

Konzerndatenschutz

Rechtshandbuch

Bearbeitet von

Herausgegeben von Axel Bussche, LL.M. (L.S.E.), und Paul Voigt, Lic. en Derecho, Bearbeitet von den
Herausgebern und von Karsten U. Bartels, LL.M., Monika Egle, Nils Hullen, LL.M., Meike Kamp, LL.M., Dr.
Moritz Karg, Dr. Olaf Koglin, Hannes Oenning, Jana Oenning, Dr. Kai-Uwe Plath, LL.M. (N.Y.), Dr. Axel
Spies, C.E.P. (Paris), Prof. Dr. Peter Wedde, und Andreas Zeller

2. Auflage 2019. Buch. XLVI, 510 S. Hardcover (In Leinen)

ISBN 978 3 406 72008 6

Format (B x L): 16,0 x 24,0 cm

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

*Dr. Jens Ambrock, Hamburg; Monika Egle, Ulm;
Dr. Nils Hullen, LL. M., Berlin; Meike Kamp, LL. M., Berlin; Dr. Moritz Karg, Kiel;
Dr. Olaf Koglin, Berlin; 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*

2019



Zitiervorschlag: von dem Bussche/Voigt/Bearbeiter



www.beck.de

ISBN 978 3 406 72008 6

© 2019 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München

Druck: Beltz Grafische Betriebe GmbH, Am Fliegerhorst 8, 99947 Bad Langensalza
Satz und Umschlaggestaltung: Druckerei C.H. Beck Nördlingen

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort zur 2. Auflage

Seit dem 25. Mai 2018 gilt in allen Mitgliedsstaaten der Europäischen Union die Datenschutz-Grundverordnung (DSGVO). Da diese zur Sanktionierung datenschutzrechtlicher Verstöße außerordentlich hohe Geldbußen in Höhe von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs einer Unternehmensgruppe vorsieht, haben die innerhalb von Konzernen auftretenden datenschutzrechtlichen Besonderheiten in der Beratungspraxis noch einmal an Relevanz gewonnen.

Ein Kernproblem des „alten“ Datenschutzrechts besteht fort: Zwar erkennt der Unionsgesetzgeber an, dass innerhalb von Unternehmensgruppen ein gesteigertes Bedürfnis nach Datenübermittlungen für interne Verwaltungszwecke besteht; ein Konzernprivileg im eigentlichen Sinne sieht die DSGVO jedoch nicht vor. Aus diesem Grund werden Datenübermittlungen innerhalb von Konzernstrukturen – obwohl Konzerne strukturell häufig wie Einzelunternehmen organisiert sind – regelmäßig genauso restriktiv behandelt wie die Datenübermittlung zwischen unabhängigen Unternehmen. Auch aus organisatorischer Sicht sind in Konzernen komplexe datenschutzrechtliche Probleme zu bewältigen: So werden häufig spezielle Konzern-datenschutzbeauftragte bestellt, welche die Datenschutzanforderungen unternehmensübergreifend koordinieren. Auch die DSGVO-konforme Ausgestaltung der in internationalen Konzernstrukturen häufig vorkommenden Datenübermittlungen in Länder, die nicht Mitglied der Europäischen Union sind (sog. Drittländer), stellt Unternehmen vor besondere Herausforderungen.

Dieses Handbuch soll Unternehmen mit Konzernstrukturen und deren Beratern praxisorientierte, fundierte und verständliche Hinweise und Hilfestellungen zur Bewältigung der datenschutzrechtlichen Problemstellungen geben. Der Schwerpunkt liegt dabei auf den konzerndatenschutzrechtlichen Besonderheiten; aber auch „allgemeine“ datenschutzrechtliche Themen mit besonderer Relevanz für Konzerne werden erläutert.

Dem Handbuch ist eine „Checkliste“ der wichtigsten datenschutzrechtlichen Pflichten vorangestellt. Diese Checkliste zeigt in Kurzform auf, welche Datenschutzthemen in Konzernen in jedem Fall beachtet werden sollten. Die Checkliste verweist dann in die entsprechenden Kapitel des Handbuchs, in denen sich praxisnahe Lösungen für die aufgeworfenen Problemstellungen finden.

Die Autoren dieses Handbuches sind ausschließlich Praktiker, die im Rahmen ihrer Tätigkeiten als Berater von Unternehmen, als Beschäftigtenvertreter oder im Rahmen der behördlichen Datenschutzaufsicht langjährige Erfahrung im Konzern-datenschutz gesammelt haben. Sie lassen den Leser in ihren Beiträgen in erheblichem Maße an ihrem Praxis-Know-how teilhaben, wofür wir ihnen an dieser Stelle – ebenso wie für die verlässliche und vertrauensvolle Zusammenarbeit – ganz herzlich danken möchten.

Unser Dank geht auch an die wissenschaftlichen Mitarbeiter, die uns bei der Vorbereitung der Beitragserstellung und bei den organisatorischen Herausgebertätigkeiten unterstützt haben. Ebenso möchten wir uns bei Frau Boettcher für die effiziente,

freundliche und sehr hilfreiche Unterstützung von Seiten des Verlags C. H. Beck bedanken.

Über Anregungen und Kritik freuen wir uns jederzeit.

Berlin, April 2019

*Axel von dem Bussche
Paul Voigt*


beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsübersicht

	Seite
Vorwort	V
Inhaltsverzeichnis	IX
Bearbeiterverzeichnis	XXXI
Abkürzungsverzeichnis.....	XXXIII
Allgemeines Literaturverzeichnis	XLIII
 Teil 1. Einführung und „Checkliste“	 1
 Teil 2. Datenschutzorganisation im Konzern	
Kapitel 1. Der Datenschutzbeauftragte	9
Kapitel 2. Datenschutzmanagementsystem im Konzern	44
Kapitel 3. Rechenschaftspflicht	67
Kapitel 4. Verzeichnis von Verarbeitungstätigkeiten im Konzern	74
Kapitel 5. Datenschutz-Folgenabschätzung	91
Kapitel 6. Informations- und Einwirkungsrechte der Betroffenen	114
Kapitel 7. Informationspflichten bei Datenschutzverletzungen ..	150
Kapitel 8. Verhaltensregeln und Zertifizierung	156
 Teil 3. Datenverarbeitung im Konzern	
Kapitel 1. Einleitung: Fehlendes Konzernprivileg	169
Kapitel 2. Grundsätze der Verarbeitung nach der DSGVO	172
Kapitel 3. Rechtliche Anforderungen an Datenverarbeitungen ..	178
Kapitel 4. Auftragsverarbeitung im Konzern	195
Kapitel 5. Verträge für den konzerninternen Datentransfer	216
Kapitel 6. Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats	228
 Teil 4. Internationale Aspekte des deutschen Datenschutzrechts	
Kapitel 1. Räumliche Anwendbarkeit der DSGVO und des BDSG	267
Kapitel 2. Datenübermittlungen in Drittländer	275
Kapitel 3. Standardvertragsklauseln	285
Kapitel 4. Privacy Shield Principles	298
Kapitel 5. Verbindliche interne Datenschutzvorschriften	323
Kapitel 6. Der Nachweis geeigneter Garantien durch Verhaltens- regeln und Zertifizierung	371
 Teil 5. Spannungsfeld zwischen Datenschutz und Compliance-Anforderungen	
Kapitel 1. Datenschutzrecht und Compliance	373
Kapitel 2. E-Discovery	394
Kapitel 3. Technischer Datenschutz	407

	Seite
Teil 6. Datenschutz bei M&A-Transaktionen	423
Teil 7. Cloud Computing	445
Teil 8. Aufsichtsbehördlicher Vollzug und Sanktionen	465
Sachverzeichnis	503

Inhaltsverzeichnis

	Seite
Vorwort	V
Inhaltsübersicht	VII
Bearbeiterverzeichnis	XXXI
Abkürzungsverzeichnis	XXXIII
Allgemeines Literaturverzeichnis	XLIII

Teil 1. Einführung und „Checkliste“

A. Datenschutzorganisation	2
I. Bestellung von (Konzern-)Datenschutzbeauftragten	2
II. Verzeichnis von Verarbeitungstätigkeiten	2
III. Datenschutzfolgenabschätzung	3
IV. Technische und organisatorische Maßnahmen	3
V. Informationspflichten bei Datenerhebung	3
VI. Betroffenenrechte	3
VII. Informationspflichten bei Datenschutzverletzungen	3
B. Rechtmäßigkeit der Datenverarbeitung	4
I. Accountability (Rechenschaftspflicht)	4
II. Übermittlung zwischen Konzerngesellschaften	4
III. Auftragsverarbeitungen	4
IV. Verträge für den konzerninternen Datentransfer	5
V. (Konzern-)Betriebsvereinbarungen	5
VI. Allgemeine Anforderungen an die Datenverarbeitung	5
VII. Internationale Datenschutzthemen	5
VIII. Standardvertragsklauseln	5
IX. Privacy Shield Principles	6
X. Binding Corporate Rules	6
XI. Verhaltensregeln und Zertifizierungen	6
C. Wichtige Spezialthemen	6
I. Datenschutzrecht versus Compliance	6
II. E-Discovery	7
III. Datenschutz bei Transaktionen	7
IV. Cloud Computing	7
V. Aufsichtsbehördlicher Vollzug und Sanktionen	7

Teil 2. Datenschutzorganisation im Konzern	Seite
Kapitel 1. Der Datenschutzbeauftragte	
A. Grundlegende Funktion des Datenschutzbeauftragten	10
B. Benennungspflicht	11
I. Grundsatz der Benennungspflicht	11
1. Vorgaben des BDSG	11
2. Zusätzliche Vorgaben der DSGVO	13
a) Überwachung von Personen	13
b) Verarbeitung sensibler Daten	15
c) Verhältnis der BDSG- und DSGVO-Benennungspflichten zueinander	16
II. Die zur Benennung verpflichtete Stelle, Konzerndatenschutzbeauftragter	17
C. Die Person des Datenschutzbeauftragten	18
I. Interner vs. externer Datenschutzbeauftragter	18
II. Fachliche und persönliche Anforderungen	19
1. Berufliche Qualifikationen	19
2. Fachkunde	20
3. Fähigkeiten zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben	22
D. Ordnungsgemäße Benennung des Datenschutzbeauftragten; vertragliches Verhältnis zwischen Datenschutzbeauftragten und Verpflichtetem	23
I. Ordnungsgemäße Benennung als Datenschutzbeauftragter	23
II. Vertragsverhältnis, gegebenenfalls erforderliche Abänderung	24
III. Organisation innerhalb von Konzernstrukturen	25
E. Stellung des Datenschutzbeauftragten	26
I. Frühzeitige Einbindung des Datenschutzbeauftragten	26
II. Unterstützungspflicht des Arbeitgebers	26
III. Unabhängigkeit und Weisungsfreiheit des Datenschutzbeauftragten...	27
IV. Benachteiligungsverbot und Abberufungsschutz	28
V. Berichtsrecht des Datenschutzbeauftragten	28
VI. Zugang Betroffener zum Datenschutzbeauftragten	28
VII. Geheimhaltungspflicht	28
VIII. Schutz vor Interessenkonflikten	29
IX. Verhältnis zwischen Datenschutzbeauftragtem und Mitarbeitervertretungen	29
F. Aufgaben des Datenschutzbeauftragten	30
I. Beratungs- und Überwachungspflicht	30
II. Anlaufstelle für Betroffene; Verschwiegenheitspflicht	32
III. Beratung- und Überwachung der Datenschutz-Folgenabschätzung	33

	Seite
IV. Zusammenarbeit mit der Aufsichtsbehörde	33
V. Schulungs- und Fortbildungsfunktion	34
VI. Sonstige Pflichten des Datenschutzbeauftragten	35
VII. Rechtsfolgen bei Verstößen	35
G. Abberufung, Kündigung, sonstige Beendigung	36
I. Abberufung und Abberufungsschutz	36
1. Abberufung auf Verlangen der Aufsichtsbehörde	36
2. Abberufung durch den Verantwortlichen oder Auftragsverarbeiter	36
II. Kündigung des zugrundeliegenden Vertragsverhältnisses	37
III. Verhältnis zwischen Widerruf und Kündigung	38
1. Interner Datenschutzbeauftragter	38
2. Externer Datenschutzbeauftragter	38
IV. Fortbestand bzw. Wegfall des Amts bei gesellschaftsrechtlichen Umstrukturierungen	39
V. Sonstige Beendigungstatbestände	41
H. Haftung des Datenschutzbeauftragten	41
I. Ansprüche des Verantwortlichen	42
II. Ansprüche der Betroffenen	42
Kapitel 2. Datenschutzmanagementsystem im Konzern	
A. Einleitung	45
B. Datenschutzmanagementsystem in Konzernstrukturen	46
I. Grundsätzliche Ziele	46
1. Erfüllung rechtlicher Vorgaben	47
2. Verlässliches Datenschutzrisikomanagement durch Integration des Datenschutzes in das interne Kontrollsystem	47
3. Konzernübergreifendes und effizientes Datenschutzmanagement- system	48
II. Methodik	48
III. Struktur	50
1. Leitlinie	51
2. Managementprozesse	51
3. Zielgruppenorientierte Richtlinie	54
4. Konkrete Hilfestellung und Werkzeuge	54
IV. Datenschutzorganisation	54
1. Konzernleitung	54
2. Konzerndatenschutzbeauftragter	55
3. Leitung der Einzelgesellschaft	55
4. Lokaler Datenschutzbeauftragter einer Einzelgesellschaft	55
5. Datenschutzkoordinatoren	56
6. Geschäftsprozessverantwortliche	56
7. Entscheider/Führungskräfte	57
8. Benutzer	57

	Seite
V. Einbettung der Datenschutzorganisation in Konzernstrukturen	57
1. Zentrale Struktur	57
2. Dezentrale Struktur	58
C. Vorgehensweise beim Aufbau eines konzernweiten Datenschutzmanagementsystems	60
I. Modell zur Konzeption	60
II. Modell zur Einführung	61
1. Analyse	62
2. Konzeption	64
3. Einführung	65
4. Betrieb	66

Kapitel 3. Rechenschaftspflicht

A. Einleitung	67
B. Inhalt der Rechenschaftspflicht	67
I. Verantwortlichkeit	68
II. Nachweispflicht	69
C. Rechtsfolgen	70
D. Tabellarische Übersicht wichtiger Nachweispflichten	70

Kapitel 4. Verzeichnis von Verarbeitungstätigkeiten im Konzern

A. Einleitung	74
B. Das Verzeichnis von Verarbeitungstätigkeiten	75
I. Verpflichtung zur Erstellung und Form	75
II. Inhalt des Verzeichnisses von Verarbeitungstätigkeiten	76
1. Adressatenkreis: Verantwortliche und ggf. deren Vertreter (Art. 30 Abs. 1 Satz 2 DSGVO)	76
2. Adressatenkreis: Auftragsverarbeiter und ggf. deren Vertreter (Art. 30 Abs. 2 DSGVO)	78
C. Struktur und Bedeutung eines konzernweiten Verzeichnisses von Verarbeitungstätigkeiten	80
D. Aufbau und Betrieb eines konzernweiten Verzeichnisses von Verarbeitungstätigkeiten	83
I. Analyse	83
II. Konzeption	83
III. Einführung	86
1. Stufe: Erstellung der Übersicht der Verarbeitungstätigkeiten	86
2. Stufe: Erstellung der Beschreibungen der Verarbeitungstätigkeiten	87
a) Variante 1: Erstellung der Beschreibungen der Verarbeitungstätigkeiten durch die jeweiligen Benutzer/Entscheider	88

Inhaltsverzeichnis	XIII
--------------------	------

	Seite
b) Variante 2: Erstellung der Beschreibungen der Verarbeitungstätigkeiten durch einen Beauftragten	89
IV. Betrieb	89

Kapitel 5. Datenschutz-Folgenabschätzung nebst vorheriger Konsultation

A. Einleitung	94
B. Voraussetzungen für die Durchführung	95
I. Formale Voraussetzungen	95
1. Fälle ohne Wertungsmöglichkeit	95
2. Kategorien des Art. 35 Abs. 3 lit. a–c DSGVO	96
3. Generalklausel des Art. 35 Abs. 1 DSGVO („hohes Risiko“)	98
II. Positivlisten der Aufsichtsbehörden	98
1. Positivliste der BfDI und WP 248: „Zwei aus Neun“	99
2. Positivlisten der Landesbehörden: Merkmalslisten	101
III. Pragmatischer Ansatz im Konzern	103
1. Abkürzung der Vorprüfung durch freiwillige Durchführung	104
2. Vereinfachter Bewertungskatalog	104
3. Einzelfragen	105
4. Umgang mit Bestandssystemen und erneute Folgenabschätzung ...	106
C. Inhalt der Datenschutz-Folgenabschätzung	107
I. Vorbereitungsphase (Art. 35 Abs. 7 lit. a DSGVO)	107
II. Bewertungsphase (Art. 35 Abs. 7 lit. b und c DSGVO)	108
III. Maßnahmenphase (Art. 35 Abs. 7 lit. d DSGVO)	108
IV. Durchführung, Dokumentation und Checklisten	109
D. Prozesse und Zuständigkeiten der Datenschutz-Folgenabschätzung	110
I. Zuständigkeiten und Delegation an den Datenschutzbeauftragten	111
II. Einbindung Dritter, insb. vorherige Konsultation	112
III. Inhalt und Ausrichtung der internen Prozesse	112
E. Bußgelder	113

Kapitel 6. Informations- und Einwirkungsrechte der Betroffenen

A. Einleitung	116
B. Adressat der Pflichten	116
C. Verfahrens- und Transparenzregelungen, Art. 12 DSGVO	117
I. Berechtigter	117
II. Transparenz	117
III. Form	117
IV. Zeitpunkt der Informationspflicht	118

	Seite
V. Unentgeltlichkeit	118
VI. Rechtsfolge	118
D. Informationspflichten gegenüber dem Betroffenen	119
I. Bei Direkterhebung (Art. 13 DSGVO)	119
1. Informationspflichten bei Erhebung nach Art. 13 Abs. 1 DSGVO ...	119
2. Informationspflichten bei Erhebung nach Art. 13 Abs. 2 DSGVO ...	120
3. Zeitpunkt der Information nach Art. 13 Abs. 1 und 2 DSGVO	123
4. Informationspflichten bei Zweckänderung nach Art. 13 Abs. 3 DSGVO	123
5. Ausnahme von der Informationspflicht bei Kenntnis, Art. 13 Abs. 4 DSGVO	123
6. Ausnahme von der Informationspflicht nach § 32 BDSG	124
II. Bei Erhebung bei Dritten (Art. 14 DSGVO)	125
1. Informationspflichten der Art. 14 Abs. 1 und 2 DSGVO	125
2. Ausnahmen von der Informationspflicht nach §§ 29 und 33 BDSG	126
E. Auskunftsrechte des Betroffenen (Art. 15 DSGVO)	126
I. Inhalt der Auskunftspflicht	127
II. Form und Frist der Auskunftserteilung	128
III. Ausnahmen von der Auskunftspflicht	129
1. Ausnahmen von der Auskunftspflicht nach §§ 27, 28, 29 und 34 BDSG	129
2. Ausnahmen von der Pflicht zur Herausgabe einer Kopie nach Art. 15 Abs. 4 DSGVO	130
F. Weitere Rechte des Betroffenen	130
I. Recht auf Berichtigung und Vervollständigung, Art. 16 DSGVO	131
1. Berichtigung unrichtiger personenbezogener Daten, Art. 16 Satz 1 DSGVO	131
2. Vervollständigung unvollständiger personenbezogener Daten, Art. 16 Satz 2 DSGVO	131
II. Anspruch auf Löschung und „Recht auf Vergessenwerden“, Art. 17 DSGVO	132
1. Anspruch und Pflicht zur Löschung, Art. 17 Abs. 1 DSGVO	132
2. Informationspflicht des Verantwortlichen, Art. 17 Abs. 2 DSGVO	133
3. Ausnahmen von der Löschpflicht nach Art. 17 Abs. 3 DSGVO	134
4. Ausnahmen von der Löschpflicht nach § 35 BDSG	136
III. Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO	137
1. Inhalt des Anspruchs	137
2. Verarbeitung trotz Einschränkung	138
3. Die Aufhebung der Einschränkung nach Art. 18 Abs. 3 DSGVO ...	138
4. Ausnahmen des Anspruchs auf Einschränkung nach § 28 Abs. 3 BDSG	138

	Seite
IV. Recht auf Datenübertragbarkeit, Art. 20 DSGVO	138
1. Verpflichteter und Ausübung	138
2. Anspruch aus Art. 20 Abs. 1 DSGVO	139
a) Durch den Antragsteller bereitgestellte personenbezogene Daten	139
b) Einwilligung oder Vertrag als Grundlage	139
c) Verarbeitung mittels automatisierter Verfahren	139
d) Inhalt des Anspruchs	140
3. Übermittlung der Daten	140
4. Beschränkung der Ansprüche durch Art. 20 Abs. 3 und 4 DSGVO und § 28 Abs. 4 BDSG	140
5. Beschäftigungskontext	141
6. Verhältnis zum Recht auf Löschung, Art. 17 DSGVO	141
V. Widerspruchsrecht des Betroffenen, Art. 21 DSGVO	142
1. Form des Widerspruchsrechts aus Art. 21 DSGVO	142
2. Gründe für einen Widerspruch gegen die Verarbeitung	142
a) Besondere Situation der betroffenen Person	142
b) Widerspruchsrecht aus Art. 21 Abs. 2 und 3 DSGVO bei Direktwerbung	143
c) Verarbeitung zu Forschungszwecken oder zu statistischen Zwecken	143
d) Rechtsfolge	144
3. Hinweispflicht auf das Bestehen des Widerspruchsrechts, Art. 21 Abs. 4 DSGVO	144
4. Widerspruch mittels automatisierter Verfahren bei Nutzung von Diensten der Informationsgesellschaft, Art. 21 Abs. 5 DSGVO	144
5. Ausnahmen nach den §§ 27, 28, 36 BDSG	144
VI. Automatisierte Entscheidungen, Art. 22 DSGVO	145
1. Art. 22 Abs. 1 DSGVO	145
2. Erlaubte automatisierte Entscheidungen nach Art. 22 Abs. 2 DSGVO	146
3. Pflichten des Verantwortlichen bei einer automatischen Entscheidung nach Art. 22 Abs. 2 DSGVO	146
4. Besondere Kategorien von Daten, Art. 22 Abs. 4 DSGVO	147
5. Sonderregelungen bei Scoring und Bonitätsauskünften, § 31 BDSG	147
a) Scoring	147
b) Bonitätsauskunft	148
6. Bereichsausnahmen nach § 37 BDSG	148
G. Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung	148
H. Sanktionsmöglichkeiten bei Verstößen	149
I. Anwendbarkeit weiterer Datenschutzregelungen neben der DSGVO	149
I. Regelungen für Diensteanbieter neben der DSGVO	149
II. Anwendbarkeit der Datenschutzregelungen des TMG neben der DSGVO	149

Kapitel 7. Informationspflichten bei Datenschutzverletzungen	Seite
A. Einleitung	150
B. Adressat der Pflichten	151
C. Informationspflichten bei Datenschutzverletzungen	151
I. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DSGVO	151
1. Verletzung des Schutzes personenbezogener Daten	151
2. Meldefrist	152
3. Meldepflicht des Auftragsverarbeiters	152
4. Mindestanforderungen an die Meldung	152
5. Teilmeldungen	153
6. Ausnahmen von der Meldepflicht	153
II. Benachrichtigung des Betroffenen bei Datenschutzverletzungen, Art. 34 DSGVO	153
D. Dokumentation einer Datenschutzverletzung nach Art. 33 DSGVO	154
E. Sanktionsmöglichkeiten bei Verstößen	155
 Kapitel 8. Verhaltensregeln und Zertifizierung	
A. Einleitung	157
B. Verhaltensregeln	157
I. Verhaltensregeln als Instrument der Ko-Regulierung	157
1. Vorteile	158
2. Präzisierung der DSGVO	159
II. Anwendung im Unternehmen	159
1. Vertretung durch Verbände und Vereinigungen	159
2. Gegenstand der Verhaltensregeln	160
3. Bindung und Kontrolle	160
4. Genehmigungsverfahren	161
III. Rechtsfolgen	162
IV. Überwachung der Verhaltensregeln	163
C. Zertifizierung	163
I. Allgemeines	163
1. Vorteile	164
2. Zertifizierung	165
II. Anwendung im Unternehmen	165
1. Zertifizierungsstellen	165
2. Zertifizierungskriterien	166
3. Verfahren	166
III. Rechtsfolgen	167
IV. Geltungsdauer und Widerruf	167
D. Fazit	167

Inhaltsverzeichnis	XVII
--------------------	------

Teil 3. Datenverarbeitung im Konzern	Seite
--------------------------------------	-------

Kapitel 1. Einleitung: Fehlendes Konzernprivileg	169
--	-----

Kapitel 2. Grundsätze der Verarbeitung nach der DSGVO

A. Einleitung	172
---------------------	-----

B. Grundsätze der Verarbeitung	172
--------------------------------------	-----

I. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	173
--	-----

II. Zweckbindung	174
------------------------	-----

1. Legitimität	174
----------------------	-----

2. Detaillierungsgrad des Verarbeitungszwecks (Eindeutigkeit)	174
---	-----

III. Datenminimierung	175
-----------------------------	-----

IV. Richtigkeit	175
-----------------------	-----

V. Speicherbegrenzung	175
-----------------------------	-----

VI. Integrität und Vertraulichkeit	175
--	-----

C. Risikobasierter Ansatz der DSGVO	176
---	-----

Kapitel 3. Rechtliche Anforderungen an Datenverarbeitungen

A. Grundbegriffe	179
------------------------	-----

I. Personenbezogene Daten, betroffene Person und Verantwortlicher	179
--	-----

II. Der Begriff der Verarbeitung	180
--	-----

B. Anwendbarkeit der DSGVO	180
----------------------------------	-----

C. Verbot mit Erlaubnisvorbehalt	181
--	-----

I. Einwilligung	181
-----------------------	-----

1. Wirksamkeitsvoraussetzung	181
------------------------------------	-----

a) Form und Zeitpunkt der Einwilligung	182
--	-----

b) Informierte Einwilligung	182
-----------------------------------	-----

c) Freiwillige Einwilligung	183
-----------------------------------	-----

d) Widerruf	183
-------------------	-----

e) Sonderfall: Die Einwilligung von Kindern	184
---	-----

f) Alteinwilligung	184
--------------------------	-----

2. Probleme der konzerninternen Datenverarbeitung auf Grundlage einer Einwilligung	185
--	-----

II. Erlaubnistatbestände nach Art. 6 Abs. 1 Satz 1 lit. b–f DSGVO	185
---	-----

1. Datenverarbeitung im Rahmen von Verträgen gemäß Art. 6	
---	--

Abs. 1 Satz 1 lit. b DSGVO	186
----------------------------------	-----

2. Sonderfall: Verarbeitung im Beschäftigtenkontext	187
---	-----

3. Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung ...	189
--	-----

4. Datenverarbeitung zum Schutz lebenswichtiger Interessen	189
--	-----

5. Datenverarbeitung im öffentlichen Interesse oder durch	
---	--

öffentliche Gewalt	189
--------------------------	-----

6. Datenverarbeitung zur Wahrung berechtigter Interessen	189
--	-----

	Seite
III. Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO	192
IV. Sonstige Sonderfälle der Datenverarbeitung	193
1. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilung und Straftaten	193
2. Zweckänderung	193
3. Auftragsverarbeitung	194
Kapitel 4. Auftragsverarbeitung im Konzern	
A. Allgemeines zur Auftragsverarbeitung	196
I. Besonderheiten der Auftragsverarbeitung	196
1. Privilegierung der Auftragsverarbeitung	196
2. Voraussetzung: Auftragsverarbeitungsvereinbarung	198
3. Verhältnis der Auftragsverarbeitung zu Berufsgeheimnissen	198
II. Sachlicher Anwendungsbereich der Auftragsverarbeitung	199
1. „Funktionsübertragung“ obsolet	199
2. Abgrenzung zur (gemeinsamen) Verantwortlichkeit	200
III. Checkliste: Auftragsverarbeitung oder Verantwortlichkeit?	201
B. Einsatzmöglichkeiten der Auftragsverarbeitung im Konzern	203
I. Call-Center	203
II. E-Mail-System	204
1. Anwendungsbereich des TKG	204
2. Auftragsverarbeitung im Rahmen des TKG	205
III. Personaldatenverwaltung	207
IV. Adressverwaltung	208
V. Lohn- und Gehaltsabrechnung	208
VI. IT-Dienste	208
C. Gesetzliche Voraussetzungen der Auftragsverarbeitung	209
I. Auftragsverarbeitungsvertrag	209
1. Verarbeitung nur auf dokumentierte Weisung hin (lit. a)	209
2. Pflicht zur Vertraulichkeit und Verschwiegenheit (lit. b)	210
3. Maßnahmen gemäß Art. 32 DSGVO (lit. c)	210
4. Einhaltung der Bedingungen für den Unterauftrag (lit. d)	210
5. Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen (lit. e)	211
6. Unterstützung des Verantwortlichen bei der Einhaltung der Art. 32–36 DSGVO	211
7. Löschung oder Rückgabe nach Abschluss der Verarbeitung (lit. g) ...	211
8. Zurverfügungstellung von Informationen und Ermöglichung von Überprüfungen (lit. h)	212
9. Fortgeltung bereits bestehender Verträge	212
II. Pflichten des Auftraggebers	212
III. Pflichten des Auftragnehmers	213

Inhaltsverzeichnis	XIX
--------------------	-----

	Seite
D. Auftragsverarbeitung mit Auslandsbezug	214
I. Auftragnehmer im Ausland	214
II. Auftraggeber im Ausland	215

Kapitel 5. Verträge für den konzerninternen Datentransfer

A. Einleitung	216
B. Arten konzerninterner Datenübermittlung	217
I. Konzerninterne Auftragsverarbeitung	217
II. Rechtfertigung sonstiger konzerninterner Datenübermittlungen	218
1. Rechtsgrundlagen unternehmensübergreifender Datenübermittlung	218
2. Anforderungen an konzerninterne Datenübermittlungsverträge	220
3. Grenzüberschreitende konzerninterne Datenübermittlung	221
III. Gemeinsame Verantwortlichkeit im Konzern	221
1. Voraussetzungen der gemeinsamen Verantwortlichkeit	222
2. Rechtsfolge: Notwendigkeit eines Joint-Controller-Vertrages	224
a) Form	224
b) Inhalt	224
3. Praxistipp: Der „Joint-Controller-Plus“-Vertrag	225
4. Grenzüberschreitende gemeinsame Verantwortlichkeit	226
C. Umsetzung in Mehrparteienkonstellationen	226
I. Einzelvertragslösung	226
II. Rahmenvertragslösung	226

Kapitel 6. Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats

A. Einleitung	229
B. Datenschutzrechtliche Rahmenbedingungen	230
I. Datenschutzrechtliche Zulässigkeit unternehmensübergreifender Datenverarbeitungen	231
1. Erforderlichkeit von Datenverarbeitungen nach § 26 Abs. 1 BDSG	233
2. Konzernweite Datenverarbeitung zur Wahrung eigener berechtigter Interessen nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO	239
3. Konzernweite Datenverarbeitung zur Wahrung berechtigter Interessen eines Dritten nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO	241
4. Konzernweite Verarbeitung auf der Grundlage von Betriebsvereinbarungen	242
5. Konzernweite Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung	243
6. Weitere datenschutzrechtliche Vorgaben mit Relevanz zu konzernweiten Datenverarbeitungen	245
7. Auftragsverarbeitung von Beschäftigtendaten im Konzern	248

	Seite
II. Datenschutzrechtliche Vorgaben im TKG bzw. im TMG	250
1. Datenschutzvorgaben des TKG	250
2. TMG	252
C. Kollektivrechtlicher Rahmen für die Verarbeitung von Beschäftigtendaten im Konzern – Mitwirkungs- und Mitbestimmungsrechte	252
I. Kollektivrechtliche Zuständigkeit	253
II. Mitwirkungs- und Mitbestimmungsrechte	254
III. Überwachungspflichten nach § 80 Abs. 1 Nr. 1 BetrVG	255
IV. Weitere Mitwirkungsrechte	257
V. Mitbestimmungsrechte	259
1. § 87 Abs. 1 Nr. 6 BetrVG: Mitbestimmung bei der Einführung und Anwendung von technischen Einrichtungen	260
2. § 87 Abs. 1 Nr. 7 BetrVG: Mitbestimmung im Bereich des Arbeits- und Gesundheitsschutzes	263
a) Allgemeines	263
b) Auswirkungen des Mitbestimmungsrechts innerhalb eines Konzerns	263
3. § 87 Abs. 1 Nr. 1 BetrVG: Ordnung des Betriebes und Verhalten der Arbeitnehmer	264
a) Allgemeines	264
b) Umsetzung von verbindlichen Richtlinien zur konzernweiten Datenverarbeitung	265

Teil 4. Internationale Aspekte des Datenschutzrechts

Kapitel 1. Räumliche Anwendbarkeit der DSGVO und des BDSG

A. Einleitung	267
B. Datenverarbeitung im Rahmen der Tätigkeiten von Niederlassungen innerhalb der EU	269
I. Begriff der Niederlassung	269
II. Im Rahmen ihrer Tätigkeiten	270
C. Verarbeitung personenbezogener Daten von innerhalb der EU befindlichen Personen	271
I. Anbieten von Waren oder Dienstleistungen	271
1. Waren	271
2. Dienstleistungen	271
3. Anbieten innerhalb der Union	271
II. Verhaltensbeobachtung	272
III. Aufenthaltsort betroffener Personen	273
D. Räumliche Anwendbarkeit des BDSG	274

Inhaltsverzeichnis	XXI
--------------------	-----

Kapitel 2. Datenübermittlungen in Drittländer	Seite
A. Einleitung	275
B. Anforderungen an die Datenübermittlung in Drittländer	276
I. Die Übermittlung personenbezogener Daten in Drittländer nach Art. 44 ff. DSGVO	276
1. Angemessenheitsbeschlüsse	277
2. Sonderfall: EU-US-Privacy-Shield	277
3. Datenübermittlung vorbehaltlich geeigneter Garantien	278
a) Standardvertragsklauseln	278
b) Binding Corporate Rules	279
c) Sonstige Garantien	279
d) Genehmigungspflichtige Garantievereinbarungen	280
II. Die Ausnahmen nach Art. 49 DSGVO	280
1. Ausnahmetatbestände des Art. 49 UAbs. 1 DSGVO	280
a) Einwilligung	280
b) Vertragserfüllung	281
c) Wichtige Gründe des öffentlichen Interesses	281
d) Geltendmachung von Rechtsansprüchen	282
e) Schutz lebenswichtiger Interessen	282
f) Datenübermittlung aus einem Register	282
2. Der Ausnahmetatbestand des Art. 49 Abs. 1 UAbs. 2 DSGVO	282

Kapitel 3. Standardvertragsklauseln	
A. Allgemeine Grundlagen	286
I. Vertragsparteien	287
II. Unterschiedliche Varianten der Standardvertragsklauseln	288
B. Standardvertragsklauseln Set I und Set II	289
C. Standardvertragsklauseln zur Auftragsverarbeitung	291
I. Abgrenzung zu den Standardvertragsklauseln aus dem Jahr 2001	292
II. Zulässigkeit der Auftragsverarbeitung im Drittland	293
III. Ergänzungen der Standardvertragsklauseln gemäß Art. 28 Abs. 3 DSGVO	293
IV. Räumlicher Anwendungsbereich der Standardvertragsklauseln zur Auftragsverarbeitung	294
D. Checkliste zum Abschluss von Datenübermittlungsverträgen	295

Kapitel 4. Privacy Shield Principles	
A. Einleitung	299
B. Privacy-Shield-Grundsätze	300
I. Anwendungsbereich	300
II. Befugnisse der FTC und des DoT	301

	Seite
III. Grundsätze des Privacy Shields	301
1. Grundsatz der „Informationspflicht“ (Notice)	301
2. Grundsatz der „Wahlmöglichkeit“ (Choice)	303
3. Grundsatz der „Weitergabe“ (Onward Transfer)	303
4. Grundsatz des „Auskunftsrechts“	305
5. Grundsätze der „Datenintegrität“ (Data Integrity), „Datensicherheit“ (Data Security) und der „Zweckbindung“ (Purpose Limitation)	306
6. Grundsatz der „Durchsetzung“ (Recourse)	306
a) Schlichtungsverfahren	307
b) Anlassunabhängig Prüfung und Kontrolle	307
c) Abhilfe und Sanktionen	308
IV. Compliance Maßnahmen im Unternehmen	308
V. Beitritt zum Privacy Shield	310
1. Mitteilung gegenüber dem DoC	310
2. Privacy-Shield-Liste	311
C. Datenübermittlung an ein Privacy-Shield-Unternehmen	312
I. Allgemeines	312
II. Datenübermittlung als Auftragsverarbeitung	313
III. Übermittlung von Personaldaten und Patientendaten	315
D. Privacy Shield aus Sicht der Aufsichtsbehörde	315
I. Kritische Sicht auf den Privacy Shield	315
II. Anforderung an eine Mindestprüfung	318
III. Aussetzungsbefugnis der Datenschutzbehörden	319
IV. Die Zukunft des Privacy Shields	320
 Kapitel 5. Verbindliche interne Datenschutzvorschriften	
A. Einleitung	325
B. Rechtliche Aspekte des Drittlandverkehrs	328
I. Zweiteilige Zulässigkeitsprüfung (Art. 44 Satz 1 DSGVO)	328
II. Übermittlungen auf der Basis geeigneter Garantien (Art. 46 DSGVO)	330
III. Weiterübermittlungen im Drittland (Art. 44 Satz 1 aE DSGVO)	331
C. Verbindliche interne Datenschutzvorschriften	331
I. Adressaten – Verantwortliche und Auftragsverarbeiter	332
II. Unternehmensgruppen und Gruppen von Unternehmen mit gemeinsamer Wirtschaftstätigkeit	333
III. Geeignete Garantien und Genehmigungserfordernis	334
D. Rechtsverbindlichkeit, praktische Befolgung und durchsetzbare Rechte	334
I. Interne und externe Rechtsverbindlichkeit	335

	Seite
II. Mechanismen zur Herstellung von interner Rechtsverbindlichkeit	335
1. Vertragliche Lösungen	336
2. Unternehmensinterne Regelungen	337
3. Einseitige Verpflichtungen („Unilateral Undertakings“)	337
III. Herstellung der Verbindlichkeit gegenüber Beschäftigten (Art. 47 Abs. 1 lit. a aE DSGVO)	338
IV. Praktische Durchsetzung durch die Gruppenmitglieder und deren Beschäftigte	339
V. Durchsetzbare Rechte für die betroffenen Personen (Art. 47 Abs. 1 lit. b DSGVO)	340
E. Anforderungen an die verbindlichen internen Datenschutzvorschriften	342
I. Angaben zur Struktur und Kontaktdaten (Art. 47 Abs. 2 lit. a DSGVO)	343
II. Beschreibung der Datenübermittlungen (Art. 47 Abs. 2 lit. b DSGVO)	343
1. Festlegung des Anwendungsbereichs	344
2. Detaillierungsgrad der Beschreibungen	345
3. Definitionen	345
4. Begriff des „Datenexporteurs“ und des „Datenimporteurs“	346
III. Angaben zur Rechtsverbindlichkeit (Art. 47 Abs. 2 lit. c DSGVO)	346
IV. Datenschutzgrundsätze (Art. 47 Abs. 2 lit. d DSGVO)	346
1. Zweckbindung	348
2. Rechtmäßigkeit, Treu und Glauben und Transparenz	349
3. Datenminimierung, begrenzte Speicherfristen	351
4. Datenqualität und Richtigkeit	351
5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung	352
6. Datensicherheit	352
7. Anforderungen an die Weiterübermittlung an nicht an die internen Datenschutzvorschriften gebundenen Stellen	353
V. Betroffenenrechte und Rechtsbehelfe (Art. 47 Abs. 1 lit. e DSGVO) ...	354
1. Rechte der betroffenen Personen und Mittel zur Wahrnehmung	354
2. Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde	356
3. Wirksamer gerichtlicher Rechtsbehelf	356
VI. Haftung (Art. 47 Abs. 2 lit. f DSGVO)	356
VII. Zugang zu den internen Datenschutzvorschriften (Art. 47 Abs. 2 lit. g DSGVO)	357
VIII. Datenschutzbeauftragte bzw. sonstiges Datenschutzpersonal (Art. 47 Abs. 2 lit. h DSGVO)	359
IX. Beschwerdeverfahren (Art. 47 Abs. 2 lit. i DSGVO)	360
X. Interne Datenschutzkontrolle (Art. 47 Abs. 2 lit. j DSGVO)	362
XI. Verfahren bei Änderung der internen Datenschutzvorschriften (Art. 47 Abs. 2 lit. k DSGVO)	364

	Seite
XII. Zusammenarbeit mit der Aufsichtsbehörde (Art. 47 Abs. 2 lit. 1 DSGVO)	365
XIII. Verfahren bei Änderungen im Recht des Drittlandes (Art. 47 Abs. 2 lit. m DSGVO)	365
XIV. Datenschutzschulungen (Art. 47 Abs. 2 lit. n DSGVO)	365
F. Format und Verfahren für den Informationsaustausch	366
G. Genehmigungsverfahren	366

Kapitel 6. Der Nachweis geeigneter Garantien durch Verhaltensregeln und Zertifizierung

A. Einleitung	371
B. Verhaltensregeln	371
C. Zertifizierung	372

Teil 5. Spannungsfeld zwischen Datenschutz und Compliance-Anforderungen

Kapitel 1. Datenschutzrecht und Compliance

A. Einleitung	374
B. Begriff und Bedeutung von Compliance	374
C. Rechtlicher Hintergrund der Compliance	375
I. Gesetzliche Verpflichtung zur Einrichtung von Compliance-Systemen	375
II. Sonstige Gründe zur Einrichtung von Compliance-Maßnahmen	377
1. Vertragliche Verpflichtungen	377
2. Freiwillig auferlegte Verpflichtungen	378
3. Prüfungsstandards	378
D. Datenschutzrechtliche Ausgestaltung von Compliance-Maßnahmen	379
I. Datenschutzrechtliche Voraussetzungen	379
1. Einwilligung als Erlaubnistatbestand	379
2. Gesetzliche Grundlagen für repressive Compliance-Maßnahmen ...	380
a) Die Aufdeckung von Straftaten	380
b) Die Aufdeckung von nicht-strafbaren Pflichtverletzungen	381
c) Heimliche Arbeitnehmerüberwachung	382
3. Gesetzliche Grundlagen für präventive Compliance-Maßnahmen	383
a) Spezialgesetzliche Regelungen	383
b) § 26 Abs. 1 Satz 1 BDSG und Erlaubnistatbestände der DSGVO	384
4. Arbeitsrechtliche Kollektivvereinbarungen als Rechtsgrundlage für präventive Compliance-Maßnahmen	384

	Seite
5. Allgemeine datenschutzrechtliche Anforderungen	385
a) Datenminimierung und Speicherbegrenzung	385
b) Transparenzpflichten	385
c) Dokumentationspflichten	385
d) Löschpflichten	386
II. Pre-Employment-Screening	387
1. Überprüfung der fachlichen Qualifikationen	388
2. Überprüfung der kriminellen Vergangenheit	388
3. Überprüfung der finanziellen Situation	390
E. Kooperation bei Anfragen der öffentlichen Verwaltung	391
I. Auskunftsverlangen der Finanzbehörden	391
II. Auskunftsverlangen der Strafverfolgungsbehörden	392

Kapitel 2. E-Discovery

A. Einführung und Begriff	394
B. Herausgabeansprüche durch die andere Partei	396
I. Schritt 1: Identifizierung der „Custodians“	396
II. Schritt 2: Sicherung und Sichtung der Dokumente	397
III. Schritt 3: Sortierung der Dokumente	397
IV. Schritt 4: Vorlage der Dokumente	398
C. Mögliche Strategien der Konzernunternehmen zur Vermeidung der Herausgabe	398
D. Datenschutzrechtliche Implikationen	401

Kapitel 3. Technischer Datenschutz

A. Einleitung	408
B. Pflichtenkanon des Art. 32 Abs. 1 DSGVO	408
I. Mindestanforderungen	408
1. „Pseudonymisierung und Verschlüsselung“	409
2. Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	409
3. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	411
4. „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“	411
II. Angemessenes Schutzniveau	411
1. Eintrittswahrscheinlichkeit und Schwere der Risiken	412

	Seite
2. Art, Umfang, Umstände und Zweck der Verarbeitung	413
3. Stand der Technik	413
4. Implementierungskosten	413
5. Ergebnis: Datenschutzkonzept	414
III. Verletzungsfolgen	415
C. Exkurs: Verpflichtungen nach dem IT-Sicherheitsgesetz und dem NIS-RL- Umsetzungsgesetz	415
I. §§ 8a Abs. 1, 8c Abs. 1 BSIG	416
1. Betreiber kritischer Infrastrukturen (§ 8a Abs. 1 BSIG)	416
2. Pflichten der Betreiber Kritischer Infrastrukturen	417
3. Anbieter digitaler Dienste (§ 8c Abs. 1 BSIG)	417
4. Pflichten der Anbieter digitaler Dienste	418
5. Verletzungsfolgen	419
II. § 13 Abs. 7 Satz 1 TMG	419
1. Diensteanbieter	419
2. Verhältnis zur DSGVO und dem TMG	419
3. Pflichtumfang	420
4. Verletzungsfolgen	420
D. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DSGVO	420
I. Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DSGVO)	421
II. Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	421
Teil 6. Datenschutz bei M&A-Transaktionen	
A. Einleitung	424
B. Kategorisierung von Unternehmenstransaktionen	424
C. Datenschutzrechtliche Anforderungen an Due-Diligence-Prüfungen	425
I. Gegenstand und Ablauf der Due-Diligence-Prüfung	425
II. Rechtsgrundlage für die Offenlegung von Daten im Rahmen der Due-Diligence-Prüfung	426
1. Rechtsgrundlage für die Offenlegung beim Asset Deal	426
a) Anwendbarkeit der DSGVO	426
b) Einwilligung	427
c) Gesetzliche Erlaubnisform	427
d) Zweckänderung	429
2. Rechtsgrundlage für die Offenlegung beim Share Deal	429
3. Rechtsgrundlage für die Offenlegung bei der Umwandlung	429
4. Rechtsgrundlage für die Offenlegung pseudonymisierter Daten im Rahmen von Unternehmenstransaktionen	429
III. Typische Fallkonstellationen bei der Offenlegung von Daten im Rahmen der Due-Diligence-Prüfung	430
1. Mitarbeiterdaten	430
2. Kundendaten	432

	Seite
3. Personenbezogene Daten in Vertragsdokumenten	432
4. Einschaltung von Service-Providern	433
5. Datentransfer in Drittstaaten außerhalb der EU	434
6. Benachrichtigungspflichten	435
7. Vertraulichkeitsvereinbarungen	436
D. Datenschutzrechtliche Anforderungen an den Vollzug von Unternehm-	
enstransaktionen	437
I. Datenschutzrechtliche Anforderungen an den Vollzug von Share Deals	437
II. Datenschutzrechtliche Anforderungen an den Vollzug von Asset	
Deals	438
III. Datenschutzrechtliche Anforderungen an den Vollzug von	
Transaktionen nach dem UmwG	441
IV. Datenschutzrechtliche Anforderungen an den Vollzug von	
Transaktionen über den Erwerb von Arztpraxen und Kanzleien	442
Teil 7. Cloud Computing	
A. Vor- und Nachteile des Cloud Computing	446
I. Relevanz des Themas für Konzerne	446
II. Risiken von Cloud Computing	447
B. Formen von Cloud-Diensten (Übersicht)	449
I. Bereitstellungsmodelle (Deployment-Models)	449
II. Dienstleistungsmodelle (Service-Models)	449
C. Allgemeine datenschutzrechtliche Konfliktbereiche des Cloud Computing	449
D. EU-datenschutzrechtliche Grundlagen des Cloud Computing	452
I. DSGVO	452
II. Stellungnahme 05/2012 der Art.-29-Datenschutzgruppe	453
1. Anwendbarkeit des EU-Rechts	453
2. Cloud-Anwender und Cloud-Anbieter	453
3. Sicherheitsmaßnahmen und Organisation	453
4. Ausgestaltung des Vertrags zwischen Anbieter und Anwender	454
III. CISPE Code of Conduct	454
E. Stellungnahmen und Vorschläge in Deutschland	455
I. Cloud-Anbieter und Cloud-Anwender, Sondergesetze	455
II. Pflichten innerhalb des Cloud-Auftragsverhältnisses	456
III. Ausgestaltung des Cloud-Computing-Vertrages	457
IV. Technische und organisatorische Sicherheitsmaßnahmen	457
V. Verschlüsselung von Daten	458
VI. Cloud Computing und unsichere Drittländer	459
F. Ratschläge für Cloud-Nutzer zur Ausgestaltung des Cloud Computing	460

Teil 8. Aufsichtsbehördlicher Vollzug und Sanktionen	Seite
A. Einrichtungsgarantie, Merkmale und Organisation der Aufsichtsbehörde ..	466
I. Unabhängigkeit Art. 52 DSGVO	469
1. Organisatorisch-institutionelle Unabhängigkeit	470
2. Personelle und persönliche Unabhängigkeit der Aufsichtsbehörde	472
II. Besetzung und Amtszeit der Leitung der Aufsichtsbehörde	473
III. Personelle und materielle Ausstattung der Aufsichtsbehörde	475
IV. Vertraulichkeit der Aufgabenwahrnehmung	476
B. Zuständigkeitsverteilung zwischen den Aufsichtsbehörden – One-Stop-Shop-Verfahren	477
I. Grundprinzip der territorialen Zuständigkeit auf Europäischer Ebene	478
1. Zuständigkeit der betroffenen Aufsichtsbehörde	480
a) Tatbestand „Niederlassung“	480
b) Tatbestand „Beschwerdeerhebung“	480
c) Tatbestand „Erhebliche Auswirkung“	480
2. Zuständigkeit der federführenden Aufsichtsbehörde – One-Stop-Shop	481
a) Niederlassung und Hauptniederlassung des Verantwortlichen ...	481
b) Niederlassung und Ort der Verarbeitung	482
c) Kein One-Stop-Shop für nicht in der EU niedergelassene Stellen	482
3. Ausnahmen vom One-Stop-Shop	483
4. Verfahrenskoordination auf europäischer Ebene	484
a) Verfahren der Zusammenarbeit	484
b) Amtshilfe	486
c) Gemeinsame Maßnahmen	487
d) Kohärenzverfahren und Streitbeilegung	487
II. Zuständigkeitsverteilung zwischen nationalen Aufsichtsbehörden	488
1. System der nationalen Aufsichtsbehörden	488
2. Ausnahmen von der Zuständigkeit staatlicher Aufsichtsbehörden	489
3. Federführende Behörde auf nationaler Ebene	490
C. Durchsetzung und Sanktionen	491
I. Verwaltungsrechtliche Sanktionen und Anordnungen	491
1. Kontrollbefugnisse der Aufsichtsbehörden (Art. 58 Abs. 1 lit. a–c, e und f DSGVO)	491
2. Anordnungsbefugnisse (Art. 58 Abs. 2 lit. a–g DSGVO)	492
a) Warnung und Verwarnung (Art. 58 Abs. 2 lit. a und b DSGVO)	492
b) Anweisung (Art. 58 Abs. 2 lit. c–e, g DSGVO)	493
c) Untersagung (Art. 58 Abs. 2 lit. f, j DSGVO)	494
3. Rechtsschutzverfahren (Art. 78 DSGVO iVm VwVfG und VwGO)	494
II. Ordnungswidrigkeiten und Straftatbestände, Art. 83 DSGVO	495
1. Materielle Bußgeldtatbestände (Art. 83 DSGVO und § 43 BDSG)	495

	Seite
2. Bußgeldverfahren (Art. 58 Abs. 2 lit. i DSGVO iVm BDSG und OWiG)	496
a) Unternehmensbegriff	497
b) Verhalten von Mitarbeitern und Externen	498
c) Kriterien für die Bußgeldverhängung	499
d) Bußgeldhöhe	499
3. Rechtsschutzverfahren (Art. 78 DSGVO iVm OWiG)	500
4. Straftatbestände	501
5. Wettbewerbsrecht	501
III. Zivilrechtliche Verfahren und Verbraucherschutz	501
1. Schadensersatz (Art. 82 DSGVO)	501
2. Verbandsklagerecht und Verbraucherschutz (Art. 80 DSGVO und UKlaG)	502
Sachverzeichnis	503