

# Beschäftigtendatenschutz und Compliance

Effektive Compliance im Spannungsfeld von 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.)

Institut für Arbeitsrecht und Recht der Sozialen Sicherheit,  
Universität Bonn

Dr. Thomas Granetzny

Rechtsanwalt in Köln

Dr. Stephan Pötters, LL.M. (Cantab.)

Institut für Arbeitsrecht und Recht der Sozialen Sicherheit,  
Universität Bonn

Dr. Johannes Traut

Rechtsanwalt in Köln

2. Auflage 2014



# Inhaltsverzeichnis

Vorwort .....	V
Abkürzungs- und Literaturverzeichnis .....	XIX
 <b>§ 1. Der Beschäftigtendatenschutz als Aufgabe für Gesetzgebung und Rechtsprechung</b> .....	 1
I. Datenschutz als Persönlichkeitsschutz .....	1
II. Ein Blick zurück – ein Blick nach vorne .....	2
III. Der Beschäftigtendatenschutz in der Entwicklung .....	3
IV. Die Forderung nach einem Beschäftigtendatenschutzgesetz und der neue § 32 BDSG .....	4
V. Der Kommissions-Entwurf für eine Datenschutz-Grundverordnung .....	5
 <b>§ 2. Compliance als Aufgabe der Unternehmensleitung</b> .....	 7
I. Begriff und rechtliche Bedeutung .....	8
1. Begriff .....	8
2. Rechtliche Bedeutung .....	9
II. Das Pflichtenheft der Unternehmensleitung .....	10
1. Legalitätspflicht .....	11
2. Überwachungspflicht .....	12
a) Grundzüge der Überwachungspflicht .....	12
b) Mangelnde Überwachung als Eigenpflichtverletzung des Vorstandes .....	13
c) Keine Pflicht zur Einführung eines allgemeinen Compliance-Systems .....	14
3. Sorgfaltspflicht i.e.S. ....	15
4. Treuepflicht .....	16
III. Folgen einer Pflichtverletzung der Unternehmensleitung .....	17
1. Rechtsfolgen .....	17
a) Folgen für die Gesellschaft .....	17
b) Folgen für die Unternehmensleitung .....	19
2. Faktische Folgen .....	21
IV. Bestandteile eines Compliance-Systems .....	22
V. Pflicht zur Compliance in der Unternehmensgruppe? .....	23
1. Ausdehnung der in der einzelnen Gesellschaft geltenden Tatbestände? .....	23
2. Eigenständiger Compliance-Tatbestand in der Unternehmensgruppe? .....	25
VI. Zusammenfassung .....	27
 <b>§ 3. Zum System des Beschäftigtendatenschutzes</b> .....	 29
I. Unions- und verfassungsrechtskonforme Auslegung des Datenschutzrechts .....	29
II. Das Tor zum Datenschutzrecht: Der Begriff des „personenbezogenen Datums“ .....	31
III. „Verbot mit Erlaubnisvorbehalt“ nach § 4 Abs. 1 BDSG .....	32
IV. Das bisherige System nach § 28 BDSG .....	33
V. § 32 BDSG als lex regia des Beschäftigtendatenschutzes: Anwendungsbereich und Abgrenzung von § 28 BDSG .....	34
1. Personaler Schutzbereich: Wer ist „Beschäftigter“? .....	34
2. § 32 Abs. 1 BDSG als Konkretisierung oder Modifizierung des § 28 Abs. 1 S. 1 Nr. 1 BDSG? .....	35
a) Erforderlichkeit der Datenerhebung .....	35
b) Begrenztheit der Zweckbestimmung .....	36
aa) Entscheidung über die Begründung des Arbeitsverhältnisses .....	36
bb) Durchführung des Arbeitsverhältnisses .....	36
c) Sonderregelung zur Aufdeckung von Straftaten, § 32 Abs. 1 S. 2 BDSG .....	37

d) Möglichkeiten präventiven Vorgehens .....	38
e) Aufdeckung von Vertragsbrüchen .....	38
3. Verbleibende Anwendbarkeit des § 28 Abs. 1 S. 1 Nr. 2 BDSG .....	39
4. Verbleibende Anwendbarkeit des § 28 Abs. 1 S. 2 BDSG .....	40
5. § 32 Abs. 2 BDSG: Keine automatisierte Verarbeitung erforderlich .....	40
6. Zulässigkeit präventiven Vorgehens nach § 32 Abs. 1 S. 1 BDSG und § 28 Abs. 1 S. 1 Nr. 2 BDSG .....	41
VI. Interessenabwägung als gemeinsames Merkmal der §§ 28, 32 BDSG .....	41
1. Grundstruktur der Abwägung .....	41
2. Kriterien der Abwägung nach der Rechtsprechung des BVerfG .....	42
a) Eine Systematisierung der Rechtsprechung .....	43
b) Grenzen der Übertragbarkeit .....	45
c) Anhaltspunkte für die Auslegung von § 32 BDSG .....	45
VII. Verhältnis von BDSG und TKG .....	46
1. Subsidiarität des BDSG .....	46
2. Anwendbarkeit des TKG bei verbotener Privatnutzung .....	47
a) Merkmale eines Anbieters i. S. d. §§ 88, 91 TKG .....	47
b) Meinungsstand zum Arbeitgeber als Anbieter – Verbot privater Nutzung .....	49
3. Anwendbarkeit des TKG bei erlaubter Privatnutzung? .....	52
a) Der Meinungsstand in Literatur und Rechtsprechung .....	53
b) Eine Gewichtung der Argumente .....	55
aa) Wortlaut .....	55
bb) Geschichte .....	57
cc) Systematik .....	58
dd) Teleologie .....	60
ee) Eine aktuelle Bestätigung .....	61
c) Fazit: Keine Anwendbarkeit des TKG auch bei erlaubter Privatnutzung .....	62
<b>§ 4. Regelbarkeit durch Kollektivvereinbarungen .....</b>	<b>63</b>
I. Betriebsvereinbarung .....	63
1. Üblichkeit einer Regelung .....	63
2. Die Betriebsvereinbarung als „andere Rechtsvorschrift“ im Sinne des § 4 BDSG .....	64
3. Die Bedeutung von § 32 Abs. 3 BDSG .....	66
4. Die Betriebsvereinbarung als gesetzliche Vorschrift im Sinne des § 88 Abs. 3 S. 3, 2 Alt. TKG .....	66
5. Regelungsgrenzen einer Betriebsvereinbarung .....	69
II. Dienstvereinbarung .....	70
III. Tarifvertrag .....	70
1. Der Tarifvertrag als „andere Rechtsvorschrift“ im Sinne des § 4 BDSG .....	71
2. Abweichung vom Schutzniveau des BDSG durch Tarifvertrag zuungunsten der Beschäftigten .....	71
3. Aussagegehalt des § 32 Abs. 3 BDSG .....	72
<b>§ 5. Die Einwilligung des Arbeitnehmers .....</b>	<b>75</b>
I. Datenschutzrechtliche Anforderungen .....	75
1. Die informierte Einwilligung .....	75
2. Zeitpunkt der Einwilligung .....	77
3. Schriftform und besondere Hervorhebung .....	77
4. Freiwilligkeit und Bestimmtheit .....	78
5. Rechtsnatur und Rechtsfolgen des Verstoßes .....	82
6. Zwingender Charakter des § 4a BDSG .....	83
II. Grenzen der Einwilligung .....	84
III. AGB-rechtliche Anforderungen .....	84
1. Verbot überraschender Klauseln .....	85

## Inhaltsverzeichnis

2. Inhaltskontrolle .....	85
IV. Das Problem der Widerruflichkeit .....	88
V. Ausblick: Datenschutzgrundverordnung .....	89
VI. Mustereinwilligung .....	90
<b>§ 6. Whistleblowing .....</b>	<b>93</b>
I. Begriff und Herkunft .....	93
1. Begriff .....	93
2. Herkunft .....	94
3. Zweck .....	95
a) Kontinentaleuropa .....	95
b) Vereinigtes Königreich .....	96
c) Recht der Europäischen Union .....	97
4. Reformbestrebungen .....	97
II. Fallgruppen des Whistleblowing .....	98
1. Anonymes und offenes Whistleblowing .....	98
2. Internes und externes Whistleblowing .....	99
3. Zentrales und dezentrales Whistleblowing .....	100
III. Wer darf melden? .....	101
IV. Was darf gemeldet werden? .....	104
V. Wie darf gemeldet werden? .....	107
VI. Vertragliche Verpflichtung zum Whistleblowing .....	111
VII. Folgen des berechtigten Whistleblowing .....	112
1. Retrospektiver Schutz .....	112
2. Präventiver Schutz .....	114
VIII. Zum Schutz des Angezeigten .....	116
IX. Datenschutzrechtliche Besonderheiten .....	117
1. Vorgaben der DS-RL .....	117
2. Möglichkeiten und Grenzen des Datenschutzrechts .....	118
3. Whistleblowing und BDSG .....	119
4. Einzelfragen .....	120
a) Anzuwendendes Recht .....	120
b) Whistleblower kein „Verantwortlicher“ .....	120
c) Ausnahme vom Grundsatz der Direkterhebung .....	121
d) Ausschluss der Einwilligung .....	121
e) Gesetzlicher Erlaubnistatbestand .....	122
f) Datenübermittlung .....	122
g) Benachrichtigung und Auskunft .....	125
h) Berichtigung, Sperrung und Löschung personenbezogener Daten .....	126
i) Stellung des Datenschutzbeauftragten und der Aufsichtsbehörden .....	126
j) Organisatorischer und technischer Schutz der Whistleblowing-Stelle .....	126
<b>§ 7. Informationserhebung bei der Einstellung und beim beruflichen Aufstieg .....</b>	<b>129</b>
I. Zusammenspiel von BDSG und AGG .....	129
II. Grenzen des BDSG .....	130
1. Grundregel des § 32 BDSG: Datennutzung nur bei Erforderlichkeit .....	130
2. Besondere Arten personenbezogener Daten .....	131
a) Relevante Fallgruppen .....	132
b) Erlaubnistatbestände .....	132
III. Konkretisierung durch die Rechtsprechung .....	134
1. Frage nach der Schwangerschaft .....	135
2. Frage nach einer Behinderung und nach der Schwerbehinderteneigenschaft .....	136

3. Frage nach Religion, Weltanschauung und sexueller Identität	138
4. Frage nach Vorerkrankungen – Gesundheits- und Drogentests	138
5. Frage nach der Gewerkschaftszugehörigkeit	140
6. Frage nach genetischen Merkmalen	140
7. Frage nach Vorstrafen und Ermittlungsverfahren, Führungszeugnis	141
IV. Übersicht: Fragerecht des Arbeitgebers	143
<b>§ 8. Der elektronische Datenabgleich</b>	145
I. Geeignetheit	146
II. Erforderlichkeit	146
1. Generalverdacht vs. Einschränkung auf eine bestimmte Personengruppe	147
2. Notwendigkeit einer Unterrichtung oder Pseudonymisierung/Anonymisierung?	148
III. Angemessenheit	148
1. Üblichkeit	149
a) Gebrauch durch staatliche Stellen	149
aa) Sozialversicherungsrecht	149
bb) Steuerrecht	150
cc) BAFöG	151
dd) Bundesrechnungshof	152
b) Gebrauch im privaten Bereich	152
c) Bewertung der Üblichkeit in der Literatur	154
d) Ein Seitenblick auf das Europarecht	156
e) Üblichkeit der Einbeziehung von Angehörigen	158
2. Das Interesse der verantwortlichen Stelle	159
3. Das Interesse der betroffenen Arbeitnehmer	159
4. Angemessenheit im engeren Sinne	160
<b>§ 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles</b>	161
I. Grundlagen	161
1. Zwecke der Speicherung und Sichtung des E-Mail-Verkehrs	161
2. Objekte des Zugriffs: Logfiles und E-Mails	163
3. Verantwortliche Stelle, Betroffene	163
4. Prüfungsrahmen: BDSG oder TKG und StGB?	164
II. Erfordernis einer Rechtfertigung (§ 4 Abs. 1 BDSG)	164
1. E-Mail-Logfiles	164
a) E-Mail-Logfiles als personenbezogene Daten	164
b) Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten	165
2. E-Mails	166
III. Rechtfertigung (§ 32 BDSG)	167
1. Ausschluss nach § 31 BDSG?	167
2. Leitlinien für die Verhältnismäßigkeitsprüfung	169
a) Zugriff auf Logfiles vs. Zugriff auf E-Mails	169
b) Privatnutzung erlaubt vs. Privatnutzung verboten	169
c) Vergleichbarkeit mit Brief oder Telefonat?	172
d) Kriterien der Interessenabwägung im Einzelfall	174
3. Aufklärung von Straftaten (§ 32 Abs. 1 S. 2 BDSG)	176
4. Zwecke des Beschäftigungsverhältnisses (§ 32 Abs. 1 S. 1 BDSG)	178
a) Compliance	178
b) Zugriff auf dienstliche Informationen	180
c) Leistungskontrolle	180
IV. Disputandi causa: Rechtmäßigkeit nach dem TKG und StGB	181
1. E-Mail-Logfiles	181
a) Das Verhältnis von Fernmeldegeheimnis und Datenschutz	181
aa) Persönlicher Schutzbereich	181
bb) Sachlicher Schutzbereich	182

cc) Abgrenzung der Schutzbereiche	184
b) Zulässigkeit der Speicherung der Verkehrsdaten	187
aa) Eingriff	187
bb) Rechtfertigung	188
c) Zulässigkeit der Speicherung einer Betreffzeile	190
d) Strafrechtliche Bewertung	191
aa) Der Tatbestand des § 206 StGB	191
bb) Rechtfertigung der Weitergabe der Daten	191
cc) Folgerungen	192
2. E-Mails	193
a) Rechtfertigung nach § 88 Abs. 3 S. 1 TKG i. V. m. § 100 Abs. 3 TKG	193
b) Rechtfertigung nach § 88 Abs. 3 S. 3 TKG	193
<b>§ 10. Überwachung von Telefonverbindungsdaten</b>	195
I. Rechtmäßigkeit nach dem BDSG	195
1. Rechtsprechung und Literatur zur generellen Erfassung	195
2. Vollständige Nummern Erfassung	197
II. Rechtmäßigkeit nach dem TKG	197
<b>§ 11. Videoüberwachung</b>	199
I. Begriff und rechtliche Bedeutung	199
1. Begriff der Videoüberwachung	200
a) Videoüberwachung i. S. d. § 6b Abs. 1 BDSG	200
b) Videoüberwachung nach der Definition des BAG	202
2. Rechtliche Bedeutung	202
II. Prüfungsrahmen	203
1. Datenschutzrichtlinie	203
2. Grundgesetz und EU-Grundrechtecharta	203
3. BDSG	204
a) Einwilligung nach §§ 4, 4a BDSG	204
b) Eingriffsnorm des § 6b BDSG	204
c) Eingriffsnormen der §§ 28, 32 BDSG	205
4. Sonstige Rechtsvorschriften	206
a) Verhältnis zum TKG	206
b) § 22 KUG	207
c) Notwehr und Notstand	207
d) „Hausrecht“	207
III. Voraussetzungen der offenen Videoüberwachung	208
1. Öffentlich zugänglicher Raum	208
a) Systematik des § 6b BDSG	208
b) Legitimer Zweck (§ 6b Abs. 1 Nr. 2 und Nr. 3 BDSG)	208
c) Geeignetheit und Erforderlichkeit (§ 6b Abs. 1 letzter Hs. BDSG)	209
d) Angemessenheit (§ 6b Abs. 1 letzter Hs. BDSG)	210
e) Hinweispflicht (§ 6b Abs. 2 BDSG)	210
f) Vorabkontrolle, Benachrichtigung und Löschung	211
2. Nicht öffentlich zugänglicher Raum	211
IV. Voraussetzungen der heimlichen Videoüberwachung	213
1. Öffentlich zugänglicher Raum	213
a) Kein Ausschluss durch § 6b Abs. 2 BDSG	213
b) Rechtsgrundlage	214
c) Voraussetzungen	215
2. Nicht öffentlich zugänglicher Raum	215
a) Rechtsgrundlage	215
b) Voraussetzungen	216

## Inhaltsverzeichnis

V. Verarbeitung und Nutzung erhobener Daten	217
1. Datensparsamkeit: Begrenzte Auswertung des aufgezeichneten Materials	217
2. Daten aus öffentlich zugänglichen Räumen	217
3. Daten aus nicht öffentlich zugänglichen Bereichen	217
VI. Löschungspflichten	218
VII. Prozessuales: Beweisverwertungsverbot	218
VIII. Videoüberwachung auf Grundlage einer Betriebsvereinbarung	220
1. Regelbarkeit durch Betriebsvereinbarung	220
2. Muster-Betriebsvereinbarung	220
IX. Übersicht: Rechtfertigung einer Videoüberwachung	224
<b>§ 12. Überwachung mobiler Arbeitnehmer</b>	<b>225</b>
I. Einleitung	225
II. Technische Möglichkeiten	226
1. Überwachung mittels Satellitenortung	226
2. Überwachung mittels RFID	227
3. Ortung mittels der Telekommunikationsnetze	228
III. Rechtliche Zulässigkeit	229
1. Überwachung mittels Satellitenortung	229
a) Prüfungsmaßstab	229
b) Personenbezogene Daten	229
c) Informationspflicht	230
d) Erlaubnistatbestände	230
e) Sanktionen bei rechtswidriger Nutzung	232
2. Überwachung mittels RFID	232
a) Prüfungsmaßstab	232
b) Personenbezogene Daten	232
c) Informationspflicht	233
d) Erlaubnistatbestände	233
e) Sanktionen bei rechtswidriger Nutzung	234
3. Ortung mittels der Telekommunikationsnetze	235
a) Prüfungsmaßstab	235
b) Personenbezogene Daten	236
c) Informationspflicht	236
d) Erlaubnistatbestände	236
e) Sanktionen bei rechtswidriger Nutzung	237
f) Disputandi causa: Zulässigkeit nach dem TKG und dem TMG	237
<b>§ 13. Personengebundene Merkmale</b>	<b>239</b>
I. Biometrische Daten	239
II. Umgang mit biometrischen Daten	240
III. Rechtfertigung nach § 32 Abs. 1 BDSG	240
1. Legitime Zwecksetzung	241
2. Erforderlichkeit	241
3. Kein Entgegenstehen schutzwürdiger Interessen des Beschäftigten – Verhältnismäßigkeit im engeren Sinne	242
IV. Exkurs: Ärztliche Untersuchungen	242
1. Datenerhebung im Wege einer ärztlichen Untersuchung	243
2. Rechtfertigung nach § 32 Abs. 1 BDSG	244
a) Notwendigkeit der ärztlichen Untersuchung	244
b) Berechtigtes Interesse	244
3. Einwilligung	245
4. Rechtsfolgen einer angeordneten Untersuchung	246
a) Zulässige Anordnung	246

## Inhaltsverzeichnis

b) Unzulässige Anordnung .....	246
5. Auswahl des Arztes und Kommunikation des Untersuchungsergebnisses .....	247
<b>§ 14. Social Media in Betrieb und Unternehmen .....</b>	<b>249</b>
I. Social Media als auch betriebliches Phänomen .....	249
II. Zugriff des Arbeitgebers auf Informationen in Internet und Social Media .....	250
1. Die Positionen in der Literatur .....	250
2. Abwägung, kein absolutes Gebot der Direkterhebung .....	252
3. Leitlinien für die Abwägung .....	253
a) Öffentlich zugänglich: Vorbelastung für Zulässigkeit (§ 28 Abs. 1 S. 1 Nr. 3 BDSG) .....	254
b) (Sonstige) Veranlassung durch Betroffenen .....	257
c) Aufgaben und berufliche Stellung des Bewerber .....	257
d) Das Problem der Zufallsfunde .....	258
e) Eingesetzte Suchwerkzeuge, „Big-Data“ .....	260
4. Zugriff für Zwecke des Beschäftigungsverhältnisses (§§ 28 Abs. 1 S. 1 Nr. 3, 32 Abs. 1 BDSG) .....	260
a) Rechtsgrundlagen und Zwecke .....	260
b) Bewerbungsphase .....	261
c) Laufendes Arbeitsverhältnis .....	262
5. Nutzung von Social Media für eigene und private Zwecke (§ 28 Abs. 1 BDSG) .....	263
6. Benachrichtigung nach § 33 BDSG? .....	264
7. Abgrenzung zum Abhören .....	264
III. Social Media Guidelines auf Grundlage des Weisungsrechts (§§ 315 Abs. 1 BGB, 106 GewO) .....	265
1. Beschränkung der Privatnutzung .....	265
a) Im Netzwerk des Arbeitgebers .....	265
b) Beschränkung privater Nutzung (§ 241 Abs. 2 BGB) .....	266
2. Social Media als Arbeitsmittel .....	267
a) Anordnung der Nutzung interner Social Media .....	267
b) Anordnung Nutzung externer Social Media .....	268
c) Allgemeine Leitlinien für den dienstlichen Umgang .....	269
IV. Social Media Guidelines auf Grundlage von Betriebsvereinbarungen .....	270
1. Persönlicher Geltungsbereich .....	272
2. Räumlicher Geltungsbereich .....	273
3. Sachlicher Geltungsbereich .....	273
4. Zeitlicher Geltungsbereich .....	274
5. Erzwingbar durch den Betriebsrat? .....	275
V. Beispiel: Social Media Anwendungsrichtlinie Pfefferminzia AG .....	276
<b>§ 15. Nutzung von Cloud-Technologien im Arbeitsverhältnis .....</b>	<b>279</b>
I. Cloud-Computing: Begriff und Bedeutung .....	279
1. Cloud-Computing – Fehlen einer einheitlichen Definition .....	279
2. Trend der Arbeitswelt: Bring Your Own Device .....	280
3. Gemeinsame Kernmerkmale und Risiken von Cloud-Technologien .....	280
II. Grundrechtsschutz in der Cloud .....	281
1. Cloud-Computing und Grundgesetz .....	281
a) Abgrenzung von Telekommunikationsfreiheit und allgemeinem Persönlichkeitsrecht .....	281
b) Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme .....	282
2. Cloud-Computing und EU-Grundrechtecharta .....	283
III. Datenschutzrechtliche Besonderheiten beim Cloud-Computing .....	283
1. Anwendbares Datenschutzrecht .....	284
a) Anwendbarkeit des nationalen Rechts nach § 1 Abs. 5 BDSG .....	284



b) Unionsrechtliche Vorgaben: Art. 4 Datenschutzrichtlinie .....	284
c) Differenzierung zwischen europäischen und internationalen Clouds .....	285
2. Verantwortlicher i.S.v. § 3 Abs. 7 BDSG .....	286
3. Cloud-Computing als Datenverarbeitung im Auftrag des Arbeitgebers .....	287
4. Probleme bei der Nutzung privater IT (Bring Your Own Device) .....	289
<b>§ 16. Datentransfer im Konzern und Zulässigkeit der Datenweitergabe an Dritte .....</b>	<b>291</b>
I. Praktische Relevanz und rechtliche Bedeutung .....	291
1. Praktische Relevanz .....	291
2. Rechtliche Bedeutung .....	292
II. Klärung der Begrifflichkeiten .....	292
1. „Verantwortliche Stelle“ (§ 3 Abs. 7 BDSG) .....	293
2. „Dritter“ (§ 3 Abs. 8 BDSG) .....	294
III. Auftragsdatenverarbeitung – Eigenverarbeitung – Funktionsübertragung .....	294
1. Auftragsdatenverarbeitung .....	294
2. Handeln der verantwortlichen Stelle selber .....	295
3. Funktionsübertragung .....	296
4. Wartungsarbeiten mit Zugriff auf personenbezogene Daten .....	298
5. Auftragswidrige Nutzung der Daten durch den Auftragnehmer .....	298
IV. Voraussetzungen für die Rechtmäßigkeit einer Auftragsdatenverarbeitung .....	299
1. Schriftlichkeit der Auftragserteilung .....	299
a) Form der Auftragserteilung .....	299
b) Umfang der Dokumentationspflicht .....	300
2. Auswahl des Auftragnehmers .....	301
<b>§ 17. Internationale Datenübermittlung .....</b>	<b>303</b>
I. Einführung .....	303
II. Anzuwendendes Recht .....	305
1. Kollisionsregel gegenüber EU/EWR-Staaten .....	305
2. Kollisionsregel gegenüber Drittstaaten .....	307
III. Zweistufige Rechtmäßigkeitsprüfung .....	308
IV. Datenübermittlung innerhalb der EU .....	308
V. Datenübermittlung in Drittstaaten .....	309
1. Angemessenes Schutzniveau .....	309
2. Ausreichende Garantien .....	310
3. Standardvertragsklauseln .....	312
a) Standardvertragsklauseln I und II .....	312
b) Standardvertragsklauseln für Auftragsverarbeiter .....	313
c) Vor- und Nachteile von Standardvertragsklauseln .....	314
4. Binding Corporate Rules .....	314
a) Empirie .....	314
b) Notwendiger Inhalt .....	315
c) Verbindlichkeit .....	316
d) Haftung .....	318
e) Genehmigung der Datenschutzbehörden .....	321
f) Vor- und Nachteile von BCR .....	322
5. Safe Harbor Principles (USA) .....	322
<b>§ 18. Informations- und Organisationspflichten     bei der Datenverarbeitung .....</b>	<b>325</b>
I. Grundrechtsschutz durch Verfahren .....	325
II. Informations- und Unterrichtungspflichten .....	327
1. Überblick über die einzelnen Unterrichtungspflichten des Arbeitgebers und Auskunftsrechte des Beschäftigten .....	327

## Inhaltsverzeichnis

2. Änderungen durch die Gesetzesnovelle 2009 .....	328
3. § 33 BDSG – Informationspflicht bei erstmaliger Speicherung von Daten .....	329
a) Tatbestandliche Voraussetzungen für die Benachrichtigungspflicht .....	331
aa) Erstmalige Speicherung .....	331
bb) Zweckänderung als erstmalige Speicherung – Sonderproblem Datenabgleich .....	331
cc) Speicherung ohne Kenntnis des Betroffenen .....	332
b) Entbehrlichkeit der Benachrichtigung .....	334
aa) Vorhandene Kenntnis des Betroffenen – § 33 Abs. 2 Nr. 1 BDSG .....	334
bb) Unverhältnismäßiger Aufwand – § 33 Abs. 2 Nr. 2 BDSG .....	334
cc) Geheimhaltungsinteresse – § 33 Abs. 2 Nr. 3 BDSG .....	335
dd) Durch Gesetz vorgesehene Speicherung – § 33 Abs. 2 Nr. 4 BDSG .....	336
ee) Wissenschaftsprivileg – § 33 Abs. 2 Nr. 5 BDSG .....	336
ff) Gefährdung der öffentlichen Sicherheit – § 33 Abs. 2 Nr. 6 BDSG .....	336
gg) Daten aus allgemein zugänglichen Quellen – § 33 Abs. 2 Nr. 7a BDSG ..	336
hh) Gefährdung eigener Geschäftszwecke der speichernden Stelle – § 33 Abs. 2 Nr. 7b BDSG .....	337
4. Auskunftsrecht des Betroffenen nach § 34 BDSG .....	338
a) Tatbestandliche Voraussetzungen des Auskunftsanspruchs .....	338
b) Inhalt des Auskunftsanspruchs: Daten des Betroffenen und Herkunft der Daten .....	338
c) Inhalt des Auskunftsanspruchs: Zweck der Speicherung .....	339
d) Inhalt des Auskunftsanspruchs: Empfänger oder Kategorien von Empfängern ..	340
5. Informationspflicht vor Erhebung der Daten beim Betroffenen – § 4 Abs. 3 BDSG .....	340
6. Informationspflicht vor Erteilung einer Einwilligung – § 4a BDSG .....	341
7. Informationspflicht bei der Übermittlung ins Ausland – § 4b BDSG .....	341
8. Unterrichtungspflicht im Rahmen der Videoüberwachung – § 6b Abs. 4 BDSG .....	342
9. Mobile personenbezogene Speicher- und Verarbeitungsmedien – § 6c BDSG .....	342
10. Informationspflicht bei unrechtmäßiger Kenntniserlangung – § 42a BDSG .....	342
11. Meldepflicht vor Inbetriebnahme von Verfahren automatisierter Verarbeitung – § 4d Abs. 1 BDSG .....	347
12. Meldepflicht bei Vorhaben automatisierter Verarbeitung – § 4g BDSG .....	349
13. Unterrichtungspflicht bei der Einrichtung automatisierter Abrufverfahren – § 10 BDSG .....	349
III. Drohende Sanktionen bei der Verletzung von Unterrichtungspflichten .....	349
IV. Sonstige Auskunftsrechte und Informationspflichten .....	350
V. Technische und organisatorische Maßnahmen (§ 9 BDSG) .....	350
VI. Schutz durch Verpflichtung auf das Datengeheimnis nach § 5 BDSG .....	351
1. § 5 BDSG und seine Funktion im Arbeitsverhältnis .....	351
2. Mustererklärung: Belehrung und Verpflichtung zur Wahrung des Datengeheimnisses .....	352
<b>§ 19. Die Einbindung des betrieblichen Datenschutzbeauftragten –     Partner in der Compliance .....</b>	<b>353</b>
I. Der Datenschutzbeauftragte im Betrieb .....	353
II. Pflicht zur Bestellung eines Datenschutzbeauftragten .....	353
III. Qualifikationsanforderungen .....	354
IV. Bestellung, zugrunde liegendes Rechtsverhältnis und Widerruf .....	356
V. Die Aufgaben des Datenschutzbeauftragten .....	357
VI. Sicherung der Aufgabenerfüllung .....	359
VII. Die strafrechtliche Verantwortung des Datenschutzbeauftragten .....	359

<b>§ 20. Betriebsverfassungsrechtliche Zulässigkeit einer Datenverarbeitung</b>	<b>361</b>
I. Allgemeine Fragen des § 87 BetrVG	361
1. Persönlicher Anwendungsbereich	361
2. Erfordernis kollektiver Maßnahmen	362
3. Keine gesetzliche Regelung – Sperre des § 87 Abs. 1 Einleitungssatz BetrVG	363
II. Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG	364
1. Zweck des Mitbestimmungsrechts	364
2. Umfang des Mitbestimmungsrechts	365
a) Technische Einrichtung	366
b) Zur Überwachung	366
aa) Überwachung als Erhebung, Verarbeitung und Auswertung	366
bb) Selbständige Kontrollwirkung	368
cc) Überwachung vs. Kontrolle?	368
dd) Durchführung der Überwachung durch Dritte	369
ee) Natur der einbezogenen Daten	370
ff) Von Verhalten und Leistung der Arbeitnehmer	371
gg) Bestimmung zur Überwachung	372
3. Rechtsfolgen	372
a) Individualrechtliche Folgen	373
b) Beweisrechtliche Folgen	373
c) Unterlassungsansprüche	375
d) Straf- und Bußgeldvorschriften des BetrVG: § 119 BetrVG	375
aa) Störung oder Behinderung der Tätigkeit der Betriebsverfassungsorgane	376
bb) Tauglicher Täter	377
cc) Subjektiver Tatbestand	377
dd) Verschulden	378
ee) Antragsdelikt	378
ff) Verjährung	378
III. Weitere Mitbestimmungs- und Beteiligungsrechte	379
1. Anwendungsbereich	379
2. Rechtsfolgen	381
IV. Informationsrechte des Betriebsrats beim Beschäftigtendatenschutz gemäß § 80 Abs. 2 BetrVG	381
1. Wahrscheinlichkeit des Aufgabenbezugs	382
2. Erforderlichkeit	384
3. Insbesondere: Informationen bei Internal Investigations	385
a) Bedeutung	385
b) Ablauf einer Internal Investigation	386
c) Informations- und Mitbestimmungsrechte des Betriebsrats	386
aa) Informationsbeschaffung	386
bb) Bewertung und Auswertung von Informationen	386
cc) Investigation Report	387
d) Regelung durch Betriebsvereinbarung	388
V. Übersicht: Datenschutzkompetenzen des Betriebsrat zum BetrVG	388
VI. Muster-Betriebsvereinbarung IT	389
VII. Datenschutz gegenüber dem Betriebsrat	394
1. Der Betriebsrat als Adressat des BDSG?	394
2. Datenschutzrechtliche Rechtfertigungstatbestände	394
3. Das Betriebsverfassungsrecht als Grenze von Datenerhebung, -verarbeitung oder -nutzung	396
4. Kontrolle des Betriebsrats durch den Arbeitgeber?	397
VIII. Parallele Regelungen des Personalvertretungsrechts	397
1. § 75 Abs. 3 Nr. 17 BPersVG	398
2. Negative Abweichung vom BDSG durch Dienstvereinbarung?	398

<b>§ 21. Rechtsfolgen unerlaubter Datenverarbeitung</b>	<b>399</b>
I. Unionsrechtlicher Hintergrund	399
1. Spezielle Vorgaben der Datenschutzrichtlinie 95/46/EG	399
2. Allgemeine Vorgaben des EuGH	400
II. Zivilrechtliche Folgen	400
1. Zurückbehaltungsrecht des Beschäftigten	400
2. Schadensersatzansprüche	402
a) §§ 7, 8 BDSG	402
b) § 280 Abs. 1 S. 1 BGB i.V.m. § 241 Abs. 2 BGB/§ 311 Abs. 2 BGB	405
c) §§ 823 Abs. 1 und 2, 824, 826 BGB	406
d) Hilfspersonen	408
aa) Haftung für Hilfspersonen	408
bb) Haftung der Hilfsperson	408
e) Konkurrenzen	409
3. Unterlassungs-, Beseitigungs- und Gegendarstellungsansprüche	409
4. Herausgabeansprüche und Gewinnabschöpfung	410
III. Straf- und ordnungswidrigkeitenrechtliche Folgen	410
IV. Umsetzungsdefizite des deutschen Rechts	411
V. Beweisverwertungsverbot?	413
Stichwortverzeichnis	417