Eigene Initiativen des Betriebsrats	463
c) Datenschutz im Betriebsratsbüro	465
d) Beteiligung an Informationssystemen des Arbeitgebers	467
e) Zuziehung eines Sachverständigen	468
f) Schulung und Fortbildung	474
g) Nutzung von SAP	475
h) Einleitung eines Beschlussverfahrens	476
i) Einschaltung der Aufsichtsbehörde?	476
III. Präventiver Persönlichkeitsschutz durch Ausübung von Beteiligungsrechten	477
1. Überblick	477
2. Zweck der Beteiligungsrechte	479
3. Das Beratungsrecht des § 92 BetrVG	482
4. Mitbestimmung nach § 94 BetrVG	483
a) Personalfragebogen	483
b) Formulararbeitsverträge	486
c) Aufstellung allgemeiner Beurteilungsgrundsätze .	486
5. Mitbestimmung über Auswahlrichtlinien nach § 95 BetrVG	487
6. Mitbestimmung über berufliche Weiterbildung – E-Learning	488
7. Konkurrenz von Beteiligungsrechten	490
IV. Das Verhältnis zum Datenschutzbeauftragten	491

§ 14: Mitbestimmung des Betriebsrats nach § 87 Abs. 1

Nr. 6 BetrVG	493
I. Auslegungsgrundsätze	493
1. Wortlaut	493
2. Entstehungsgeschichte	494
3. Zweck der Vorschrift	495
4. § 75 Abs. 2 und Grundcharakter des BetrVG – Rückgriff auf BDSG	497
5. Stellenwert des § 87 Abs. 1 Nr. 6 BetrVG unter verfassungsrechtlichen Aspekten	499
6. Unterstützende Erwägungen	501
II. Voraussetzungen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG	502
1. Überwachung durch »Technik«	503
2. Was versteht man unter »Überwachung?«	505
a) Begriffsbestimmungen	505
b) Stellungnahme	507
c) Mitbestimmung bei den einzelnen Phasen des Überwachungsprozesses	510
d) Einzelfragen	514
3. Der Gegenstand der Überwachung	515
a) »Verhalten oder Leistung der Arbeitnehmer«	516
b) Die Qualität der gespeicherten Daten	519
c) Überwachung einzelner Arbeitnehmer und Gruppenüberwachung	521
d) Die Bedeutung von Zusatzwissen	524
4. Definition: Zur Überwachung »bestimmt«	527
a) Geeignetheit	528
b) Das Unmittelbarkeitserfordernis	529
c) Das Programmerfordernis	531
d) Kritik und Gegenposition: Auch Hardware mitbestimmungspflichtig	532
5. Das »System« als Gegenstand der Mitbestimmung	534
6. Die mitbestimmungspflichtigen Arbeitgebermaßnahmen: Einführung und Anwendung	536
a) Grundsätze	536
b) Mitbestimmung über die Datenverwendung	537
c) Auftragsdatenverarbeitung	538

d) Veränderung der technischen Einrichtung	539
e) Alt-Einrichtungen	540
7. Gesetzes- und Tarifvorbehalt	541
8. Besonderheiten im Tendenzbetrieb?	544
III. Rechtliche Schranken für eine Regelung durch Betriebsrat und Arbeitgeber	544
1. Allgemeine Grenzen	545
a) Zwingendes Recht	545
b) Grundrechtsbindung	545
c) »Billiger« Ausgleich der Interessen	546
d) Einbeziehung aller »Beschäftigten«?	547
2. Betriebsvereinbarung und Einigungsstellenspruch als Erlaubnisnorm nach § 4 Abs. 1 BDSG?	547
3. Der Persönlichkeitsschutz des Arbeitnehmers als Grenze für Betriebsvereinbarungen und Einigungs- stellensprüche	549
4. Insbesondere: Telefondatenerfassung	551
5. Billige Abwägung der beiderseitigen Interessen . .	553
a) Versuche zur Beschränkung des Regelungs- spielraums	553
b) Die abzuwägenden Interessen	555
c) Was ist »billiger« Ausgleich?	556
6. Überwachung des Betriebsrats	559
IV. Ausübung und Durchsetzung des Mitbestimmungsrechts	561
1. Einzelbetriebsrat, Gesamtbetriebsrat oder Konzernbetriebsrat?	561
2. Initiativrechte des Betriebsrats	564
3. Rahmenbetriebsvereinbarungen	565
4. Ausübung des Mitbestimmungsrechts durch Regelungsabrede?	566
5. Durchsetzung des Mitbestimmungsrechts	567
V. Anwendung des § 87 Abs. 1 Nr. 6 BetrVG auf Probleme der gegenwärtigen Entwicklung	568
1. Probleme um den PC	569
a) Das isolierte Gerät	569
b) Das vernetzte Gerät.	571
2. Anwendung auf E-Mail und Internet	572
3. Integration sozialer Netzwerke in den Arbeitsprozess	573

4. Videoüberwachung	574
5. Weitere Problemfälle: Erfassung biometrischer Merkmale, Bestimmung des Aufenthaltsorts und Nutzung mobiler Geräte	574
6. Maßnahmen auf Veranlassung einer ausländischen Konzernspitze	575
VI. Sanktionen bei Verletzung des Mitbestimmungs- rechts	575
VII. Verwertungsverbot?	577
1. Allgemeiner Grundsatz	577
2. Ablehnung des Verwertungsverbots durch die Rechtsprechung	577
3. Gegenargumente	578
4. Erkenntnisse über Dritte	579
§ 15: Besonderheiten der Personalvertretung	581
I. Überblick	581
II. Die Rechtmäßigkeitskontrolle durch den Personalrat nach § 68 Abs. 1 Nr. 2 BPersVG	584
1. Worauf bezieht sich die Kontrollfunktion des Personalrats?	584
2. Formen der Umsetzung	584
a) Information des Personalrats durch den Dienst- stellenleiter	584
b) Eigene Ermittlungen des Personalrats	586
c) Zuziehung eines Sachverständigen	587
d) Schulung und Fortbildung	588
e) Einleitung eines Beschlussverfahrens	588
f) Einschaltung des Datenschutzbeauftragten	590
g) Verschwiegenheitspflicht	590
III. Präventiver Persönlichkeitsschutz durch Ausübung von Beteiligungsrechten	591
1. Überblick	591
2. Zweck der Beteiligungsrechte	593
3. Inhalt von Personalfragebogen nach § 75 Abs. 3 Nr. 8 und § 76 Abs. 2 Nr. 2 BPersVG	594
4. Beurteilungsrichtlinien nach § 75 Abs. 3 Nr. 9 bzw. § 76 Abs. 2 Nr. 3 BPersVG	596

5. Auswahlrichtlinien nach § 76 Abs. 2 Nr. 8 BPersVG.	596
6. Mitbestimmung nach § 75 Abs. 3 Nr. 17 BPersVG	596
7. Konkurrenz von Beteiligungsrechten.	601
8. Stufenvertretung	601
§ 16: Staatlicher Zugriff auf Beschäftigtendaten.	602
I. Überblick	602
II. Arbeitnehmerdaten als Gegenstand der Rasterfahndung	603
1. Rechtsgrundlagen	603
2. Datenschutzrechtliche und arbeitsrechtliche Konsequenzen	605
a) Recht des Arbeitgebers zur Datenübermittlung	605
b) Information des Betroffenen	605
c) Verdachtskündigung?	606
d) Verdachtsversetzung?	607
III. Überwachung der Telekommunikation	607
IV. Behördlich angeordnete Maßnahmen im Betrieb	609
V. Sicherheitsüberprüfung	610
1. Das Verfahren der Sicherheitsüberprüfung	610
a) Erfasster Personenkreis	610
b) Zuständige Behörde	611
c) Sicherheitserklärung	611
d) Kriterien für die Sicherheitsüberprüfung	611
e) Anhörung des Betroffenen	612
f) Entscheidung	612
g) Wiederholung des Verfahrens.	613
h) Behandlung der angefallenen Daten	613
2. Handhabung der Zuverlässigkeitsskriterien durch die Rechtsprechung	613
3. Erfasste Bereiche	615
4. Arbeitsrechtliche Folgen	617
a) Personenbedingte Kündigung	617
b) Ausdehnung auf nicht vom SÜG erfasste Bereiche?	618
5. Rechtsschutzmöglichkeiten bei verweigertem Zugang zu sicherheitsempfindlichen Bereichen	619
VI. Abgleichung mit Antiterroristen	620

VII. ECHELON und NSA	623
1. Echelon	623
2. NSA	623
§ 17: Einige Perspektiven	625
I. Die permanente Reformdiskussion	625
II. Datenschutz als Wettbewerbsfaktor	627
III. Transparenz des Datenschutzrechts	629
IV. Positive Impulse aus Europa?	630
V. Die nicht bewältigten Probleme	631
1. Cloud Computing	631
2. Big Data	632
3. Datenschutz im Internet	633
Literaturverzeichnis	635
Stichwortverzeichnis	697