

Meldepflichten im IT-Sicherheitsrecht

Datenschutz, Kritische Infrastrukturen und besondere IT-Dienste

Bearbeitet von
Florian Schneider

1. Auflage 2017. Buch. Rund 605 S. Softcover
ISBN 978 3 8487 3672 0

[Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > IT-Recht, Internetrecht, Informationsrecht](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Florian Schneider

Meldepflichten im IT-Sicherheitsrecht

Datenschutz, Kritische Infrastrukturen
und besondere IT-Dienste



Nomos

Sicherheit und Gesellschaft.
Freiburger Studien des Centre for Security and Society

herausgegeben von
Prof. Dr. Hans-Helmuth Gander
Prof. Dr. Walter Perron
Prof. Dr. Ralf Poscher
Prof. Dr. Gisela Riescher
Prof. Dr. Thomas Würtenberger

Band 11

Florian Schneider

Meldepflichten im IT-Sicherheitsrecht

Datenschutz, Kritische Infrastrukturen
und besondere IT-Dienste



Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Freiburg, Univ., Diss., 2016

ISBN 978-3-8487-3672-0 (Print)

ISBN 978-3-8452-8024-0 (ePDF)

1. Auflage 2017

© Nomos Verlagsgesellschaft, Baden-Baden 2017. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Inhaltsverzeichnis

Abkürzungsverzeichnis	31
Einleitung	35
A. Ausgangslage	35
B. Ziele der Arbeit	38
C. Fokus und Zuschnitt der Arbeit	38
D. Gang der Darstellung	40
§ 1 Einführung	43
A. Begriffsklärung	43
I. IT-Sicherheit	43
II. IT-System	44
III. Sicherheitsvorfall	45
IV. Melde- und Benachrichtigungspflicht	47
B. Funktion und Beispiele gesetzlicher Meldepflichten in anderen Rechtsgebieten	48
I. Beispiele auf europäischer Ebene	49
II. Beispiele auf nationaler Ebene	50
C. Überblick über das Gebiet der IT-Sicherheit	51
I. Aktuelle Themenfelder und Beispiele für die Bedrohungslage	51
II. Schutzziele der IT-Sicherheit	54
1. Vertraulichkeit	55
2. Verfügbarkeit	56
3. Integrität	56
III. Bedrohungen und Angriffsmethoden	57
IV. Akteure	59
D. Besonderheiten auf dem Gebiet der IT-Sicherheit	63
I. Weltweite Vernetzung und Interaktivität	63
II. Systemvielfalt und Dynamik	64
III. Ambivalenz von Sicherheitswissen	65
E. Außergesetzliche Maßnahmen auf dem Gebiet der IT-Sicherheit	66
I. Standardisierung, Normung und Zertifizierung	67
II. Öffentlich-private Partnerschaften zur Erhöhung der IT-Sicherheit	69

Inhaltsverzeichnis

III. Weitere Maßnahmen der Europäischen IT-Sicherheitspolitik	70
IV. Weitere Maßnahmen der nationalen IT-Sicherheitspolitik	70
§ 2 Meldepflichten bei IT-Sicherheitsvorfällen im Kontext des IT-Sicherheitsrechts	73
A. Europäischer Rechtsrahmen des IT-Sicherheitsrechts	73
I. Übersicht über die Meldepflichten im Europäischen Recht	73
II. Primärrechtliche Bestimmungen des IT-Sicherheitsrechts	74
1. Kompetenzen für Maßnahmen auf dem Gebiet der IT-Sicherheit	74
a) Datenschutz	75
b) Transeuropäische Netze	77
c) Industrie	78
d) Umwelt	79
e) Energie	80
f) Katastrophenschutz	82
g) Forschung und technologische Entwicklung	83
h) Raum der Freiheit, der Sicherheit und der Rechts	83
aa) Polizeiliche Zusammenarbeit, Europol und Eurojust	83
bb) Allgemeine Zusammenarbeit und Koordinierung	86
cc) Straftaten mit grenzüberschreitender Dimension und Kriminalprävention	86
i) Binnenmarkt	87
2. Vorgaben aus den Europäischen Grundrechten und Rechtsgrundsätzen	88
a) Datenschutz	89
b) Fernmeldegeheimnis	91
c) Recht auf Leben und körperliche Unversehrtheit	92
d) Berufsfreiheit und unternehmerische Freiheit	92
e) Schutz von Betriebs- und Geschäftsgeheimnissen	94
f) <i>Nemo-tenetur</i> -Grundsatz	95
III. Sekundärrechtliche Bestimmungen des IT-Sicherheitsrechts	97
1. Datenschutz-Grundverordnung	98
a) Regelungsinhalte mit Bezug zur IT-Sicherheit	98
b) Meldepflicht gemäß Art. 33 DSGVO	99
c) Verhältnis zu anderen Meldepflichten	99
2. Datenschutzrichtlinie	100
3. ENISA-Verordnung	100
4. NIS-Richtlinie	101
a) Regelungsinhalte	102
aa) Sicherheitsstrategie und Behördenkooperation	102

bb) Sicherheitsanforderungen	103
b) Meldepflichten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste gemäß Art. 14 Abs. 3 und Art. 16 Abs. 3 NIS-RL	104
5. EU-Rechtsrahmen für elektronische Kommunikationsnetze und -dienste	104
a) EU-Rechtsrahmen für elektronische Kommunikationsnetze und -dienste bis zum Jahr 2009	106
aa) Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität von Telefonnetzen und -Diensten gemäß Art. 23 RL 2002/22/EG	106
bb) Maßnahmen zur Gewährleistung der Dienstesicherheit gemäß Art. 4 Abs. 1 RL 2002/58/EG	106
cc) Maßnahmen zur Sicherstellung der Vertraulichkeit der Kommunikation gemäß Art. 5 Abs. 1 RL 2002/58/EG	107
b) Ergänzungen durch die Richtlinie 2009/140/EG	107
aa) Maßnahmen zur Erhöhung der Sicherheit von Netzen und Diensten gemäß Art. 13a Abs. 1 RRL	108
bb) Maßnahmen zur Gewährleistung der Integrität und Verfügbarkeit von Netzen und Diensten gemäß Art. 13a Abs. 2 RRL	108
cc) Meldepflicht bei der Verletzung des Schutzes personenbezogener Daten gemäß Art. 4 Abs. 3-5 RL 2002/58/EG	108
dd) Meldepflicht bei Sicherheitsverletzung oder Integritätsverlust gemäß Art. 13a Abs. 3 RRL	109
6. eIDAS-Verordnung	109
a) Sicherheitsvorgaben	110
b) Meldepflicht bei Sicherheitsverletzung oder Integritätsverlust gemäß Art. 19 Abs. 2 eIDAS-VO	111
7. Richtlinie über die Ermittlung und Ausweisung europäischer Kritischer Infrastrukturen	111
8. Richtlinie über Angriffe auf Informationssysteme	112
9. Richtlinie zum Datenschutz in der Strafverfolgung	113
B. Nationaler Rechtsrahmen des IT-Sicherheitsrechts	114
I. Übersicht über die Meldepflichten im nationalen Recht	114
II. Verfassungsrechtliche Vorgaben des IT-Sicherheitsrechts	115
1. Kompetenzen für Maßnahmen auf dem Gebiet der IT-Sicherheit	115
2. Vorgaben aus den Grundrechten und Rechtsgrundsätzen	115
a) Datenschutz	116
b) Fernmeldegeheimnis	117

Inhaltsverzeichnis

c) Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	117
d) Recht auf Leben und körperliche Unversehrtheit	118
e) Berufsfreiheit	118
f) Schutz von Betriebs- und Geschäftsgeheimnissen	120
g) <i>Nemo-tenetur</i> -Grundsatz	120
h) Keine Verfassungsrechtliche Pflicht zur Normierung von Meldepflichten bei IT-Sicherheitsvorfällen	122
3. Gewährleistung von IT-Sicherheit als nationalstaatliche Aufgabe	124
a) Landesverteidigung	125
b) Luft- und Eisenbahnverkehrsverwaltung	126
c) Post- und Telekommunikation	126
d) Informationstechnische Systeme	127
III. Einfachgesetzliche Bestimmungen des IT-Sicherheitsrechts	127
1. Datenschutzgesetze	128
a) Regelungen des Bundesdatenschutzgesetzes	128
b) Regelungen der Landesdatenschutzgesetze	130
c) Meldepflichten der Datenschutzgesetze	130
aa) Meldepflicht des § 42a BDSG	130
bb) Meldepflichten der Landesdatenschutzgesetze	131
d) Meldepflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten gemäß § 83a SGB X	131
2. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik	131
a) Allgemeine Aufgaben und Befugnisse des BSI	131
b) Mindestsicherheitsstandards für Betreiber Kritischer Infrastrukturen gemäß § 8a BSIG	132
c) Meldepflicht für Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 BSIG	133
d) Meldepflicht für Bundesbehörden gemäß § 4 Abs. 2 Nr. 2 BSIG	134
3. Telekommunikationsgesetz	134
a) Allgemeine Regelungen zur IT-Sicherheit	134
aa) Vorgaben für Diensteanbieter gemäß § 109 Abs. 1 TKG	135
bb) Zusätzliche Vorgaben für Betreiber öffentlicher TK-Netze und Anbieter öffentlich zugänglicher TK-Dienste gemäß § 109 Abs. 2 TKG	136
b) Meldepflicht bei Beeinträchtigungen von TK-Diensten und -Netzen gemäß § 109 Abs. 5 TKG	138
c) Meldepflicht bei Datenschutzverletzungen gemäß § 109a Abs. 1 TKG	138

4. Energiewirtschaftsgesetz	139
a) Regelungen mit Vorgaben zur IT-Sicherheit	139
b) Meldepflicht bei Störungen der IT-Systeme gemäß § 11 Abs. 1c EnWG	140
c) Meldepflicht bei unrechtmäßiger Kenntniserlangung von Daten gemäß § 21h Abs. 2 EnWG	141
5. Telemediengesetz	141
a) Regelungen mit Vorgaben zur IT-Sicherheit	141
b) Meldepflicht bei unrechtmäßiger Kenntniserlangung von Daten für TK-Diensteanbieter gemäß § 15a TMG	142
6. Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen	142
7. Allgemeines Eisenbahngesetz	143
8. Kreditwesen- und Wertpapierhandelsgesetz	143
9. Allgemeine gesellschaftsrechtliche Pflichten	144
10. Zivilrechtliche Regelungen	145
11. Strafrechtliche Regelungen	145
C. Zusammenfassung und Folgerungen	145
I. Fokussierung der Meldepflichten auf die Bereiche Datenschutz sowie Kritische Infrastrukturen und besondere IT-Dienste	147
II. Normierungszusammenhang mit Sicherheitsvorgaben	148
§ 3 Datenschutzrechtliche Meldepflichten bei IT-Sicherheitsvorfällen	149
A. Meldepflicht bei Datenschutzverletzungen gemäß § 42a BDSG	149
I. Ziele und Zwecke	150
1. Schutz der Persönlichkeitsrechte	151
2. Ermöglichung behördlicher Datenschutzmaßnahmen	151
3. Präventive Erhöhung der Datensicherheit	152
4. Keine weitergehenden Schutzziele	152
5. Betroffenenbenachrichtigung: Verringerung von Schäden	152
II. Kompetenzen	153
III. Adressaten	153
1. Nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen	154
2. Nicht erfasst: Öffentliche Stellen	154
3. Sonderfall: Auftragsdatenverarbeitung	155
IV. Räumlicher Anwendungsbereich	156
1. Extraterritoriale Anwendung nationalen Rechts	157
2. Völkerrechtliche Vorgaben	159
3. Grundgesetzliche Vorgaben	161
4. Anknüpfungsprinzipien	162

Inhaltsverzeichnis

a) Territorialitätsprinzip	163
b) Schutzprinzip	163
c) Wirkungsprinzip	164
d) Personalitätsprinzip	165
e) Weltrechtsprinzip	166
f) Organisationshoheitsprinzip	167
5. Extraterritoriale Anwendung des § 42a BDSG	167
a) Übersicht zu § 1 Abs. 5 BDSG	168
b) Sitz der Stelle im Inland	168
c) Sitz der Stelle im europäischen Ausland (§ 1 Abs. 5 S. 1 BDSG)	170
d) Sitz der Stelle im europäischen Ausland mit Niederlassung im Inland (§ 1 Abs. 5 S. 1 Hs. 2 BDSG)	172
e) Sitz der Stelle im außereuropäischen Ausland (§ 1 Abs. 5 S. 2 BDSG)	178
f) Sitz der Stelle im außereuropäischen Ausland mit Niederlassung im Inland (§ 1 Abs. 5 S. 2 BDSG)	180
g) Zusammenfassung	181
V. Meldepflichtige Vorfälle	182
1. Erfasste Datenkategorien	182
2. Bei der Stelle gespeicherte Daten	183
3. Feststellung der unrechtmäßigen Kenntniserlangung durch Dritte	183
a) Unrechtmäßigkeit	184
b) Feststellung	184
c) Wahrscheinlichkeitsgrad der Kenntniserlangung	186
4. Drohen schwerwiegender Beeinträchtigungen	188
a) Gefahrenprognose	188
b) Betroffenheit einer Einzelperson	189
c) Schwerwiegende Beeinträchtigung durch Gesamtschau	190
d) Bereits eingetretene Schäden und Rückgängigmachung von Schäden	191
VI. Inhalt der Meldung	192
1. Inhalte bei der Betroffenenbenachrichtigung	192
2. Inhalt bei der Meldung an die Aufsichtsbehörde	194
VII. Adressaten, Forum und Zeitpunkt der Meldung	195
1. Adressaten	195
2. Form	196
a) Form bei der Meldung an die Aufsichtsbehörde	196
b) Form bei der Betroffenenbenachrichtigung	197
3. Zeitpunkt	198
a) Ausnahme bei der Betroffenenbenachrichtigung: <i>responsible disclosure</i>	198

b) Ausnahme bei der Betroffenenbenachrichtigung:	
Strafverfolgung	199
VIII. Daten- und Geheimnisschutz	200
1. Datenschutz	200
2. Geheimnisschutz	201
IX. Verhältnismäßigkeit	202
X. Rechtsdurchsetzung	203
1. Kenntnis von einem Pflichtverstoß	204
2. Vollstreckung	205
a) Rückgriff auf allgemeine verwaltungsrechtliche Vollstreckungsmechanismen	205
b) Betroffenenbenachrichtigung durch die Behörde	205
c) Verpflichtung der Stelle zur Betroffenen- benachrichtigung	206
3. Sanktionen	208
a) Vorsätzlich nicht bzw. fehlerhaft erfolgte Meldung oder Benachrichtigung	208
b) Fahrlässig unterbliebene Feststellung	209
c) Kritik an Bestimmtheit	210
XI. Weitere Verwendung der übermittelten Informationen	211
1. Übermittlung personenbezogener Daten an andere Behörden	211
a) Keine Ausnahmen vom Zweckbindungsgrundsatz	212
b) Übermittlung personenbezogener Daten an nationale und internationale Aufsichtsbehörden	215
c) Unterrichtung zuständiger Stellen bei Datenschutzverstößen	216
d) Keine Übermittlung personenbezogener Daten im Wege der Amtshilfe	217
e) Übermittlungseinschränkungen	217
f) Zusammenfassung	218
2. Übermittlung nicht-personenbezogener Daten an andere Behörden	218
a) Keine Geltung des besonderen Zweckbindungsgrundsatzes	218
b) Übermittlungsvoraussetzungen	219
c) Übermittlungseinschränkungen	220
d) Zusammenfassung	222
3. Verwendung im Straf- und Ordnungswidrigkeitsverfahren	222
a) Verwendungsverbot und der <i>nemo-tenetur</i> -Grundsatz	222
b) Anwendungsbereich des <i>nemo-tenetur</i> -Grundsatzes bei juristischen Personen	223
c) Verwendungsverbot und Fernwirkung	224

Inhaltsverzeichnis

d) Zusammenfassung	228
4. Veröffentlichung	228
a) Veröffentlichungsbegriff	229
b) Rechtliche Ausgangslage und Interessen	230
c) Informierung der Öffentlichkeit durch die Aufsichtsbehörde gemäß § 38 Abs. 1 S. 6 BDSG	231
d) Unterrichtung der Öffentlichkeit durch Tätigkeitsberichte	232
e) Öffentlichkeitsinformierung ohne gesetzliche Ermächtigungsgrundlage	234
f) Informationszugangsrechte	237
g) Verhältnismäßigkeit	238
h) Zusammenfassung	239
XII. Zivilrechtliche Auswirkungen	240
1. Ansprüche bei Verstößen gegen § 42a BDSG	240
a) Unterlassene oder fehlerhafte Meldung	240
b) Zu Unrecht erfolgte Meldung	241
c) Auswirkungen einer falschen Behördenauskunft	242
2. Meldung gemäß § 42a BDSG als Wissenserklärung	242
3. Einfluss des § 42a BDSG auf die Ausgestaltung der Auftragsdatenverarbeitung	244
B. Meldepflicht bei Datenschutzverletzungen gemäß Art. 33 DSGVO	244
I. Ziele und Zwecke	245
1. Schutz der Persönlichkeitsrechte	245
2. Ermöglichung behördlicher Datenschutzmaßnahmen	246
3. Präventive Erhöhung der Datensicherheit	246
4. Betroffenenbenachrichtigung: Verringerung von Schäden	247
II. Kompetenzen	247
III. Adressaten	247
IV. Räumlicher Anwendungsbereich	248
1. Sitzprinzip für Stellen und Niederlassungen innerhalb der EU	249
2. Marktortprinzip für Stellen und Niederlassungen außerhalb der EU	249
3. Anwendbarkeit aufgrund internationalen Rechts	251
V. Meldepflichtige Vorfälle	251
1. Erfasste Datenkategorien	251
2. Meldetatbestand	252
a) Schutzverletzung	252
b) Übermittlung, Speicherung oder Verarbeitung auf sonstige Weise	254
c) Bekanntwerden der Verletzung	254

d) Risiko für die Rechte und Freiheiten natürlicher Personen	255
e) Wahrscheinlichkeit für ein hohes Risiko (bei Betroffenenbenachrichtigung gemäß Art. 34 DSGVO)	256
3. Entfallen der Betroffenenbenachrichtigung gemäß Art. 34 Abs. 3 DSGVO	257
VI. Inhalt der Meldung	258
VII. Adressaten, Form und Zeitpunkt der Meldung	259
1. Adressaten	259
a) Sonderfall: Meldeadressat für Stellen mit Sitz in Drittstaaten	260
b) Sonderfall: Meldeadressat bei Datenschutzverletzungen in Niederlassungen	261
2. Form	261
3. Zeitpunkt	262
a) Zeitpunkt der Informierung der Aufsichtsbehörde	262
b) Zeitpunkt der Benachrichtigung der Betroffenen	263
c) Ausnahmen von der unverzüglichen Meldung und Benachrichtigung	264
4. Besonderheit: Dokumentationspflicht	265
VIII. Daten- und Geheimnisschutz	265
1. Datenschutz	266
2. Geheimnisschutz	267
IX. Verhältnismäßigkeit	268
X. Rechtsdurchsetzung	269
1. Vollstreckung	270
2. Sanktionen	271
XI. Weitere Verwendung der übermittelten Informationen	273
1. Übermittlung personenbezogener Daten an andere Behörden	273
2. Übermittlung nicht-personenbezogener Daten an andere Behörden	275
3. Verwendung im Straf- und Ordnungswidrigkeitsverfahren	275
a) Vorliegen der nemo-tenetur-Problematik	275
b) Ungeschriebenes Verwendungsverbot	276
4. Veröffentlichung	277
a) Informierung der Öffentlichkeit durch die Aufsichtsbehörde	277
b) Informationszugangsrechte	278
XII. Zivilrechtliche Auswirkungen	279
1. Haftung bei Verstößen gegen Art. 33 und Art. 34 DSGVO	279
2. Haftung von Auftragsdatenverarbeitern	280
3. Gerichtszuständigkeit	281

Inhaltsverzeichnis

C. Meldepflicht für Betreiber elektronischer Kommunikationsdienste	281
I. Europarechtliche Vorgaben gemäß Art. 4 Abs. 3-5 EK-DSRL und VO Nr. 611/2013 EU	281
1. Allgemeines	281
2. Detailregelungen in VO Nr. 611/2013 EU	282
3. Kompetenz	283
4. Tatbestand	284
a) Adressaten	284
b) Meldetatbestand	286
5. Rechtsfolgen	286
II. Meldepflicht gemäß § 109a Abs. 1 TKG	287
1. Ziele und Zwecke	288
a) Schutz der Persönlichkeitsrechte	288
b) Ermöglichung behördlicher Datenschutzmaßnahmen	288
c) Präventive Erhöhung der Datensicherheit	289
d) Keine weitergehenden Schutzziele	289
e) Betroffenenbenachrichtigung: Verringerung von Schäden	290
2. Kompetenzen	290
3. Adressaten	291
a) Öffentlich zugängliche Telekommunikationsdienste	291
b) Verhältnis zu § 15a TMG	291
aa) Abgrenzung TKG - TMG	292
bb) Sonderfall: Anwendung der Datenschutz- regelungen des TKG gemäß § 11 Abs. 3 TMG	293
c) Benachrichtigungspflicht gegenüber Betroffenen auch für Anbieter nicht-öffentlicher TK-Dienste	294
d) Diensteeerbringung durch Dritte	295
4. Räumlicher Anwendungsbereich	295
a) Anknüpfung an Diensteeerbringung im Inland	296
b) Analoge Anwendung des § 1 Abs. 5 BDSG	297
aa) Sitz des Erbringers im Inland	299
bb) Sitz des Erbringers im europäischen Ausland	299
cc) Sitz des Erbringers im europäischen Ausland mit Niederlassung im Inland	300
dd) Sitz des Erbringers im außereuropäischen Ausland	300
ee) Sitz des Erbringers im außereuropäischen Ausland mit Niederlassung im Inland	301
ff) Zusammenfassung	301
5. Meldepflichtige Vorfälle	302
a) Erfasste Datenkategorien	302
b) Meldetatbestand	303
aa) Zusammenhang mit der Diensteeerbringung	303

bb) Verletzung der Datensicherheit	304
cc) Feststellung der Schutzverletzung	307
dd) Unrechtmäßige Verwendung personenbezogener Daten	308
ee) Unrechtmäßiger Zugang zu personenbezogenen Daten	309
ff) Bei Betroffenenbenachrichtigung: Schwerwiegende Beeinträchtigung	309
c) Entfallen der Betroffenenbenachrichtigung gemäß § 109a Abs. 1 S. 3 TKG	310
aa) Zeitpunkt des Nachweises eines Sicherheitskonzepts	310
bb) Kein Ausreichen eines abstrakten Sicherheitskonzepts	311
cc) Anforderungen an das Sicherheitskonzept	311
6. Inhalt der Meldung	312
a) Inhalte der Meldung an die Aufsichtsbehörden	312
aa) Art und Inhalt der betroffenen personenbezogenen Daten	314
bb) Kontaktstellen iSd. § 109a Abs. 2 S. 1 Nr. 2 TKG	314
b) Inhalte bei der Betroffenenbenachrichtigung	315
7. Adressat, Form und Zeitpunkt der Meldung	315
a) Adressaten	315
b) Form	316
c) Zeitpunkt	317
aa) Zeitpunkt der Meldung an die Aufsichtsbehörden	318
bb) Zeitpunkt der Betroffenenbenachrichtigung	318
cc) Ausnahmen von der unverzüglichen Benachrichtigung der Betroffenen	319
d) Besonderheit: Verzeichniserstellung	320
8. Daten- und Geheimnisschutz	320
a) Datenschutz	321
b) Geheimnisschutz	321
9. Verhältnismäßigkeit	322
10. Rechtsdurchsetzung	324
a) Vollstreckung	324
aa) Unmittelbare Benachrichtigung der Betroffenen durch die BNetzA	324
bb) Unmittelbare Benachrichtigung der Betroffenen durch den BfDI	325
cc) Verpflichtung der meldepflichtigen Stelle zur Unterrichtung der Betroffenen	326
b) Sanktionen	327

Inhaltsverzeichnis

aa) Vorsätzlich nicht oder fehlerhaft erfolgte Meldung	327
bb) Fahrlässig unterbliebene Feststellung	328
11. Weitere Verwendung der Informationen	329
a) Informationsübermittlung an andere Behörden	329
aa) Übermittlung personenbezogener Daten durch den BfDI	329
bb) Übermittlung personenbezogener Daten durch die BNetzA	330
cc) Übermittlungseinschränkungen	331
dd) Übermittlung nicht-personenbezogener Daten	331
b) Verwendung im Straf- und Ordnungswidrigkeitsverfahren	332
c) Veröffentlichung	332
aa) Keine Informierung der Öffentlichkeit gemäß § 38 Abs. 1 S. 6 BDSG	333
bb) Informierung der Öffentlichkeit im Wege der Ersatzvornahme	333
cc) Unterrichtung der Öffentlichkeit durch Tätigkeitsberichte	334
dd) Öffentlichkeitsinformierung ohne spezielle gesetzliche Ermächtigungsgrundlage	334
ee) Informationszugangsrechte	335
12. Zivilrechtliche Auswirkungen	335
D. Sonstige datenschutzrechtliche Meldepflichten im nationalen Recht	336
I. Meldepflicht für Diensteanbieter gemäß § 15a TMG	337
1. Allgemeines	337
2. Tatbestand	338
3. Rechtsfolgen	340
II. Meldepflicht im Zusammenhang mit Sozialdaten gemäß § 83a SGB X	340
1. Allgemeines	341
2. Tatbestand	341
3. Rechtsfolgen	342
III. Meldepflicht im Zusammenhang mit intelligenten Strommesssystemen gemäß § 21h Abs. 2 EnWG	343
1. Allgemeines	343
2. Tatbestand	343
3. Rechtsfolgen	345
IV. Meldepflichten in den Landesdatenschutzgesetzen	346
1. Berlin: Meldepflicht gemäß § 18a BlnDSG	346
2. Rheinland-Pfalz: Meldepflicht gemäß § 18a LDSG-RP	347
3. Schleswig-Holstein: Meldepflicht gemäß § 27a LDSG-SH	348

E. Exkurs: Die Nutzerbenachrichtigungspflicht gemäß § 109a	
Abs. 4 TKG	349
I. Unklare Ziele und Zwecke	349
1. Schutz der Persönlichkeitsrechte und Verringerung von Schäden	349
2. Nicht: Schutz der Integrität und Verfügbarkeit der TK-Dienste und TK-Infrastruktur	350
II. Räumlicher Anwendungsbereich	351
III. Unklarer Tatbestand	351
1. Bezugsobjekt	352
2. Art und Ausmaß der Störung	354
IV. Rechtsfolgen	354
V. Verhältnismäßigkeit	356
VI. Zivilrechtliche Auswirkungen	357
§ 4 Meldepflichten im Bereich Kritischer Infrastrukturen und besonderer IT-Dienste	361
A. Meldepflichten für Kritische Infrastrukturen und digitale Dienste in der NIS-RL	361
I. Ziele und Zwecke	362
1. Verbesserung des Funktionieren des Binnenmarktes	362
2. Funktionsfähigkeit der wesentlichen Dienste	362
3. Förderung der IT-Sicherheit durch Informationsaustausch	363
4. Präventive Erhöhung der IT-Sicherheit	364
5. Keine Strafverfolgung und Datenschutz	364
II. Kompetenzen	365
1. Vereinheitlichung des Binnenmarktes	366
a) Der Begriff des Binnenmarktes	366
b) Subjektive Zielsetzung	367
c) Notwendigkeit eines objektiven Binnenmarktbezugs	367
d) Objektiver Binnenmarktbezug zur Verwirklichung der Grundfreiheiten	368
e) Objektiver Binnenmarktbezug zur Beseitigung von Wettbewerbsverzerrungen	372
f) Rechtsprechungspraxis des EuGH zum Binnenmarktbezug	373
g) Verpflichtung auf ein hohes Schutzniveau	376
h) Schranke des Subsidiaritätsgrundsatzes	376
i) Zwischenergebnis	377
2. Transeuropäische Netze	377
3. Polizeiliche Zusammenarbeit	377

Inhaltsverzeichnis

4. Energiepolitik	379
III. Adressaten	379
1. Betreiber wesentlicher Dienste	379
a) Verfahren zur Ermittlung der erfassten Betreiber	380
aa) Beschränkung auf die Art der Einrichtungen	380
bb) Erbringung eines wesentlichen Dienstes	380
cc) Abhängigkeit des Dienstes von Netzen und Informationssystemen	381
dd) Erhebliche Störungsauswirkungen	381
ee) Sonderfall: Dienstebereitstellung in mindestens zwei Mitgliedstaaten	382
b) Betreiber	382
c) Sektoren	383
2. Anbieter digitaler Dienste	383
3. Einschränkungen des Adressatenkreises	384
IV. Räumlicher Anwendungsbereich	385
V. Meldepflichtige Vorfälle	386
1. Meldetatbestand des Art. 14 Abs. 3 NIS-RL	386
2. Meldetatbestand des Art. 16 Abs. 3 NIS-RL	387
VI. Inhalt der Meldung	388
VII. Adressat, Form und Zeitpunkt der Meldung	388
VIII. Daten- und Geheimnisschutz	389
IX. Verhältnismäßigkeit	389
X. Rechtsdurchsetzung	390
XI. Weitere Verwendung der Informationen	390
1. Übermittlung an andere Behörden	391
a) Informationsaustausch zwischen zuständiger Behörde, CSIRT und zentraler Anlaufstelle	391
b) Informationsaustausch zwischen den Mitgliedsstaaten	391
2. Verwendung im Straf- und Ordnungswidrigkeitsverfahren	392
3. Veröffentlichung	393
XII. Zivilrechtliche Auswirkungen	393
B. Meldepflichten für Betreiber Kritischer Infrastrukturen im nationalen Recht	394
I. Meldepflicht für Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 BSIG	394
1. Ziele und Zwecke	395
a) Funktionsfähigkeit der Kritischen Infrastrukturen und Sicherstellung des Funktionierens des Gemeinwesens	395
b) Förderung der IT-Sicherheit Kritischer Infrastrukturen	395
aa) Informationen nicht als Wissensgrundlage für weitere Maßnahmen durch das BSI	396
bb) Anordnungen durch die Aufsichtsbehörden	397

c)	Kenntnis von der Sicherheitslage bei Kritischen Infrastrukturen	397
d)	Präventive Erhöhung der IT-Sicherheit Kritischer Infrastrukturen	398
e)	Keine Strafverfolgung und Schutz der IT-Sicherheit von Privatpersonen	398
2.	Kompetenzen	399
a)	Sektorspezifische Gesetzgebungskompetenzen	399
b)	Gesetzgebungskompetenz aus Art. 74 Abs. 1 Nr. 11 GG	399
c)	Subsidiaritätsklausel des Art. 72 Abs. 2 GG	401
3.	Adressaten	404
a)	Zum Begriff der Kritischen Infrastrukturen	404
aa)	Begriffsbestandteile <i>Kritisch</i> und <i>Infrastruktur</i>	405
bb)	Verwendung in der Rechts- und Wirtschaftswissenschaft	406
cc)	Keine Begriffsaufteilung in der Definition des § 2 Abs. 10 BSIG	407
b)	Einrichtungen und Anlagen	408
aa)	Einrichtungen	408
bb)	Anlagen	408
cc)	Teile von Einrichtungen und Anlagen	410
dd)	Funktionales Verständnis	410
c)	Hohe Bedeutung für das Funktionieren des Gemeinwesens	411
aa)	Funktionieren des Gemeinwesen	412
bb)	Begriff der hohen Bedeutung	413
cc)	Beeinträchtigungs- und Ausfallfolgen	414
d)	Sektoren	417
e)	Konkretisierung durch Rechtsverordnung	419
aa)	Verfassungsmäßigkeit der Verordnungsermächtigung des § 10 Abs. 1 S. 2 BSIG	420
bb)	Kriterien zur Konkretisierung	422
f)	Betreiber	423
g)	Zusätzliche branchenspezifische Einschränkungen	425
h)	Zusätzliche größenspezifische Einschränkung	426
i)	Ausgestaltung der BSI-KritisV	427
4.	Räumlicher Anwendungsbereich	428
a)	Feststellung der extraterritorialen Anwendung des § 8b Abs. 4 BSIG durch Auslegung	429
aa)	Territorialitätsprinzip	431
bb)	Schutzprinzip	432
cc)	Wirkungsprinzip	433
dd)	Personalitätsprinzip	434

Inhaltsverzeichnis

ee) Weltrechtsprinzip	435
ff) Organisationshoheitsprinzip	435
gg) Zwischenergebnis	436
b) Reichweite der extraterritorialen Anwendung in unterschiedlichen Sachverhaltskonstellationen	436
aa) Allein IT-System im Ausland	436
bb) Allein Betreibersitz im Ausland	438
cc) Allein Kritische Infrastruktur im Ausland	439
dd) IT-System und Kritische Infrastruktur im Ausland	440
ee) Betreibersitz und Kritische Infrastruktur im Ausland	440
ff) Betreibersitz und IT-System im Ausland	441
gg) Sonderfall: Kritische Infrastruktur im Ausland mit Inlandsauswirkungen	441
c) Völker- und verfassungsrechtliche Grenzen	443
d) Zusammenfassung	444
5. Meldepflichtige Vorfälle	445
a) Begriff der Störung	445
b) Erheblichkeit der Störung	446
aa) Ausfall oder Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen	448
bb) Prognoseentscheidung	449
c) Bezugspunkt der Störung	450
6. Inhalt der Meldung	450
a) Notwendige Inhalte	450
b) Nennung des Betreibers	453
7. Adressat, Form und Zeitpunkt der Meldung	453
a) Adressat	453
b) Form	454
c) Zeitpunkt	454
aa) Gestufte Meldung	455
bb) Keine Ausnahme: <i>responsible disclosure</i>	456
cc) Keine Ausnahme: Strafverfolgung	457
8. Daten- und Geheimnisschutz	457
a) Datenschutz	457
b) Geheimnisschutz	458
9. Verhältnismäßigkeit	459
10. Rechtsdurchsetzung	460
a) Kenntnis von einem Pflichtverstoß	460
b) Vollstreckung	461
aa) Anordnungsbefugnis	461
bb) Verwaltungsvollstreckung	463
c) Sanktionen	463

11. Weitere Verwendung der Informationen	464
a) Übermittlung personenbezogener Daten an andere Behörden	465
aa) Keine Ausnahmen vom Zweckbindungsgrundsatz	465
bb) Übermittlung personenbezogener Daten gemäß § 8b Abs. 2 Nr. 1 BSIG	466
cc) Übermittlung personenbezogener Daten gemäß § 8b Abs. 2 Nr. 2 BSIG	467
dd) Übermittlung personenbezogener Daten gemäß § 8b Abs. 2 Nr. 3 BSIG	468
ee) Übermittlung personenbezogener Daten gemäß § 8b Abs. 2 Nr. 4 BSIG	468
ff) Keine Übermittlung personenbezogener Daten im Wege der Amtshilfe	470
gg) Übermittlungseinschränkungen	470
b) Übermittlung nicht-personenbezogener Daten an andere Behörden	470
aa) Übermittlungsvoraussetzungen	471
bb) Übermittlungseinschränkungen	472
cc) Übermittlungspflicht	472
c) Verwendung im Straf- und Ordnungswidrigkeitsverfahren	473
aa) Vorliegen der <i>nemo-tenetur</i> -Problematik	473
bb) Folgen	474
d) Veröffentlichung	477
aa) Rechtliche Ausgangslage und betroffene Interessen	477
bb) Informierung anderer Betreiber durch das BSI gemäß § 8b Abs. 2 Nr. 4 BSIG	478
cc) Unterrichtung der breiten Öffentlichkeit gemäß § 7 BSIG	480
dd) Unterrichtung der Öffentlichkeit durch den Tätigkeitsbericht gemäß § 13 BSIG	485
ee) Öffentlichkeitsinformierung ohne spezielle gesetzliche Ermächtigungsgrundlage	485
ff) Informationszugangsrechte	486
gg) Verhältnismäßigkeit	487
hh) Zwischenergebnis	488
12. Zivilrechtliche Auswirkungen	488
a) Ansprüche Dritter bei Verstößen gegen § 8b Abs. 4 BSIG	489
b) Einfluss des § 8b Abs. 4 BSIG auf zivilrechtliche Ansprüche	490

Inhaltsverzeichnis

c) Einfluss des § 8b Abs. 4 BSIG auf die Vertragsgestaltung bei der Auslagerung von IT-Systemen	491
II. Meldepflicht für atomrechtliche Genehmigungsinhaber gemäß § 44b AtomG	492
1. Ziele und Zwecke	492
2. Kompetenzen	493
3. Adressaten	493
4. Räumlicher Anwendungsbereich	494
5. Meldepflichtige Vorfälle	494
a) Beeinträchtigungen informationstechnischer Systeme, Komponenten oder Prozesse	495
b) Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit	496
6. Inhalt der Meldung	497
7. Adressat, Form und Zeitpunkt der Meldung	497
8. Daten- und Geheimnisschutz	497
9. Verhältnismäßigkeit	498
10. Rechtsdurchsetzung	498
11. Weitere Verwendung der Informationen	498
a) Informationsübermittlung an andere Behörden	499
b) Verwendung im Straf- und Ordnungswidrigkeitsverfahren	499
c) Veröffentlichung	499
12. Zivilrechtliche Auswirkungen	500
III. Meldepflicht für Betreiber von Energieversorgungsnetzen und Energieanlagen gemäß § 11 Abs. 1c EnWG	501
1. Ziele und Zwecke	501
2. Kompetenzen	501
3. Adressaten	502
4. Räumlicher Anwendungsbereich	502
5. Meldepflichtige Vorfälle	503
6. Inhalt der Meldung	503
7. Adressat, Form und Zeitpunkt der Meldung	504
a) Meldung über eine übergeordnete Ansprechstelle	504
b) Keine Obliegenheit zu einer geschwärzten Meldung	505
8. Daten- und Geheimnisschutz	506
9. Verhältnismäßigkeit	507
10. Rechtsdurchsetzung	507
11. Weitere Verwendung der Informationen	507
a) Informationsübermittlung an andere Behörden	507
b) Verwendung im Straf- und Ordnungswidrigkeitsverfahren	508
c) Veröffentlichung	509

12. Zivilrechtliche Auswirkungen	509
IV. Umsetzungsbedarf hinsichtlich der NIS-Richtlinie	510
1. Adressatenkreis	510
a) Kein Umsetzungsbedarf bei Betreibern wesentlicher Dienste	510
b) Umsetzungsbedarf bei Anbietern digitaler Dienste	511
2. Kein Umsetzungsbedarf beim Meldetatbestand	513
3. Pseudonymisierte Meldungen	513
4. Informationsverwendung	514
5. Haftungsfolgen	514
C. Meldepflichten für TK-Unternehmen	514
I. Europarechtliche Vorgaben für TK-Unternehmen durch Art. 13a Abs. 3 RRL	514
1. Allgemeines	515
2. Kompetenz	515
3. Tatbestand	516
a) Adressaten	516
b) Meldetatbestand	517
4. Rechtsfolgen	518
II. Meldepflicht für TK-Unternehmen gemäß § 109 Abs. 5 TKG	520
1. Ziele und Zwecke	520
a) Förderung leistungsfähiger TK-Infrastrukturen und die flächendeckende Gewährleistung von TK-Dienstleistungen	520
b) Schutz der Integrität und Verfügbarkeit der Netze und Dienste	521
c) Kenntnis von der Sicherheitslage	522
d) Präventive Erhöhung der IT-Sicherheit	522
e) Kein Schutz der erbrachten Dienste oder einzelner Nutzersysteme	523
f) Kein Datenschutz	523
2. Kompetenzen	524
3. Adressaten	524
4. Räumlicher Anwendungsbereich	525
a) Keine analoge Anwendung des § 1 Abs. 5 BDSG	525
b) Anknüpfung an Netzbetrieb und Dienstleistung im Inland	526
c) Kein zusätzlicher Inlandsbezug notwendig	526
5. Meldepflichtige Vorfälle	527
a) Beeinträchtigungen	528
b) Beträchtliche Sicherheitsverletzungen	528
c) Störungen der Dienstverfügbarkeit und Möglichkeit des Zugriffs auf Nutzersysteme	529

Inhaltsverzeichnis

d) Kriterien im Umsetzungskonzept	530
6. Inhalt der Meldung	531
7. Adressat, Form und Zeitpunkt der Meldung	531
8. Daten- und Geheimnisschutz	532
9. Verhältnismäßigkeit	533
10. Rechtsdurchsetzung	534
11. Weitere Verwendung der Informationen	534
a) Übermittlung personenbezogener Daten an andere Behörden	535
aa) Keine spezielle Zweckbindung	535
bb) Übermittlungsbefugnisse	535
b) Übermittlung nicht-personenbezogener Daten an andere Behörden	537
c) Verwendung im Straf- und Ordnungswidrigkeitsverfahren	538
d) Veröffentlichung	538
aa) Ermächtigungsgrundlage in § 109 Abs. 5 S. 7 TKG	538
bb) Unterrichtung der Öffentlichkeit durch Tätigkeitsberichte	540
cc) Öffentlichkeitsinformierung ohne spezielle gesetzliche Ermächtigungsgrundlage	540
dd) Informationszugangsrechte	540
12. Zivilrechtliche Auswirkungen	540
D. Meldepflicht für Vertrauensdiensteanbieter gemäß Art. 19 Abs. 2 eIDAS-VO	541
I. Ziele und Zwecke	542
1. Förderung des Vertrauens in elektronische Transaktionen und des Binnenmarkts	542
2. Schutz von Persönlichkeitsrechten	542
3. Förderung der Sicherheit der Vertrauensdiensteanbieter	543
4. Betroffenenbenachrichtigung: Verringerung von Schäden	543
II. Kompetenzen	544
III. Adressaten	544
IV. Räumlicher Anwendungsbereich	544
V. Meldepflichtige Vorfälle	545
1. Sicherheitsverletzung und Integritätsverlust	545
2. Erhebliche Auswirkungen	546
VI. Inhalt der Meldung	547
VII. Adressaten, Form und Zeitpunkt der Meldung	547
1. Adressaten	548
2. Form	548
3. Zeitpunkt	548
VIII. Daten- und Geheimnisschutz	549

IX. Verhältnismäßigkeit	549
X. Rechtsdurchsetzung	550
XI. Weitere Verwendung der Informationen	550
XII. Zivilrechtliche Auswirkungen	551
§ 5 - Folgerungen	553
A. Ziele und Zwecke gesetzlicher Meldepflichten	553
I. Keine ausdrücklichen Zielbestimmungen	553
II. Systematisierung der identifizierten Ziele und Zwecke	554
1. Ziele und Zwecke der datenschutzrechtlichen Meldepflichten	554
2. Ziele und Zwecke der Meldepflichten im Bereich Kritischer Infrastrukturen und besonderer IT-Dienste	556
3. Wesentliche Unterschiede	557
III. Meldepflichten nicht speziell zu Strafverfolgungszwecken	557
B. Kompetenzgrundlagen für Meldepflichten bei IT-Sicherheitsvorfällen	558
C. Adressaten der Meldepflicht	559
I. Bestimmung des Adressatenkreises durch Rechtsverordnung	560
II. Beschränkung der Adressaten auf eine gewisse Mindestgröße	560
III. Beauftragung Dritter	561
D. Räumlicher Anwendungsbereich von Meldepflichten	561
I. Fehlende Regelungen zum räumlichen Anwendungsbereich	562
II. Prämissen für ausdrückliche Regelungen im Datenschutzrecht	563
III. Prämissen für ausdrückliche Regelungen im Bereich Kritischer Infrastrukturen und besonderer IT-Dienste	564
E. Meldepflichtige Vorfälle	566
I. Uneinheitliche Meldetatbestände	566
II. Feststellung eines Sicherheitsvorfalls	568
III. Bedeutung der Verschlüsselung im Datenschutzrecht	568
H. Formvorschriften	569
F. Meldeinhalt	570
I. Präzise Vorgaben zu Meldeinhalten wünschenswert	570
II. Pseudonymisierte Meldungen	571
G. Adressaten der Meldungen	573
I. Zeitpunkt der Meldungen und Benachrichtigungen	574
J. Daten- und Geheimnisschutz	575
L. Verhältnismäßigkeit von Melde- und Benachrichtigungspflichten	576
M. Durchsetzung von Melde- und Benachrichtigungspflichten	577
N. Weitere Verwendung der Informationen	579

Inhaltsverzeichnis

I. Stärkere Ausgestaltung der gesetzlichen Regelungen zur Informationsverwendung	579
II. Informationsverwendung im Datenschutzrecht auch zu präventiven Zwecken	580
III. Anonymisierter europaweiter Informationsaustausch	580
IV. Verwendungsverbote im Straf- und Ordnungswidrigkeitsverfahren	581
V. Veröffentlichung von meldepflichtigen Vorfällen und Informationen	582
IV. Informationszugangsrechte	583
O. Zivilrechtliche Auswirkungen von Meldepflichten	583