

Konzerndatenschutz

Rechtshandbuch

Herausgegeben von

Dr. Axel Frhr. von dem Bussche, LL. M. (L. S. E.)
Hamburg

Paul Voigt, Lic. en Derecho
Hamburg

Bearbeitet von
den Herausgebern und von

Monika Egle, Ulm; *Nils Hullen*, LL. M., Brüssel;
Meike Kamp, LL. M., Berlin; *Dr. Flemming Moos*, Hamburg;
Hannes Oenning, Frankfurt a. M.; *Jana Oenning*, Gütersloh;
Dr. Kai-Uwe Plath, LL. M. (N. Y.), Hamburg;
Dr. Axel Spies, C. E. P. (Paris), Washington;
Prof. Dr. Peter Wedde, Frankfurt a. M.; *Andreas Zeller*, Ulm

2014



C.H. BECK

Inhaltsübersicht

	Seite
Vorwort	V
Bearbeiterverzeichnis	XXV
Abkürzungsverzeichnis.....	XXVII
Allgemeines Literaturverzeichnis	XXXVII
Teil 1. Einführung und „Checkliste“	1
Teil 2. Datenschutzorganisation im Konzern	
Kapitel 1. Der Datenschutzbeauftragte	7
Kapitel 2. Datenschutzmanagement im Konzern	35
Kapitel 3. Verarbeitungsübersicht und Verfahrensverzeichnis	54
Kapitel 4. Verarbeitungsübersicht im Konzern.....	59
Kapitel 5. Vorabkontrolle.....	67
Kapitel 6. Verpflichtung auf das Datengeheimnis	71
Kapitel 7. Informations- und Einwirkungsrechte der Betroffenen	73
Teil 3. Datenverarbeitung im Konzern	
Kapitel 1. Einleitung: Fehlendes Konzernprivileg.....	93
Kapitel 2. Rechtliche Anforderungen an Datenverarbeitungen ...	95
Kapitel 3. Auftragsdatenverarbeitung im Konzern.....	115
Kapitel 4. Verträge für den konzerninternen Datentransfer	146
Kapitel 5. Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats	171
Teil 4. Internationale Aspekte des deutschen Datenschutzrechts	
Kapitel 1. Räumliche Anwendbarkeit des BDSG	201
Kapitel 2. Datenübermittlungen in Drittländer.....	215
Kapitel 3. Standardvertragsklauseln	224
Kapitel 4. Safe Harbor Principles	236
Kapitel 5. Binding Corporate Rules.....	249
Teil 5. Spannungsfeld zwischen Datenschutz und Compliance-Anforderungen	
Kapitel 1. Datenschutzrecht und Compliance.....	289
Kapitel 2. E-Discovery.....	311
Teil 6. Datenschutz bei M&A-Transaktionen	323
Teil 7. Cloud Computing	345
Teil 8. Ausblick auf die EU-Datenschutz-Grundverordnung	373
Sachverzeichnis	405

Inhaltsverzeichnis

	Seite
Vorwort	V
Bearbeiterverzeichnis	XXV
Abkürzungsverzeichnis	XXVII
Allgemeines Literaturverzeichnis	XXXVII

Teil 1. Einführung und „Checkliste“

A. Datenschutzorganisation	1
B. Rechtmäßigkeit der Datenverarbeitung	3
C. Wichtige Spezialthemen	5
D. Ausblick auf die EU-Datenschutz-Grundverordnung	6

Teil 2. Datenschutzorganisation im Konzern

Kapitel 1. Der Datenschutzbeauftragte

A. Grundlegende Funktion des Datenschutzbeauftragten	8
B. Grundsätzliche Bestellungspflicht; verpflichtete Stelle	9
I. Grundsatz der Bestellungspflicht	10
II. Die zur Bestellung verpflichtete Stelle; insbesondere innerhalb von Konzernstrukturen	11
C. Die Person des Datenschutzbeauftragten	11
I. Interner vs. externer Datenschutzbeauftragter	11
II. Fachliche und persönliche Anforderungen	12
1. Fachkunde	12
2. Zuverlässigkeit, insbesondere Interessenkonflikt	14
D. Ordnungsgemäße Bestellung des Datenschutzbeauftragten; vertragliches Verhältnis zwischen Datenschutzbeauftragten und verantwortlicher Stelle	15
I. Ordnungsgemäße Bestellung als Datenschutzbeauftragter	15
II. Vertragsverhältnis, gegebenenfalls erforderliche Abänderung	16
III. Rechtsfolgen fehlerhafter oder unterlassener Bestellung	17
E. Organisatorische Stellung des Datenschutzbeauftragten; zentrale konzernweite Organisation des Datenschutzes	17
I. Position in der Unternehmensstruktur	17
II. Organisation innerhalb von Konzernstrukturen	18
III. Unabhängigkeit und Weisungsfreiheit des Datenschutzbeauftragten	19

	Seite
IV. Verhältnis zwischen Datenschutzbeauftragtem und Mitarbeitervertretungen	20
V. Unterstützungspflicht des Arbeitgebers	20
F. Aufgaben des Datenschutzbeauftragten	21
I. Allgemeine Hinwirkungspflicht	22
II. Programmüberwachung	23
III. Schulungs- und Fortbildungsfunktion	24
IV. Anrufungsrecht der Betroffenen; Verschwiegenheitspflicht	24
V. Sonstige Pflichten des Datenschutzbeauftragten	25
G. Einschaltung der Aufsichtsbehörde	26
H. Abberufung, Kündigung, sonstige Beendigung	26
I. Abberufung und Abberufungsschutz	26
1. Abberufung auf Verlangen der Aufsichtsbehörde	26
2. Abberufung durch die verantwortliche Stelle	27
II. Kündigung des zugrundeliegenden Vertragsverhältnisses	27
III. Verhältnis zwischen Widerruf und Kündigung	28
1. Interner Datenschutzbeauftragter	28
2. Externer Datenschutzbeauftragter	29
IV. Fortbestand bzw. Wegfall des Amts bei gesellschaftsrechtlichen Umstrukturierungen	29
V. Sonstige Beendigungstatbestände	31
I. Haftung des Datenschutzbeauftragten	31
I. Ansprüche der verantwortlichen Stelle	32
II. Ansprüche der Betroffenen	32
J. Aussicht auf die EU-Datenschutz-Grundverordnung	33
 Kapitel 2. Datenschutzmanagement im Konzern 	
A. Einleitung	36
B. Vorgehensweise beim Aufbau eines Datenschutzmanagements	37
I. Vorgehensmodell zur Implementierung konzernweit gültiger technischer und organisatorischer Maßnahmen	37
II. Vorgehensmodell zum Aufbau eines Datenschutzmanagementsystems	38
1. Analyse	39
2. Konzeption	41
3. Einführung	42
4. Betrieb	43
C. Datenschutzmanagement in Konzernstrukturen	44
I. Grundsätzliche Ziele	44
1. Erfüllung rechtlicher Vorgaben	44

2. Transparentes Risikomanagement durch Integration des Datenschutzes in das interne Kontrollsystem	44
3. Konzernübergreifendes und effizientes Datenschutzmanagement ..	45
II. Datenschutzmanagementsystem	45
III. Datenschutzorganisation	47
1. Konzernleitung	47
2. Konzerndatenschutzbeauftragter	48
3. Leitung der Einzelgesellschaft	48
4. Lokaler Datenschutzbeauftragter einer Einzelgesellschaft	49
5. Datenschutzkoordinatoren	49
6. Geschäftsprozessverantwortliche	50
7. Entscheider/Führungskräfte	50
8. Benutzer	50
IV. Einbettung der Datenschutzorganisation in Konzernstrukturen	50
1. Zentrale Struktur	51
2. Dezentrale Struktur	51

Kapitel 3. Verarbeitungsübersicht und Verfahrensverzeichnis

A. Einleitung	54
B. Die interne Verarbeitungsübersicht	54
I. Verpflichtung zur Erstellung	55
II. Inhalt der internen Verarbeitungsübersicht	56
C. Externes Verfahrensverzeichnis	57

Kapitel 4. Verarbeitungsübersicht im Konzern

A. Einleitung	59
B. Struktur einer konzernweiten internen Verarbeitungsübersicht	60
C. Aufbau und Betrieb einer konzernweiten internen Verarbeitungsübersicht	60
I. Analyse	61
II. Konzeption	61
III. Einführung	63
1. Stufe 1: Erstellung einer Verfahrensübersicht	63
2. Stufe 2: Erstellung der Verfahrensbeschreibungen	63
a) Variante 1: Erstellung der Verfahrensbeschreibungen durch die jeweiligen Benutzer/Entscheider	64
b) Variante 2: Erstellung der Verfahrensbeschreibungen durch einen Beauftragten	65
IV. Betrieb	65

Kapitel 5. Vorabkontrolle

A. Einleitung	67
B. Anwendungsbereich der Vorabkontrolle	68

	Seite
C. Prüfungsmaßstab und -umfang	69
D. Rechtsfolgen	70
Kapitel 6. Verpflichtung auf das Datengeheimnis	71
Kapitel 7. Informations- und Einwirkungsrechte der Betroffenen	
A. Einleitung	74
B. Benachrichtigungspflichten gegenüber dem Betroffenen	74
I. Bei der Direkterhebung	74
II. Bei Erhebung ohne Kenntnis des Betroffenen	76
C. Auskunftsrechte des Betroffenen	78
D. Ansprüche des Betroffenen auf Berichtigung, Löschung und Sperrung	80
I. Berichtigung	81
II. Löschung	81
III. Sperrung	83
IV. Widerspruchsrecht des Betroffenen	83
V. Nachberichtspflicht	84
VI. Sonstiges	84
E. Informationspflicht bei Datenpannen	84
I. Verpflichtete Stellen	85
II. Informationspflicht nur bei Risikodaten	85
III. Unrechtmäßige Kenntniserlangung durch Dritte	86
IV. Schwerwiegende Beeinträchtigung	86
V. Informationspflicht gegenüber Betroffenen	87
VI. Informationspflicht gegenüber der Aufsichtsbehörde	88
F. Unterrichts- und Auskunftspflichten von Telemediendiensteanbietern	88
I. Unterrichtungspflicht	89
II. Auskunftspflicht	90
Teil 3. Datenverarbeitung im Konzern	
Kapitel 1. Einleitung: Fehlendes Konzernprivileg	93
Kapitel 2. Rechtliche Anforderungen an Datenverarbeitungen	
A. Grundbegriffe	96
I. Personenbezogene Daten, Betroffener und verantwortliche Stelle	96
II. Der Umgang mit personenbezogenen Daten	97
B. Anwendbarkeit des BDSG	97

	Seite
C. Verbot mit Erlaubnisvorbehalt	98
I. Einwilligung	98
1. Wirksamkeitsvoraussetzungen	99
a) Form und Zeitpunkt der Einwilligung	99
b) Informierte Einwilligung	100
c) Freiwillige Einwilligung	100
d) Widerruf	101
2. Probleme des konzerninternen Datenumgangs auf Grundlage einer Einwilligung	102
II. Erlaubnistatbestände nach § 28 BDSG	102
1. Datenerhebung, -verarbeitung und -nutzung im Rahmen von Verträgen gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG	103
2. Datenerhebung, -verarbeitung und -nutzung nach Interessen- abwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG	103
3. Datenerhebung, -verarbeitung und -nutzung von allgemein zugänglichen Daten gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG	105
4. Datenerhebung, -verarbeitung und -nutzung bei Zweckänderung gemäß § 28 Abs. 2 BDSG	106
5. Erhebung, -verarbeitung und -nutzung besonderer Arten personenbezogener Daten gemäß § 28 Abs. 6 bis 9 BDSG	107
6. Datenverarbeitung oder -nutzung zu Zwecken der Werbung und des Adresshandels gemäß § 28 Abs. 3 BDSG	107
a) Einwilligung	108
b) Das Listenprivileg gemäß § 28 Abs. 3 Satz 2 BDSG	108
III. Geschäftsmäßige Datenerhebung, -verarbeitung und -nutzung zum Zweck der Übermittlung gemäß § 29 BDSG	110
1. Abgrenzung zu den übrigen Erlaubnisnormen	111
2. Zulässigkeit der Erhebung, Speicherung, Veränderung und Nutzung	112
IV. Datenübermittlung an Auskunftfeien gemäß § 28 a BDSG	113
V. Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten gemäß § 32 BDSG	114
VI. Auftragsdatenverarbeitung	114
Kapitel 3. Auftragsdatenverarbeitung im Konzern	
A. Allgemeines zur Auftragsdatenverarbeitung	116
I. Besonderheiten der Auftragsdatenverarbeitung	116
1. Privilegierung der Auftragsdatenverarbeitung	117
2. Voraussetzung: Auftragsdatenverarbeitungsvereinbarung	118
3. Verhältnis der Auftragsdatenverarbeitung zu Berufsheim- nissen	119
II. Sachlicher Anwendungsbereich der Auftragsdatenverarbeitung/ Abgrenzung zur sog. „Funktionsübertragung“	120
III. Checkliste zur Abgrenzung Auftragsdatenverarbeitung/ Funktionsübertragung	122

	Seite
B. Einsatzmöglichkeiten der Auftragsdatenverarbeitung im Konzern	123
I. Call-Center	124
II. E-Mail-System	125
1. Anwendungsbereich des TKG	125
2. Auftragsdatenverarbeitung im Rahmen des TKG	126
III. Personaldatenverwaltung	127
IV. Adressverwaltung	129
V. Lohn- und Gehaltsabrechnung	129
VI. IT-Dienste	129
C. Gesetzliche Voraussetzungen der Auftragsdatenverarbeitung	130
I. Auftragsdatenverarbeitungsvertrag	130
II. Pflichten des Auftraggebers	133
III. Pflichten des Auftragnehmers	134
IV. Technische und organisatorische Maßnahmen	134
D. Auftragsdatenverarbeitung mit Auslandsbezug	137
I. Anwendbarkeit des BDSG	137
II. Auftragsdatenverarbeitung bei Nutzung ausländischer Auftragnehmer	137
1. Auftragnehmer in EU/EWR	138
2. Auftragnehmer im Drittland	138
III. USA PATRIOT Act	141
1. Grundsätzliche Zulässigkeit der Weitergabe	143
2. Zulässigkeit der Übermittlung in die USA	143
3. Das BDSG als Verbotsgesetz zur Verhinderung der Datenweitergabe	144
4. Handlungsempfehlungen	145

Kapitel 4. Verträge für den konzerninternen Datentransfer

A. Das Modell einer Vertragslösung für Konzern-Datentransfers	147
B. Ansatzpunkte für Datentransferverträge im Konzern	149
I. Zulässigkeit von Datentransfers auf 1. und 2. Stufe	149
II. Rechtsgrundlagen für die Übermittlungen personenbezogener Daten im Konzern	149
1. Einwilligung der Betroffenen	150
2. Gesetzliche Erlaubnisvorschriften	151
a) Datenübermittlungen im Rahmen von konzerndimensionalen Arbeitsverhältnissen	151
b) Datenübermittlungen im Rahmen von Funktionsübertragungen	153
c) Datenübermittlungen zu sonstigen Zwecken	154

	Seite
d) Datenübermittlungen zur Durchführung von Betriebsvereinbarungen	154
III. Zulassung einer Ausnahme vom angemessenen Datenschutzniveau nach § 4 c BDSG	155
C. Anforderungen an konzerninterne Verträge zum Datentransfer	157
I. Vorgaben für konzerninterne Datenübermittlungsverträge auf 1. Stufe	157
1. Orientierung am Maßstab für Auftragsdatenverarbeitungsverträge	157
2. Orientierung am Maßstab für Erlaubnisvorschriften in Betriebsvereinbarungen	161
3. Sonderregelungen nach dem Code of Conduct für die Versicherungswirtschaft	162
II. Vorgaben für Verträge über Datenübermittlungen ins Ausland (2. Stufe)	163
III. Beachtung der Wechselwirkungen zwischen Anforderungen der 1. und 2. Stufe	164
1. Ergänzung des Standardvertrages II bei der Verwendung von Beschäftigtendaten	164
2. Ergänzungen wegen Datenzugriffen ausländischer Behörden	165
3. Ergänzungen wegen sonstiger weitergehender Verpflichtungen auf 1. Stufe	165
4. Ergänzungen wegen Verpflichtungen aus Betriebsvereinbarungen	165
5. Sonstige Änderungen	166
D. Modelle zur Umsetzung: Rahmen- und Einzelverträge	167
I. Die Strukturierung des Vertrages	167
II. Umsetzung in Mehrparteien-Konstellationen	167
1. Einzelvertragslösung	167
2. Rahmenvertragslösung	168
III. Lösung über eine Garantieerklärung	169
E. Mögliche Auswirkungen der EU-Datenschutz-Grundverordnung	170
Kapitel 5. Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats	
A. Einleitung	172
B. Datenschutzrechtliche Rahmenbedingungen	173
I. Datenschutzrechtliche Zulässigkeit unternehmensübergreifender Datenverarbeitungen nach dem BDSG	174
1. Erforderlichkeit von Datenerhebungen, -verarbeitungen und -nutzungen nach § 32 Abs. 1 BDSG	174
2. Konzernweite Datenverarbeitung für eigene Geschäftszwecke auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG	177
3. Konzernweite Datenverarbeitung zur Wahrung berechtigter Interessen eines Dritten	179

	Seite
4. Unternehmensübergreifende Datenverarbeitung auf der Grundlage von Betriebsvereinbarungen	180
5. Konzernweite Erhebung, Verarbeitung oder Nutzung personenbezogener Daten auf der Grundlage einer Einwilligung gemäß § 4a BDSG	181
6. Allgemeine datenschutzrechtliche Vorgaben mit Relevanz zu konzernweiten Datenverarbeitungen	182
7. Auftragsdatenverarbeitung von Arbeitnehmerdaten im Konzernrahmen	183
II. Datenschutzrechtliche Vorgaben im TKG bzw. im TMG	184
1. Datenschutzvorgaben des TKG	184
2. TMG	186
C. Kollektivrechtlicher Rahmen für Konzerndatenverarbeitung – Mitwirkungs- und Mitbestimmungsrechte	186
I. Kollektivrechtliche Zuständigkeit	187
II. Mitwirkungs- und Mitbestimmungsrechte	188
III. Allgemeine Überwachungspflichten nach § 80 Abs. 1 Nr. 1 BetrVG ..	189
IV. Weitere Mitwirkungsrechte	191
VI. Mitbestimmungsrechte	193
1. § 87 Abs. 1 Nr. 6 BetrVG: Mitbestimmung bei der Einführung und Anwendung von technischen Einrichtungen	194
2. § 87 Abs. 1 Nr. 7 BetrVG: Mitbestimmung im Bereich des Arbeits- und Gesundheitsschutzes	196
a) Allgemeine Ausführungen	196
b) Auswirkungen des Mitbestimmungsrechts innerhalb eines Konzerns	197
3. § 87 Abs. 1 Nr. 1 BetrVG: Ordnung des Betriebes und Verhalten der Arbeitnehmer	197
a) Allgemeine Ausführungen	197
b) Umsetzung von verbindlichen Richtlinien zur konzernweiten Datenverarbeitung	198
D. Umsetzung in konzernweite Regelungen	199

Teil 4. Internationale Aspekte des deutschen Datenschutzrechts

Kapitel 1. Räumliche Anwendbarkeit des BDSG

A. Einleitung	202
B. Datenverarbeitung durch die verantwortliche Stelle selbst	204
I. Datenverarbeitung in Deutschland durch deutsche verantwortliche Stelle	204
II. Datenverarbeitung in Deutschland durch verantwortliche Stelle mit Sitz in der EU/dem EWR	204
1. Eigenständige Verarbeitung durch die verantwortliche Stelle	204
2. Verarbeitung durch eine Niederlassung in Deutschland	205

	Seite
III. Datenverarbeitung in Deutschland durch verantwortliche Stelle in Drittland	205
1. Eigenständige Verarbeitung durch die verantwortliche Stelle	206
2. Verarbeitung durch eine Niederlassung in Deutschland	206
3. Verarbeitung durch eine Niederlassung im EU-/EWR-Ausland	207
IV. Datenverarbeitung in der EU/dem EWR durch eine deutsche verantwortliche Stelle	207
1. Eigenständige Verarbeitung durch die verantwortliche Stelle	207
2. Verarbeitung durch eine Niederlassung im EU-/EWR-Ausland	208
V. Datenverarbeitung in einem Drittland durch eine deutsche verantwortliche Stelle	208
1. Eigenständige Verarbeitung durch die verantwortliche Stelle	208
2. Verarbeitung durch eine selbstständige Niederlassung im Drittland	209
3. Verarbeitung durch eine unselbstständige Niederlassung im Drittland	209
C. Verarbeitung durch einen Auftragsdatenverarbeiter	211
I. Auftraggeber in Deutschland	211
1. Auftragnehmer in Deutschland	212
2. Auftragnehmer im Ausland	212
II. Auftraggeber in der EU/dem EWR und Auftragnehmer in Deutschland	212
III. Auftraggeber im Drittland und Auftragnehmer in Deutschland	213
Kapitel 2. Datenübermittlungen in Drittländer	
A. Einleitung	215
B. Anforderungen an die Datenübermittlung in Drittländer	216
I. Die Übermittlung personenbezogener Daten ins Ausland nach § 4 b BDSG	216
1. Besondere Anforderungen an die Drittlandübermittlung	217
a) Angemessenes Schutzniveau	217
b) Pflichten und Verantwortung der übermittelnden Stelle	218
2. Sonderfall: Der Datentransfer in die USA – Safe Harbor- Principles	219
II. Die Ausnahmen nach § 4 c BDSG	219
1. Die gesetzlichen Ausnahmen nach § 4 c Abs. 1 BDSG	220
2. Einzelfallbezogene behördliche Ausnahmegenehmigungen nach § 4 c Abs. 2 BDSG	221
Kapitel 3. Standardvertragsklauseln	
A. Allgemeine Grundlagen	225
I. Vertragsparteien	227
II. Unterschiedliche Varianten der Standardvertragsklauseln	228
B. Standardvertragsklauseln Set I und Set II	228

	Seite
C. Standardvertragsklauseln zur Auftragsdatenverarbeitung	231
I. Abgrenzung zu den Standardvertragsklauseln aus dem Jahr 2001	231
II. Zulässigkeit der Auftragsdatenverarbeitung im Drittland	232
III. Notwendige Ergänzungen der Standardvertragsklauseln gemäß § 11 Abs. 2 BDSG	233
IV. Räumlicher Anwendungsbereich der Standardvertragsklauseln zur Auftragsdatenverarbeitung	233

Kapitel 4. Safe Harbor Principles

A. Einleitung	235
B. Verpflichtung auf die Safe Harbor-Grundsätze	236
I. Anwendungsbereich	236
II. Befugnisse der FTC und des DoT	237
III. Safe Harbor-Grundsätze	237
1. Grundsatz der „Wahlmöglichkeit“	237
2. Grundsatz der „Weitergabe“	238
3. Grundsatz der „Informationspflicht“ und des „Auskunftsrechts“	239
4. Grundsatz der „Datenintegrität“ und der „Sicherheit“	240
5. Grundsatz der „Durchsetzung“	240
a) Schlichtungsverfahren	240
b) Anlassunabhängige Prüfung und Kontrolle	240
c) Abhilfe und Sanktionen	240
IV. Safe Harbor-FAQ	241
V. Beitritt zu den Safe Harbor-Grundsätzen	242
1. Mitteilung gegenüber dem DoC	242
2. Safe Harbor-Liste	243
C. Datenübermittlung an ein Safe Harbor-Unternehmen	244
I. Allgemeines	244
II. Datenübermittlung als Auftragsdatenverarbeitung	244
III. Übermittlung von Personaldaten	245
D. Safe Harbor aus Sicht der Aufsichtsbehörde	245
I. Kritische Sicht auf Safe Harbor	245
II. Anforderung an eine Mindestprüfung nach dem Safe Harbor-Beschluss des Düsseldorfer Kreises	246
III. Aussetzungsbefugnis der Datenschutzbehörden	247

Kapitel 5. Binding Corporate Rules

A. Einleitung	251
B. Rechtliche Aspekte des Drittstaatenverkehrs	253
C. Vorüberlegungen	255
I. Einsatzszenarien für BCR	255
II. BCR als ausreichende Garantien	256

	Seite
D. Verbindlichkeit der BCR	257
I. Unterscheidung zwischen interner und externer Verbindlichkeit	258
II. Mechanismen zur Herstellung von Verbindlichkeit	258
1. Vertragliche Lösungen	259
2. Konzernrichtlinie bzw. konzerninterne Weisung	260
3. Einseitige Erklärung („Unilateral Declaration“)	260
III. Herstellung der Verbindlichkeit gegenüber den Mitarbeitern	261
IV. Rechtliche Durchsetzbarkeit	262
E. Bestandteile verbindlicher Unternehmensregelungen	263
I. Sprache	263
II. Festlegung des Anwendungsbereichs	263
III. Beschreibung der Datenflüsse	264
1. Detaillierungsgrad der Beschreibungen	264
2. Prüfungsgrundlage für Aufsichtsbehörden	265
IV. Definitionen	265
1. EG-Datenschutzrichtlinie als Vorlage für die Definitionen	265
2. Definition des Datenexporteurs und Datenimporteurs	265
V. Datenschutzgarantien	266
1. Begrenzung der Zwecke und Zweckbestimmung	267
2. Datenqualität und -aktualität	267
3. Erforderlichkeit	268
4. Rechtsgrundlage für die Datenverarbeitung	268
5. Transparenz, Fairness, Unterrichtung und Benachrichtigung	269
6. Betroffenenrechte	269
7. Datensicherheit	270
8. Beschränkung der Weiterübermittlung	270
VI. Auftragsdatenverarbeitung innerhalb der Unternehmensgruppe	270
VII. Auftragsdatenverarbeitung außerhalb des Konzerns und Weiterübermittlungen („onward transfers“)	271
1. Auftragsdatenverarbeitung außerhalb der Gruppe aber innerhalb der EU/des EWR	271
2. Auftragsdatenverarbeitung außerhalb der Gruppe im Drittstaat ...	271
3. Weiterübermittlungen („onward transfers“)	272
VIII. Konflikte mit dem nationalen Recht	273
IX. Sicherstellung der Befolgung	273
1. Schaffung eines Mitarbeiterstabs	274
2. Verfahren zur Gewährleistung von Betroffenenrechten	275
3. Schulungen der Beschäftigten	275
4. Durchführung von Audits	275
5. Beschwerdeverfahren	277
6. Kooperation mit den Datenschutzbehörden	278
X. Drittbegünstigung	279
XI. Haftung	280

	Seite
XII. Gerichtsstand	281
XIII. Aktualisierungen und Änderungen	281
XIV. Übergangsfrist	281
F. Verfahren zur Anerkennung der BCR als „ausreichende Garantien“	282
I. Mutual Recognition-Verfahren (MR-Verfahren)	282
1. Vorarbeiten und erforderliche Unterlagen	283
2. Antragsteller	284
3. Identifizierung der federführenden Behörde (Lead Authority)	285
4. Weiteres Verfahren	285
5. Nationale Anforderungen für die Autorisierung	286
6. Bisher abgeschlossene Verfahren	286
II. Autorisierungen in Deutschland	286
G. BCR für Auftragsverarbeiter	287
Teil 5. Spannungsfeld zwischen Datenschutz und Compliance-Anforderungen	
Kapitel 1. Datenschutzrecht und Compliance	
A. Einleitung	290
B. Begriff und Bedeutung von Compliance	290
C. Rechtlicher Hintergrund der Compliance	291
I. Gesetzliche Verpflichtung zur Einrichtung von Compliance-Systemen	291
II. Sonstige Gründe zur Einrichtung von Compliance-Maßnahmen	293
1. Vertragliche Verpflichtungen	293
2. Freiwillig auferlegte Verpflichtungen	294
3. Prüfungsstandards	294
D. Datenschutzrechtliche Ausgestaltung von Compliance-Maßnahmen	295
I. Datenschutzrechtliche Voraussetzungen	295
1. Einwilligung als Erlaubnistatbestand	296
2. Gesetzliche Grundlagen	296
a) Rechtsgrundlage für repressive Maßnahmen	296
b) Präventive Maßnahmen	297
c) Zwischenresümee	298
3. Allgemeine datenschutzrechtliche Anforderungen	298
a) Benachrichtigungspflichten	298
b) Löschpflichten	300
c) Dokumentationspflichten	301
II. Pre-Employment-Screening	301
1. Überprüfung der fachlichen Qualifikationen	303
2. Überprüfung der kriminellen Vergangenheit	303
3. Überprüfung der finanziellen Situation	304
E. Kooperation bei Anfragen der öffentlichen Verwaltung	306
I. Auskunftsverlangen der Finanzbehörden	306

	Seite
II. Auskunftsverlangen der Strafermittlungsbehörden	307
1. Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit (§ 28 Abs. 2 Nr. 2 lit. b BDSG)	307
2. Zur Wahrung berechtigter Interessen der verantwortlichen Stelle (§ 28 Abs. 2 Nr. 1 iVm Abs. 1 Nr 2 BDSG)	309
Kapitel 2. E-Discovery	
A. Einführung und Begriff	311
B. Herausgabeansprüche durch die andere Partei	313
I. Schritt 1: Identifizierung der „Custodians“	313
II. Schritt 2: Sicherung und Sichtung der Dokumente	314
III. Schritt 3: Sortierung der Dokumente	314
IV. Schritt 4: Vorlegung der Dokumente	315
C. Mögliche Strategien der Konzernunternehmen zur Vermeidung der Herausgabe	315
D. Datenschutzrechtliche Implikationen	318
Teil 6. Datenschutz bei M&A-Transaktionen	
A. Einleitung	324
B. Kategorisierung von Unternehmenstransaktionen	324
C. Datenschutzrechtliche Anforderungen an Due Diligence-Prüfungen	325
I. Gegenstand und Ablauf der Due Diligence-Prüfung	325
II. Rechtsgrundlage für die Offenlegung von Daten im Rahmen der Due Diligence-Prüfung	326
1. Rechtsgrundlage für die Offenlegung beim Asset Deal	326
a) Anwendbarkeit des BDSG	326
b) Einwilligung	327
c) Betriebsvereinbarung	327
d) Gesetzliche Erlaubnisnorm	327
2. Rechtsgrundlage für die Offenlegung beim Share Deal	329
3. Rechtsgrundlage für die Offenlegung bei der Umwandlung	330
4. Rechtsgrundlage für die Offenlegung anonymisierter und pseudo- nymisierter Daten im Rahmen von Unternehmenstransaktionen ...	331
III. Typische Fallkonstellationen bei der Offenlegung von Daten im Rahmen der Due Diligence-Prüfung	332
1. Mitarbeiterdaten	332
2. Kundendaten	333
3. Personenbezogene Daten in Vertragsdokumenten	334
4. Einschaltung von Service-Providern	335
5. Datentransfer in Drittstaaten außerhalb der EU	335
6. Benachrichtigungspflichten	336
7. Vertraulichkeitsvereinbarungen	337

	Seite
D. Datenschutzrechtliche Anforderungen an den Vollzug von Unternehmens- transaktionen	338
I. Datenschutzrechtliche Anforderungen an den Vollzug von Share Deals	339
II. Datenschutzrechtliche Anforderungen an den Vollzug von Asset Deals	339
III. Datenschutzrechtliche Anforderungen an den Vollzug von Transaktionen nach dem UmwG	341
IV. Datenschutzrechtliche Anforderungen an den Vollzug von Transaktionen über den Erwerb von Arztpraxen und Kanzleien	343
Teil 7. Cloud Computing	
A. Vor- und Nachteile des Cloud Computing	346
I. Relevanz des Themas für Konzerne	346
II. Risiken von Cloud Computing	348
B. Formen von Cloud-Diensten (Übersicht)	349
I. Bereitstellungsmodelle (Deployment Models)	349
II. Dienstleistungsmodelle (Service-Models)	349
C. Allgemeine datenschutzrechtliche Konfliktbereiche des Cloud Computing	350
D. EU-datenschutzrechtliche Grundlagen des Cloud Computing	352
I. Rechtsgrundlagen	352
II. Stellungnahme 05/2012 der Art.-29-Datenschutzgruppe	353
1. Anwendbarkeit des EU-Rechts	353
2. Cloud-Anwender und Cloud-Anbieter	353
3. Sicherheitsmaßnahmen und Organisation	354
4. Audits/Zertifizierungen durch unabhängige Dritte	354
5. Datenweitergabe aus der EU/dem EWR heraus	354
6. Cloud-Dienste und außereuropäische Sicherheitsbehörden	355
7. Ausgestaltung des Vertrags zwischen Anbieter und Anwender	355
III. Strategiepapier der EU-Kommission zum Cloud Computing	356
E. Stellungnahmen und Vorschläge einiger nationaler Datenschutzbehörden/ -gremien	357
I. Dänemark	357
II. Deutschland	358
1. Cloud-Anbieter und Cloud-Anwender, Sondergesetze	359
2. Pflichten innerhalb des Cloud-Auftragsverhältnisses	359
3. Ausgestaltung des Cloud Computing-Vertrages	360
4. Technische und organisatorische Sicherheitsmaßnahmen	361
5. Verschlüsselung von Daten	361
6. Cloud Computing und unsichere Drittländer	362
III. Frankreich	363

	Seite
IV. Großbritannien	364
V. Vereinigte Staaten	365
F. Ratschläge für Cloud-Nutzer zur Ausgestaltung des Cloud Computing	366
Teil 8. Ausblick auf die EU-Datenschutz-Grundverordnung	
A. Auf dem Weg zu einer EU-Datenschutz-Grundverordnung	374
B. Der Entwurf der EU-Datenschutz-Grundverordnung im Überblick	377
I. Anwendungsbereich	377
II. Einwilligung	378
III. Erlaubnistatbestände	379
IV. Profilbildung	381
V. Verhaltensregeln und Zertifizierung	381
VI. Recht auf Vergessenwerden	383
VII. Recht auf Datenübertragbarkeit	383
VIII. Delegierte Rechtsakte	384
IX. Sanktionen	385
C. Regelungen zum Konzerndatenschutz	386
I. One-Stop-Shop und Kohärenzverfahren	386
II. Übermittlung personenbezogener Daten in Drittländer	389
1. Übersicht	390
2. Binding Corporate Rules	391
a) Verfahren	391
b) Inhaltliche Anforderungen	392
3. Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses	392
4. Standarddatenschutzklauseln	393
5. Übermittlung oder Weitergabe, die nicht im Einklang mit dem Unionsrecht stehen	393
III. Auftragsdatenverarbeitung	394
1. Rechtliche Ausgestaltung	395
2. Auswirkungen in der Praxis	398
IV. Datenschutzbeauftragter	399
1. Der Datenschutzbeauftragte im europäischen Kontext	399
2. Die Regelungen zum Datenschutzbeauftragten im Überblick	400
a) Benennung eines Datenschutzbeauftragten	400
b) Stellung des Datenschutzbeauftragten	402
c) Aufgaben des Datenschutzbeauftragten	402
3. Auswirkungen auf die Praxis	402
Sachverzeichnis	405