

# Inhaltsübersicht

Inhaltsverzeichnis	11
1 Einleitung	25
1.1 Untersuchungsgegenstand und Begrifflichkeiten	25
1.2 Relevanz des Untersuchungsgegenstands	26
1.3 Stand der Forschung	28
1.4 Ziele der Arbeit	32
1.5 Gang der Untersuchung	33
1.6 Case Study	34
2 Überblick über den europäischen und nationalen Rechtsrahmen	37
2.1 Entwicklung des europäischen Datenschutzrechts vor der DSGVO	38
2.2 Der geltende Rechtsrahmen	43
2.3 Schutzgüter und Regelungsziele des europäischen Datenschutzrechts	51
3 Definition „Personal Data Breach“	65
3.1 Gesetzgebungsgeschichte	66
3.2 Tatbestandsmerkmale des Art. 4 Ziff. 12 DSGVO	67
3.3 Anwendungsbereich	69
3.4 Verletzung der Sicherheit	69
3.5 Erfolgseintritt	83
3.6 Case Study: Scraping	90
3.7 Zwischenergebnis zu Abschnitt 3	93
4 Bedeutung und Auswirkungen von Personal Data Breaches	95
4.1 Globale Daten zu Data Breaches	95

## *Inhaltsübersicht*

4.2 Zahlen zu Data-Breach-Meldungen in Europa	99
4.3 Zahlen zu Data-Breach-Meldungen in Deutschland	101
4.4 Auswirkungen eines Data Breach	105
4.5 Zwischenergebnis zu Abschnitt 4	108
5 Risikobasierter Ansatz in Bezug auf Personal Data Breaches	111
5.1 Risikobegriff	111
5.2 Risikobasierter Ansatz der DSGVO in Bezug auf Personal Data Breaches	112
5.3 Maßgebliche Risiken bei Personal Data Breaches	114
5.4 Bezugssubjekt: Konkrete betroffene Person oder abstrakt alle potenziell betroffenen Personen	115
5.5 Bestimmung des Risikos und Risikoerhöhung durch einen Personal Data Breach	117
5.6 Kann die betroffen Person in Risiken einwilligen?	119
5.7 Zwischenergebnis zu Abschnitt 5	125
6 Melde-, Benachrichtigungs- und Dokumentationspflichten	127
6.1 Entwicklung des Rechtsrahmens in Deutschland und Europa	127
6.2 Regelungszweck der Melde- und Benachrichtigungspflichten, systematische Stellung	129
6.3 Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO	131
6.4 Benachrichtigung der betroffenen Personen	163
6.5 Melde- und Benachrichtigungspflichten in der Praxis	180
6.6 Dokumentationspflichten	190
6.7 Kritik und Verbesserungsvorschläge	192
6.8 Case Study: Scraping	194
6.9 Zwischenergebnis zu Abschnitt 6	196

7	Aufsichtsbehördliche Befugnisse	199
7.1	Aufsichtsbehördliche Maßnahmen nach Art. 58 DSGVO	199
7.2	Aufsichtsbehördliche Bußgelder infolge von Personal Data Breaches	202
7.3	Zwischenergebnis zu Abschnitt 7	213
8	Spannungsverhältnis zwischen Meldepflicht, Selbstbelastungsfreiheit und nationalen Beweisverwendungsverboten	215
8.1	Case Study	216
8.2	Regelungsinhalt der §§ 42 Abs. 4 und 43 Abs. 4 BDSG	217
8.3	Abgrenzung Beweiserhebungs-, verwendungs und -verwertungsverbot	218
8.4	Rechtsnatur der §§ 42 Abs. 4 und 43 Abs. 4 BDSG: Verwertungs- oder Verwendungsverbot?	220
8.5	Selbstbelastungsfreiheit in der Rspr. von BVerfG, EuGH und EGMR	227
8.6	Konflikt der Melde- und Benachrichtigungspflichten mit der Selbstbelastungsfreiheit?	235
8.7	Von den Beweisverwendungsverboten erfasste Tatsachen	238
8.8	Subjektive Reichweite der Verwertungsverbote	241
8.9	Kollision zwischen den §§ 42 Abs. 4 und 43 Abs. 4 BDSG und dem Europarecht	247
8.10	Aussageverweigerungsrecht nach § 40 Abs. 4 Satz 2 BDSG	261
8.11	Rechtmäßige Handhabung durch die Aufsichtsbehörde	262
8.12	Case study: Scraping	264
8.13	Verbesserungsmöglichkeiten	265
8.14	Zwischenergebnis zu Abschnitt 8	266

## *Inhaltsübersicht*

<b>9 Zivilrechtliche Rechtsdurchsetzung infolge von Personal Data Breaches</b>	<b>269</b>
9.1 Ansprüche auf Schadensersatz nach Art. 82 DSGVO	270
9.2 Nationale Anspruchsgrundlagen neben Art. 82 DSGVO	328
9.3 Art und Höhe des Schadensersatzanspruchs	339
9.4 Ansprüche auf Unterlassung	348
9.5 Beweisführung im Zivilprozess unter dem Einfluss der DSGVO	351
9.6 Case Study: Schadensersatz für Scraping in der zivilgerichtlichen Realität	366
9.7 Mehrwert im System des Datenschutzrechts?	367
9.8 Zwischenergebnis zu Abschnitt 9	369
<b>10 Zusammenfassung der wesentlichen Ergebnisse und Schlussbetrachtung</b>	<b>371</b>
10.1 Allgemeiner Rechtsrahmen, Definition und Bedeutung von Personal Data Breaches	371
10.2 Meldepflichten als zentrales Regelungsinstrument	372
10.3 Zusammenspiel von unionsrechtlich geprägten Kompetenzen der Aufsichtsbehörden und nationalem Verfahrensrecht	373
10.4 Die Rolle zivilrechtlicher Rechtsdurchsetzung	375
10.5 Schlussbetrachtung	377
<b>Literaturverzeichnis</b>	<b>379</b>

# Inhaltsverzeichnis

1	Einleitung	25
1.1	Untersuchungsgegenstand und Begrifflichkeiten	25
1.2	Relevanz des Untersuchungsgegenstands	26
1.3	Stand der Forschung	28
1.4	Ziele der Arbeit	32
1.5	Gang der Untersuchung	33
1.6	Case Study	34
2	Überblick über den europäischen und nationalen Rechtsrahmen	37
2.1	Entwicklung des europäischen Datenschutzrechts vor der DSGVO	38
2.1.1	Frühphase der Verrechtlichung	38
2.1.2	OECD-Leitlinien und die Konvention 108 des Europarats	39
2.1.3	Erste Phase der europäischen Vereinheitlichung: Datenschutzrichtlinien	40
2.1.4	Datenschutzrecht in Deutschland vor dem Inkrafttreten der DSGVO	42
2.2	Der geltende Rechtsrahmen	43
2.2.1	Charta der Grundrechte der Europäischen Union	43
2.2.2	Grundrechte und einfachgesetzliche Regelungen in Deutschland	44
2.2.3	Verhältnis zwischen nationalen und europäischen Grundrechten	44
2.2.4	Die DSGVO: Ein Kompromiss	46
2.2.5	Wesentliche Regelungen der DSGVO	46
2.2.6	Regelungsspielraum der nationalen Gesetzgeber	47
2.2.7	Anwendungsbereich und wesentliche Regelungen des BDSG	49
2.2.8	Wesentliche Regelungen der Datenschutzgesetze der Länder	50

## *Inhaltsverzeichnis*

2.2.9	Relevante nationale Regelungen für Personal Data Breaches	50
2.3	Schutzgüter und Regelungsziele des europäischen Datenschutzrechts	51
2.3.1	Das europäische Datenschutzgrundrecht als maßgebliches Schutzgut der DSGVO	51
2.3.1.1	Bedeutung des Art. 8 EMRK für die Ausprägung europäischen Datenschutzrechts	53
2.3.1.2	(Weiter-)Entwicklung des europäischen Grundrechts auf Datenschutz durch den EuGH	53
2.3.1.3	Art. 8 GRCh	56
2.3.1.4	Das Verhältnis von Art. 7 und Art. 8 GRCh	60
2.3.1.5	Schlussfolgerungen: Kern des europäischen Datenschutzgrundrechts und zugleich Schutzgut der DSGVO	61
2.3.2	Weitere Regelungsziele des Datenschutzgrundrechts und der DSGVO	62
3	Definition „Personal Data Breach“	65
3.1	Gesetzgebungsgeschichte	66
3.2	Tatbestandsmerkmale des Art. 4 Ziff. 12 DSGVO	67
3.3	Anwendungsbereich	69
3.4	Verletzung der Sicherheit	69
3.4.1	Funktion des Tatbestandsmerkmals	70
3.4.2	IT-Sicherheit und Sicherheit der Verarbeitung personenbezogener Daten	71
3.4.3	Auslegung anhand anerkannter Begriffe der IT-Sicherheit	73
3.4.4	Vertraulichkeit, Integrität oder Verfügbarkeit	76
3.4.5	Wann liegt eine Verletzung vor?	77
3.4.6	Keine Pflichtwidrigkeit notwendig	78
3.4.7	Konkrete Gefährdung ausreichend?	79
3.4.8	Bezug zu technisch-organisatorischen Maßnahmen („TOM-Test“)	80
3.4.9	Zwischenergebnis und Vorschlag einer Definition für Verletzung der Sicherheit	83

3.5	Erfolgseintritt	83
3.5.1	Vernichtung, Verlust oder Veränderung	84
3.5.2	Unbefugtes Offenlegen oder Zugänglichmachen	85
3.5.2.1	Offenlegen oder Zugänglichmachen	85
3.5.2.2	Unbefugt	86
3.5.3	Unrechtmäßiger oder ungewollter Verletzungserfolg	88
3.5.4	Kausalität zwischen Verletzung der Sicherheit und Erfolg	89
3.6	Case Study: Scraping	90
3.6.1	Verletzung der Sicherheit durch Scraping	90
3.6.2	Erfolgseintritt und Kausalität	92
3.6.3	Subsumption und Zwischenergebnis	92
3.7	Zwischenergebnis zu Abschnitt 3	93
4	Bedeutung und Auswirkungen von Personal Data Breaches	95
4.1	Globale Daten zu Data Breaches	95
4.2	Zahlen zu Data-Breach-Meldungen in Europa	99
4.3	Zahlen zu Data-Breach-Meldungen in Deutschland	101
4.4	Auswirkungen eines Data Breach	105
4.4.1	Wirtschaftliche Auswirkungen für ein betroffenes Unternehmen	105
4.4.2	Auswirkungen auf betroffene Personen	106
4.4.3	Auswirkungen von Personal Data Breaches auf die Schutzgüter und Regelungsziele des Datenschutzrechts	107
4.5	Zwischenergebnis zu Abschnitt 4	108
5	Risikobasierter Ansatz in Bezug auf Personal Data Breaches	111
5.1	Risikobegriff	111
5.2	Risikobasierter Ansatz der DSGVO in Bezug auf Personal Data Breaches	112
5.3	Maßgebliche Risiken bei Personal Data Breaches	114
5.4	Bezugssubjekt: Konkrete betroffene Person oder abstrakt alle potenziell betroffenen Personen	115
5.5	Bestimmung des Risikos und Risikoerhöhung durch einen Personal Data Breach	117

## *Inhaltsverzeichnis*

5.6 Kann die betroffen Person in Risiken einwilligen?	119
5.7 Zwischenergebnis zu Abschnitt 5	125
6 Melde-, Benachrichtigungs- und Dokumentationspflichten	127
6.1 Entwicklung des Rechtsrahmens in Deutschland und Europa	127
6.1.1 Entwicklung in der EU	127
6.1.2 Entwicklung in Deutschland	128
6.2 Regelungszweck der Melde- und Benachrichtigungspflichten, systematische Stellung	129
6.3 Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO	131
6.3.1 Entstehungsgeschichte: Vorbilder in den USA und in Europa	131
6.3.2 Meldepflichtiges Ereignis	132
6.3.3 Ausnahmen	133
6.3.3.1 Keine Meldepflicht bei lediglich sehr geringem Risiko	133
6.3.3.2 Zwischenergebnis	136
6.3.3.3 Typische Fallkonstellationen	136
6.3.3.4 Haushaltsausnahme des Art. 2 Abs. 2 lit. c DSGVO	140
6.3.4 Adressat der Meldepflicht	143
6.3.4.1 Verantwortlicher und Auftragsverarbeiter	143
6.3.4.2 Arbeitgeber und Arbeitnehmer bei Mitarbeiterexzessen	144
6.3.5 Empfänger der Meldung	145
6.3.5.1 Nationale Zuständigkeit	146
6.3.5.2 Internationale Zuständigkeit: Anwendbarkeit des Art. 56 DSGVO auf Art. 33 DSGVO?	146
6.3.5.3 Zuständige Behörde in der Union bei grenzüberschreitenden Fällen nach Art. 56 DSGVO	147
6.3.5.4 Ausnahmefall: „local case“	149
6.3.5.5 Zuständige Aufsichtsbehörde bei Verantwortlichem in Drittstaat	151
6.3.5.6 Zwischenergebnis	151
6.3.6 Inhalt der Meldung	152
6.3.6.1 Beschreibung des Vorfalls	152

6.3.6.2	Name und Kontaktdaten des Datenschutzbeauftragten oder eines Ansprechpartners	153
6.3.6.3	Wahrscheinliche Folgen	154
6.3.6.4	Ergriffene oder geplante Maßnahmen	154
6.3.7	Form	154
6.3.8	Frist	155
6.3.8.1	Unverzüglich	155
6.3.8.2	Berechnung der 72 Stunden	156
6.3.8.3	Meldung an eine unzuständige Behörde	160
6.3.9	Meldepflicht nach § 65 BDSG	162
6.4	Benachrichtigung der betroffenen Personen	163
6.4.1	Adressat der Benachrichtigungspflicht	164
6.4.2	Empfängerkreis	164
6.4.3	Hohes Risiko für die betroffene Person	164
6.4.4	Benachrichtigung der betroffenen Person aufgrund Anweisung durch die Aufsichtsbehörde	167
6.4.5	Benachrichtigung der betroffenen Person durch die Aufsichtsbehörde, Art. 34 Abs. 4 und Art. 58 Abs. 2 lit. e DSGVO	168
6.4.6	Entfallen der Pflicht	170
6.4.6.1	Nachfolgende Sicherheitsvorkehrungen: Art. 34 Abs. 3 lit. a. und b. DSGVO	170
6.4.6.2	Geheimhaltungspflichten: § 29 Abs. 1 Satz 3 BDSG	171
6.4.6.3	Ausnahmen in den Landesdatenschutzgesetzen	173
6.4.6.4	Verzicht der betroffenen Person	174
6.4.7	Inhalt der Benachrichtigung	174
6.4.8	Frist	175
6.4.9	Öffentliche Benachrichtigung bei unverhältnismäßigem Aufwand, Art. 34 Abs. 3 lit. c DSGVO	176
6.4.10	Benachrichtigung nach § 66 BDSG	178
6.5	Melde- und Benachrichtigungspflichten in der Praxis	180
6.5.1	Positionierung und Beispiele des EDSA	180
6.5.2	Meldepflichten bei Phishing	182
6.5.2.1	Zurechenbarkeit	183
6.5.2.2	Vorliegen einer Schutzverletzung i. S. d. Art. 4 Ziff. 12 DSGVO	183

## *Inhaltsverzeichnis*

6.5.2.3 Einschränkung der Meldepflicht: Kenntnis und Risiko	185
6.5.2.4 Zusammenfassung	186
6.5.3 Meldepflichten bei einem (E-Mail-)Fehlversand	186
6.5.3.1 Schutzverletzung	187
6.5.3.2 Einschränkung der Meldepflicht: Risiko für Betroffene	189
6.6 Dokumentationspflichten	190
6.6.1 Dokumentationspflichten der DSGVO	190
6.6.2 Dokumentationspflicht nach § 65 Abs. 5 BDSG	191
6.7 Kritik und Verbesserungsvorschläge	192
6.8 Case Study: Scraping	194
6.9 Zwischenergebnis zu Abschnitt 6	196
 7 Aufsichtsbehördliche Befugnisse	199
7.1 Aufsichtsbehördliche Maßnahmen nach Art. 58 DSGVO	199
7.1.1 Aufsichtsbehördliche Maßnahmen aufgrund von Verstößen gegen Meldepflichten	199
7.1.2 Aufsichtsbehördliche Maßnahmen aufgrund unzureichender TOM	200
7.1.3 Aufsichtsbehördliche Maßnahmen aufgrund einer Verarbeitung ohne Rechtsgrundlage	201
7.2 Aufsichtsbehördliche Bußgelder infolge von Personal Data Breaches	202
7.2.1 Das Bußgeldverfahren bei Verstößen gegen die DSGVO	203
7.2.1.1 Anknüpfungspunkte: Unterlassene oder verspätete Meldung oder vorgelagerte Verstöße	203
7.2.1.2 Anwendbare Vorschriften im Bußgeldverfahren	203
7.2.1.3 Inkompatibilität von deutschem Individualstrafrecht und europäischen Unternehmenssanktionen	204
7.2.1.4 Konzeptionelle Vereinbarkeit der europäischen Vorgaben mit dem deutschen Verfahrensrecht bei Verfahren gegen natürliche Personen	205
7.2.1.5 Erforderlicher Verschuldensgrad	206

7.2.2	Bußgelder gegen juristische Personen: Originäre Verbandshaftung oder Täterprinzip?	209
7.2.2.1	Streitstand und Stellungnahme	209
7.2.2.2	Rechtsprechung in Deutschland und Entscheidung des Streits durch den EuGH	212
7.2.2.3	Zwischenergebnis	213
7.3	Zwischenergebnis zu Abschnitt 7	213
8	Spannungsverhältnis zwischen Meldepflicht, Selbstbelastungsfreiheit und nationalen Beweisverwendungsverboten	215
8.1	Case Study	216
8.2	Regelungsinhalt der §§ 42 Abs. 4 und 43 Abs. 4 BDSG	217
8.3	Abgrenzung Beweiserhebungs-, verwendungs und -verwertungsverbot	218
8.3.1	Beweiserhebungsverbote und Beweisverwertungsverbote	218
8.3.2	Selbstständige und unselbstständige Beweisverwertungsverbote	218
8.3.3	Beweisverwertungs- und -verwendungsverbote	219
8.4	Rechtsnatur der §§ 42 Abs. 4 und 43 Abs. 4 BDSG: Verwertungs- oder Verwendungsverbot?	220
8.4.1	Wortlaut und Systematik	221
8.4.2	Sinn und Zweck der Regelung	221
8.4.3	Historische Auslegung	222
8.4.3.1	Inhalt und Unstimmigkeiten in der Gesetzesbegründung	222
8.4.3.2	Orientierung an § 97 Abs. 1 S. 3 InsO	224
8.4.3.3	Zwischenergebnis zu 8.4.3	226
8.4.4	Zwischenergebnis zu 8.4	226
8.5	Selbstbelastungsfreiheit in der Rspr. von BVerfG, EuGH und EGMR	227
8.5.1	Herleitung	227
8.5.2	Persönlicher Schutzbereich: Juristische Personen erfasst?	229
8.5.3	Sachlicher Schutzbereich	230
8.5.4	Zwischenergebnis: Differenzierung zwischen natürlichen und juristischen Personen	233

## *Inhaltsverzeichnis*

8.6 Konflikt der Melde- und Benachrichtigungspflichten mit der Selbstbelastungsfreiheit?	235
8.6.1 Art 33 und 34 DSGVO im Ordnungswidrigkeiten- und Verwaltungsverfahren	235
8.6.2 Auflösung des Konflikts durch die §§ 42 Abs. 4 und 43 Abs. 4 BDSG?	237
8.7 Von den Beweisverwendungsverboten erfasste Tatsachen	238
8.7.1 Tatsachen, die über die Pflichtangaben hinausgehen	238
8.7.2 Tatsachen, von denen die Aufsichtsbehörde bereits Kenntnis hat	239
8.7.3 Irrtum über Meldepflicht	240
8.8 Subjektive Reichweite der Verwertungsverbote	241
8.8.1 Kein Strafverfahren gegen Unternehmen	241
8.8.2 Anwendbarkeit von § 43 Abs. 4 BDSG auf juristische Personen	241
8.8.2.1 Wortlaut, Gesetzgebungsgeschichte und Rechtsprechung	242
8.8.2.2 Kritik und Ausblick	243
8.8.2.3 Zwischenergebnis	244
8.8.3 Subjektive Reichweite des Verwertungsverbots: Beschäftigte von Unternehmen	245
8.9 Kollision zwischen den §§ 42 Abs. 4 und 43 Abs. 4 BDSG und dem Europarecht	247
8.9.1 Regelungskonflikte zwischen nationalen Normen und dem Unionsrecht	248
8.9.2 Kollision zwischen §§ 42 Abs. 4, 43 Abs. 4 BDSG und dem Unionsrecht?	249
8.9.2.1 Regelungskonflikt zwischen § 42 Abs. 4 BDSG und dem Unionsrecht	249
8.9.2.2 Regelungskonflikt zwischen § 43 Abs. 4 BDSG und dem Unionsrecht	250
8.9.2.3 Zwischenergebnis	251
8.9.3 Art. 58 Abs. 4 und 83 Abs. 8 DSGVO als Öffnungsklausel für § 43 Abs. 4 BDSG	251
8.9.3.1 § 43 Abs. 4 BDSG als Verfahrensgarantie i. S. d. Art. 83 Abs. 8 DSGVO?	252
8.9.3.2 Ist § 43 Abs. 4 BDSG angemessen?	253

8.9.3.3 Zwischenergebnis	257
8.9.4 Vereinbarkeit eines umfassenden Verwendungsverbotes für natürliche Personen mit dem Effektivitäts- und dem Äquivalenzgrundsatz	257
8.9.4.1 Vereinbarkeit mit dem Effektivitätsgrundsatz	257
8.9.4.2 Vereinbarkeit mit dem Äquivalenzgrundsatz	260
8.10 Aussageverweigerungsrecht nach § 40 Abs. 4 Satz 2 BDSG	261
8.11 Rechtmäßige Handhabung durch die Aufsichtsbehörde	262
8.12 Case study: Scraping	264
8.12.1 Waren die Nachfragen der Aufsichtsbehörde in diesem Fall zulässig? Kann der Verantwortliche die Antwort verweigern?	264
8.12.2 Dürfen die Angaben für ein nachfolgendes Bußgeldverfahren gegen die Verantwortlichen überhaupt verwendet werden oder besteht ein Beweisverwertungsverbot?	264
8.12.3 Wie weit reicht ein mögliches Verwertungsverbot? Erfasst dieses auch solche Tatsachen, die der Verantwortliche nicht im Zuge der Meldung, sondern erst auf Nachfrage mitgeteilt hat?	265
8.13 Verbesserungsmöglichkeiten	265
8.14 Zwischenergebnis zu Abschnitt 8	266
 9 Zivilrechtliche Rechtsdurchsetzung infolge von Personal Data Breaches	269
9.1 Ansprüche auf Schadensersatz nach Art. 82 DSGVO	270
9.1.1 Rechtslage vor der DSGVO	271
9.1.2 Haftungsbegründung	271
9.1.2.1 Verstoß gegen die DSGVO oder abgeleitetes Recht	272
9.1.2.2 Data Breach als Verstoß i. S. d. Art. 82 Abs. 1 DSGVO?	273
9.1.2.2.1 Verstöße im Vorfeld des Data Breach (Art. 5 Abs. 1 lit. f, 25 und 32 DSGVO)	274
9.1.2.2.2 Verstöße nach Eintritt des Data Breach	274

## *Inhaltsverzeichnis*

9.1.2.2.3 Verstöße gegen Rechenschafts- und Dokumentationspflichten	276
9.1.2.3 Verschuldenserfordernis und Exkulpation (Art. 82 Abs. 3 DSGVO)	276
9.1.2.3.1 Meinungsstand zu Verschuldenserfordernis in der Literatur	277
9.1.2.3.2 Mögliche dritte Lesart des Art. 82 Abs. 3 DSGVO: Regelung über haftungsausfüllende Kausalität	278
9.1.2.3.3 Entscheidung des EuGH in der Rechtssache C-667/21	279
9.1.2.3.3.1 Wesentliche Elemente der Entscheidung und offene Fragen	279
9.1.2.3.3.2 Kritik	280
9.1.2.3.4 Bewertung und Zwischenergebnis	281
9.1.2.3.5 Exkulpation nach Art. 82 Abs. 3 DSGVO	282
9.1.2.4 Anspruchsberechtigte	284
9.1.2.5 Anspruchsgegner und gesamtschuldnerische Haftung	286
9.1.2.5.1 Anspruchsgegner	286
9.1.2.5.2 Gesamtschuldnerische Haftung	287
9.1.3 Haftungsausfüllung	287
9.1.3.1 Schadensbegriff	288
9.1.3.2 Materielle Schäden	289
9.1.3.2.1 Materielle Folgeschäden	290
9.1.3.2.2 Personenbezogene Daten als Vermögensschaden	291
9.1.3.2.3 Wirtschaftlicher Wert personenbezogener Daten?	291
9.1.3.2.4 Vermögenseinbuße, wirtschaftliche Verwertbarkeit der eigenen Daten	292
9.1.3.2.5 Wirtschaftlicher Wert der eigenen personenbezogenen Daten als individuelle Vermögensposition	293

9.1.3.2.6 Bezifferbarkeit des Werts personenbezogener Daten	294
9.1.3.2.6.1 Bezugspunkt: Wert auf b2b- Datenmarktplätzen	295
9.1.3.2.6.2 Bezugspunkt: Wert der Daten für Unternehmen, Daten als Gegenleistung	296
9.1.3.2.6.3 Bezugspunkt: Willingness to accept	298
9.1.3.2.6.4 Bezugspunkt: Verkaufspreise im Darknet	300
9.1.3.2.6.5 Zwischenfazit	301
9.1.3.2.7 Negativer wirtschaftlicher Saldo bei der betroffenen Person	301
9.1.3.2.8 Fazit	303
9.1.3.3 Immaterielle Schäden	304
9.1.3.3.1 Bagatellgrenze	304
9.1.3.3.2 (Bloßes) Unbehagen und/oder Furcht als Schaden?	306
9.1.3.3.3 Kontrollverlust als Schaden i. S. v. Art. 82 DSGVO?	309
9.1.3.3.3.1 Wille des Gesetzgebers	310
9.1.3.3.3.2 Kein Recht auf Kontrolle über eigene personen- bezogene Daten und daher kein Schaden?	313
9.1.3.3.3.3 Zwischenergebnis	316
9.1.3.4 Strafschaden	317
9.1.3.5 Zwischenergebnis	317
9.1.3.6 Haftungsausfüllende Kausalität	318
9.1.3.6.1 Besondere Problemfelder bei Personal Data Breaches im Hinblick auf die haftungsausfüllende Kausalität	318
9.1.3.6.2 Unionsrechtliche Aspekte	321
9.1.3.6.3 Auslegung nach nationalem Verständnis	323
9.1.3.6.3.1 Äquivalenz	323
9.1.3.6.3.2 Adäquanz	324
9.1.3.6.3.3 Schutzzweck der Norm	326

## *Inhaltsverzeichnis*

9.1.3.6.4 Zivilgerichtliche Rechtsprechung zur Kausalität bei Art. 82 DSGVO	327
9.1.3.6.5 Vereinbarkeit der deutschen Auslegung mit dem Unionsrecht	327
<b>9.2 Nationale Anspruchsgrundlagen neben Art. 82 DSGVO</b>	<b>328</b>
9.2.1 Schuldrechtliche Ansprüche unter Berücksichtigung des reformierten Schuldrechts	328
9.2.1.1 Mangel bei Lieferung digitaler Produkte	328
9.2.1.2 Unzureichende Aktualisierung digitaler Produkte	329
9.2.1.3 Verhältnis zur DSGVO	331
9.2.2 Deliktsrechtliche Ansprüche	332
9.2.2.1 Verhältnis des allgemeinen Deliktsrechts zur DSGVO	332
9.2.2.2 Sonstige Rechte i. S. d. § 823 Abs. 1 BGB	333
9.2.2.3 Schutzgesetze i. S. d. § 823 Abs. 2 BGB	335
9.2.3 Bereicherungsrechtliche Ansprüche	337
9.2.3.1 Ansprüche gegen den Verantwortlichen, bei dem der Data Breach eingetreten ist	338
9.2.3.2 Ansprüche gegen Dritte, denen Daten offengelegt wurden	338
<b>9.3 Art und Höhe des Schadensersatzanspruchs</b>	<b>339</b>
9.3.1 Vermögensschäden	340
9.3.2 Nichtvermögensschäden	341
9.3.2.1 Strafschaden und Straffunktion	341
9.3.2.2 Präventiv- bzw. Abschreckungsfunktion	343
9.3.2.3 Genugtuungsfunktion	344
9.3.2.4 Rechtsprechung zur Bemessung von immateriellem Schaden	345
9.3.2.5 Konkrete Bestimmung der Höhe bei Nichtvermögensschäden	346
<b>9.4 Ansprüche auf Unterlassung</b>	<b>348</b>
9.4.1 Unterlassungsanspruch aus dem BGB und Verhältnis zur DSGVO	348
9.4.2 Anspruchsvoraussetzungen § 1004 Abs. 1 Satz 2 BGB i. V. m. DSGVO	350

9.4.3	Anwendung und Besonderheiten bei Data-Breach-Sachverhalten	350
9.5	Beweisführung im Zivilprozess unter dem Einfluss der DSGVO	351
9.5.1	Beweislastverteilung und Rechenschaftspflicht (Art. 5 Abs. 2 und 24 Abs. 1 DSGVO)	352
9.5.1.1	Regelungsinhalt der Art. 5 Abs. 2 und 24 Abs. 1 DSGVO	352
9.5.1.2	Handelt es sich bei Art. 5 Abs. 2 DSGVO um eine zivilprozessuale Regelung?	355
9.5.2	Folgen für die zivilprozessuale Beweislastverteilung	357
9.5.3	Auswirkungen der Art. 33 und 34 DSGVO im Zivilprozess	359
9.5.3.1	Informationszugang über Art. 33 Abs. 1 und 34 Abs. 1 DSGVO	359
9.5.3.2	Verwertbarkeit der Dokumentation nach Art. 33 Abs. 5 Satz 1 DSGVO	360
9.5.4	Zivilprozessuale Beweisverwertungsverbote	361
9.5.4.1	Beweisrelevante Daten, die aus einem Data Breach stammen	364
9.5.4.2	Beweisverwertungsverbot aus §§ 42 Abs. 4, 43 Abs. 4 BDSG (analog)	365
9.6	Case Study: Schadensersatz für Scraping in der zivilgerichtlichen Realität	366
9.7	Mehrwert im System des Datenschutzrechts?	367
9.8	Zwischenergebnis zu Abschnitt 9	369
10	Zusammenfassung der wesentlichen Ergebnisse und Schlussbetrachtung	371
10.1	Allgemeiner Rechtsrahmen, Definition und Bedeutung von Personal Data Breaches	371
10.2	Meldepflichten als zentrales Regelungsinstrument	372
10.3	Zusammenspiel von unionsrechtlich geprägten Kompetenzen der Aufsichtsbehörden und nationalem Verfahrensrecht	373
10.3.1	Kompetenzen der Aufsichtsbehörden und Verbandssanktionen	373
10.3.2	Beweisverwendungsverbote und Selbstbelastungsfreiheit	374

*Inhaltsverzeichnis*

10.4 Die Rolle zivilrechtlicher Rechtsdurchsetzung	375
10.5 Schlussbetrachtung	377
Literaturverzeichnis	379