

Inhaltsverzeichnis

Abkürzungsverzeichnis XIX

Abbildungsverzeichnis XXVI

Tabellenverzeichnis XXVII

1 Einführung 1

2 Versicherungsbetrug in der Kraftfahrzeug-Haftpflichtversicherung 4

2.1 Zivilrechtliche Haftung bei Straßenverkehrsunfällen 4

2.1.1 Haftung nach § 7 Abs. 1 StVG 6

2.1.2 Haftung nach § 18 Abs. 1 StVG 8

2.1.3 Haftung nach § 823 Abs. 1 und 2 BGB 9

2.2 Grundverständnis und Funktionsweise der Kraftfahrzeug-Haftpflichtversicherung 11

2.2.1 Kraftfahrzeug-Haftpflichtversicherung als Teil der Kraftfahrtversicherung 12

2.2.2 Schutzzweck der Kraftfahrzeug-Haftpflichtversicherung 13

2.2.3 Rechtsrahmen 15

2.2.3.1 Versicherungsvertragsrecht 15

2.2.3.2 Versicherungsaufsichtsrecht 16

2.2.3.3 Versicherungsunternehmensrecht 16

2.2.4 Versichertes Risiko 16

2.2.4.1 Primäre Risikobeschreibung 17

2.2.4.2 Sekundäre Risikobeschreibung 17

2.2.4.3 Tertiäre Risikobeschreibung 18

2.2.5 Beteiligte Personen und Rechtsbeziehungen 18

2.2.5.1 Versicherungsnehmer 19

2.2.5.2 Mitversicherte Personen 19

2.2.5.3 Geschädigter 19

2.2.6 Leistungen des Versicherungsunternehmens 20

2.2.6.1 Befriedigung von begründeten Schadensersatzansprüchen 21

2.2.6.2 Abwehr von unbegründeten Schadensersatzansprüchen 21

2.2.6.3 Ablauf der Schadensbearbeitung 21

2.3 „Crash for Cash“ – Versicherungsbetrug durch manipulierte Straßenverkehrsunfälle 23

2.3.1 Erscheinungsformen manipulierter Unfälle 24

2.3.1.1 Der fiktive Unfall 24

- 2.3.1.2 Der ausgenutzte Unfall 25
 - 2.3.1.3 Der provozierte Unfall 25
 - 2.3.1.4 Der gestellte Unfall 26
 - 2.3.2 Gelegenheitstäter und professionelle Täter 28
 - 2.3.3 Verbreitung und Schadensvolumen 28
 - 2.3.4 Geschädigte 29
- 3 Bekämpfung von Versicherungsbetrug mittels Big Data 31
 - 3.1 Grundzüge der Betrugsbekämpfung durch Versicherungsunternehmen..... 31
 - 3.1.1 Prävention..... 31
 - 3.1.2 Erkennung 32
 - 3.1.2.1 Bedeutung von Betrugsindikatoren 33
 - 3.1.2.2 Einsatz von Menschen und Technologie..... 37
 - 3.1.3 Aufarbeitung..... 38
 - 3.2 Betrugserkennung mittels Big-Data-Verfahren..... 40
 - 3.2.1 Grundlegendes zu Big Data..... 40
 - 3.2.1.1 Big Data als Beschreibung des Datenvorkommens 41
 - 3.2.1.1.1 *Volume* 41
 - 3.2.1.1.2 *Velocity* 43
 - 3.2.1.1.3 *Variety*..... 43
 - 3.2.1.1.4 *Veracity*..... 44
 - 3.2.1.1.5 *Value*..... 44
 - 3.2.1.2 Big Data als Beschreibung der Datenverarbeitung und -nutzung – insbesondere *Analytics* 46
 - 3.2.1.2.1 Einsatz von Algorithmen 47
 - 3.2.1.2.2 Analyseformen und -charakteristika..... 47
 - 3.2.1.2.3 Verhältnis zwischen Big Data und Künstlicher Intelligenz..... 50
 - 3.2.1.3 Big Data als Beschreibung der Technologielandschaft..... 50
 - 3.2.1.3.1 In-Memory Datenbanken..... 52
 - 3.2.1.3.2 MapReduce 53
 - 3.2.2 Konkrete Big-Data-Verfahren zur Erkennung von Versicherungsbetrug 54
 - 3.2.2.1 Überblick..... 54
 - 3.2.2.2 Soziale Netzwerkanalyse zur Erkennung von komplexen Betrugsnetzwerken 55
 - 3.2.2.2.1 Erkennung von Betrugsnetzwerken als Herausforderung für herkömmliche Technologien 56
 - 3.2.2.2.2 Grundlagen der sozialen Netzwerkanalyse und Graphentheorie 57

3.2.2.2.2.1	Mikroebene: Akteure	58
3.2.2.2.2.2	Mesoebene: Gruppen	61
3.2.2.2.2.3	Makroebene: Gesamtnetzwerk	63
3.2.2.2.3	Anwendung der sozialen Netzwerkanalyse auf konkrete Versicherungsfälle	63
3.2.2.2.3.1	Festlegung der Akteure und Beziehungen	63
3.2.2.2.3.2	Erkennung verdächtiger Teilnetzwerke	65
3.2.2.2.3.3	Erkennung verdächtiger Akteure	65
3.2.2.2.3.4	Aussteuerung und Visualisierung der Ergebnisse	66
3.2.3	Zusammenfassung	67
4	Rechtsrahmen des europäischen und nationalen Datenschutzrechts	68
4.1	Unionsrecht	70
4.1.1	Verfassungsrecht	70
4.1.1.1	Schutz personenbezogener Daten (Art. 8 GRCh)	71
4.1.1.1.1	Schutzbereich	72
4.1.1.1.2	Eingriff	72
4.1.1.1.3	Rechtfertigung	73
4.1.1.2	Achtung des Privat- und Familienlebens (Art. 7 GRCh)	73
4.1.1.2.1	Schutzbereich	73
4.1.1.2.2	Eingriff	74
4.1.1.2.3	Rechtfertigung	74
4.1.1.3	Adressaten und Drittwirkung	74
4.1.2	Einfaches Recht	75
4.1.2.1	Datenschutz-Grundverordnung	75
4.1.2.2	Bereichsspezifisches Datenschutzrecht	79
4.2	Bundesrecht	82
4.2.1	Verfassungsrecht	82
4.2.1.1	Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)	82
4.2.1.1.1	Schutzbereich	83
4.2.1.1.2	Eingriff	84
4.2.1.1.3	Rechtfertigung	84
4.2.1.2	Weitere Grundrechte	84
4.2.1.3	Adressaten und Drittwirkung	85
4.2.2	Einfaches Recht	85
4.2.2.1	Bundesdatenschutzgesetz	85

- 4.2.2.2 Bereichsspezifisches Datenschutzrecht..... 87
- 4.3 Landesrecht 88
- 4.4 Zusammenspiel zwischen europäischem und nationalem Datenschutzrecht und Prüfungsmaßstab 89
- 5 Anwendungsbereich der Datenschutz-Grundverordnung 91
 - 5.1 Sachlicher Anwendungsbereich (Art. 2 DS-GVO) 91
 - 5.1.1 Personenbezogene Daten als zentraler Anknüpfungspunkt 91
 - 5.1.1.1 „Alle Informationen“ 92
 - 5.1.1.2 „die sich auf [...] beziehen“ 93
 - 5.1.1.3 „identifizierte oder identifizierbare“ 94
 - 5.1.1.3.1 Identifiziertheit 95
 - 5.1.1.3.2 Identifizierbarkeit 96
 - 5.1.1.4 „natürliche Person“ 97
 - 5.1.1.5 Sonderkonstellationen 98
 - 5.1.1.5.1 Besondere Kategorien personenbezogener Daten 98
 - 5.1.1.5.2 Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten 100
 - 5.1.1.5.3 Anonyme Daten 102
 - 5.1.1.5.4 Pseudonyme Daten 104
 - 5.1.2 Ganz oder teilweise automatisierte Verarbeitung oder nichtautomatisierte Verarbeitung bei Speicherung in Dateisystem 105
 - 5.1.3 Keine Ausnahmetatbestände – Insbesondere Abgrenzung zur Richtlinie für Justiz und Inneres (JI-RL) 110
 - 5.2 Räumlicher Anwendungsbereich (Art. 3 DS-GVO) 111
 - 5.3 Persönlicher Anwendungsbereich – Steigende Komplexität bei Big-Data-Anwendungen..... 113
 - 5.3.1 Betroffene Person (Art. 4 Nr. 1 DS-GVO)..... 113
 - 5.3.2 Verantwortlicher (Art. 4 Nr. 7 DS-GVO) 115
 - 5.3.2.1 Geeigneter Akteur 115
 - 5.3.2.2 Entscheidungsmacht über Zwecke und Mittel 116
 - 5.3.2.2.1 Entscheidungsmacht aufgrund rechtlicher Umstände 117
 - 5.3.2.2.2 Entscheidungsmacht aufgrund faktischer Umstände 118
 - 5.3.2.3 Alleinige oder gemeinsame Verantwortlichkeit 119
 - 5.3.2.4 Folgen der Verantwortlichkeit 121
 - 5.3.3 Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) 123
 - 5.4 Zusammenfassung zur Anwendbarkeit der Datenschutz-Grundverordnung 126

6	Anforderungen der Datenschutz-Grundverordnung.....	128
6.1	Big Data und die Technologieneutralität der Datenschutz-Grundverordnung.....	128
6.2	Datenschutzgrundsätze in der Datenschutz-Grundverordnung.....	130
6.2.1	Die allgemeinen Verarbeitungsgrundsätze des Art. 5 DS-GVO – Datenschutzgrundsätze im engeren Sinne.....	130
6.2.2	Weitere Prinzipien und Charakteristika der Datenschutz-Grundverordnung – Datenschutzgrundsätze im weiteren Sinne.....	132
6.3	Rechtmäßigkeit.....	135
6.3.1	Rechtmäßigkeit nach Art. 6 DS-GVO.....	136
6.3.1.1	Einwilligung (Art. 6 Abs. 1 S. 1 a) DS-GVO).....	137
6.3.1.1.1	Wirksame Erteilung.....	138
6.3.1.1.1.1	Höchstpersönliche Erklärung?.....	138
6.3.1.1.1.2	Vorherige Erklärung.....	140
6.3.1.1.1.3	Unmissverständliche Erklärung.....	143
6.3.1.1.1.4	Freiwilligkeit.....	144
6.3.1.1.1.4.1	Kein Machtungleichgewicht.....	144
6.3.1.1.1.4.2	Keine Koppelung von Einwilligungen.....	145
6.3.1.1.1.4.3	„Generalklausel“ des EWG 42 S. 5 DS-GVO.....	147
6.3.1.1.1.4.4	Einräumung zusätzlicher Wahlmöglichkeiten.....	150
6.3.1.1.1.5	Bestimmtheit.....	151
6.3.1.1.1.6	Informiertheit.....	152
6.3.1.1.2	Kein Widerruf.....	154
6.3.1.2	Erforderlichkeit zur Vertragserfüllung oder zum Vertragsabschluss (Art. 6 Abs. 1 S. 1 b) DS-GVO).....	155
6.3.1.2.1	Vertrag mit betroffener Person.....	156
6.3.1.2.1.1	Versicherungsnehmer als betroffene Person.....	156
6.3.1.2.1.1.1	Einschränkung der Privatautonomie durch Versicherungspflicht.....	157
6.3.1.2.1.1.2	Teleologische Reduktion?.....	159
6.3.1.2.1.2	Mitversicherte Person als betroffene Person.....	160
6.3.1.2.1.3	Geschädigter als betroffene Person.....	160
6.3.1.2.1.3.1	Vertragliches Schuldverhältnis aufgrund Direktanspruch gemäß § 115 VVG?.....	161
6.3.1.2.1.3.2	Erstreckung von Art. 6 Abs. 1 S. 1 b) DS-GVO auf Dritte? ..	161
6.3.1.2.1.4	Zeuge als betroffene Person.....	162
6.3.1.2.2	Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung.....	162

- 6.3.1.2.2.1 Vertragserfüllung..... 163
 - 6.3.1.2.2.1.1 Abstrakte oder konkrete Vertragsinhalte als Maßstab? 163
 - 6.3.1.2.2.1.2 „Was ist versichert?“ (A.1.1.2 und A.1.1.3 AKB 2015) 164
 - 6.3.1.2.2.1.3 „Was ist nicht versichert?“ (A.1.5.1 AKB 2015) 165
 - 6.3.1.2.2.1.4 „Welche Pflichten haben Sie im Schadenfall?“ (E.1.1.3 AKB 2015) 166
- 6.3.1.2.2.2 Erforderlichkeit..... 167
 - 6.3.1.2.2.2.1.1 Geeignetheit..... 167
 - 6.3.1.2.2.2.1.2 Keine zumutbare mildere, gleich effektive Alternative... 169
 - 6.3.1.2.2.2.1.2.1 Subsidiarität der Betrugsprüfung 171
 - 6.3.1.2.2.2.1.2.2 Alternative Schadensregulierung mit definierten Kooperationspartnern 172
 - 6.3.1.2.2.2.1.2.3 Anonyme Daten..... 172
 - 6.3.1.2.2.2.1.2.4 Pseudonyme Daten 172
 - 6.3.1.2.2.2.1.2.5 Weniger schutzwürdige Daten 172
 - 6.3.1.2.2.2.1.2.6 Geringere Menge an personenbezogenen Daten 173
 - 6.3.1.2.2.2.1.2.7 Personenbezogene Daten aus öffentlich zugänglichen Quellen 173
 - 6.3.1.2.2.2.1.2.8 Genauere, aktuellere, vollständigere personenbezogenen Daten..... 173
 - 6.3.1.2.2.2.1.2.9 Geringere Anzahl an datenverarbeitenden Akteuren .. 174
 - 6.3.1.2.2.2.1.2.10 Geringere Anzahl an betroffenen Personen 175
 - 6.3.1.2.2.2.1.2.11 Geringere Anzahl an datenverarbeitenden Akteuren mit Drittstaatbezug 175
 - 6.3.1.2.2.2.1.2.12 Keine besonders risikobehaftete Datenverarbeitung 175
 - 6.3.1.2.2.2.1.2.13 Geringere Speicherdauer..... 176
 - 6.3.1.2.2.2.1.2.14 Seltener Datenverarbeitung 176
- 6.3.1.2.2.3 Ergebnis 176
- 6.3.1.3 Erforderlichkeit zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 S. 1 c) i.V.m. Abs. 2 und 3 DS-GVO)..... 176
 - 6.3.1.3.1 Rechtliche Verpflichtung des Verantwortlichen?..... 177
 - 6.3.1.3.1.1 Auskunftspflicht (§ 31 Abs. 1 und 2, § 119 Abs. 3 VVG) 177
 - 6.3.1.3.1.2 Hauptleistung (§ 100 VVG) 178
 - 6.3.1.3.1.3 Risikomanagement (§ 26 VAG)..... 179
 - 6.3.1.3.2 Ergebnis 179

6.3.1.4	Erforderlichkeit zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 S. 1 f) DS-GVO)	180
6.3.1.4.1	Berechtigtes Interesse des Verantwortlichen oder eines Dritten	181
6.3.1.4.2	Erforderlichkeit der Datenverarbeitung zur Wahrung des berechtigten Interesses	183
6.3.1.4.3	Kein Überwiegen der Interessen, Grundrechten oder Grundfreiheiten der betroffenen Person	183
6.3.1.4.3.1	Waagschale des Verantwortlichen	185
6.3.1.4.3.1.1	Bedeutung des berechtigten Interesses	185
6.3.1.4.3.1.1.1	Anerkennung durch Grundrechte	185
6.3.1.4.3.1.1.2	Anerkennung durch andere Rechtsinstrumente	186
6.3.1.4.3.1.1.3	Anerkennung durch Allgemeinheit	187
6.3.1.4.3.1.2	Bedeutung der Datenverarbeitung	188
6.3.1.4.3.2	Waagschale der betroffenen Person	189
6.3.1.4.3.2.1	Bedeutung des Interesses	189
6.3.1.4.3.2.2	Bedeutung der Datenverarbeitung – Das „3x5-Modell“	189
6.3.1.4.3.2.2.1	Erste Dimension: Daten	190
6.3.1.4.3.2.2.1.1	Personenbezug der Daten	190
6.3.1.4.3.2.2.1.2	Art der Daten	191
6.3.1.4.3.2.2.1.3	Menge der Daten	192
6.3.1.4.3.2.2.1.4	Quelle der Daten	195
6.3.1.4.3.2.2.1.5	Qualität der Daten	196
6.3.1.4.3.2.2.2	Zweite Dimension: Akteure	197
6.3.1.4.3.2.2.2.1	Menge der datenverarbeitenden Akteure	197
6.3.1.4.3.2.2.2.2	Menge der betroffenen Personen	198
6.3.1.4.3.2.2.2.3	Machtverhältnis zwischen dem Verantwortlichen und der betroffenen Person	199
6.3.1.4.3.2.2.2.4	Vernünftige Erwartungen der betroffenen Person	201
6.3.1.4.3.2.2.2.5	Drittstaatbezug eines datenverarbeitenden Akteurs	204
6.3.1.4.3.2.2.3	Dritte Dimension: Datenverarbeitung	205
6.3.1.4.3.2.2.3.1	Art der Datenerhebung	205
6.3.1.4.3.2.2.3.2	Art der Datenverarbeitung	205
6.3.1.4.3.2.2.3.3	Dauer der Datenspeicherung	207
6.3.1.4.3.2.2.3.4	Häufigkeit der Datenverarbeitung	207
6.3.1.4.3.2.2.3.5	Zwecke der Datenverarbeitung	208
6.3.1.4.3.2.2.4	Matrix zur Bedeutung der Datenverarbeitung	209

6.3.1.4.3.3	Abwägung im engeren Sinne.....	211
6.3.1.4.4	Widerspruchsrecht (Art. 21 DS-GVO).....	212
6.3.1.4.4.1	Voraussetzungen.....	213
6.3.1.4.4.2	Rechtsfolge.....	214
6.3.2	Besondere Verarbeitungssituationen – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DS-GVO).....	215
6.3.2.1	Anwendungsbereich.....	217
6.3.2.1.1	Entscheidung mit Rechtswirkung oder ähnlicher erheblicher Beeinträchtigung	218
6.3.2.1.2	Beruhens auf automatisierter Verarbeitung einschließlich Profiling	220
6.3.2.1.3	Ausschließlichkeit – Taxonomie durch das „Levels of Automation in Man-Computer Decision-Making“-Modell.....	222
6.3.2.2	Ergebnis.....	227
6.3.3	Ergebnis zur Rechtmäßigkeit	227
6.4	Treu und Glauben.....	228
6.5	Transparenz	229
6.5.1	Inhalt der zu erteilenden Information.....	230
6.5.1.1	Informationen zum Verantwortlichen	232
6.5.1.2	Informationen zur spezifischen Verarbeitung	233
6.5.1.3	Informationen zu den Betroffenenrechten.....	237
6.5.2	Zeitpunkt der Informationserteilung	237
6.5.3	Art und Weise der Informationserteilung.....	239
6.5.4	Ausnahmen von der Informationserteilung.....	243
6.5.4.1	Ausnahmen bei Direkterhebung nach Art. 13 DS-GVO.....	243
6.5.4.2	Ausnahmen bei sonstiger Erhebung nach Art. 14 DS-GVO.....	244
6.5.4.3	Ausnahmen bei Auskunftserteilung nach Art. 15 DS-GVO	244
6.5.4.4	Typische Herausforderungen bei Big-Data-Verfahren	245
6.5.4.4.1	Befreiung von Art. 13 und 14 DS-GVO wegen großer Menge betroffener Personen?.....	246
6.5.4.4.2	Befreiung von Art. 15 DS-GVO wegen großer Menge verarbeiteter personenbezogener Daten?.....	248
6.6	Zweckbindung.....	253
6.6.1	Zweckfestlegung	254
6.6.1.1	„festgelegte“ – Verbot von explorativen Datenanalysen und multifunktionaler Verwendung?.....	254
6.6.1.2	„eindeutige“.....	257
6.6.1.3	„legitime“	258

6.6.1.4 „Zwecke“ – Existenz einer Höchstanzahl von Verarbeitungszwecken?	258
6.6.2 Zweckbindung	259
6.6.2.1 Weiterverarbeitung zu identischen Zwecken	260
6.6.2.2 Weiterverarbeitung zu anderen Zwecken	260
6.6.2.2.1 Einwilligung	261
6.6.2.2.2 Rechtsvorschrift der Union oder der Mitgliedstaaten	261
6.6.2.2.3 Vereinbarkeit von Primär- und Sekundärzwecken	262
6.6.2.2.3.1 Vermutete Vereinbarkeit für privilegierte Sekundärzwecke – Big Data als wissenschaftliche Forschung oder Statistik?	262
6.6.2.2.3.2 Festgestellte Vereinbarkeit für sonstige Sekundärzwecke	264
6.6.3 Ergebnis	266
6.7 Datenminimierung	269
6.7.1 Vermeidung personenbezogener Daten	269
6.7.2 Begrenzung personenbezogener Daten – Unterschiede zum Prinzip der Datensparsamkeit aus § 3a BDSG a.F.	270
6.7.3 Datenminimierung als Widerspruch zum Big-Data-Merkmal <i>Volume</i> ?	271
6.7.4 Pseudonymisierung im Rahmen der sozialen Netzwerkanalyse	272
6.7.4.1 Verfahren zur Pseudonymisierung	272
6.7.4.1.1 Erstellung von Pseudonymen in Listen	273
6.7.4.1.2 Erstellung von Pseudonymen durch Berechnungsverfahren	273
6.7.4.1.3 Interne und externe Erstellung von Pseudonymen	276
6.7.4.2 Aufbewahrung der zusätzlichen Informationen	277
6.7.4.3 Hinzuziehung der zusätzlichen Informationen	279
6.8 Datenrichtigkeit	280
6.8.1 Kriterien der Datenrichtigkeit	280
6.8.1.1 Sachliche Richtigkeit	280
6.8.1.2 Aktualität	281
6.8.1.3 Vollständigkeit	282
6.8.2 Implikationen für Big Data	283
6.8.2.1 Fehlerhafte Daten als Informationsgrundlage – Akzeptanz von Big Data <i>Veracity</i> ?	283
6.8.2.1.1 Eigene Maßnahmen des Verantwortlichen	284
6.8.2.1.2 Reaktion auf Betroffenenrechte	286
6.8.2.2 Fehlerhafte Verfahren	287
6.8.2.3 Fehlerhafte Daten als Ergebnis bzw. fehlerhafte Interpretation derselben – Zulässige Verwendung von Korrelationen?	290

6.9	Speicherbegrenzung	292
6.9.1	Eigene Maßnahmen des Verantwortlichen	292
6.9.2	Reaktion auf Betroffenenrechte	296
6.9.3	Implikationen für Big Data	297
6.10	Datensicherheit.....	301
6.10.1	Ziele der Datensicherheit	301
6.10.1.1	Vertraulichkeit personenbezogener Daten	302
6.10.1.2	Integrität personenbezogener Daten.....	302
6.10.1.3	Verfügbarkeit personenbezogener Daten	302
6.10.2	Technische und organisatorische Maßnahmen zur Gewährleistung von Datensicherheit.....	303
6.10.2.1	Risikoangemessenes Schutzniveau	303
6.10.2.2	Geeignete technische und organisatorische Maßnahmen.....	304
6.10.3	Risikobewertung und Ableitung risikoangemessener Maßnahmen für soziale Netzwerkanalyse	306
6.10.3.1	Beschreibung des Datenverarbeitungsvorgangs.....	307
6.10.3.2	Bewertung der Schwere möglicher Folgen	308
6.10.3.2.1	Folgen bei Verletzung der Vertraulichkeit	309
6.10.3.2.2	Folgen bei Verletzung der Integrität.....	309
6.10.3.2.3	Folgen bei Verletzung der Verfügbarkeit.....	309
6.10.3.2.4	Gesamtbewertung	310
6.10.3.3	Bewertung der Eintrittswahrscheinlichkeit möglicher Bedrohungen	310
6.10.3.4	Bewertung des Risikos für betroffene Personen	311
6.10.3.5	Ableitung risikoangemessener Maßnahmen	312
6.11	Rechenschaft	314
6.11.1	Risikobasierter Ansatz der Datenschutz-Grundverordnung.....	314
6.11.2	„Big Data – Big Accountability“ – Elemente eines Datenschutzmanagementsystems für Big Data	315
6.11.2.1	Governance und Organisation	316
6.11.2.1.1	Zustimmung und Unterstützung durch höchste Managementebene... 317	
6.11.2.1.2	Zuweisung von Rollen und Verantwortlichkeiten.....	318
6.11.2.1.3	Zusammenarbeit mit anderen Organisationsbereichen.....	320
6.11.2.1.4	Einrichtung eines Berichtswesens	321
6.11.2.2	Übersicht und Risikomanagement	322
6.11.2.2.1	Verzeichnis von Verarbeitungstätigkeiten.....	322
6.11.2.2.2	Risikomanagement und Datenschutz-Folgenabschätzung	324

6.11.2.2.1	Voraussetzungen der Datenschutz-Folgenabschätzung.....	325
6.11.2.2.2	Methodik der Datenschutz-Folgenabschätzung.....	329
6.11.2.2.3	Ergebnisse der Datenschutz-Folgenabschätzung.....	330
6.11.2.3	Richtlinien und Prozesse	330
6.11.2.4	Kommunikation.....	332
6.11.2.5	Externe Akteure.....	334
6.11.2.6	Datensicherheit und Behandlung von Sicherheitsverletzungen	335
6.11.2.7	Sensibilisierung und Schulungen	338
6.11.2.8	Prüfung, Bewertung und Evaluierung	339
7	Zusammenfassung.....	343
	Literaturverzeichnis.....	354