

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung .....</b>	<b>1</b>
<b>2</b>	<b>Cloud Computing .....</b>	<b>7</b>
2.1	Eigenschaften der Cloud .....	8
2.2	Beteiligte.....	10
2.3	Cloud-Dienste.....	11
2.4	Organisationsmodelle .....	14
2.5	Phasenmodell für rechtlich relevante Datenwege .....	15
<b>3</b>	<b>Cloud Computing für den Mittelstand .....</b>	<b>17</b>
<b>4</b>	<b>Normative Grundlagen des Datenschutzrechts.....</b>	<b>23</b>
4.1	Vereinte Nationen und OECD .....	23
4.2	Europarat .....	24
4.3	Charta der Grundrechte der Europäischen Union .....	26
4.4	Artikel 16 AEUV .....	28
4.5	Datenschutzrichtlinie .....	29
4.6	Deutscher Grundrechtsschutz .....	30
4.6.1	Recht auf informationelle Selbstbestimmung .....	30
4.6.1.1	Von der Sphärenbetrachtung zur Selbstbestimmung .....	31
4.6.1.2	Verwendungszusammenhang und Kontextabhängigkeit.....	32
4.6.1.3	Unsicherheit als gesellschaftliches Beteiligungshemmnis .....	34
4.6.1.4	Auswirkung auf Gleichordnungsverhältnisse .....	35
4.6.2	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme .....	36
4.7	Vorrang des unions-grundrechtlichen Datenschutzes? .....	38
4.7.1	Vorrang Europäischer Grundrechte aus Sicht des Europäischen Gerichtshofs .....	39
4.7.2	Eingeschränktes Vorrangverhältnis aus Sicht des Bundesverfassungsgerichts .....	39
4.7.3	Grundrechtsvorrang im Umsetzungsspielraum von Richtlinien .....	43
4.7.4	Umsetzungsspielräume in der Datenschutzrichtlinie .....	45
4.7.5	Verbleibender Anwendungsbereich für das Recht auf informationelle Selbstbestimmung.....	48
<b>5</b>	<b>Anwendungsbereich des einfachgesetzlichen Datenschutzrechts .....</b>	<b>51</b>
5.1	Sachlicher Anwendungsbereich.....	52
5.1.1	Einzelangaben.....	53

5.1.2	Persönliche und sachliche Verhältnisse einer Person.....	53
5.1.3	Natürliche Person.....	55
5.1.4	Bestimmte und bestimmbare Person.....	56
5.1.4.1	Bestimmte Person.....	56
5.1.4.2	Bestimmbare Person.....	57
5.1.4.2.1	Praktische Bestimmbarkeit.....	57
5.1.4.2.2	Aufwand-Nutzen-Relation.....	58
5.1.4.2.3	Veränderungen im Aufwand-Nutzen-Verhältnis.....	59
5.1.4.3	Relativität des Personenbezugs.....	60
5.1.4.4	Gegenmeinung: objektiver Personenbezug.....	63
5.1.4.5	Rechtliche Unmöglichkeit.....	64
5.1.4.6	Fortgeltung des relativen Ansatzes.....	65
5.1.5	Folgen für die Cloud.....	69
5.1.6	Anonymisierung.....	71
5.1.7	Pseudonymisierung.....	74
5.1.8	Kryptographische Verschlüsselung.....	75
5.1.8.1	Verschlüsselung.....	76
5.1.8.1.1	Symmetrische Verschlüsselung.....	76
5.1.8.1.2	Asymmetrische Verschlüsselung.....	78
5.1.8.1.3	Eingrenzung.....	78
5.1.8.2	Hashfunktionen.....	79
5.1.8.3	Technische Sicherheit der Kryptographie.....	80
5.1.8.4	Folgen für den datenschutzrechtlichen Personenbezug.....	82
5.1.9	Verschlüsselung in der Cloud.....	84
5.1.9.1	Richtwerte für die Verschlüsselung in der Cloud.....	85
5.1.9.2	Einfluss des Risikos zukünftiger Kryptoanalysen.....	86
5.1.9.2.1	Stand der Wissenschaft und Technik zur Risikoprognose im Umwelt- und Technikrecht.....	87
5.1.9.2.2	Risikoprognose bei Verschlüsselungen.....	90
5.1.9.2.3	Rechtssicheres Verschlüsseln de lege ferenda.....	91
5.1.9.2.4	Neuverschlüsselung und Verhinderung missbräuchlicher Datenkopien.....	94
5.1.10	Unverschlüsselte Verarbeitung von Daten.....	95
5.1.11	Datenversiegelung zum betreibersicheren Cloud Computing.....	96
5.1.11.1	Lösungsansatz Versiegelung.....	97
5.1.11.2	Bewertung und Folgen für den Personenbezug sowie die Anwendung des Datenschutzrechts.....	100
5.1.11.2.1	Datenübertragung und -verarbeitung.....	100
5.1.11.2.2	Risiken zukünftiger technischer Entwicklungen.....	104
5.1.11.2.3	Zugriff durch andere Stellen.....	106
5.1.11.3	Anforderungen an die Betreibersicherheit.....	108
5.1.12	Unverschlüsselbare Metadaten.....	109
5.2	Persönlicher Anwendungsbereich.....	111
5.2.1	Verantwortliche Stelle im Internet.....	111
5.2.2	Entscheidung über Zwecke und Mittel der Verarbeitung.....	112
5.2.3	Verantwortung mehrerer Akteure.....	113
5.2.3.1	Datenumgang des Anbieters zur Dienstbereitstellung und -erbringung.....	113
5.2.3.2	Datenumgang des Anbieters zu weiteren Zwecken.....	115

5.2.3.3	Kumulative oder kollektive Verantwortung.....	116
5.2.4	Folgen für das Cloud Computing.....	120
5.2.4.1	Die Cloud als Infrastrukturmiete .....	121
5.2.4.2	Die Cloud als Anwendungsumgebung.....	122
5.2.4.3	Die Cloud als selbstständig datenerhebender Dienst.....	124
5.2.4.4	Kollektive Verantwortung im Rahmen der Cloud .....	125
5.2.5	Auftragsdatenverarbeitung.....	127
5.2.5.1	Verantwortlichkeit in der Auftragsdatenverarbeitung.....	128
5.2.5.2	Auftragsdatenverarbeitung in Abgrenzung zur Funktionsübertragung .....	129
5.2.5.3	Weisungs- und Kontrollbindung der Vertragstheorie als neue Abgrenzungskriterien .....	131
5.2.5.4	Verhältnis der Auftragsdatenverarbeitung zu § 11 BDSG .....	134
5.2.5.5	Folgen für das Cloud Computing.....	137
5.2.6	Auswirkungen auf verschiedene Betroffenenkonstellationen .....	138
5.2.6.1	Verantwortung des Cloud-Nutzers gegenüber Betroffenen .....	138
5.2.6.2	Verantwortung des Cloud-Anbieters gegenüber Betroffenen .....	139
5.3	Räumlicher Anwendungsbereich .....	140
5.3.1	Einordnung in das Kollisionsrecht.....	140
5.3.1.1	Kollisionsvermeidung.....	141
5.3.1.2	Verhältnis zu allgemeinen Kollisionsnormen .....	142
5.3.1.3	Verhältnis zu Kollisionsnormen des Telemediengesetzes.....	143
5.3.2	Innereuropäische Kollisionsvermeidung.....	144
5.3.2.1	Abgeschwächtes Sitzlandprinzip .....	144
5.3.2.2	Niederlassung .....	145
5.3.2.3	Datenumgang im Rahmen der Niederlassung.....	146
5.3.2.4	Auftragsdatenverarbeitung in einem Mitgliedstaat .....	149
5.3.2.5	Folgen für das Cloud Computing.....	150
5.3.3	Anwendungsbereich bei Drittlandbezug .....	151
5.3.3.1	Richtlinienkonforme Auslegung.....	152
5.3.3.2	Mittel.....	153
5.3.3.3	Rückgriff auf Mittel als Gegenstand der Verantwortlichkeit .....	154
5.3.3.3.1	Serverstandort.....	155
5.3.3.3.2	Adressatentheorie .....	156
5.3.3.3.3	Schwächen der Adressaten- und Servertheorie.....	158
5.3.3.4	Folgen für das Cloud Computing.....	159
5.3.3.4.1	Übertragung von Daten durch den Cloud-Nutzer .....	159
5.3.3.4.2	Cloud-basierte Datenverarbeitung im Rahmen der Auftragsdatenverarbeitung .....	160
5.3.3.4.3	Bereitstellung und Betrieb von Infrastruktur durch den Cloud-Anbieter .....	160
5.3.3.4.4	Selbstständige Datenerhebung durch den Cloud-Anbieter beim Cloud-Nutzer.....	161
5.3.3.4.5	„Forum Shopping“ durch Gründung einer Niederlassung?.....	163
5.3.3.5	Anwendungsausnahme bei reiner Durchleitung.....	164
5.3.4	Durchsetzung.....	166
5.3.4.1	Benennung eines inländischen Vertreters .....	166
5.3.4.2	Datenschutzaufsicht.....	167
5.4	Anwendbarkeit des Telekommunikations- und Telemediengesetzes.....	168

5.4.1	Cloud Computing und Telekommunikationsgesetz .....	169
5.4.2	Cloud Computing und Telemediengesetz .....	171
5.4.3	Daten beim Cloud Computing .....	172
5.4.3.1	Verschiedene Datenkategorien .....	172
5.4.3.2	Bestandsdaten .....	172
5.4.3.3	Nutzungsdaten .....	173
5.4.3.4	Inhaltsdaten .....	173
5.4.4	Folgen für das Cloud Computing .....	174
5.4.4.1	Aufruf der Cloud-Webseite .....	174
5.4.4.2	Anmeldung und Registrierung .....	175
5.4.4.3	Nutzung des Cloud-Dienstes .....	176
5.4.4.3.1	Cloud als Infrastrukturdienst .....	176
5.4.4.3.2	Cloud als Softwaredienst .....	177
5.4.5	Keine Anwendbarkeit des Telekommunikations- und Telemediengesetzes auf den Datenumgang in der Cloud .....	180
<b>6</b>	<b>Datenschutzrechtliche Zulässigkeit .....</b>	<b>183</b>
6.1	Erfordernis einer Einwilligung oder einer gesetzlichen Erlaubnis .....	183
6.2	Gesetzliche Erlaubnistatbestände .....	184
6.3	Erhebung von Daten beim Betroffenen .....	186
6.4	Eigene Geschäftszwecke in Abgrenzung zu geschäftsmäßigem Handeln .....	190
6.4.1	Datenumgang durch den Cloud-Nutzer .....	192
6.4.2	Datenumgang durch den Cloud-Anbieter .....	194
6.4.3	Datenumgang in der Cloud für eigene Geschäftszwecke .....	197
6.5	Zulässigkeit des Datenumgangs zur Erfüllung eigener Geschäftszwecke .....	197
6.5.1	Erforderlichkeit für die Begründung, Durchführung oder Beendigung von Schuldverhältnissen .....	199
6.5.1.1	Datenumgang durch den Cloud-Nutzer .....	201
6.5.1.2	Datenumgang durch den Cloud-Anbieter .....	203
6.5.1.2.1	Umgang des Cloud-Anbieters ausschließlich mit Daten des Cloud-Nutzers als Betroffenen .....	204
6.5.1.2.2	Umgang auch mit Daten betroffener Dritter .....	206
6.5.1.3	Keine geeignete Rechtsgrundlage für das Cloud Computing .....	207
6.5.2	Datenumgang aufgrund berechtigter Interessen .....	208
6.5.2.1	Übermittlung von Daten in die Cloud durch den Cloud-Nutzer .....	212
6.5.2.1.1	Erforderlichkeit für die Wahrung berechtigter Interessen des Cloud-Nutzers ...	212
6.5.2.1.2	Abwägung mit schutzwürdigen Interessen des Betroffenen .....	216
6.5.2.1.3	Auswirkungen technisch-organisatorischer Maßnahmen zur Datensicherheit .....	219
6.5.2.1.3.1	Datenverschlüsselung .....	220
6.5.2.1.3.2	Datenversiegelung .....	221
6.5.2.2	Eröffnung eines Zugangs durch den Cloud-Nutzer .....	223
6.5.2.3	Datenumgang durch den Cloud-Anbieter .....	223
6.5.3	Umgang mit allgemein zugänglichen Daten .....	227

6.5.4	Zweckbindung und Zweckänderung.....	229
6.5.4.1	Zweckbindungsgrundsatz .....	229
6.5.4.2	Zweckänderung im Rahmen des Cloud Computing.....	231
6.5.4.2.1	Zweckänderung zur Wahrung berechtigter Interessen der verantwortlichen Stelle.....	232
6.5.4.2.2	Zweckänderung zur Wahrung berechtigter Interessen eines Dritten und staatlicher Stellen .....	233
6.5.4.2.3	Zweckänderung im Forschungsinteresse .....	234
6.5.4.2.4	Zweckänderung zur Werbung oder zum Adresshandel .....	236
6.5.5	Keine umfassende gesetzliche Grundlage zum Datenumgang in der Cloud .....	238
6.6	Einwilligung .....	239
6.6.1	Herleitung aus dem Recht auf informationelle Selbstbestimmung .....	240
6.6.2	Rechtsnatur der Einwilligung .....	241
6.6.3	Freiwilligkeit .....	242
6.6.3.1	Soziale Abhängigkeitsverhältnisse .....	243
6.6.3.2	Wirtschaftliches Ungleichgewicht .....	245
6.6.3.3	Kopplungsverbot .....	247
6.6.4	Informiertheit.....	250
6.6.5	Formulärmäßige Einwilligungen .....	251
6.6.6	Bestimmtheit.....	254
6.6.7	Formale Anforderungen.....	256
6.6.8	Folgen für die Einwilligung beim Cloud Computing.....	259
<b>7</b>	<b>Datenweitergabe im Rahmen der Auftragsdatenverarbeitung.....</b>	<b>263</b>
7.1	Auswahl und Kontrolle des Auftragnehmers durch den Auftraggeber .....	265
7.1.1	Sorgfältige Auswahl des Auftragnehmers .....	265
7.1.2	Überprüfung des Auftragnehmers.....	267
7.1.3	Auswahl und Kontrolle in der IT-basierten Auftragsdatenverarbeitung .....	268
7.1.3.1	Höchstpersönliche Vor-Ort-Kontrolle in herkömmlichen Rechenzentren .....	268
7.1.3.2	Umsetzungsprobleme im Cloud-Umfeld .....	270
7.1.3.3	Bewertung durch die jüngere Literatur .....	271
7.1.3.4	Gesetzesauslegung zur höchstpersönlichen Vor-Ort-Kontrolle .....	273
7.1.4	Selbstkontrolle durch den Auftragnehmer oder Fremdkontrolle.....	275
7.2	Weitere Anforderungen an den Auftraggeber .....	276
7.2.1	Dokumentation .....	276
7.2.2	Schriftliche Auftragserteilung.....	277
7.2.3	Zehn-Punkte-Katalog.....	278
7.2.3.1	Klauseldiktat des Cloud-Anbieters .....	279
7.2.3.2	Allgemeine Vertragsklauseln .....	279
7.2.3.3	Unterauftragsverhältnisse .....	281
7.2.3.4	Kontrollrechte und Duldungspflichten.....	283
7.2.3.5	Regelungen zum Vertragsende .....	284
7.2.4	Weisungsbindung .....	285

<b>8</b>	<b>Entwicklung einer rechtssicheren Zertifizierung de lege ferenda .....</b>	<b>287</b>
8.1	Rechtsunsicherheit trotz Zertifizierung.....	287
8.2	Reformen des Kontrollrechts als Reaktion auf die Rechtsunsicherheit.....	288
8.2.1	Veränderung der Verantwortungsstruktur.....	288
8.2.2	Rücknahme der Kontrollpflicht unter Einführung eines Haftungsregimes .....	289
8.2.3	Reform der Kontrollpflichten nach § 11 Abs. 2 S. 4 BDSG .....	289
8.3	Grundbedingungen eines zukünftigen Zertifizierungssystems.....	290
8.3.1	Zertifizierung als Gegenstand gestufter Prüfsysteme.....	290
8.3.2	Gesetzlich geregeltes Zertifikat statt privatwirtschaftlicher Standardisierung .....	291
8.3.3	Konformitätsbestätigende statt rein marktfördernder Zertifizierung.....	293
8.3.4	Prüfgegenstand und Prüfgruppen.....	295
8.3.4.1	Prüfgegenstand einer Zertifizierung.....	295
8.3.4.2	Bildung standardisierter Prüfgruppen .....	296
8.3.5	Konkretisierung der Prüfinhalte.....	297
8.3.5.1	Selbstregulatorische Ansätze .....	297
8.3.5.2	Gesetzliche Festlegung .....	298
8.3.5.3	Technische Normierung.....	299
8.4	Möglichkeiten der Ausgestaltung auf Grundlage bestehender Systeme .....	300
8.4.1	Ausgestaltung als privatrechtliches Testat in Anlehnung an die Wirtschaftsprüfung? .....	300
8.4.2	Ausgestaltung als Verwaltungsakt in Anlehnung an die Kraftfahrzeug-Hauptuntersuchung?.....	302
8.4.2.1	Prüfkriterien.....	303
8.4.2.2	Ablauf und Rechtsfolgen .....	303
8.4.2.3	Behördliche Zertifizierung durch Beliehene .....	305
8.4.3	Ausgestaltung als Konformitätsbewertung mit Vermutungswirkung in Anlehnung an das Umwelt- oder Produktsicherheitsrecht? .....	308
8.4.3.1	Prüfkriterien.....	311
8.4.3.2	Ablauf und Rechtsfolge .....	312
8.4.3.3	Abgrenzung zum Verwaltungsverfahren .....	314
8.4.4	Ausgestaltung als „freiwillige öffentlich-rechtliche Zertifizierung“ in Anlehnung an das Signaturrecht? .....	316
8.4.4.1	Freiwillige Akkreditierung nach dem Signaturgesetz .....	317
8.4.4.2	Vergleichbare Gestaltung der Auftragsdatenverarbeitung?.....	319
8.4.5	Gestaltungsoffenheit.....	320
8.5	Qualitätssicherung durch Akkreditierung und Ermächtigung .....	322
8.5.1	Akkreditierung am Beispiel des harmonisierten Produktsicherheitsrechts .....	323
8.5.2	Akkreditierung am Beispiel des Signaturrechts .....	324
8.5.3	Umsetzung der Akkreditierung für die Zertifizierung der Auftragsdatenverarbeitung.....	325
8.6	Chancen und Risiken der Auftragsdatenverarbeitung für die Cloud.....	327

<b>9</b>	<b>Internationales Cloud Computing</b> .....	<b>329</b>
9.1	Datenumgang innerhalb der EU und des EWR.....	330
9.2	Drittlandbezug .....	331
9.2.1	Drittlandbezug bei Auseinanderfallen des Sitzes der datenverarbeitenden Stelle vom Ort des Datenumgangs.....	331
9.2.2	Zulässigkeitsvoraussetzungen für den Datenexport in Drittländer.....	333
9.2.2.1	Zwei-Stufenprüfung.....	334
9.2.2.2	Angemessenes Datenschutzniveau .....	334
9.2.2.2.1	Regelbeispiel oder Tatbestandsmerkmal .....	334
9.2.2.2.2	Bezugspunkt der Angemessenheit.....	335
9.2.2.2.3	Angemessenheitsbeschlüsse der Europäischen Kommission.....	338
9.2.2.2.4	Folgerung für das Cloud Computing .....	340
9.2.2.2.5	Zur Angemessenheit des Datenschutzniveaus in den USA: Safe Harbor .....	341
9.2.2.3	Ausnahmen trotz nicht angemessenem Schutzniveaus .....	347
9.2.2.3.1	Gesetzlicher Ausnahmenkatalog.....	348
9.2.2.3.1.1	Einwilligung in den Datenexport .....	349
9.2.2.3.1.2	Weitere Ausnahmetatbestände .....	350
9.2.2.3.2	Ausreichende Garantien .....	351
9.2.2.3.2.1	Allgemeine Vertragsklauseln.....	352
9.2.2.3.2.2	Verbindliche Unternehmensregelungen.....	354
9.2.2.3.2.3	Standardvertragsklauseln .....	356
9.2.2.3.3	Bedingungen für den Cloud-Datenexport.....	358
9.2.3	Auswirkungen des Datenexports auf die allgemeinen Zulässigkeitstatbestände... ..	359
9.2.3.1	Zulässigkeit einer Übermittlung .....	359
9.2.3.2	Internationale Auftragsdatenverarbeitung.....	359
9.2.3.2.1	Richtlinienkonforme Auslegung.....	360
9.2.3.2.2	Analoge Anwendung .....	363
9.2.3.2.3	Modifizierte Interessenabwägung.....	365
9.2.3.2.4	Keine pauschale Zulässigkeitsfiktion .....	367
9.2.3.3	Internationale Unterauftragsverarbeitung .....	371
9.2.3.3.1	Fallgruppe 1: Auftragnehmer und Unterauftragnehmer in Drittländern .....	372
9.2.3.3.2	Fallgruppe 2: Auftraggeber und Auftragnehmer innerhalb der Europäischen Union und Unterauftragnehmer in einem Drittland .....	374
9.2.3.3.3	Sonderfall: unselbstständige Niederlassung oder eigener Server des inländischen Auftragnehmers im Drittland.....	378
9.2.3.4	Inländische Auftragsdatenverarbeitung bei Auftrag aus dem Drittland .....	379
9.2.4	Unüberwindbare Hürden für das internationale Cloud Computing? Herkömmlicher Regelungen als „Cloud-Stopper“? .....	380
9.2.5	Processor Binding Corporate Rules als Lösungsansatz für die Cloud?.....	381
<b>10</b>	<b>Cloud Computing und ausländische Behörden – Beispiel USA</b> .....	<b>389</b>
10.1	Erweiterte Zugriffsbefugnisse auf Daten nach dem „PATRIOT Act“ .....	389
10.1.1	Strafverfolgung nach dem Electronic Communications Privacy Act (ECPA) .....	389
10.1.2	Terrorismusbekämpfung und Geheimdiensttätigkeiten durch FISA-Anordnungen und National Security Letters (NSL).....	392

10.1.3	Zugriff auf Cloud-Server außerhalb der USA.....	394
10.2	Electronic Discovery (E-Discovery).....	397
<b>11</b>	<b>Betroffenenrechte .....</b>	<b>403</b>
11.1	Dispositionsverbot und Weiterleitungsgebot .....	404
11.2	Transparenzrechte.....	405
11.2.1	Benachrichtigung.....	405
11.2.2	Auskunft .....	409
11.2.3	Technische Umsetzung von Benachrichtigung und Auskunft in der Cloud.....	411
11.3	Gestaltungsrechte.....	412
11.3.1	Beschwerde.....	412
11.3.2	Widerspruch bei rechtmäßigem Datenumgang .....	413
11.3.3	Eingriffsrechte bei unrechtmäßigem Datenumgang.....	414
11.3.3.1	Berichtigung, Sperrung und Löschung .....	415
11.3.3.2	Berichtigung, Löschung und Sperrung beim Cloud Computing .....	416
11.3.3.3	Schadensersatz.....	418
<b>12</b>	<b>Technische und organisatorische Maßnahmen .....</b>	<b>421</b>
12.1	Erforderlichkeit und Verhältnismäßigkeit.....	422
12.2	Einzelne Maßnahmen nach der Anlage zu § 9 S. 1 BDSG .....	424
12.2.1	Organisationskontrolle.....	425
12.2.2	Zutrittskontrolle .....	426
12.2.3	Zugangskontrolle .....	427
12.2.4	Zugriffskontrolle.....	428
12.2.5	Weitergabekontrolle .....	429
12.2.6	Eingabekontrolle.....	430
12.2.7	Auftragskontrolle.....	431
12.2.8	Verfügbarkeitskontrolle.....	432
12.2.9	Trennungsgebot .....	432
12.2.10	Verschlüsselung.....	433
<b>13</b>	<b>Geheimnisschutz .....</b>	<b>435</b>
13.1	Strafbewahrter Berufsgeheimnisschutz.....	435
13.1.1	Geheimnisschutz und Bundesdatenschutzgesetz.....	436
13.1.2	Anvertrautes Geheimnis .....	438
13.1.3	Offenbarung durch Nutzung der Cloud.....	439
13.1.3.1	Tathandlung.....	440
13.1.3.2	Taterfolg .....	442
13.1.3.3	Keine Offenbarung durch sichere Verschlüsselung .....	444
13.1.4	Gehilfe und Auftragsdatenverarbeitung.....	444
13.1.4.1	Direktionsrecht und dienstorganisatorische Einbindung? .....	445

13.1.4.2	Weisungsbindung .....	446
13.1.4.3	Verbindung der Gehilfenstellung zur Auftragsdatenverarbeitung.....	447
13.1.5	Einwilligung als Befugnis zur Offenbarung?.....	449
13.1.6	Schutz betroffener Dritter .....	450
13.1.7	Verbleibende Risiken.....	451
13.2	Geschäfts- und Betriebsgeheimnisse nach § 17 UWG.....	453
<b>14</b>	<b>Europäische Reformbemühungen im Datenschutz.....</b>	<b>455</b>
14.1	Wechsel zur Verordnung .....	457
14.2	Anwendungsbereich .....	461
14.2.1	Persönlicher Anwendungsbereich.....	461
14.2.2	Sachlicher Anwendungsbereich.....	462
14.2.3	Räumlicher Anwendungsbereich.....	464
14.3	Zulässigkeit der Datenverarbeitung .....	465
14.3.1	Einwilligung .....	465
14.3.2	Erlaubnistatbestände .....	466
14.4	Auftragsdatenverarbeitung.....	466
14.5	Betroffenenrechte .....	468
14.6	Internationale Datenverarbeitungen.....	470
14.7	Technische und organisatorische Maßnahmen .....	471
14.8	Datenschutzaufsicht.....	472
<b>15</b>	<b>Rechtsverträgliches Cloud Computing.....</b>	<b>475</b>
15.1	Regulative Begrenzung der Cloud.....	475
15.2	Cloud-fördernde Funktion des Rechts .....	477
15.3	Rechtliche Technikgestaltung.....	479
	<b>Literaturverzeichnis .....</b>	<b>483</b>