

# Betrieblicher Datenschutz

Rechtshandbuch

von

Prof. Dr. Nikolaus Forgó, Prof. Dr. Marcus Helfrich, Prof. Dr. Jochen Schneider, Marian Arning, Till Baer, Benno Barnitzke, Dr. Christiane Bierekoven, Dr. Dirk Bieresborn, Prof. Dr. Georg Borges, Tobias Born, Isabell Conrad, Dr. Kai Cornelius, Dr. Eugen Ehmann, Dr. Sandro Gaycken, Dr. Uwe Günther, Dr. Nils Christian Haag, Dr. Oliver M. Habel, Dr. Stefan Hanloser, Dominik Hausen, Christian Hawellek, Joerg Heidrich, Dr. Michael Karger, Lars Klatte, JProf. Dr. Timoleon Kosmides, Dr. Jens Lütcke, Dr. Flemming Moos, Eckart C. Müller, Dr. Stephan Ott, Hans-Hermann Schild, Dr. Fabian Schmieder, Jörn Schoof, Dr. Christian Schröder, Georg F. Schröder, Dr. Axel Spies, Dr. Christoph Wegener, Hans Peter Wiesemann, Dr. Anna Zeiter

1. Auflage

[Betrieblicher Datenschutz – Forgó / Helfrich / Schneider / et al.](#)

schnell und portofrei erhältlich bei [beck-shop.de](http://beck-shop.de) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Datenschutz- und Melderecht](#)



Verlag C.H. Beck München 2014

Verlag C.H. Beck im Internet:

[www.beck.de](http://www.beck.de)

ISBN 978 3 406 63468 0

# beck-shop.de

Forgó/Helfrich/Schneider  
Betrieblicher Datenschutz

**beck-shop.de**

## Betrieblicher Datenschutz

Rechtshandbuch

Herausgegeben von

**Prof. Dr. Nikolaus Forgó**  
Hannover

**Prof. Dr. Marcus Helfrich**  
München

**Prof. Dr. Jochen Schneider**  
München

Bearbeitet von  
den Herausgebern und von

*Marian Arning LL. M., Hamburg; Till Baer, München; Benno Barnitzke LL. M., Hannover;  
Dr. Christiane Bierehoven, Nürnberg; Dr. Dirk Bieresborn, Kassel; Prof. Dr. Georg Borges,  
Bochum; Tobias Born, Düsseldorf; Isabell Conrad, München; Dr. Kai Cornelius LL. M., Frankfurt  
a. M.; Dr. Eugen Ehmann, Ansbach; Dr. Sandro Gaycken, Berlin; Dr. Uwe Günther, München;  
Dr. Nils Christian Haag, Hamburg; Dr. Oliver M. Habel, München; Dr. Stefan Hanloser,  
München; Dominik Hausen, München; Christian Hawellek, Hannover; Joerg Heidrich,  
Hannover; Dr. Michael Karger, München; Lars Klatte, Köln; JProf. Dr. Timoleon Kosmides  
LL. M. Eur., München/Thessaloniki; Dr. Jens Lütcke M.B.L.-HSG, Gauting; Dr. Flemming Moos,  
Hamburg; Eckart C. Müller, München; Dr. Stephan Ott, München; Laura Schabmair  
LL. B., München; Hans-Herrmann Schild, Wiesbaden; Dr. Fabian Schmieder, Hannover; Jörn  
Schoof, Nürnberg; Dr. Christian Schröder, Düsseldorf; Dr. Georg F. Schröder LL. M., München;  
Dr. Axel Spies, Washington DC/Frankfurt a. M.; Dr. Christoph Wegener, Gevelsberg;  
Dr. Hans Peter Wiesemann, München; Dr. Anna Zeiter, Hamburg/Stanford*

2014

# beck-shop.de

Zitiervorschlag: Forgó/Helfrich/Schneider/*Bearbeiter*

[www.beck.de](http://www.beck.de)

ISBN 978 3 406 63468 0

© 2014 Verlag C. H. Beck oHG  
Wilhelmstraße 9, 80801 München  
Druck: Beltz Bad Langensalza  
Neustädter Straße 1–4, 99947 Bad Langensalza  
Satz: Druckerei C. H. Beck Nördlingen

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

# beck-shop.de

## Vorwort

Das Datenschutzrecht bildete in seinen Anfängen eine Randmaterie und fand lange Zeit als Sonderbereich des öffentlichen Rechts wenig Beachtung in privatrechtlichen Zusammenhängen. Mit der wachsenden Bedeutung der Informationsgesellschaft im Wirtschafts- und Rechtsleben kommt dem Datenschutz jedoch auch für private Unternehmen eine besondere Rolle zu. Die Beachtung des Datenschutzes ist inzwischen eine unternehmenskritische Aufgabe, deren Erfüllung Priorität beanspruchen muss.

Vom Datenschutzbeauftragten bis zum Datensicherheitsrecht, von der Zusammenarbeit mit Aufsichtsbehörden und dem Betriebsrat bis zur Präsentation des Unternehmens in sozialen Netzwerken reicht das Spektrum relevanter Rechtsfragen. Diese treten häufig und in unterschiedlichen Zusammenhängen auf, sie sind für den Nichtfachmann durchaus schwierig zu durchschauen und erfahren gleichzeitig starke Beachtung durch Kunden und Öffentlichkeit.

Das Datenschutzrecht ist auch Gegenstand der rechtspolitischen Diskussion und gesetzgeberischen Arbeit.

In diesem Werk wird zwar stets auf den aktuellen Rechtsstand abgestellt. Darüber hinaus wird aber auch versucht, die europäischen Anstrengungen, insbesondere der EU-Kommission, bei der Weiterentwicklung des Rechtsgebiets zu berücksichtigen und darauf hinzuweisen.

Das vorliegende Werk breitet das Spektrum der Aufgaben- und Problemfelder, die sich im Zusammenhang mit der Verarbeitung personenbezogener Daten im Betrieb ergeben, aus und deckt dieses durch die Beiträge von Autorinnen und Autoren mit unterschiedlichem Blickwinkel ab. Die praktische Verwertbarkeit des Dargestellten für die Rechtsberatung des Unternehmens ist das gemeinsame Anliegen. Es folgt daher dem Anspruch, ein Instrument zur Bewältigung des datenschutzrechtlichen Alltags – eben ein Handbuch – zu sein, mit dem typische Probleme rasch und zuverlässig erkannt und damit zusammenhängende Fragen beantwortet werden können. Es soll dazu dienen, das Datenschutzrecht im Unternehmen proaktiv zu gestalten und nicht nur darauf zu hoffen, dass schon nichts geschehen werde, um dann erst reaktiv tätig zu werden.

Die Herausgeber danken den Autorinnen und Autoren für die angenehme Zusammenarbeit und Frau Ruth Schrödl als zuständiger Lektorin für die große Geduld, Umsicht und fördernde Begleitung des Vorhabens.

Hannover/München, Oktober 2013

*Nikolaus Forgó  
Marcus Helfrich  
Jochen Schneider*

**beck-shop.de**

## Inhaltsübersicht

	Seite
Vorwort .....	V
Bearbeiterverzeichnis .....	XLV
Abkürzungsverzeichnis .....	XLIX

### Teil I. Allgemeine datenschutzrechtliche Grundlagen und Strukturen

Kapitel 1. Entwicklung des Datenschutzes in der Informationsgesellschaft ...	1
Kapitel 2. Datenschutz im öffentlichen und nicht-öffentlichen Bereich .....	38
Kapitel 3. Die Europäische Dimension des Datenschutzes .....	49
Kapitel 4. Internationaler Datenschutz .....	69
Kapitel 5. Der internationale Anwendungsbereich des BDSG .....	81

### Teil II. Datenschutzorganisation

Kapitel 1. Betrieblicher Datenschutzbeauftragter .....	107
Kapitel 2. Datenschutzmanagement und Datenschutzprozesse .....	130
Kapitel 3. Selbstkontrolle und Datenschutzaufsicht .....	142
Kapitel 4. Datenschutz und Zertifizierung .....	152

### Teil III. Archivierung und Entsorgung

Kapitel 1. Datenschutzkonzepte .....	167
Kapitel 2. Technische und organisatorische Maßnahmen .....	198
Kapitel 3. Archivierung und Protokollierung als Problem des betrieblichen Datenschutzes .....	210

### Teil IV. Datenschutz und Personal: Arbeitnehmer-/ Beschäftigtendatenschutz

Kapitel 1. Beschäftigtendatenschutz .....	219
Kapitel 2. „Bring Your Own Device“ und Datenschutz .....	244
Kapitel 3. Datenschutz und Mitbestimmung .....	257
Kapitel 4. Sozialdatenschutz .....	269
Kapitel 5. Compliance und Datenschutz .....	310

### Teil V. Datenschutz in Betrieb, Unternehmen und Konzern

Kapitel 1. Konzerndatenschutz .....	327
Kapitel 2. Internationaler Datenverkehr .....	346
Kapitel 3. Compliance-Organisation und Whistleblowing im Konzern .....	361
Kapitel 4. Datenschutz in der Unternehmenstransaktion .....	390



## Teil VI. Outsourcing und neue Technologien als Herausforderung für den Datenschutz

Kapitel 1. Outsourcing .....	409
Kapitel 2. Auftragsdatenverarbeitung .....	423
Kapitel 3. Customer Relationship Management und Datenschutz .....	450
Kapitel 4. Nachweispflicht für die Datenherkunft .....	465
Kapitel 5. Cloud Computing .....	473
Kapitel 6. Cyberwar und Datenschutz .....	516
Kapitel 7. Smart Metering und E-Mobility .....	533

## Teil VII. Datenschutz in Telemediendiensten, Telekommunikation, Internet und anderen Kommunikationsformen

Kapitel 1. Datenschutz im Internet .....	555
Kapitel 2. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen .....	568
Kapitel 3. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis .....	607
Kapitel 4. Datenschutz in der Telekommunikation .....	618
Kapitel 5. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten .....	644

## Teil VIII. E-Commerce

Kapitel 1. Kundendatenschutz .....	665
Kapitel 2. Bonitätsbewertung .....	674
Kapitel 3. Opt-in/Opt-out .....	694
Kapitel 4. Datenweitergabe an Handelspartner und Offenlegungspflichten; Shophosting .....	711
Kapitel 5. Online-Zahlungsverkehr .....	742

## Teil IX. Datenschutz im Gesundheitssektor

Kapitel 1. Umgang mit Patientendaten .....	761
Kapitel 2. Elektronische Patientenakte .....	793
Kapitel 3. Telemonitoring .....	806

## Teil X. Information als Wirtschaftsgut

Kapitel 1. Adresshandel .....	819
Kapitel 2. RFID, Smartcards und Cookies .....	833
Kapitel 3. Werbung im Internet .....	850
Kapitel 4. Bewertungsportale .....	869
Kapitel 5. Datenschutzkonformer Einsatz von Suchmaschinen und ihrer Zusatzdienste im Unternehmen .....	876

# beck-shop.de

Inhaltsübersicht	IX
<b>Teil XI. Datensicherheit</b>	
Kapitel 1. Technische und organisatorische Maßnahmen .....	895
Kapitel 2. Schutz von Betriebs- und Geschäftsgeheimnissen .....	915
<b>Teil XII. Konfliktmanagement im Datenschutz</b>	
Kapitel 1. Strategie und Taktik im Umgang mit Datenschutzverletzungen ....	925
Kapitel 2. E-Discovery .....	934
Kapitel 3. Haftungsrisiken und deren Versicherung .....	956
<b>Teil XIII. Straftaten und Ordnungswidrigkeiten .....</b>	<b>983</b>
Sachverzeichnis .....	1001

**beck-shop.de**

## Inhaltsverzeichnis

	Seite
Vorwort .....	V
Bearbeiterverzeichnis .....	XLV
Abkürzungsverzeichnis .....	XLIX

### Teil I. Allgemeine datenschutzrechtliche Grundlagen und Strukturen

#### Kapitel 1. Entwicklung des Datenschutzes in der Informationsgesellschaft

<b>A. Entwicklung des Datenschutzes</b> .....	4
I. BDSG .....	4
II. Weitere Kodifikationen und europäische Regelungen .....	6
1. Kompetenz .....	9
2. Errungenschaften .....	9
III. Recht auf informationelle Selbstbestimmung .....	9
<b>B. Zum Stand des Datenschutzrechts</b> .....	11
I. Allgemeines .....	11
II. BDSG .....	12
1. Anwendung .....	12
2. Adressat .....	12
3. Begriffe, Definitionen .....	13
4. Verbotprinzip .....	13
5. Aufgabe und Zweck des BDSG .....	14
<b>C. Modernisierungsbedarf</b> .....	15
I. Modernisierungsbedarf aufgrund der Rechtsprechung .....	15
1. Innerer Bereich der Zurückgezogenheit .....	15
2. Zweckbindung .....	15
3. Recht auf informationelle Selbstbestimmung .....	16
II. Modernisierungsbedarf aufgrund der sonstigen Entwicklung .....	21
1. Ansätze, Materialien .....	21
2. EU: Digitale Agenda .....	22
3. USA-Impulse .....	22
4. Europarat .....	23
III. Unvollständiger Ansatz zum Beschäftigtendatenschutz (2009) .....	24
IV. Entwurf der Datenschutz-Grundverordnung vom 25.1.2012 .....	25
1. Grundbausteine .....	25
2. Neue Instrumente .....	26
3. Nicht eingelöste Vorgaben vom 4.11.2010 .....	27
4. Kritik .....	27

	Seite
V. Einzelne Aspekte der Defizite geltenden Rechts .....	28
1. Intransparenz .....	28
2. Technisch veraltet .....	28
3. Keine Berücksichtigung der Rechtsprechung(sentwicklung) .....	29
4. Zahnloses Gesetz, schwache Sanktion .....	29
5. BDSG keine Marktverhaltensregelung? .....	30
6. Nebeneinander der diversen Rechtsinstitute .....	30
D. Grundrecht auf Netzzugang .....	31
E. Informationsethik und Datenschutz .....	34
<b>Kapitel 2. Datenschutz im öffentlichen und nicht-öffentlichen Bereich</b>	
A. Datenschutzrechtlicher Regelungszweck und Normadressaten .....	39
I. Verfassungsrechtliches Differenzierungsgebot .....	40
1. Grundrechtliche Konkordanz .....	40
2. Normadressaten .....	41
II. Sachzusammenhang und Regelungskompetenz .....	41
1. Sachzusammenhang.....	41
2. Regelungskompetenz .....	42
B. Öffentliche und nicht-öffentliche Stellen als Normadressaten .....	42
I. Begriff der öffentlichen und nicht-öffentlichen Stelle .....	42
1. Abgrenzungsfragen .....	42
2. Öffentliche Unternehmen.....	44
3. Religionsgemeinschaften.....	44
4. Nicht-öffentliche Stellen .....	45
II. Auswirkungen auf die datenschutzrechtliche Regelungssystematik .....	45
C. Subsidiaritätsprinzip im Datenschutz .....	46
I. BDSG als Auffangregelung .....	46
II. Bereichsspezifische Vorschriften.....	46
1. Öffentlicher Bereich.....	46
2. Nicht-öffentlicher Bereich.....	47
<b>Kapitel 3. Die Europäische Dimension des Datenschutzes</b>	
A. Europarechtlicher Rahmen .....	51
I. Motivation .....	51
II. Gegenwärtiger Rechtszustand .....	51
1. Richtlinien .....	51
2. Sonstiges Sekundärrecht .....	52
3. Primärrecht .....	52
4. Weitere Normen und „Softlaw“ .....	56
III. Sekundärrechtlich determinierte europäische datenschutzrechtliche Grundsätze .....	57
1. Anwendbarkeit nur bei Personenbezug und nur bei natürlichen Personen .....	57

Inhaltsverzeichnis	XIII
	Seite
2. Verarbeitung nach Treu und Glauben (Art. 6 Abs. 1a DSRL) .....	57
3. Zweckbindungsgrundsatz (Art. 6 Abs. 1a und 1b DSRL) .....	57
4. Richtigkeit (Art. 6 Abs. 1d DSRL) .....	58
5. Datenvermeidung und Datensparsamkeit (Art. 6 Abs. 1c und 1e DSRL) .....	58
6. Unterscheidung sensible/nicht sensible Daten (Art. 7 und 8 DSRL) ....	58
7. Verbot mit Erlaubnisvorbehalt .....	58
8. Betroffenenrechte .....	59
9. Unabhängige Vorabkontrolle .....	59
IV. Aktuelle Entwicklungen de lege ferenda .....	59
1. Datenschutzgrundverordnung (DS-GVO) .....	59
2. Richtlinie .....	62
<b>B. Judikatur</b> .....	62
I. Lindqvist (C-101/01) .....	63
II. Österreichischer Rundfunk (C-465/00, C-138/01, C-139/01) .....	63
III. Vorratsdatenspeicherung (C-201/06) .....	63
IV. Markkinapörssi (C-73/07) .....	63
V. Datenschutzbeauftragter I (C-518/07) .....	63
VI. Rijkeboer (C-553/07) .....	63
VII. Datenschutzbeauftragter II (C-614/10) .....	64
VIII. Bavarian Lager (C-28/08 P) .....	64
IX. Agrarbeihilfen (C-92/09, 93/09) .....	64
X. ASNEF (C-468/10, C-469/10) .....	64
XI. Promusicae (C-275/06) .....	64
XII. Scarlet (C-70/10) .....	64
XIII. Vorratsdatenspeicherung (C-293/12, C-594/12, C-46/13) .....	64
<b>C. Internationale Vorgaben</b> .....	65
<b>D. Internationaler Datentransfer</b> .....	66
I. De lege lata .....	66
1. Datenverarbeitung durch eine inländische verantwortliche Stelle .....	67
2. Datenverarbeitung durch eine ausländische Stelle mit Sitz im EU-Ausland .....	67
3. Datenverarbeitung durch eine ausländische Stelle mit Sitz in einem Drittstaat .....	67
4. Übermittlung in einen Drittstaat .....	67
II. De lege ferenda .....	68
<b>Kapitel 4. Internationaler Datenschutz</b>	
<b>A. Einführung</b> .....	70
<b>B. Nordamerika</b> .....	71
I. USA .....	71

	Seite
II. Einige Konsequenzen .....	74
III. Kanada .....	75
<b>C. Asien .....</b>	<b>76</b>
I. Indien .....	76
II. Volksrepublik China/Hongkong .....	77
III. Japan .....	78
<b>D. Südamerika .....</b>	<b>79</b>
<b>E. Australien/Neuseeland .....</b>	<b>79</b>
<b>Kapitel 5. Der internationale Anwendungsbereich des BDSG</b>	
<b>A. Einführung .....</b>	<b>83</b>
I. Die kollisionsrechtliche Regelung des BDSG .....	83
II. Die Vorgaben der Datenschutzrichtlinie .....	83
III. Die Reform des europäischen Datenschutzrechts .....	84
IV. Anknüpfungsmerkmale und Kollisionsnorm des BDSG .....	85
<b>B. Unternehmen mit Sitz im EWR .....</b>	<b>87</b>
I. Sitz der verantwortlichen Stelle .....	87
1. Verantwortliche Stelle .....	87
2. Die Bestimmung des Sitzes der verantwortlichen Stelle .....	87
3. Die Maßgeblichkeit des Rechts am Sitz der verantwortlichen Stelle ...	89
II. Die Maßgeblichkeit der Niederlassung .....	89
1. Die Bedeutung der Belegenheit der Niederlassung .....	89
2. Begriff und Belegenheit der Niederlassung .....	90
3. Einzelfälle .....	96
4. Niederlassung und Websites .....	96
5. Niederlassungsbegriff und Cloud Computing .....	98
6. Datenverarbeitung durch Niederlassungen in Drittstaaten .....	98
<b>C. Unternehmen mit Sitz außerhalb des EWR .....</b>	<b>99</b>
I. Ort der Datenverarbeitung und anwendbares Datenschutzrecht .....	99
II. Belegenheit von Niederlassungen oder Rechnern im Inland .....	100
III. Datenverarbeitung über Websites .....	102
IV. Fremdgesteuerte Datenverarbeitung auf dem Rechner des Internet- nutzers .....	102
V. Erhebung von Daten im Inland bei grenzüberschreitender Kommunika- tion .....	103
VI. Nichtanwendung des BDSG auf Datentransit .....	104
<b>D. Überblick: Anwendbarkeit des BDSG in Fallgruppen .....</b>	<b>105</b>
I. Sitz des Unternehmens in Deutschland .....	105
II. Sitz des Unternehmens in einem anderen EWR-Staat .....	105
III. Sitz des Unternehmens in einem Drittstaat .....	105

**Teil II. Datenschutzorganisation**

**Kapitel 1. Betrieblicher Datenschutzbeauftragter**

<b>A. Bestellung des betrieblichen Datenschutzbeauftragten</b> .....	108
I. Bestellungspflicht .....	108
1. Allgemeines .....	108
2. Voraussetzungen .....	109
II. Ordnungsgemäße Bestellung durch Bestellsurkunde .....	110
1. Schriftlicher Vertrag .....	110
2. Zeitpunkt der Bestellung .....	111
3. Inhaltliche Gestaltung .....	111
4. Bestellung eines externen Datenschutzbeauftragten .....	111
5. Bestellung zum Konzerndatenschutzbeauftragten .....	112
6. Befristung der Bestellung .....	112
7. Mitbestimmung des Betriebsrats .....	112
III. Abberufung eines Datenschutzbeauftragten .....	113
1. Wichtiger Grund für die Abberufung .....	113
2. Arbeitsrechtliche Anforderungen an die Abberufung .....	114
3. Sonderfall: Fusionen und Übernahmen (M&A) .....	114
4. Abberufung eines externen Datenschutzbeauftragten .....	115
5. Abberufung auf Verlangen der Aufsichtsbehörde .....	116
IV. Sanktionen .....	116
<b>B. Anforderungen an den betrieblichen Datenschutzbeauftragten</b> .....	116
I. Erforderliche Fachkunde .....	116
1. Allgemeines .....	116
2. Juristische Kenntnisse .....	118
3. IT-Kenntnisse .....	119
4. Sonstige Fähigkeiten .....	120
II. Erforderliche Zuverlässigkeit .....	120
1. Allgemeines .....	120
2. Subjektive Kriterien .....	120
3. Objektive Kriterien/Interessenkollisionen .....	121
<b>C. Die rechtliche Stellung des Datenschutzbeauftragten im Unternehmen</b> .....	124
I. Weisungsfreiheit .....	124
II. Anbindung an die Unternehmensleitung .....	124
III. Benachteiligungsverbot .....	125
IV. Unterstützungspflicht .....	125
V. Besonderer Kündigungsschutz .....	126
<b>D. Aufgaben und Pflichten des betrieblichen Datenschutzbeauftragten</b> .....	126
I. Hinwirken .....	126
II. Unterstützung durch die Aufsichtsbehörde .....	127
III. Einzelne Aufgaben .....	127
IV. Verschwiegenheitspflicht .....	128
<b>E. Haftung des betrieblichen Datenschutzbeauftragten</b> .....	128



	Seite
<b>Kapitel 2. Datenschutzmanagement und Datenschutzprozesse</b>	
<b>A. Datenschutzmanagement und Datenschutzprozesse .....</b>	<b>130</b>
<b>B. Auswahl des Datenschutzbeauftragten: intern oder extern? .....</b>	<b>131</b>
<b>C. Datenschutzaudit und Bewertung des Datenschutzrisikos .....</b>	<b>132</b>
I. Erfassung aller datenschutzrelevanten Prozesse .....	133
II. Rechtliche Bewertung und Risikoanalyse.....	134
<b>D. Verfahrensverzeichnisse .....</b>	<b>135</b>
I. Öffentliches Verfahrensverzeichnis .....	135
II. Interne Verfahrensübersichten .....	136
<b>E. Implementierung von Datenschutzprozessen .....</b>	<b>138</b>
I. Prozess: Einbindung des Datenschutzbeauftragten bei neuen Verfahren .....	139
II. Prozess: Datenschutzrechtliche Prüfung .....	139
III. Prozess: Schulungen und Verpflichtung auf das Datengeheimnis .....	140
IV. Weitere Prozesse .....	140
<b>Kapitel 3. Selbstkontrolle und Datenschutzaufsicht</b>	
<b>A. Allgemeines, Aufgaben .....</b>	<b>142</b>
<b>B. Verhältnis der beiden Einrichtungen zueinander .....</b>	<b>144</b>
I. Unterstützung des Beauftragten .....	144
II. Befugnis der Aufsichtsbehörde zu Anordnungen .....	145
III. Abberufung .....	145
IV. Betretungsrechte .....	145
<b>C. Weitere Formen der Selbstkontrolle und der Fremdkontrolle .....</b>	<b>146</b>
I. Audit .....	146
II. DS-GVO .....	147
<b>D. Grundsätze, Instrumente .....</b>	<b>148</b>
<b>E. Der Betriebsrat als datenschutzrechtliche „Kontrollinstanz“ .....</b>	<b>150</b>
<b>Kapitel 4. Datenschutz und Zertifizierung</b>	
<b>A. Einführung .....</b>	<b>153</b>
<b>B. Selbstregulierung .....</b>	<b>154</b>
<b>C. Datenschutzaudit im BDSG .....</b>	<b>156</b>
<b>D. Besonderheiten bei Cloud Computing .....</b>	<b>159</b>
<b>E. Verhaltensregeln, Branchenregeln .....</b>	<b>159</b>
<b>F. Safe Harbor – eine Art Test .....</b>	<b>162</b>

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

	Seite
G. Pläne/Entwürfe .....	164
I. DS-GVO (E) .....	164
II. Datenschutzstiftung .....	165

## Teil III. Archivierung und Entsorgung

### Kapitel 1. Datenschutzkonzepte

A. Speicherpraxis zwischen Aufbewahrungs- und Löschpflicht .....	169
I. Fortschreitende Digitalisierung, billiger Speicherplatz und Auslagerung als Herausforderungen an die betriebliche Gedächtnisorganisation .....	169
II. Begriffe: Aufbewahrung, Archivierung, Speicherung, Ablage, Löschung, Vernichtung, Entsorgung .....	171
III. Schwierigkeiten der Phasenabgrenzung .....	174
IV. Praxis der Datenschutzbehörden .....	175
B. Archivierung .....	182
I. Bedeutung: Revisions- und IT-Sicherheit, IT-Compliance, E-Discovery, Beweisqualität von E-Mails .....	182
II. Rechtsgrundlagen .....	182
1. Datenschutzrechtliche Speicherbefugnis (§§ 28, 29, § 9, § 31 BDSG) .....	182
2. Handels- und steuerrechtliche Anforderungen, GoB, GoBS, GdPDU ..	183
3. Papierloses Büro, ersetzendes Scannen .....	189
4. Betriebliche Mitbestimmung .....	191
C. Entsorgung .....	192
I. Bedeutung .....	192
II. Gesetzliche Anforderungen an Löschung und Entsorgung von personenbezogenen Daten .....	193
1. Begriff des Löschens .....	193
2. Differenzierung nach Art des Datenträgers .....	194
3. Datenschutzrechtlicher Löschanpruch .....	195

### Kapitel 2. Technische und organisatorische Maßnahmen

A. Archivierung .....	198
I. Zentrale/dezentrale Archivierung .....	198
II. Langzeitarchivierung .....	199
1. Archivierung von Arbeitsprozessdaten .....	199
2. Archivierung digitaler Signaturen .....	200
III. Dokumentenmanagementsysteme .....	202
IV. Externe Archivierung .....	202
B. Entsorgung .....	203
I. Technische Lösungsverfahren .....	203
1. Löschen durch Überschreiben .....	203

	Seite
2. Magnetische Durchflutung und thermische Zerstörung .....	204
3. Mechanische Zerstörung .....	204
4. Unterstützung durch neue DIN 663 99 .....	207
II. Datenschutzgerechte Entsorgungskonzepte .....	207
III. Entsorgung durch Dienstleister .....	208
<b>Kapitel 3. Archivierung und Protokollierung als Problem des betrieblichen Datenschutzes</b>	
<b>A. Konflikt zwischen IT-Sicherheit/Revisionssicherheit und Datenschutz .....</b>	<b>210</b>
I. Erlaubte Privatnutzung .....	211
II. Rückgabe von Firmengeräten/Ausscheidensregelung .....	213
<b>B. Urheberrechtliche Zulässigkeit der Archivierung .....</b>	<b>214</b>
<b>C. Umgang mit Datenbeständen, insbesondere mit Altbeständen .....</b>	<b>215</b>
I. Cloud-Storage und Dokumentenmanagementsysteme in der Cloud .....	215
II. Big Data .....	216
<b>Teil IV. Datenschutz und Personal: Arbeitnehmer-/Beschäftigtendatenschutz</b>	
<b>Kapitel 1. Beschäftigtendatenschutz</b>	
<b>A. Einleitung .....</b>	<b>221</b>
<b>B. Kodifikation des Beschäftigtendatenschutzes .....</b>	<b>222</b>
<b>C. Datenschutzbezogene Betriebsvereinbarungen .....</b>	<b>224</b>
I. Datenschutzbezogene Betriebsvereinbarungen de lege lata .....	225
II. Datenschutzbezogene Betriebsvereinbarungen de lege ferenda .....	227
III. Kritik .....	227
<b>D. Fragerecht des Arbeitgebers .....</b>	<b>228</b>
I. Fragerecht des Arbeitgebers de lege lata .....	228
1. Arbeitsrecht .....	229
2. Datenschutzrecht .....	229
II. Fragerecht des Arbeitgebers de lege ferenda .....	232
1. Namen und Kontaktdaten .....	232
2. Fachliche und persönliche Qualifikation .....	232
3. Politische Meinungen und Gewerkschaftszugehörigkeit .....	232
4. Geschlecht, insbesondere Schwangerschaft .....	233
5. Gesundheit, Vermögensverhältnisse und Vorstrafen bzw. laufende Ermittlungsverfahren .....	233
6. Schwerbehinderten- und Gleichstellungseigenschaft .....	234
III. Kritik .....	234
<b>E. Datenabgleich zu Compliance-Zwecken .....</b>	<b>235</b>
I. Datenabgleich de lege lata .....	238

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

	Seite
1. Präventive Kontrollen; Verhinderung statt Aufdeckung .....	239
2. Aufdeckung von Ordnungswidrigkeiten und Vertragsverletzungen .....	239
II. Datenabgleich de lege ferenda .....	239
III. Kritik .....	240
<b>F. Videoüberwachung am Arbeitsplatz .....</b>	<b>240</b>
I. Videoüberwachung de lege lata .....	241
1. Videoüberwachung von Arbeitsplätzen in öffentlich zugänglichen Bereichen .....	241
2. Videoüberwachung von Arbeitsplätzen in öffentlich nicht zugänglichen Betriebsbereichen .....	241
II. Videoüberwachung de lege ferenda .....	242
III. Kritik .....	242

## Kapitel 2. „Bring Your Own Device“ und Datenschutz

<b>A. Einleitung .....</b>	<b>245</b>
<b>B. BYOD und die rechtlichen Implikationen .....</b>	<b>245</b>
I. Erscheinungsformen des BYOD .....	245
1. Nutzung privater IT zu dienstlichen Zwecken .....	246
2. Unechtes BYOD .....	247
II. BYOD im rechtlichen Kontext .....	247
1. Gewerbliche Schutzrechte .....	247
2. Arbeitsrecht .....	248
3. Handels- und steuerrechtliche Dokumentations- und Aufbewahrungspflichten .....	249
4. Datenschutz .....	249
III. BYOD und Datenschutz .....	249
1. Anwendbarkeit datenschutzrechtlicher Vorschriften .....	249
2. Kontrollrechte und -pflichten .....	251
3. Einführung des BYOD im Unternehmen .....	254
4. Skandalisierungspflicht .....	255
<b>C. Zusammenfassung .....</b>	<b>256</b>

## Kapitel 3. Datenschutz und Mitbestimmung

<b>A. Einleitung .....</b>	<b>258</b>
<b>B. Datenschutz und Mitbestimmung .....</b>	<b>259</b>
I. Der Schutz des allgemeinen Persönlichkeitsrechts als mitbestimmungsrechtliche Aufgabe .....	259
1. Datenschutzrechtliche Anknüpfungspunkte .....	259
2. Mitbestimmungsrechtliche Tatbestände .....	260
II. § 87 Abs. 1 Nr. 6 BetrVG als tatbestandliche Grundlage für die mitbestimmungsrechtliche Verankerung des Datenschutzes .....	263
III. Datenschutz innerhalb der Arbeitnehmervertretung .....	264

	Seite
IV. Verhältnis des Arbeitnehmerdatenschutzes nach dem BetrVG zum BDSG	265
1. Anwendbarkeit des BDSG – Subsidiaritätsgrundsatz .....	265
2. Möglichkeit der Verschlechterung .....	266
V. Betrieblicher Datenschutzbeauftragter und das Verhältnis zur Mitbestimmung .....	267
VI. Typische Regelungsmaterien für datenschutzrechtliche Betriebsvereinbarungen .....	267
<b>Kapitel 4. Sozialdatenschutz</b>	
<b>A. Bedeutung des Sozialdatenschutzes für Arbeitnehmer .....</b>	<b>272</b>
<b>B. Das System des Sozialdatenschutzes .....</b>	<b>272</b>
I. Rechtsgrundlagen .....	272
II. Sozialgeheimnis .....	273
III. Begriff der Sozialdaten .....	274
1. Allgemeines .....	274
2. In § 35 SGB I genannte Stellen .....	274
3. Zweckbindung .....	275
4. Betriebs- und Geschäftsgeheimnisse .....	275
5. Anonymisierte und pseudonymisierte Daten .....	276
6. Gutachten als Sozialdaten .....	277
IV. Verlängerter Sozialdatenschutz .....	277
V. Technische Vorkehrungen .....	278
<b>C. Erheben von Daten .....</b>	<b>280</b>
I. Begriff des Erhebens .....	280
II. Erhebung auf Grundlage einer Einwilligung .....	281
III. Erforderlichkeit der Erhebung .....	283
1. Allgemeines .....	283
2. Erhebung auf Vorrat .....	284
3. Die Erhebung spezifischer Daten .....	285
4. Unzulässige Erhebungsmethoden .....	286
<b>D. Auswirkungen auf Mitwirkungspflichten .....</b>	<b>287</b>
<b>E. Die Nutzung und Verarbeitung von Daten .....</b>	<b>288</b>
I. Speichern, Verändern, Nutzen von Daten .....	288
II. Übermitteln von Daten .....	289
1. Abgrenzung Übermittlung/Nutzung .....	289
2. Voraussetzungen einer Übermittlungsbefugnis .....	289
3. Verhältnismäßigkeit der Übermittlung .....	291
4. Aktenübersendung an Sozialgerichte .....	292
5. Übermittlungsbefugnis durch Einwilligung? .....	293
6. Übermittlung ohne Einwilligung oder normative Befugnis .....	294
7. Verantwortung für die Übermittlung .....	294
8. Übermittlungen ohne Ersuchen .....	294

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

	Seite
F. Erhebung, Verarbeitung und Nutzung von Sozialdaten im Auftrag .....	295
G. Der Anspruch auf Berichtigung, Löschung und Sperrung gemäß § 84 SGB X .....	297
H. Auskunftsanspruch .....	299
I. Der Datenschutzbeauftragte .....	300
J. Sanktionsnormen .....	301
K. Schadensersatz .....	302
I. Allgemeines .....	302
II. Haftung nach § 82 Satz 1 SGB X .....	303
III. Haftung nach § 82 Satz 2 SGB X .....	303
L. Datenschutz im sozialgerichtlichen Verfahren .....	305
I. Geltung des Datenschutzes auch im Gerichtsverfahren .....	305
II. Die in Betracht kommenden Datenschutznormen .....	305
III. Datenschutz innerhalb desselben Gerichts .....	306
IV. Übermittlung von Daten außerhalb des Sozialgerichtsprozesses .....	307
V. Konsequenzen von Verstößen gegen das Recht auf informationelle Selbstbestimmung .....	307

## Kapitel 5. Compliance und Datenschutz

A. Einführung .....	311
B. Der Begriff Compliance .....	313
I. Verwendung in Normen .....	313
II. Definition Compliance und Abgrenzung zu Governance .....	314
C. Compliance und Datenschutz .....	316
I. Rechtsgrundlagen .....	316
II. Verantwortlichkeit .....	319
1. Meldung – Verfahrensverzeichnis .....	319
2. Vorabkontrolle .....	320
3. Betrieblicher Datenschutzbeauftragter .....	320
4. Auftragsdatenverarbeitung .....	321
D. Datenschutz bei Governance .....	322
E. Folgen fehlender Beachtung datenschutzrechtlicher Regelungen .....	323

## Teil V. Datenschutz in Betrieb, Unternehmen und Konzern

### Kapitel 1. Konzerndatenschutz

A. Einleitung .....	328
B. Grundlagen des Konzerndatenschutzes .....	329

	Seite
I. Fehlendes Konzernprivileg .....	329
II. Datenübermittlungsverbot mit Erlaubnisvorbehalt .....	331
<b>C. Datenschutzkonforme Ausgestaltung von Datenweitergaben im Konzern .....</b>	<b>331</b>
I. Auftragsdatenverarbeitung .....	331
II. Datenübermittlungen im Rahmen von Funktionsübertragungen .....	332
1. Übermittlung von Beschäftigtendaten im „konzerndimensionalen Arbeitsverhältnis“ .....	333
2. Übermittlung von Beschäftigtendaten im Rahmen von Funktions- übertragungen .....	335
3. Übermittlung besonderer Arten personenbezogener Daten .....	336
III. Datenübermittlungen auf Basis von Betriebsvereinbarungen .....	337
IV. Datenübermittlungen auf Basis von Einwilligungen .....	337
<b>D. Datenweitergaben bei Umstrukturierungen und Umwandlungen .....</b>	<b>338</b>
I. Betriebsübergang .....	338
II. Due Diligence-Prüfungen .....	338
III. Umwandlungen (Verschmelzung, Abspaltung etc.) .....	338
<b>E. Fallgruppen praxisrelevanter Datenübermittlungen und -verarbeitungen    im Konzern .....</b>	<b>339</b>
I. Organisationsbezogene Datenübermittlungen .....	339
1. Konzernweites Kommunikationsverzeichnis .....	339
2. Matrix-Strukturen .....	340
3. Aufteilung von Produktions- und Arbeitsprozessen .....	340
4. Zentralisierung von Compliance-Funktionen .....	340
II. Zentralisierung von Human Resources-Aufgaben .....	341
1. Lohn- und Gehaltsabrechnung .....	341
2. Zentrale Personalverwaltung .....	341
3. Konzernübergreifende Skill-Datenbanken .....	343
III. Sonstige Shared Services .....	344
1. IT-Leistungen .....	344
2. Werbe- und Marketingleistungen .....	344
3. Übermittlung von Kundendaten .....	344
<b>F. Internationale Datentransfers .....</b>	<b>345</b>
<b>Kapitel 2. Internationaler Datenverkehr</b>	
<b>A. EU-Datenschutz für den Datentransfer ins Ausland .....</b>	<b>347</b>
<b>B. Datenschutz im Geschäftsverkehr mit den Vereinigten Staaten/außerhalb    der EU .....</b>	<b>349</b>
1. Safe Harbor Framework .....	350
2. Standardvertragsklauseln .....	353
3. Binding Corporate Rules (BCR) .....	355

Inhaltsverzeichnis	XXIII
	Seite
C. Outsourcing .....	356
D. Vertragsgestaltung im internationalen Datenverkehr .....	357
 <b>Kapitel 3. Compliance-Organisation und Whistleblowing im Konzern</b>	
A. Einleitung .....	363
B. Allgemeine Vorgaben für eine Compliance-Organisation .....	364
C. Elektronische Systeme zur präventiven Compliance .....	365
I. Verpflichtung zur Vorhaltung von Systemen und Daten? .....	366
1. Allgemeine Compliance-Vorgaben .....	366
2. Vorgaben für Banken, Versicherungen und Wertpapierdienstleistungsunternehmen .....	366
II. Allgemeine Vorgaben zum Zugriff auf Daten bei Datenabgleichen .....	367
1. Vorgaben des BDSG zur präventiven Compliance .....	368
2. Datenabgleiche beschränkende Sondernormen .....	370
3. Mitbestimmungsrecht des Betriebsrats .....	371
4. Pflicht zur Information des betrieblichen Datenschutzbeauftragten ...	372
5. Pflicht zur Information des/der betroffenen Arbeitnehmer(s) .....	372
6. Sanktionen bei Verletzung des Datenschutzrechts .....	372
III. Empfehlungen für die Praxis .....	373
1. Begrenzungen des automatisierten Datenabgleichs .....	373
2. Trennung von dienstlichen und privaten E-Mails .....	375
3. Abschluss von Betriebsvereinbarungen .....	376
D. Whistleblowing-Systeme .....	377
I. Einleitung .....	377
II. Aufbau eines Whistleblowing-Systems .....	377
III. Inhaltlicher Anwendungsbereich .....	378
IV. Datenschutzrechtliche Vorgaben .....	379
1. Einwilligung .....	379
2. Grundsätzliche Anforderungen an Aufnahme und Verarbeitung von Hinweisen .....	379
3. Anonymität des Hinweisgebers .....	381
4. Einbindung eines externen Ombudsmanns .....	382
5. Übermittlung an andere Konzerngesellschaften .....	382
6. Sonstige datenschutzrechtliche Anforderungen .....	383
7. Einbindung des Datenschutzbeauftragten .....	383
8. Einbindung des Betriebsrats und Betriebsvereinbarung .....	383
V. Empfehlungen für die Praxis .....	384
E. System zur Security Breach Notification nach § 42a BDSG .....	385
F. Stellung des Datenschutzbeauftragten im Verhältnis zum Compliance-Beauftragten .....	385
I. Einleitung .....	385



	Seite
II. Rechtliche Anforderungen an Aufgabe und Stellung des Datenschutzbeauftragten .....	386
III. Rechtliche Anforderungen an Aufgabe und Stellung des Compliance-Beauftragten .....	387
IV. Bewertung .....	388
<b>Kapitel 4. Datenschutz in der Unternehmenstransaktion</b>	
<b>A. Einleitung .....</b>	<b>391</b>
<b>B. Datenschutzrechtlicher Rahmen für die Übermittlung von personenbezogenen Daten an Interessenten und deren Berater .....</b>	<b>392</b>
I. Beschäftigtendaten .....	393
1. Einwilligung .....	393
2. Betriebsvereinbarungen .....	394
3. Zulässigkeit nach §§ 28, 32 BDSG .....	395
II. Kunden- und Lieferantendaten .....	396
III. Besondere personenbezogene Daten .....	396
IV. Durch Sondernormen geschützte Daten .....	397
V. Sanktionen bei Verletzung des Datenschutzrechts .....	397
<b>C. Übermittlung von personenbezogenen Daten im Rahmen der Due Diligence und Verhandlungen .....</b>	<b>398</b>
I. Grundsätze der Zulässigkeitsprüfung .....	398
II. Daten der Vorstände bzw. Geschäftsführer .....	400
III. Beschäftigtendaten .....	400
IV. Kunden- und Lieferantendaten .....	401
<b>D. Übermittlung von personenbezogenen Daten in der Phase zwischen Signing und Closing .....</b>	<b>401</b>
<b>E. Übermittlungen von personenbezogenen Daten nach dem Closing .....</b>	<b>402</b>
I. Share Deal .....	402
II. Asset Deal .....	403
III. Unternehmenserwerb durch Verschmelzung oder Abspaltung .....	404
<b>F. Vorbereitung der Unternehmenstransaktion .....</b>	<b>404</b>
I. Vorbereitung von Listen .....	405
II. Abschluss von Vertraulichkeitsvereinbarungen .....	405
1. Allgemeines .....	405
2. Drittlandstransfer .....	406
III. Abschluss eines Auftragsdatenverarbeitungsvertrags mit Datenraum- anbietern .....	406
IV. Einbindung des betrieblichen Datenschutzbeauftragten .....	407
V. Einbindung des Betriebsrats .....	407
VI. Benachrichtigung der Betroffenen .....	408

Inhaltsverzeichnis	XXV
--------------------	-----

Seite

## Teil VI. Outsourcing und neue Technologien als Herausforderung für den Datenschutz

### Kapitel 1. Outsourcing

A. Ausschreibung und Vergabe von Aufträgen	410
I. Begriff	410
II. Formen	411
III. Verhandlung, Auftragserteilung, Vergabe	413
IV. Cloud-Besonderheiten	414
V. Big Data	416
B. SLA-Gestaltung im Hinblick auf den Datenschutz	417
C. Transition und Betriebsübergang, Retransition	420

### Kapitel 2. Auftragsdatenverarbeitung

A. Nationale Auftragsdatenverarbeitung	424
I. Privilegierung nach § 11 i. V. m. § 3 Abs. 8 BDSG	424
II. „Funktionsübertragung“	427
III. Voraussetzungen, Maßgaben, Durchführung	428
1. Vertragsvorgaben BDSG 2009	428
2. Maßgaben	429
3. Vertrag	429
4. Zehn Punkte	429
5. Vertragsformulierung	430
6. Aufgaben und Formen	431
IV. Ausführungen zu den zehn Vertragspunkten im Einzelnen	434
1. Gegenstand und Dauer	434
2. Umfang, Art und Zweck	435
3. Technische und organisatorische Maßnahmen	435
4. Berichtigung, Löschung und Sperrung	435
5. Nach Abs. 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen	436
6. Berechtigung zur Begründung von Unterauftragsverhältnissen	436
7. Kontrollrechte des Auftraggebers	437
8. Mitzuteilende Verstöße	437
9. Umfang der Weisungsbefugnisse	437
10. Rückgabe überlassener Datenträger	438
V. Auswahl, Kontrolle	438
VI. Entsprechende Geltung von § 11 Abs. 1 bis 4 BDSG	441
VII. Beauftragter für den Datenschutz	443
B. Internationale Auftragsdatenverarbeitung	445
I. EU-Standardvertragsklauseln	445
II. BCR	446

	Seite
III. Safe Harbor .....	447
IV. Spezialprobleme .....	448
<b>Kapitel 3. Customer Relationship Management und Datenschutz</b>	
<b>A. Customer Relationship Management – Pflege und Profilbildung als betriebswirtschaftliches Instrument .....</b>	<b>451</b>
<b>B. CRM und Datenschutz .....</b>	<b>452</b>
I. Grundsatz .....	452
II. Gegenstand des CRM – personenbezogene Daten .....	453
III. Erfordernis der Einwilligung .....	453
IV. Hinweispflicht .....	455
V. Gesetzlicher Erlaubnistatbestand .....	455
1. Eigene geschäftliche Zwecke .....	456
2. Wahrung berechtigter Interessen der verantwortlichen Stelle .....	457
3. Allgemein zugängliche Daten .....	458
VI. Verarbeitung oder Nutzung zu Werbezwecken .....	459
1. CRM als Kundenbindungs- und Akquisemittel .....	459
2. Listenprivileg .....	460
3. Besondere Zweckbindung .....	460
VII. Datenpflege und -veredelung .....	461
1. Hinzuspeichern .....	461
2. Besondere Anforderungen an den Datenbestand infolge erweiterter Auskunftspflichten .....	461
<b>C. CRM im Konzern .....</b>	<b>462</b>
I. Konzernbegriff und fehlendes Konzernprivileg .....	462
II. Datenarten und Datenherkunft bei Übermittlungen im Konzern .....	464
III. Zusammenfassung .....	464
<b>Kapitel 4. Nachweispflicht für die Datenherkunft</b>	
<b>A. Herkunftsnachweis im Zusammenhang mit Auskunftsansprüchen .....</b>	<b>465</b>
I. Sinn und Zweck der Regelung .....	466
1. Herkunft der personenbezogenen Daten .....	466
2. Speicherverpflichtung aus § 34 Abs. 1 BDSG .....	466
II. Sonderregelung bei geschäftsmäßiger Übermittlung (§ 34 Abs. 1 Satz 3, 4 BDSG) .....	467
1. Auskunfts- und Speicherpflicht .....	467
2. Sonderregelung (§ 34 Abs. 1 Satz 4 BDSG) .....	467
<b>B. Herkunftsnachweis nach § 34 Abs. 1 lit. a BDSG .....</b>	<b>468</b>
I. Inhalt der Regelung .....	468
II. Problematik der Regelung – die Rijkeboer-Entscheidung des EuGH .....	469
III. Übergangsfrist (§ 47 BDSG) .....	470

Inhaltsverzeichnis	XXVII
--------------------	-------

	Seite
1. Inhalt der Regelung .....	470
2. Beschluss des Düsseldorfer Kreises vom 27.11.2009 .....	470
<b>C. Herkunftsnachweis gemäß § 9 BDSG .....</b>	<b>471</b>
I. Regelungsinhalt .....	471
II. Rechtsprechung und Bewertung .....	472
<b>D. Fazit.....</b>	<b>472</b>

## Kapitel 5. Cloud Computing

<b>A. Cloud Computing und Datenschutz .....</b>	<b>475</b>
I. Einführung, Definition, technische Hintergründe .....	475
1. Definition und Abgrenzung .....	475
2. Basis des Cloud Computing: Virtualisierung .....	476
3. Cloud-Modelle .....	477
4. Cloud Service-Typen .....	478
5. Aspekte der Datensicherheit .....	479
II. Cloud Computing und Datenschutz .....	481
1. Anwendbares Datenschutzrecht .....	481
2. Verlagerung von personenbezogenen Daten in die Cloud .....	482
3. Übermittlung der Daten ins Ausland .....	484
III. Lösungsansätze .....	484
1. Verschlüsselung von personenbezogenen Daten in der Cloud .....	484
2. Nutzung von Trusted Computing-Technologien .....	486
3. Nutzung von Private Clouds .....	487
IV. Fazit .....	487
<b>B. Transnationale Clouds .....</b>	<b>488</b>
I. Die transnationale Dimension des Cloud Computing .....	490
II. Anwendbares Datenschutzrecht bei transnationalen Clouds .....	490
1. Anwendbarkeit des BDSG auf Cloud Provider mit Niederlassung im Inland .....	492
2. In einem anderen EU-Mitgliedstaat belegener Cloud Provider .....	494
3. In einem Drittland belegener Cloud Provider .....	494
III. Auftragsdatenverarbeitung unter Beteiligung von Cloud Providern in Drittländern .....	495
1. Cloud Provider als Auftragnehmer in einem Drittland .....	495
2. Cloud Provider als Auftraggeber in einem Drittland .....	496
IV. Weitergabe personenbezogener Daten an Cloud Provider im Ausland .....	496
1. Voraussetzungen .....	497
2. Angemessenes Datenschutzniveau im Empfängerland .....	497
3. Kein angemessenes Datenschutzniveau im Empfängerland .....	497
4. Zulässigkeit der Übermittlung .....	503
<b>C. Entnetzung .....</b>	<b>504</b>
I. Grundsätzliche Erwägungen .....	504

	Seite
1. Zunehmendes Bedrohungspotential durch die zunehmende Vernetzung .....	504
2. Abschottung und Entnetzung als technisch-organisatorische Gegenstrategie .....	504
II. Abschottung und Entnetzung von Systemen als datenschutzrechtlich gebotene Maßnahme .....	507
1. Gesetzliche Bestimmungen zur IT-Sicherheit .....	507
2. Schutz und Entnetzung unternehmensinterner Systeme .....	510
3. Vernetzung mit externen Systemen, Outsourcing, Cloud Computing ..	515
<b>Kapitel 6. Cyberwar und Datenschutz</b>	
<b>A. Vernetzung</b> .....	518
I. Einführung .....	518
II. Gesetzliche Grundlagen .....	519
III. Code is Law .....	519
IV. Cyber-Terrorismus .....	520
<b>B. Der Datenschutzbezug, vor allem über Sicherheit und Prävention</b> .....	521
I. Informationssicherheit .....	521
II. Datenbevorratung .....	522
III. Cyberwar- und Spionageabwehr .....	523
IV. Aufgabenstellung .....	524
V. Sensible Schwachstellen .....	524
VI. Mitarbeiter .....	525
VII. Whistleblowing .....	527
VIII. Funktionsübertragung .....	527
IX. Sicherheitsüberprüfungen .....	528
<b>C. Haftung</b> .....	531
<b>Kapitel 7. Smart Metering und E-Mobility</b>	
<b>A. Einleitung</b> .....	534
<b>B. Grundlagen des Smart Metering und der E-Mobility</b> .....	535
I. Technische Grundlagen des Smart Metering und der E-Mobility .....	535
II. Wesentliche Anwendungsgebiete des Smart Metering und der E-Mobility ..	536
III. Sektorspezifische rechtliche Grundlagen des Smart Metering und der E-Mobility .....	537
<b>C. Datenschutz beim Smart Metering und der E-Mobility</b> .....	537
I. Art und Umfang der betroffenen personenbezogenen Daten .....	537
1. Art der betroffenen personenbezogenen Daten .....	538
2. Umfang der betroffenen personenbezogenen Daten .....	538
II. Mögliche Beteiligte und zum Datenumgang berechtigte Stellen .....	539

Inhaltsverzeichnis	XXIX
	Seite
1. Mögliche Beteiligte .....	539
2. Zum Datenumgang berechnete Stellen .....	539
III. Anwendbare allgemeine datenschutzrechtliche Grundsätze, insbesondere Direkterhebung sowie Datenvermeidung und -sparsamkeit .....	540
IV. Sektorspezifische datenschutzrechtliche Regelungen im Bereich des Smart Metering .....	541
1. Erhebung, Verarbeitung und Nutzung personenbezogener Daten .....	541
2. Auskunfts-, Einsichts- und Informationspflichten .....	544
3. Löschungspflichten und weitere Betroffenenrechte .....	546
4. Sanktionen .....	547
V. Besondere datenschutzrechtliche Probleme der E-Mobility .....	547
1. Bewegungsprofile .....	547
2. Authentifizierung und Datenübermittlung .....	547
D. Datensicherheit beim Smart Metering und der E-Mobility .....	548
I. Allgemein zu berücksichtigende Grundsätze der Datensicherheit .....	549
II. Spezielle Anforderungen an das Smart Meter Gateway .....	551
III. Spezielle Anforderungen an das Sicherheitsmodul .....	552

## Teil VII. Datenschutz in Telemediendiensten, Telekommunikation, Internet und anderen Kommunikationsformen

### Kapitel 1. Datenschutz im Internet

A. Internetregulierung in Deutschland .....	556
I. Vom IuKDG zum TMG .....	557
II. Personenbezug von IP-Adressen .....	558
1. Objektiver Personenbezug .....	558
2. Relativität des Personenbezugs .....	559
3. Infektionstheorie .....	561
4. Bewertung bei IPv6 .....	561
B. Das Telemediengesetz .....	562
I. Überblick .....	562
II. Anwendungsbereich .....	562
1. Begriff der Telemedien .....	562
2. Ausnahme für dienstliche Telemediennutzungen .....	563
III. Verhältnis zum BDSG .....	564
IV. Zentrale Vorschriften .....	564
1. Datenverarbeitungsverbot mit Erlaubnisvorbehalt .....	565
2. Spezielle Erlaubnisvorschriften .....	565
3. Einwilligung des Nutzers .....	565
4. Sonstige Sonderregelungen .....	566

	Seite
<b>Kapitel 2. Web 2.0, Mobile Apps und die datenschutzrechtlichen Anforderungen</b>	
<b>A. Einführung – Datenschutzrechtliche Besonderheit des Web 2.0</b> .....	569
<b>B. Rechtsverhältnisse und Konstellationen</b> .....	571
<b>C. Rechtsgrundlagen</b> .....	571
I. Europäische Rechtsgrundlagen .....	571
II. Deutsche Rechtsgrundlagen .....	572
1. Allgemeines Datenschutzrecht .....	572
2. Besonderes Datenschutzrecht .....	572
<b>D. Rechtliche Einordnung von Web 2.0-Diensten</b> .....	573
I. Telemediendienste .....	573
II. Telekommunikationsdienste .....	574
1. Übertragung lediglich beim selben Provider .....	574
2. Aufspaltung von Web 2.0-Dienstebündeln in Einzeldienste .....	575
3. Klassifizierung einzelner Dienste im Web 2.0 .....	575
III. Telekommunikationsgestützte Dienste (§ 3 Nr. 25 TKG) .....	576
IV. Rundfunk und telemedienrechtliche Vorschriften im RStV .....	577
V. Zusammenfassende Einordnung .....	577
VI. Zivilrechtliche Regelungen .....	578
<b>E. Personenbezogene Daten im Web 2.0</b> .....	578
<b>F. Datenschutzrechtliche Verantwortlichkeit im Web 2.0</b> .....	579
I. Erwägungen der Art.-29-Datenschutzgruppe .....	580
II. Einzelfälle im Web 2.0 .....	581
1. Plattformbetreiber .....	581
2. Plattformnutzer .....	582
3. Dritte (Anbieter von Software/Apps) .....	584
<b>G. Das datenschutzrechtliche Verhältnis zwischen Plattformbetreiber und Nutzer</b> .....	584
I. Die telemedienrechtlichen Anforderungen .....	584
1. Zulässigkeit der Datenverarbeitung durch den Plattformbetreiber .....	585
2. Einwilligung .....	591
3. Nutzungsvertrag, AGB und Privacy Policy (Datenschutzerklärung) ...	596
4. Sonstige Pflichten des Plattformbetreibers .....	597
II. Die telekommunikationsrechtlichen Anforderungen .....	599
III. Pflichten des Plattformbetreibers gegenüber Dritten (Betroffenen) .....	600
<b>H. Das datenschutzrechtliche Verhältnis zwischen Nutzern und anderen Nutzern/Dritten</b> .....	601
<b>I. Das datenschutzrechtliche Verhältnis zwischen Dritten und Nutzern (Apps und Mobile Apps)</b> .....	603
<b>J. Ausblick und Würdigung</b> .....	605

Inhaltsverzeichnis	XXXI
--------------------	------

Seite

## Kapitel 3. Social Communities und deren datenschutzrechtliche Auswirkungen auf die Unternehmenspraxis

A. Überblick	607
B. Einsatz als Marketing-Instrument	608
I. Technische und wirtschaftliche Rahmenbedingungen	608
II. Datenschutzkonforme Erhebung von Nutzerprofilen?	609
1. Anwendbarkeit deutschen Datenschutzrechts	609
2. Erhebung der Daten/Tracking	609
III. Nutzung als Marketing-Instrument	610
1. Datenverarbeitung im Auftrag (§ 11 BDSG)	611
2. Datenschutzrechtliche Zulässigkeit des „Like“-Button	611
3. Impressum	612
4. Datenschutzerklärung bei eigenen Social-Media-Netzwerken	612
IV. Inhaltskontrolle	612
C. Einsatz von Social-Media-Plattformen als Recruiting-Instrument	613
I. Rechtliche Rahmenbedingungen	613
1. Aktuelle Rechtslage	613
2. Frei zugängliche Quellen	613
3. Soziale Netzwerke	614
II. Zivilrechtliche Zugehörigkeit des Xing-Accounts	614
D. Schutz des Unternehmens vor Meinungsäußerungen Dritter	615
I. Rechtliche Rahmenbedingungen	615
II. Datenschutzrechtliche Aspekte	615
III. Social-Media-Policy	616

## Kapitel 4. Datenschutz in der Telekommunikation

A. Vorbemerkung	619
B. Wesentliche Regelungen des TKG zum Datenschutz	620
I. Grundsätzliche Anwendung (§ 91 TKG)	620
1. Einleitung	620
2. Adressaten des § 91 TKG	621
3. Lex specialis TKG	621
4. Zusammenfassung zu § 91 TKG	622
II. Datenübermittlung an ausländische nicht-öffentliche Stellen (vormals § 92 TKG 2004)	622
1. Einleitung	622
2. Adäquanzprinzip	622
III. Informationspflichten (§ 93 TKG)	623
1. Grundsätze der Informationspflichten	623
2. Inhalt der Informationspflichten	624
3. Wahlrecht bei Verkehrsdaten	625



	Seite
4. Auskunftsrecht juristischer Personen .....	626
5. Unentgeltlichkeit und Schriftlichkeit der Auskunft .....	626
6. Unrechtmäßige Erlangung von Daten .....	626
IV. Nutzung von Bestandsdaten gemäß § 95 TKG .....	626
1. Bestandsdatennutzung .....	626
2. Bestandsdaten .....	626
3. Speicherung von Bestandsdaten .....	627
4. Speicherung für Werbung, Marketing .....	627
5. Datenspeicherung nach Vertragsende gemäß § 95 Abs. 3 TKG .....	627
6. Vorlage eines amtlichen Ausweises .....	628
V. Verkehrsdaten (§ 96 TKG) .....	628
1. Fernmeldegeheimnis .....	628
2. Auswertung von Verkehrsdaten .....	629
3. Verwendung von Verkehrsdaten .....	629
4. Sonderproblem des § 101 UrhG .....	630
VI. Entgeltermittlung und -abrechnung (§ 97 TKG) .....	631
1. Grundsätze .....	631
2. Faktische Beweislastumkehr bei Löschung von Verkehrsdaten .....	632
3. Austausch von Daten zwischen Anbietern (Interconnection) .....	632
VII. Standortdaten (§ 98 TKG) .....	633
1. Einleitung .....	633
2. Notrufnummern und Standortdaten .....	634
VIII. Einzelverbindungs nachweis (§ 99 TKG) .....	634
1. EVN im Haushalt und in Betrieben/Behörden .....	634
2. Wahlrecht des Teilnehmers .....	634
IX. Störung von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten (§ 100 TKG) .....	635
X. Mitteilen ankommender Verbindungen (§ 101 TKG) .....	635
1. Einleitung .....	635
2. Verfahren „Fangen“ .....	636
XI. Rufnummernanzeige und -unterdrückung (§ 102 TKG) .....	637
XII. Automatische Anrufweiterschaltung (§ 103 TKG) .....	637
XIII. Teilnehmersverzeichnisse (§ 104 TKG) .....	637
XIV. Auskunftserteilung (§ 105 TKG) .....	638
XV. Telegrammdienst (§ 106 TKG) und Nachrichtenübermittlungssysteme mit Zwischenspeicherung (§ 107 TKG) .....	639
<b>C. Regelungen zur öffentlichen Sicherheit im Zusammenhang mit Datenschutz in der Kommunikation .....</b>	<b>639</b>
I. Technische Schutzmaßnahmen (§ 109 TKG) .....	640
II. Datensicherheit (§ 109a TKG) .....	641
III. Überwachungsmaßnahmen (§ 110 TKG) .....	642
IV. Daten für Auskunftersuchen (§ 111 TKG) und automatisiertes Aus- kunftsverfahren (§ 112 TKG) .....	642

Inhaltsverzeichnis	XXXIII
--------------------	--------

	Seite
V. Auskunftsverfahren/-ersuchen (§§ 113, 113a, 113b, 114 TKG) .....	643
VI. Kontrolle und Durchsetzung von Verpflichtungen (§ 115 TKG) .....	643

## Kapitel 5. Pflichten zur Herausgabe von und zur Auskunftserteilung über Daten

<b>A. Einleitung</b> .....	645
<b>B. Herausgabe von Daten für Auskunfts- und Verzeichnisdienste</b> .....	645
I. Inhalt des Herausgabeanspruchs .....	646
II. Arten der herauszugebenden Daten .....	646
III. Beachtung der Datenschutzvorschriften .....	647
<b>C. Auskünfte über Urheberrechtsverletzungen</b> .....	648
I. Voraussetzungen des Auskunftsanspruchs .....	648
1. Anspruchsberechtigte .....	649
2. Klageerhebung oder offensichtliche Rechtsverletzung .....	650
3. Tätigkeit in gewerblichem Ausmaß .....	650
4. Gerichtliche Anordnung bezüglich Verwendung von Verkehrsdaten ..	651
II. Verpflichtung zur Vorhaltung der Verkehrsdaten .....	655
1. Divergierende Judikatur zur Frage der Speicherpflicht auf Zuruf .....	655
2. Stellungnahme .....	656
3. Unvereinbarkeit der Speicherung von Verkehrsdaten auf Zuruf mit datenschutzrechtlichen Vorschriften .....	659
4. Beschränkung des Datenspeicherungsanspruchs auf konkrete Verbindungen .....	661
<b>D. Auskünfte an Sicherheitsbehörden</b> .....	662
I. Datenerhebungspflicht .....	662
II. Beauskunftung der Daten .....	663
1. Automatisiertes Auskunftsverfahren .....	663
2. Manuelles Auskunftsverfahren .....	663

## Teil VIII. E-Commerce

### Kapitel 1. Kundendatenschutz

<b>A. Einleitung</b> .....	666
I. Begriffsdefinition .....	666
II. Überblick .....	666
<b>B. Einzelne Regelungsbereiche</b> .....	666
I. Adresshandel und Werbung .....	666
1. Allgemeines .....	666
2. Regelungsüberblick .....	667
II. CRM-Systeme, Profilbildung und Data-Mining .....	667
1. Allgemeines/Problemstellung .....	667
2. Regelungsbereiche .....	667

	Seite
III. Online-Datenschutz und Webtracking .....	669
1. Online-Datenschutz .....	669
2. Webtracking .....	671
<b>Kapitel 2. Bonitätsbewertung</b>	
<b>A. Kreditwesengesetz .....</b>	<b>675</b>
I. Bonitätsbewertung und Risikosteuerung .....	676
1. Scoring, Rating, Adressausfallrisiko, Bonitätsbewertung .....	676
2. Verfahren der Bonitätsbewertung .....	677
II. Scorewert – ein personenbezogenes Datum .....	677
1. Bildung einer Vergleichsgruppe und der Bezug zum Betroffenen .....	677
2. Prognosedaten und deren Personenbezug .....	677
III. Abgrenzung zwischen BDSG und KWG .....	678
1. Anwendung Scoringvorschrift des BDSG .....	678
2. Subsidiaritätsprinzip des § 1 Abs. 3 BDSG .....	679
3. § 10 KWG als bereichsspezifische Vorschrift .....	679
IV. Anwendungsbereich des § 10 Abs. 1 Satz 3 bis 8 KWG .....	679
1. Verbot mit Erlaubnisvorbehalt und die Bedeutung des § 10 Abs. 1 Satz 3 KWG .....	679
2. Adressausfallrisiko .....	679
3. Interne Ratingsysteme .....	680
V. Normative Voraussetzungen für die Datenerhebung und -verwendung ....	680
1. Verantwortliche Stellen .....	680
2. Betroffener Personenkreis .....	680
3. Zweckbindung .....	680
4. Privilegierung der Entwicklung und Weiterentwicklung von Ratingsystemen .....	681
VI. Datenarten und Erhebungsquellen .....	681
1. Datenarten .....	681
2. Erhebungsquellen .....	682
3. Internet als allgemein zugängliche Quelle .....	683
4. Benachrichtigungspflicht .....	683
VII. Datenübermittlung .....	684
VIII. Zusammenfassung .....	684
<b>B. Bonitätsbewertung im Rahmen des BDSG .....</b>	<b>685</b>
I. Bedeutung und Wesen der Bonitätsbewertung im gegenwärtigen sozioökonomischen Rahmen .....	685
II. Rechtliche Beurteilung der Bonitätsbewertung aufgrund des BDSG .....	687
1. Persönlicher Anwendungsbereich .....	687
2. Überblick über die Rechtsgrundlagen .....	687
3. Einwilligung (§§ 4, 4a BDSG) .....	688
4. Zulässigkeitstatbestände für einen der Bonitätsbewertung dienenden Datenumgang (§§ 28 ff. BDSG) .....	689
5. Rechte des Betroffenen (§§ 33 ff. BDSG) .....	693

Inhaltsverzeichnis XXXV

Seite

## Kapitel 3. Opt-in/Opt-out

<b>A. Bedeutung des Themas</b> .....	695
I. Schlagwortfunktion der Begriffe .....	695
II. Allgemeine Charakterisierung der Begriffe .....	696
III. Datenschutzrechtliche Relevanz des Themas .....	696
IV. Wirtschaftliche Relevanz des Themas .....	697
1. Kundenbindungs- und Rabattsysteme .....	697
2. Soziale Netzwerke .....	697
V. Rechtspolitische Aspekte des Themas .....	698
<b>B. Rechtsgrundlagen</b> .....	698
I. Allgemeiner Hinweis .....	698
II. Regelungen des BDSG .....	698
1. Einwilligung als Zulässigkeitstatbestand .....	698
2. Die Regelung des § 28 Abs. 3 BDSG .....	699
3. § 4a Abs. 1 Satz 1 BDSG als Sedes Materiae der Diskussion .....	699
III. § 7 Abs. 2 UWG .....	700
IV. Einwilligungserklärung als AGB-Klausel .....	700
<b>C. Gang der BGH-Rechtsprechung</b> .....	700
I. Überblick .....	700
II. Wesentliche Erkenntnisse der „Payback“-Entscheidung .....	701
1. Darstellung der strittigen Klausel .....	701
2. Bewertung als „Opt-out“-Klausel .....	702
3. Unterscheidung zwischen datenschutzrechtlicher und wettbewerbsrechtlicher Einwilligung .....	702
4. Bewertung der datenschutzrechtlichen Einwilligung .....	703
5. Bewertung der wettbewerbsrechtlichen Einwilligung .....	704
6. Hinweis für die Praxis .....	704
III. Wesentliche Erkenntnisse der „Happy Digits“-Entscheidung .....	704
1. Darstellung der strittigen Klausel .....	704
2. Bewertung anhand der Regelungen des BDSG .....	705
IV. Konsequenzen der BGH-Rechtsprechung .....	705
<b>D. Meldungen an die SCHUFA</b> .....	706
<b>E. Verfahrensrechtliche Fragen</b> .....	706
I. Klagemöglichkeiten nach dem UKlaG .....	706
II. Nachweis des Vorliegens einer Einwilligung durch „Double-opt-in“ .....	707
III. Unsicherheiten aufgrund des Urteils des OLG München vom 27.9.2012 .....	709
<b>F. Ausblick auf die künftige Rechtsentwicklung</b> .....	710

	Seite
<b>Kapitel 4. Datenweitergabe an Handelspartner und Offenlegungspflichten; Shophosting</b>	
<b>A. Webshop-Lösungen als datenschutzrechtliche Herausforderung</b> .....	712
I. Thematische Einordnung .....	712
II. Shophosting und Webshop-Outsourcing als Geschäftsmodell .....	714
III. Möglichkeiten und Grenzen von Auftragsdatenverarbeitung .....	715
IV. Datenschutzrechtliche Vorgaben an Offenlegungspflichten .....	717
1. Nachbesserungsbedarf bei Auftragsdatenverarbeitungsverträgen zwischen Online-Händlern und ihren Dienstleistern .....	717
2. Nutzereinigilligungen selten wirksam .....	719
3. Unterrichtung gemäß § 13 Abs. 1 TMG („Datenschutzerklärung“) ...	725
4. Externe Links .....	729
<b>B. Typische Beispiele für Datenweitergabe an Partnerunternehmen im Rahmen von Webshops</b> .....	729
I. Datenübermittlung an Versanddienstleister .....	729
II. Datenübermittlung im Rahmen von Financial Supply Chain Management .....	731
1. Zahlungsdienstleister .....	732
2. Datenübermittlung an Auskunftteien und Scoring-Anbieter .....	732
3. Betrugsprävention mittels Device Profiling und Tippverhaltens- profilen .....	733
4. Debitorenmanagement, Datenübermittlung an Inkassoanbieter .....	735
III. Datenübermittlung zu Werbezwecken .....	736
1. E-Mail-Marketing durch Full-Service-Dienstleister .....	736
2. Web-Analyse mit Hilfe von Web-Analysediensten .....	737
3. Behavioral Targeting und Retargeting durch Werbenetzwerke .....	738
4. Social Media Plugins .....	739
<b>C. Best Practice-Ansätze; Gütesiegel</b> .....	740
I. Datenschuttsiegel .....	740
II. Shop-Gütesiegel .....	741
<b>Kapitel 5. Online-Zahlungsverkehr</b>	
<b>A. Anwendbarkeit des Bundesdatenschutzgesetzes</b> .....	743
I. Subsidiarität des BDSG .....	743
II. Telemediengesetz .....	743
1. Anwendungsbereich .....	743
2. Abgrenzung zum BDSG .....	744
III. Telekommunikationsgesetz .....	745
<b>B. Personenbezogene Angaben im Zahlungsverkehr</b> .....	745
I. Personenbezogene Daten .....	745
II. Maßstab für Bestimmbarkeit .....	746

	Seite
<b>C. Integration einer Zahlungsmethode</b> .....	747
I. Angebot der Zahlungsart durch den Händler direkt .....	748
1. Datenschutzhinweis und Einwilligung .....	748
2. Erstellung Datenschutzhinweis bzw. Einwilligung .....	750
3. Bestimmtheit/Transparenz/Hinweispflichten .....	750
4. Aufbau eines Datenschutzhinweises .....	752
5. Zeitpunkt .....	753
6. Form .....	754
7. AGB-Kontrolle .....	755
8. Freiwilligkeit der Einwilligung .....	756
9. Datenkommunikation mit Auskunfteien .....	756
10. Verbot automatisierter Entscheidungen .....	756
11. Scoring-Maßnahmen .....	758
12. Zusammenarbeit mit Dienstleistern und Auskunfteien .....	758
II. Einsatz von Fremdsystemen .....	759
1. Keine Auftragsdatenverarbeitung .....	759
2. Hinweispflichten des Händlers .....	760
<b>D. Rechtsfolgen bei Verstoß</b> .....	760
<b>E. Zuständigkeit der Datenschutzbehörde</b> .....	760

## Teil IX. Datenschutz im Gesundheitssektor

### Kapitel 1. Umgang mit Patientendaten

<b>A. Besondere Schutzbedürftigkeit von Patientendaten</b> .....	764
<b>B. Die ärztliche Schweigepflicht</b> .....	765
<b>C. Datenerhebung, Verarbeitung und Nutzung durch den Arzt</b> .....	767
I. Allgemeines .....	767
II. Speicherung .....	768
<b>D. Erhebung, Verarbeitung und Nutzung von ärztlichen Daten durch Dritte</b> ...	769
I. Erhebung durch Sozialversicherungsträger .....	769
II. Erhebung ärztlicher Daten durch Gerichte, insbesondere Sozialgerichte ..	773
1. Die Einholung ärztlicher Befundunterlagen bzw. Vernehmung von Ärzten als Zeugen .....	773
2. Einholung medizinischer Sachverständigengutachten .....	774
III. Erhebung von Patientendaten durch sonstige Dritte .....	774
IV. Datenspeicherung, -veränderung und -nutzung .....	776
V. Übermittlung ärztlicher Daten .....	778
1. Übermittlung von (einfachen) Patientendaten .....	778
2. Übermittlung von medizinischen Sozialdaten .....	779
VI. Übermittlung von medizinischen Sozialdaten für Forschung und Planung .....	782

	Seite
VII. Erhebung, Verarbeitung und Nutzung von Patientendaten als Sozialdaten durch private Dritte .....	786
VIII. Erhebung und Verarbeitung auf Grundlage einer Einwilligung? .....	787
IX. Übermittlung ohne Einwilligung oder normative Befugnis .....	790
X. Problem des § 200 SGB VII .....	791
<b>Kapitel 2. Elektronische Patientenakte</b>	
<b>A. Elektronische Patientenakte .....</b>	<b>793</b>
I. Ziele .....	794
II. Prinzipien .....	795
III. Gesundheitsdaten als sensible Daten .....	796
IV. Verantwortliche Stelle .....	797
V. Gesetzliche Erlaubnis .....	798
VI. Einwilligung .....	802
VII. Datensicherheit .....	803
<b>B. Fazit .....</b>	<b>805</b>
<b>Kapitel 3. Telemonitoring</b>	
<b>A. Einführung .....</b>	<b>806</b>
<b>B. Anwendungsgebiete .....</b>	<b>807</b>
<b>C. Rechtlicher Kontext .....</b>	<b>807</b>
I. Grundsätzlicher rechtlicher Rahmen .....	807
II. Relevante datenschutzrechtliche Gesetzgebung .....	808
<b>D. Verarbeitung personenbezogener Daten im Rahmen des Telemonitorings .....</b>	<b>809</b>
I. Daten und Akteure .....	809
II. Technische Infrastruktur .....	810
<b>E. Anforderungen an die Einhaltung des Datenschutzes beim Telemonitoring .....</b>	<b>811</b>
I. Zulässigkeit des Verfahrens .....	811
1. Verbot mit Erlaubnisvorbehalt .....	811
2. Die Einwilligungserklärung .....	812
II. Datenverarbeitung im Auftrag .....	813
1. Allgemeines .....	813
2. Schweigepflicht und Beschlagnahmeverbot .....	814
III. Technische und organisatorische Maßnahmen .....	815
<b>F. Würdigung und Ausblick .....</b>	<b>817</b>

## Teil X. Information als Wirtschaftsgut

### Kapitel 1. Adresshandel

A. Einleitung .....	820
B. Definition des Begriffs Adresshandel .....	820
I. Adressdaten .....	821
II. Sonstige Daten .....	821
C. Erlaubnistatbestände .....	822
I. Grundsatz .....	822
1. Rechtsgrundlagen .....	822
2. Praktische Umsetzung/Nutzung der Adressdaten zu Werbezwecken ...	822
II. Adresshandel gemäß § 28 Abs. 3 BDSG .....	823
1. Voraussetzung .....	823
2. (Berechtigter) Empfängerkreis .....	823
III. Adresshandel gemäß § 29 BDSG .....	829
1. Allgemeines .....	829
2. Grundsätze .....	829
3. Besonderheiten des Adresshandels nach § 29 BDSG .....	830
D. Fazit .....	832

### Kapitel 2. RFID, Smartcards und Cookies

A. RFID-Chips und Smartcards .....	834
I. Funktionsweise von RFID-Chips und Smartcards .....	835
1. RFID .....	835
2. Smartcards .....	835
3. Anwendungsgebiete .....	835
II. Datenschutzrechtliche Zulässigkeit des Einsatzes von RFID und Smartcards sowie damit verbundene Sicherheitsrisiken .....	836
1. Verarbeitung personenbezogener Daten .....	836
2. Einwilligung oder gesetzliche Erlaubnis für die Datenverarbeitung ...	837
3. Direkterhebungsgrundsatz .....	838
4. Datenschutzrechtliche Zulässigkeit typischer Anwendungsfälle .....	839
5. Aufklärungspflichten (insbesondere aus § 6c BDSG) und Haftungs- risiken .....	842
6. Technisch-organisatorische Maßnahmen gemäß § 9 BDSG .....	845
III. Aktuelle Entwicklungen .....	845
1. Selbstverpflichtung von RFID-Anwendungsbetreibern zur Daten- schutzfolgenabschätzung .....	845
2. Kennzeichnungspflicht nach der Textilkennzeichnungsverordnung ...	846
3. Reform des Beschäftigtendatenschutzes .....	846
B. Cookies .....	846
I. Definition: Cookies .....	846



	Seite
II. Informationspflichten nach § 13 Abs. 1 TMG .....	847
III. Verwendung personenbezogener Daten .....	847
IV. Zulässigkeit der Datenverwendung .....	848
V. (Nicht-)Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation .....	848
<b>Kapitel 3. Werbung im Internet</b>	
<b>A. Beispielhafte Darstellung einzelner Konzepte .....</b>	<b>851</b>
I. Vorbemerkung .....	851
II. Konzepte für eine werbliche Nutzung personenbezogener Daten .....	852
1. Nutzung eines vorhandenen Kundendatenbestandes .....	852
2. Anforderungen bei der Nutzung vorhandener Daten .....	853
3. Angebote zur Anreicherung vorhandener Daten .....	854
III. Methoden zur Umsetzung der Konzepte .....	854
1. Soziale Netzwerke am Beispiel von Facebook und Google+ .....	854
2. Webstatistik am Beispiel von Google Analytics .....	856
3. Der Fall easycash: Kundenprofile auf Basis von Zahlungsdaten .....	858
<b>B. Rechtliche Schwerpunkte aus der Sicht des Werbenden .....</b>	<b>860</b>
I. Klarnamen, Pseudonymisierung, Anonymisierung .....	860
1. Grundlagen .....	860
2. Rechtliche Konsequenzen .....	861
II. Werbung als (Mit-)Geschäftszweck von sozialen Netzwerken – die Erlaubnisnorm .....	862
1. Datenpool .....	862
2. Art der Daten .....	862
3. Erlaubnisnorm für Inhaltsdaten .....	862
4. Informierte Einwilligung .....	864
5. Grundsatz der Zweckbindung .....	864
III. Social Plugin .....	864
1. Funktionsweise .....	864
2. Datenschutzrechtliche Problematik bei direkter Einbindung .....	865
3. Rechtskonforme Gestaltung .....	865
IV. Analyse-Programme .....	866
V. Ausblick .....	867
<b>Kapitel 4. Bewertungsportale</b>	
<b>A. „Click-mich-an“: die neue soziale Währung .....</b>	<b>869</b>
<b>B. Bewertung im Internet in den Grenzen des Datenschutzes .....</b>	<b>871</b>
I. Allgemeine rechtliche Rahmenbedingungen .....	871
1. Meinungsfreiheit .....	871
2. Wettbewerbsrecht .....	871
3. Telemedienrecht .....	872

Inhaltsverzeichnis	XLI
--------------------	-----

	Seite
II. Datenschutz .....	872
1. Anwendbarkeit datenschutzrechtlicher Vorschriften .....	873
2. Verhältnis von TMG und BDSG .....	873
3. Datenerhebung .....	874
4. Berichtigung, Sperrung, Löschung .....	875
 <b>Kapitel 5. Datenschutzkonformer Einsatz von Suchmaschinen und ihrer Zusatzdienste im Unternehmen</b>	
A. Einführung .....	877
B. Das Geschäftsmodell von Google und warum das Unternehmen Daten sammelt .....	878
C. Vorbemerkungen zum Datenschutz bei Suchmaschinen .....	880
I. Internationale Anwendbarkeit der Datenschutzbestimmungen .....	880
II. Der Klassiker: Personenbezug der IP-Adresse .....	880
D. Einzelne Fallgestaltungen .....	882
I. Personenbezogene Mitarbeiterdaten auf der Website eines Unternehmens .....	882
1. Veröffentlichung von Mitarbeiterdaten auf der Website .....	882
2. Auffindbarkeit von Mitarbeiterdaten bei Suchmaschinen .....	884
II. Google Hacking .....	885
III. Googeln von Bewerbern .....	886
IV. Webtracking .....	888
1. Sinn, Anbieter und Funktionsweise .....	888
2. Rechtliche Rahmenbedingungen .....	888
V. Bereitstellen von Werbeflächen auf der Website eines Unternehmens .....	892
E. Ergebnis .....	893

## Teil XI. Datensicherheit

### Kapitel 1. Technische und organisatorische Maßnahmen

A. Einleitung .....	896
B. Erläuterungen .....	897
I. Begrifflichkeiten .....	897
II. Anforderungen des Gesetzgebers .....	898
1. Grundsatz der Erforderlichkeit .....	898
2. Grundsatz der Verhältnismäßigkeit .....	898
3. Datenschutzgerechte Organisation .....	899
4. Kontrollmaßnahmen der Anlage zu § 9 BDSG .....	899
5. Empfehlung der Verschlüsselung .....	910
C. Rechtsschutz und Verfahrensfragen .....	910

	Seite
<b>D. Kritische Würdigung</b> .....	910
1. Unbestimmtheit des Datenschutzgesetzes .....	910
2. Komplexität und Inkompatibilität der Kontrollmaßnahmen .....	912
3. Datenschutz als Managementaufgabe .....	913
4. Datenschutzkonzepte und Datenschutzmanagement („Datenschutzprozess“) .....	913
<b>Kapitel 2. Schutz von Betriebs- und Geschäftsgeheimnissen</b>	
<b>A. Einleitung</b> .....	916
<b>B. Erläuterungen</b> .....	918
I. Entstehung des Geheimnisschutzes .....	918
II. Spezielle Anforderungen aus § 91 AktG, § 43 GmbHG und § 25a KWG .....	918
III. Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen .....	918
1. Risikoanalyse .....	918
2. Technisch-organisatorische Maßnahmen .....	918
3. Geheimnisträger im Unternehmen .....	919
4. Geheimnisträger außerhalb des Unternehmens .....	919
5. Öffentliche Auslegungsverfahren und Behördenakte .....	919
IV. Rechtsschutz und Verfahrensfragen .....	920
1. Strafrechtlicher Schutz .....	920
2. Zivilrechtlicher Schutz .....	920
V. Kritische Würdigung .....	920
1. Konflikte mit dem Datenschutz .....	920
2. Zusammenspiel mit dem Datenschutz .....	922
<b>Teil XII. Konfliktmanagement im Datenschutz</b>	
<b>Kapitel 1. Strategie und Taktik im Umgang mit Datenschutzverletzungen</b>	
<b>A. Einleitung</b> .....	925
<b>B. Datenpanne</b> .....	926
I. Anwendungsbereich .....	926
II. Inhalt und Form der Information .....	927
III. Ordnungswidrigkeiten, Straftatbestand und Haftung .....	927
<b>C. Missachtung des Datenschutzes</b> .....	928
I. Straftatbestände und Ordnungswidrigkeiten .....	928
II. Screening und Whistleblowing .....	929
1. Screening .....	929
2. Whistleblowing .....	929
<b>D. Compliance, interne Revision und Datenschutzorganisation</b> .....	930
<b>E. Kommunikation bei Datenschutzkonflikten</b> .....	931
I. Überblick und Empfehlungen .....	931
II. Kommunikationsschema .....	931
<b>F. Fazit des Konfliktmanagements im Datenschutz</b> .....	932

Inhaltsverzeichnis	XLIII
--------------------	-------

Seite

## Kapitel 2. E-Discovery

<b>A. Einführung</b> .....	935
<b>B. Wichtige Begriffe</b> .....	936
<b>C. Praktische Durchführung der E-Discovery</b> .....	940
I. Identifizierungsphase .....	941
II. Sicherungsphase .....	941
III. Sichtungsphase .....	941
IV. Vorlegungsphase .....	941
<b>D. Rechtskonflikte und deren Lösung</b> .....	942
I. Ausgangslage: Interessens- und Rechtskonflikt für internationale Unternehmen .....	942
II. Art.-29-Datenschutzgruppe Stellungnahme 1/2009 .....	943
III. Lösungsansätze der französischen Datenschutzbehörde CNIL .....	944
IV. Lösungsansätze der Sedona Conference .....	945
V. Datenexporte aus Deutschland an eine US-Muttergesellschaft .....	946
VI. E-Discovery und Schiedsverfahren .....	947
<b>E. Handlungsstrategien für Unternehmen in der EU</b> .....	948
<b>F. Beispielfälle aus der US-Rechtsprechung</b> .....	951
I. Volkswagen AG v. Valdez, Texas Supreme Court, 16.11.1995 .....	951
II. Access Data Corporation v. ALSTE Technologies GmbH, U. S. District Court for the District of Utah, 21.1.2010 .....	952
III. In re Air Cargo Shipping Services Antitrust Litigation, Eastern District of New York, 29.3.2010 .....	952
IV. In Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation, U.S. District Court for the Eastern District of New York, 27.8.2010 .....	953
V. Sofaer Global Hedge Fund, Plaintiff, v. Brightpoint, Inc. and Robert J. Laikin, Defendants, U. S. District Court, Southern District of Indiana, 12.11.2010 .....	953
VI. Eastern District of Virginia – MeadWestvaco Corp. v. Rexam PLC, U. S. District Court, Eastern District of Virginia, 14.12.2010 .....	953
VII. SunTrust v. United Guaranty Residential Insurance Co. of North, U. S. District Court, Richmond, VA, 29.3.2011 .....	954
VIII. Heraeus Kulzer GmbH v. Biomet, Inc., U. S. Court of Appeals for the 7th Circuit, 24.1.2011 .....	954
IX. Pershing Pacific v. Marinemax, U. S. District Court, Southern District of California, 13.3.2013 .....	955

## Kapitel 3. Haftungsrisiken und deren Versicherung

<b>A. Das Schadenspotential bei Datenschutzverstößen in der modernen Wirtschaftsordnung</b> .....	959
---	-----

	Seite
<b>B. Bedeutung der Haftung</b> .....	960
<b>C. Haftung des Unternehmens</b> .....	961
I. Rechtsgrundlagen der Haftung (Überblick) .....	961
II. Deliktsrechtliche Haftung .....	961
1. Haftung aus schuldhafter gesetzeswidriger Datenverwendung nach § 7 BDSG .....	961
2. Haftung aus gesetzeswidriger automatisierter Datenverwendung durch öffentlich-rechtliche Unternehmen nach § 8 BDSG .....	968
3. Haftung aus schuldhaftem Rechtsverstoß nach § 44 Abs. 1 Satz 1 i. V.m. Satz 4 TKG .....	972
4. Haftung aus schuldhafter Datenschutzverletzung nach den allgemei- nen Regeln über unerlaubte Handlungen (§§ 823, 824, 826 BGB) .....	974
III. Zusammentreffen mehrerer Haftungsgründe – vorvertragliche, vertragliche und nachvertragliche Haftung .....	975
IV. Negatorische Haftung (Beseitigungs- und Unterlassungsanspruch) .....	976
V. Verjährung .....	978
VI. Mehrheit von Schädigern .....	978
VII. Freizeichnung – Verzicht .....	978
VIII. Streitigkeiten .....	978
<b>D. Haftung des betrieblichen Datenschutzbeauftragten</b> .....	979
<b>E. Haftung des Arbeitnehmers</b> .....	980
<b>F. Versicherung</b> .....	980

## Teil XIII. Straftaten und Ordnungswidrigkeiten

<b>A. Bedeutung</b> .....	984
<b>B. Sanktionsvorschriften des BDSG</b> .....	985
I. Blankettbestimmungen .....	985
1. Gesetzlichkeitsprinzip .....	986
2. Änderung der Ausfüllungsnorm .....	987
3. Irrtumsproblematik .....	987
II. Anwendbarkeit .....	988
III. Tatbestandsstrukturen und Rechtsfolgen .....	989
1. Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG .....	989
2. Ordnungswidrigkeiten nach § 43 Abs. 2 BDSG .....	989
3. Bemessung der Geldbuße .....	990
4. Straftatbestand des § 44 BDSG .....	990
5. Keine allgemeine Zugänglichkeit personenbezogener Daten .....	991
6. Präventives Verbot mit Erlaubnisvorbehalt .....	991
IV. Die Tatbestände des § 43 Abs. 2 BDSG .....	992
1. Unbefugtes Erheben und Verarbeiten (Nr. 1) .....	992

Inhaltsverzeichnis	XLV
	Seite
2. Unbefugtes Bereithalten zum Zwecke des Datenabrufs (Nr. 2) .....	992
3. Unbefugter Datenabruf (Nr. 3) .....	992
4. Erschleichen der Übermittlung von personenbezogenen Daten durch unrichtige Angaben (Nr. 4) .....	993
5. Verstöße gegen die besondere Zweckbindung von Daten (Nr. 5) .....	993
6. Verstoß gegen das Koppelungsverbot des § 28 Abs. 3b BDSG (Nr. 5a) .....	993
7. Verstoß gegen das Verarbeitungs- und Nutzungsverbot des § 28 Abs. 4 BDSG (Nr. 5b) .....	993
8. Deanonymisierung (Nr. 6) .....	994
9. Verstoß gegen die Mitteilungspflicht bei unrechtmäßiger Kenntnis- erlangung von Daten (Nr. 7) .....	994
V. Die Strafvorschrift des § 44 BDSG .....	994
<b>C. Konfliktfelder des betrieblichen Datenschutzes aus strafrechtlicher Sicht ....</b>	<b>996</b>
I. Überwachung und Störung des Telefonverkehrs .....	996
II. Überwachung des Schriftverkehrs .....	996
III. Überwachung des E-Mail-Verkehrs .....	997
1. Eingriff in das Fernmeldegeheimnis .....	997
2. Arbeitgeber als Telekommunikationsanbieter nach § 206 StGB und Betreiber von Empfangsanlagen nach § 89 TKG .....	997
3. Tatsituation bei einem Eingriff in das Fernmeldegeheimnis .....	998
4. Rechtfertigungsgründe .....	998
IV. Datenzugriff unter Überwindung einer Zugangssicherung .....	999
V. Videoüberwachung .....	999
<b>Sachverzeichnis .....</b>	<b>1001</b>

**beck-shop.de**