

Thomas Warnecke

Identitätsmanagement und Datenschutz

**Verantwortung für einen datenschutzgerechten
Zugang zu transaktionsbezogenen E-Government-
Anwendungen unter besonderer Berücksichtigung
der De-Mail-Dienste und des neuen Personalausweises**

Wissenschaftliche Beiträge aus dem Tectum Verlag

Reihe Rechtswissenschaften

Wissenschaftliche Beiträge aus dem Tectum Verlag

Reihe Rechtswissenschaften
Band 118

Thomas Warnecke

Identitätsmanagement und Datenschutz

**Verantwortung für einen datenschutzgerechten
Zugang zu transaktionsbezogenen
E-Government-Anwendungen unter besonderer
Berücksichtigung der De-Mail-Dienste
und des neuen Personalausweises**

Tectum Verlag

Thomas Warnecke

Identitätsmanagement und Datenschutz

Verantwortung für einen datenschutzhinweis Zugang zu transaktionsbezogenen
E-Government-Anwendungen unter besonderer Berücksichtigung der De-Mail-
Dienste und des neuen Personalausweises

Zugl. Diss. Christian-Albrechts-Universität zu Kiel 2017

Wissenschaftliche Beiträge aus dem Tectum Verlag,

Reihe: Rechtswissenschaften; Bd. 118

© Tectum Verlag – ein Verlag in der Nomos Verlagsgesellschaft, Baden-Baden 2019

ISBN: 978-3-8288-4055-3

eISBN: 978-3-8288-6925-7

ePub: 978-3-8288-6926-4

ISSN: 1861-7875

Druck und Verarbeitung: CPI buchbuecher.de, Birkach

Printed in Germany

Alle Rechte vorbehalten

Informationen zum Verlagsprogramm finden Sie unter

www.tectum-verlag.de

Bibliografische Informationen der Deutschen Nationalbibliothek

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

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche
Nationalbibliografie; detailed bibliographic data are available online
at <http://dnb.ddb.de>.

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2015/2016 von der Rechtswissenschaftlichen Fakultät der Christian-Albrechts-Universität zu Kiel als Dissertation angenommen.

Bedanken möchte ich mich bei meinem Doktorvater Prof. Dr. Utz Schliesky für die Erstellung des Erstgutachtens. Bei Prof. Dr. Christoph Brüning bedanke ich mich für die zügige Erstellung des Zweitgutachtens.

Insbesondere möchte ich mich bei Herrn Lennart Giesse und Frau Claudia Fränzner für die stets hervorragende bibliothekarische Unterstützung und die stets freundschaftliche Atmosphäre in der Bibliothek bedanken. Ebenso bedanke ich mich bei Brigitte Müller-Hecht für die bibliothekarische Unterstützung.

Darüber hinaus bedanke ich mich bei Sylvia Weidenhöfer für die kollegiale Zusammenarbeit.

Meinem Kollegen Martin Stabno danke ich für fachlichen Austausch zu allen Fragen des Datenschutzes und das Lesen des Manuskriptes. Darüber hinaus danke ich meinem Kollegen Nikolai Jaklitsch für den fachlichen Austausch in der Praxis.

Dr. Andreas Neumann und Nils Löwe danke ich ebenfalls für das Lesen des Manuskripts.

Schließlich gilt mein besonderer Dank meinen Eltern, Frau Elisabeth Warnecke und Herrn Dr. Hinrich Warnecke, die immer für mich da sind. Ohne die hervorragende Unterstützung wäre die Erstellung dieser Arbeit nicht möglich gewesen. Wir freuen uns, dass wir alle wohlbehalten die Fertigstellung dieser Arbeit erleben dürfen. Ihnen widme ich diese Arbeit.

Inhaltsverzeichnis

Teil 1: Einführung in den Untersuchungsgegenstand	1
A. Problemstellung	1
B. Gang der Untersuchung	5
Teil 2: Grundbegriffe und Ausgangslage	7
A. Identität	7
I. Identität und Identifizierung	8
1. Identitätsdaten	9
a) Personalien	10
b) Personenkennzeichen	10
c) Biometrische Merkmale	11
d) Identitätsdaten bei elektronischer Kommunikation	11
e) Identität als Identifizierung durch den Kommunikationspartner	13
2. Identitätsattribute	13
3. Identifikatoren	13
4. Digitale Identitäten	14
5. Partielle Identitäten	15
II. Identität im Recht	16
III. Identitäten juristischer Personen	18
IV. Identitätsmanagement	19
B. Begriff und Steuerung des E-Governments in Deutschland	22
I. Begriff des E-Governments	22
1. Begriffsentwicklung	22
2. Abgrenzung zu E-Justice	24
3. Interaktionsstufen von E-Government	26
a) Information	26
b) Kommunikation	26
c) Transaktion	27
4. Prozessorientierung	28
II. IT-Planungsrat	28
III. Nationale E-Government-Strategie (NEGS)	30
IV. Bestandteil der Digitalen Agenda 2014-2017	31
C. Identitätsmanagement im E-Government	32
I. Medienbruchfreie Prozesse	32

II. Identifizierung des Nutzers	33
III. Gefahren und Herausforderungen der elektronischen Kommunikation	35
1. Generelle Gefahren	36
a) Die Transnationalität der Datenverarbeitung.....	36
b) Angriffe auf die Kommunikationswege und Kompromittierung von Transaktionen.....	36
aa) Unsicherheit der „einfachen“ E-Mail.....	36
bb) Angriffe auf den Login eines Nutzers	37
cc) Missbrauch einer Nutzeridentität bzw. Identitätsmissbrauch	38
dd) Man-in-the-middle-Angriffe	39
ee) Computerviren, Würmer und Trojaner	39
ff) Zugriffe durch den Staat und Private	40
c) Mangelnde Nachvollziehbarkeit von Veränderungen in der digitalen Welt.....	41
d) Mehrdimensionalität des Internets.....	41
e) Trennung in Frontoffice- und Backoffice-Strukturen	42
f) Vernetzung und Dezentralität des Internets.....	43
2. Spezifische Gefahren.....	43
a) Anwachsen der Bestände personenbezogener Daten bei informationstechnischen Kommunikationsinfrastrukturen	43
b) Verlagerung der Datenverarbeitung auf Private.....	44
c) Gefahr des Datenmissbrauchs	45
d) Angewiesenheit auf Private bei der Entwicklung der Informationstechnologie	45
3. Nutzertypologie, „Digital Natives“ und „Digital Divide“	46
a) Nutzertypologie	46
aa) Die sog. Digital Outsiders	46
bb) Die sog. Digital Immigrants.....	47
cc) Die sog. Digital Natives	48
dd) Unterschiedliche digitale Verantwortungsbereitschaft.....	49
b) Digitale Spaltung bzw. „Digital Divide“	49
c) Digitaler Graben zwischen Verwaltung und Bürger?.....	50
4. Akteure im E-Government	50
a) Vielzahl von Akteuren	50
b) Bürger und Verwaltung.....	51
c) Die Wirtschaft als Nutzer	52
5. Datenschutzbewusstsein des Nutzers	53
a) Grundsätzliche Sensibilisierung des Nutzers	53
b) Widersprüchliche Veröffentlichungsgewohnheiten in der virtuellen und der analogen Welt	54
c) Privatsphäre im Netz	55
d) Bewusstsein über Datenspuren im Netz.....	55
e) Fahrlässiges Verhalten bei einfachen Identifikator-Lösungen	55
f) Datenschutz als Bildungsaufgabe und Medienkompetenz.....	56
g) Datenhoheit des Nutzers	58

6.	Vertrauen des Nutzers	59
a)	Vertrauen gegenüber dem Kommunikationspartner	60
b)	Vertrauen in die Kommunikationsinfrastruktur	62
c)	Vertrauensbildung gegenüber dem Nutzer	63
7.	Konvergenz von Diensten und Infrastrukturen	64
a)	Infrastruktur	65
aa)	Infrastruktur zur staatlichen Aufgabenerfüllung	65
bb)	Individuelle Infrastruktur des Nutzers	66
b)	Dienste.....	66
8.	Transaktionsbezogenes E-Government durch die Verwaltung	67
a)	Multikanalprinzip als Leitbild	67
b)	Gateway-Lösungen	68
c)	Dokumentenmanagementsysteme und Vorgangsbearbeitungssysteme	68
d)	Anschlussfähigkeit der verwendeten Systeme	69
e)	Nutzenpotenziale	69
9.	Grenzen der Steuerungswirkung rechtlicher Instrumente	70
a)	Recht und Realbedingungen	70
b)	Verrechtlichung und Steuerungswirkung	70
c)	Mündiger Nutzer	72
IV.	Datenschutz und Datensicherheit.....	72
1.	Daten.....	72
2.	Informationen	73
3.	Datenschutz.....	73
4.	Datensicherheit	74
a)	Schutzziel Verfügbarkeit.....	75
b)	Schutzziel Integrität	75
c)	Schutzziel Vertraulichkeit	75
d)	Schutzziel Transparenz	75
e)	Schutzziel Nicht-Verkettbarkeit	76
f)	Schutzziel Intervenierbarkeit.....	76
g)	Bedeutung der Schutzziele	76
5.	Zielkonflikte von Datenschutz und Datensicherheit im E-Government	77
6.	Datenschutz und Datensicherheit als Akzeptanzfaktoren im E-Government.....	78
D.	Identitätsmanagement-Infrastrukturen für E-Government-Anwendungen	78
I.	Die eID-Funktion des neuen Personalausweises	79
II.	Das De-Mail-Konzept	80
1.	Mailversand über De-Mail	82
2.	Identitätsbestätigungsdiens De-Ident.....	83
3.	Dokumentensafe: De-Safe	83
4.	„Rechtssicherheit“ durch vorherige Identifizierung beider Kommunikationspartner ...	83
III.	Hybride Kommunikationsmöglichkeiten.....	84
1.	Hybride Kommunikationsformen als Übergangsmöglichkeit	84
2.	Ersetzendes Scannen.....	85

IV. Die qualifizierte elektronische Signatur.....	85
V. Das Elektronische Gerichts- und Verwaltungspostfach (EGVP)	87
VI. Die elektronische Steuererklärung (ELSTER)	87
VII. Das POSTIDENT-Verfahren.....	88
VIII. Das E-Postident-Verfahren	89
E. Zusammenfassung Teil 2	89
Teil 3: Rechtliche Grundlagen für Identitätsmanagement im E-Government	91
A. Europarechtliche Vorgaben für den Datenschutz bei elektronischer Kommunikation.....	91
I. Datenschutzkonvention des Europarats (1981)	91
II. Empfehlung des Europarates zum Schutz personenbezogener Daten im Internet von 1999	92
III. Europäische Grundrechtecharta.....	94
IV. Europäische Datenschutzrichtlinie (DSRL)	95
V. Richtlinie für den Schutz personenbezogener Daten und der Privatsphäre in der elektronischen Kommunikation 2002/58/EG	99
VI. Richtlinie für den elektronischen Geschäftsverkehr (2000/31/EG)	100
VII. Richtlinie für elektronische Signaturen 1999/93/EG.....	101
VIII. Richtlinie zur Vorratsdatenspeicherung 2006/24/EG (2006).....	103
IX. Europäische Datenschutz-Grundverordnung (DS-GVO)	106
1. Vorbemerkung zur Entwicklung	106
2. Differenzierung von öffentlichem und nicht-öffentlichen Bereich.....	107
3. Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO	108
4. Risikobasierter Ansatz und Risikoanalyse.....	109
5. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO	109
6. Privacy by Design und Privacy by Default.....	111
7. Gemeinsames Verfahren nach Art. 26 DS-GVO	112
8. Transparenzpflichten und Betroffenenrechte nach Art. 12 bis 22 DS-GVO	113
a) Rahmenregelungen in Art. 12 DS-GVO	113
b) Informationspflicht bei Direkterhebung und Dritterhebung in Art. 13 und 14 DS-GVO	114
c) Auskunftsanspruch nach Art. 15 DS-GVO.....	114
d) Recht auf Berichtigung nach Art. 16 DS-GVO.....	115
e) Recht auf Löschung nach Art. 17 DS-GVO	115
f) Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO	115
g) Mitteilungspflicht nach Art. 19 DS-GVO	116
h) Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO	116
i) Widerspruchsrecht nach Art. 21 DS-GVO	117
j) Verbot automatisierter Entscheidungen einschließlich Profiling nach Art. 22 DS-GVO	117
k) Stärkung der Datenhoheit des Nutzers	117
9. Sanktions- und Haftungsregime für den Verantwortlichen	117
10. Meldepflichten nach Art. 33 und Art. 34 DS-GVO	118

11. Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO	119
12. Anpassung von Grundprinzipien und Abgrenzung zu anderen Vorschriften	119
X. Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung).....	121
XI. Das „Safe-Harbor-Urteil“ des Europäischen Gerichtshofs (EuGH).....	123
XII. Die E-Privacy-Verordnung.....	125
B. Europäische Impulse für elektronische Behördendienste	127
I. Mitteilung der Kommission über „Die Rolle elektronischer Behördendienste (E-Government) für die Zukunft Europas“	127
II. Ministererklärung von Malmö zum E-Government	127
III. EU-Dienstleistungsrichtlinie	128
C. Verfassungsrechtliche Vorgaben.....	129
I. Das allgemeine Persönlichkeitsrecht als Grundlage	130
II. Das Grundrecht auf informationelle Selbstbestimmung.....	132
1. Volkszählungsurteil des BVerfG.....	132
2. Schutzbereich	133
a) Subjektiv-abwehrrechtliche Schutzrichtung	134
aa) Eigentumsähnliches Herrschaftsrecht?	135
bb) Normgeprägter Schutzbereich wie bei Art. 14 GG?.....	136
cc) Lösungsansatz bei § 303 a StGB?	136
dd) Lösungsansätze im Kontext von Big Data?.....	137
ee) Stellungnahme	137
b) Objektiv-rechtliche Schutzrichtung.....	138
c) Stellungnahme	143
d) Konstitutionalisierung des Grundrechts auf Datenschutz?	144
3. Folgerungen für Identitätsmanagement im E-Government.....	147
a) Datenverarbeitung durch die Verwaltung.....	147
b) Datenverarbeitung durch private Diensteanbieter	148
c) Schutzziele des Grundrechts auf informationelle Selbstbestimmung.....	151
4. Verarbeitungsstadien	151
5. Eingriff in das Grundrecht auf informationelle Selbstbestimmung.....	151
a) Eingriffe in die Privatsphäre des Bürgers vor dem Volkszählungsurteil	152
b) Eingriffe in der Rechtsprechung des BVerfG	153
c) Begrenzung des Eingriffs durch eine Erheblichkeitsschwelle.....	155
6. Rechtfertigungsanforderungen für den Eingriff in das Grundrecht auf informationelle Selbstbestimmung.....	155
a) Schranken des Grundrechts auf informationelle Selbstbestimmung.....	155
b) Schranken-Schranken	156
aa) Gebot der Normenklarheit	156
bb) Grundsatz der Verhältnismäßigkeit.....	157
cc) Zweckbindungsgrundsatz	159
dd) Grundsatz der Amtshilfefestigkeit	159

ee) Grundsatz der informationellen Gewaltenteilung	160
ff) Transparenzgebot.....	160
gg) Organisatorische und verfahrensrechtliche Vorkehrungen	161
hh) Kontrolle durch einen unabhängigen Datenschutzbeauftragten	161
ii) Verwendungszusammenhang als quasi Schranken-Schranke.....	162
7. Zwischenergebnis.....	162
III. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität	
informationstechnischer Systeme	163
1. Das Urteil des BVerfG zur Online-Durchsuchung.....	164
2. Schutzbereich	164
a) Informationstechnisches System	165
b) Vertraulichkeit und Integrität	167
aa) Vertraulichkeit	167
bb) Integrität.....	168
cc) Verhältnis von Vertraulichkeit und Integrität.....	168
c) Subjektiv-rechtliche Schutzrichtung	169
d) Objektiv-rechtliche Schutzrichtung.....	169
e) Schutzlücken der bisherigen Kommunikationsgrundrechte	170
f) Stellungnahme	171
3. Eingriff in das IT-Grundrecht	171
4. Rechtfertigungsanforderungen für den Eingriff in das IT-Grundrecht	172
a) Schranken	172
b) Schranken-Schranken	172
5. Zwischenergebnis.....	173
IV. Das Fernmeldegeheimnis Art. 10 GG.....	173
1. Schutzbereich	174
a) Unkörperliche Übermittlung von Informationen	174
b) Schutzgewährleistung nur während des Übermittlungsvorganges	175
c) Subjektiv-rechtliche Schutzrichtung	176
d) Objektiv-rechtliche Schutzrichtung.....	176
2. Eingriff in das Fernmeldegeheimnis	177
3. Rechtfertigungsanforderungen für den Eingriff	177
a) Schranken	177
b) Schranken-Schranken	177
4. Zwischenergebnis.....	178
V. Grundrechtskonkurrenzen	178
1. Abgrenzung nach Phasen der Kommunikation und Transaktion	178
2. Verhältnis des Grundrechts auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses aus Art. 10 GG	179
3. Verhältnis des Grundrechts auf informationelle Selbstbestimmung, des IT-Grundrechts und des Fernmeldegeheimnisses	180
a) Systembezogenheit als Abgrenzungskriterium	180
b) Weitere Schutzbereichsausprägung des allgemeinen Persönlichkeitsrechts.....	181
c) Subsidiarität des IT-Grundrechts	181

4. Gemeinsame Grundrechtsschranken	182
5. Zwischenergebnis.....	183
D. Einfachgesetzliche Vorgaben	183
I. Anforderungen des Verwaltungsverfahrensrechts.....	184
1. Grundsatz der Nichtförmlichkeit des Verwaltungsverfahrens § 10 VwVfG	184
2. Schriftformerfordernis im Verwaltungsverfahren als Ausnahme.....	185
a) Identitätsfunktion	186
b) Echtheitsfunktion.....	186
c) Verifikationsfunktion	186
d) Perpetuierungsfunktion	187
e) Beweisfunktion	187
f) Warnfunktion	187
g) Abschlussfunktion	187
h) Verhältnis der Schriftformfunktionen zueinander.....	188
3. Ersetzung der Schriftform nach § 3a VwVfG.....	188
4. Zugangseröffnung nach § 3a VwVfG	189
a) Zugangseröffnung auf Nutzerseite	189
b) Zugangseröffnung auf Behördenseite	191
c) Zugangsschließung auf Nutzerseite als Ausdruck des Freiwilligkeitsprinzips	191
5. Identifizierbarkeit im Rahmen der elektronischen Kommunikation.....	192
6. Einleitung des Verwaltungsverfahrens mittels Antrag § 22 VwVfG	192
7. Elektronischer Verwaltungsakt § 37 VwVfG	193
II. Anforderungen des Verwaltungszustellungsrechts	195
1. Grundsatz: Wirksamkeit mit Bekanntgabe	195
2. Elektronische Zustellung gegen Empfangsbekanntnis	196
3. Elektronische Zustellung gegen Abholbestätigung mittels De-Mail	196
III. Anforderungen des E-Government-Gesetzes des Bundes.....	198
1. Integrierter Ansatz für E-Government	198
2. Geltungsbereich	200
3. Elektronischer Zugang zur Verwaltung	201
a) Freiwilligkeit für den Nutzer	201
b) Gesetzliche Verpflichtung der Behörde.....	202
c) Gesetzliche Absicherung des Multikanalprinzips.....	202
4. Einsatz der De-Mail als Schriftformersatz.....	203
5. Einsatz des neuen Personalausweises anstelle der Schriftform	204
6. Sichere behördendeninterne Prozesse zur Ersetzung der restlichen Funktionen der Schriftform.....	205
7. Modifizierung bestehender Schriftformerfordernisse	206
8. Elektronische Aktenführung und ersetzendes Scannen	206
a) Elektronische Aktenführung.....	206
b) Ersetzendes Scannen	208

9. Elektronische Akteneinsicht, Vorlage von Nachweisen und Abfrage des Verfahrensstandes	209
a) Elektronische Akteneinsicht	209
b) Vorlage von Nachweisen.....	209
c) Prozessoptimierung und elektronische Abfrage des Verfahrensstandes	210
10. Regelungsstandort	211
11. Änderungswünsche im Bundesrat	212
III. Anforderungen des Online-Zugangsgesetzes (OZG)	213
IV. Anforderungen des De-Mail-Gesetzes	214
1. Nutzerbegriff im Sinne des De-Mail-Gesetzes	214
2. Akkreditierung der Diensteanbieter als präventive Maßnahme für Datenschutz und Datensicherheit	214
3. Identitätssicherung durch Kontoeröffnung und sicheren Login	216
4. Zwei verschiedene Schutzniveaus bei der Anmeldung und Absenderbestätigung.....	216
5. Keine gesetzlich verpflichtende Ende-zu-Ende-Verschlüsselung	217
6. Nutzerverantwortlichkeiten bei De-Mail-Diensten	218
7. Verantwortlichkeiten des De-Mail-Diensteanbieters	220
8. Verantwortlichkeiten von Verwaltungsbehörden und Gateway-Lösungen	220
9. Strenge Zweckbindung nach § 15 De-Mail-Gesetz	221
10. Verweis in § 15 De-Mail-Gesetz auf TKG, TMG und BDSG	221
11. Beendigung der Account-Nutzung und digitaler Nachlass	221
V. Datenschutzrechtliche Einordnung der De-Mail-Dienste	223
1. De-Mail-Dienste als Telemedien	223
2. De-Mail-Dienste als Telekommunikation im Sinne des TKG	223
a) Verpflichtung der Diensteanbieter zur Wahrung des Fernmeldegeheimnisses	224
b) Weitere Vorgaben des TKG.....	224
3. Zwischenergebnis.....	225
VI. Anforderungen des PAuswG	225
1. Die eID-Funktion als Mittel zur Datenhoheit des Nutzers.....	225
2. Die Vergabe von Berechtigungszertifikaten als Präventivkontrolle.....	226
3. Rolle des Nutzers bei der IT-Sicherheit des nPA.....	226
4. Änderungen des PAuswG im Zuge des EGovG	228
5. Zwischenergebnis.....	229
VII. Anforderungen des TMG und TKG	229
1. Schichtenmodell	230
a) Inhaltsebene.....	230
b) Interaktionsebene	230
c) Transportebene	230
2. Differenzierung von Bestands-, Nutzungs- und Inhaltsdaten	231
3. Vorgaben des TMG	231
4. Vorgaben des TKG.....	233
5. Erstreckung des Fernmeldegeheimnisses auf Private nach § 88 TKG.....	233
6. Nutzerverantwortlichkeiten nach TMG	233
7. Verantwortlichkeiten der Diensteanbieter.....	234

VIII. Ergänzungsfunktion der Regelungen des BDSG	234
IX. IT-Sicherheitsgesetz.....	234
X. Strafvorschriften im Bereich der elektronischen Kommunikation	237
E. Zusammenfassung Teil 3	237
Teil 4: Schutz der informationellen Selbstbestimmung des Nutzers und Verteilung der Verantwortlichkeiten	239
A. Grundrechtlicher Freiheits- und Verantwortungsbereich des Nutzers von E-Government für das „Ob“ der Nutzung	240
I. Menschenwürdegarantie Art. 1 GG	240
1. Absolutheit der Menschenwürde	240
2. Konkretisierungsproblem beim Schutzbereich der Menschenwürde	241
3. Allgemeines Prinzip der Selbstbestimmung und Selbstverantwortung.....	243
4. Schutz des Grundrechtsträgers „vor sich selbst“?.....	243
5. Zwischenergebnis.....	244
II. Allgemeine Handlungsfreiheit aus Art. 2 I GG	245
1. Privatautonomie und Selbstbestimmung als Grundvoraussetzung	245
a) Vertragsfreiheit als „Hauptfall“ der Privatautonomie	246
b) Privatautonome Entscheidung über das „Ob“ der Nutzung von transaktionsbezogenem E-Government.....	247
c) Selbstverantwortung des Nutzers als Konsequenz der Privatautonomie beim „Wie“ der Nutzung	247
d) Abwägung des Nutzers	248
e) Beschränkung der Vertragsfreiheit oder bloße Ausgestaltung?.....	248
aa) Rechtsprechung des BVerfG.....	249
bb) Konstellationen von Machtungleichgewichten als Anknüpfungspunkt	250
(1) Typisierbare Ungleichgewichtslagen.....	250
(2) Nicht typisierbare Ungleichgewichtslagen.....	251
(3) Kritik am Anknüpfungspunkt der gestörten Vertragsparität	251
(4) Stellungnahme	252
cc) Privatautonomie und Vertragsfreiheit als Gegenstand einer staatlichen Schutzpflicht	252
(1) Eingriffe in die Privatautonomie und Vertragsfreiheit	252
(2) Kollision von Grundrechtspositionen.....	253
(3) Praktische Konkordanz	253
dd) Schutz des Nutzers vor sich selbst?	254
ee) Grenzen der Selbstverantwortung des Nutzers?.....	255
2. Subjektstellung des Nutzers und korrespondierende Eigenverantwortung	256
3. Der Nutzer als Vertragspartner und im Verwaltungsverfahren bzw. Verwaltungsrechtsverhältnis	256
4. Zwischenergebnis.....	257

B. Staatliche Schutzpflichten für die informationelle Selbstbestimmung des Nutzers im transaktionsbezogenen E-Government.....	258
I. Einleitung	258
II. Die Rechtsprechung des BVerfG zu Schutzpflichten.....	259
1. Anwendungsfälle staatlicher Schutzpflichten	259
2. Untermaßverbot	260
3. Wertordnungsrechtsprechung	261
III. Dogmatische Herleitung in der Literatur.....	261
IV. Stellungnahme.....	263
V. Inhalt staatlicher Schutzpflichten.....	263
VI. Differenzierung von Schutzpflichten und Förderpflichten	265
VII. Tatbestand und Rechtsfolge einer Schutzpflicht	265
1. Tatbestand einer Schutzpflicht	265
2. Rechtsfolge einer Schutzpflicht.....	267
VIII. Adressat der Schutzpflicht	268
IX. Kein allgemeiner Vorrang staatlicher Schutzpflichten	269
X. Vorbehalt des Möglichen.....	269
XI. Grundrechtliche Schutzpflicht aus dem Grundrecht auf informationelle Selbstbestimmung	270
XII. Schutzpflicht aus „Ingerenz“ bzw. E-Government-Förderungsabsicht?	271
XIII. Schutzpflichten und Selbstverantwortung	272
1. Berücksichtigung der digital Schwachen	273
2. Verkehrspflichten des Nutzers	274
3. Schutzpflichten für Kommunikationsinfrastrukturen.....	274
a) Umsetzung der Schutzpflichten durch das De-Mail-Gesetz	275
b) Umsetzung der Schutzpflichten durch das TKG.....	275
c) Umsetzung der Schutzpflichten durch die Bereitstellung einer Kommunikationsinfrastruktur.....	276
4. Zwischenergebnis.....	276
C. Selbstschutz des Nutzers	276
I. Selbstschutzmöglichkeiten	277
II. Verantwortlichkeit des Nutzers im Rahmen des Selbstschutzes	277
1. Systematisierung von Rechtspflichten und Obliegenheiten in der Rechtsordnung	278
a) Rechtspflichten	278
b) Obliegenheiten	279
2. Datenbezogene Rechtspflichten des Nutzers im Vertragsverhältnis.....	280
a) Beispiel: Aktualisierung der Identitätsdaten	280
b) Beispiel: Überwachung der Legitimationsmedien	281
3. Rechtspflichten des Nutzers im Verwaltungsrechtsverhältnis?.....	281
4. Differenzierung nach individuellen und „öffentlichen“ Infrastrukturen	281
III. Selbstschutzpflichten und Selbstschutzboligenheiten des Nutzers	281
1. Grundsätzliche Selbstschutzboligenheit des Nutzers?	282
2. Selbstschutzpflichten des Nutzers	283

3.	Überforderung des Nutzers	284
4.	Zumutbarkeit des Selbstschutzes	285
a)	„Digitale Verantwortungsfähigkeit“.....	285
b)	Sorgfaltsmaßstab für den Nutzer.....	286
c)	„Digitale Verantwortungsbereitschaft“	286
5.	Selbstschutzmaßnahmen.....	287
a)	Einsatz von Virenscannern.....	287
b)	Einsatz von Firewalls.....	288
c)	Verhalten im E-Mail-Verkehr	289
d)	Ende-zu-Ende-Verschlüsselung der E-Mail-Kommunikation?	289
e)	Pflicht zur Sicherung der technischen Umgebung des nPA?.....	290
f)	Restrisiko für den Nutzer	291
6.	Befähigung zum Selbstschutz im Rahmen der Schutzpflicht.....	292
IV.	Zulässige Selbstgefährdung als autonome Entscheidung?	292
V.	Zwischenergebnis	293
D.	Reichweite staatlicher Schutzpflichten an ausgewählten Beispielen	293
I.	Vergleich mit dem Straßenverkehr?.....	293
II.	Vergleich mit dem Verbraucherschutzrecht.....	295
III.	Spezifika der Informationstechnologie	296
IV.	Beispiel der WLAN-Haftung.....	296
V.	Generelles Problem der Statuierung von materiellen Verhaltenspflichten im Recht	299
VI.	Zwischenergebnis	300
E.	Handlungsspielraum des Staates bei der Umsetzung staatlicher Schutzpflichten	300
I.	„Schutzpflichtenkonzept“ des Staates aus den kommunikationsbezogenen Grundrechten	301
1.	Ermessen des Gesetzgebers.....	302
2.	Konfliktlösungs- und Schutzfunktion des Rechts	303
3.	Typisierende Fallgruppen	303
4.	Prinzip der Selbstbestimmung und Selbstverantwortung	303
5.	Verantwortungsteilung zwischen Staat, Diensteanbieter und Nutzer.....	304
6.	Zwischenergebnis.....	305
II.	Untermaßverbot als untere Grenze des gesetzgeberischen Handelns	305
III.	Keine verfassungsunmittelbare Gewährleistung von Leistungsansprüchen.....	305
IV.	Anpassungs- und Erfahrungsspielräume für den Gesetzgeber	306
V.	Bloße gerichtliche Evidenzkontrolle	306
VI.	De-Mail-Konzept als datenschutzgerechter Zugang zu transaktionsbezogenem E-Government?.....	307
1.	Generelle Erforderlichkeit des De-Mail-Gesetzes	307
2.	Der Diensteanbieter als Verantwortungssubjekt	307
3.	Gesetzgeberische Nachsteuerungspflicht.....	308
VII.	Potenzielle Entwicklung zu IT-Sicherheitspflichten des Nutzers?	308
VIII.	Eigener Vorschlag: Sukzessive Weiterentwicklung des einfachen Rechts durch Obliegenheiten des Nutzers und Pflichten des Diensteanbieters	309

IX. IT-Sicherheit als Teil der Organisationsverantwortung der Verwaltung	311
1. Auswahl der Kommunikationsinfrastrukturen.....	311
2. Verwaltungsinterne IT-Sicherheit.....	311
3. Steuerung über Dienstanweisungen.....	312
F. Zusammenfassung Teil 4	313
Teil 5: Ausgewählte Fragestellungen.....	315
A. Regelung einer Ende-zu-Ende Verschlüsselung im De-Mail-Gesetz oder separat?.....	315
B. Praxisbeispiel: E-Government-Anwendung iKfz.....	316
I. Das Projekt iKfz.....	316
II. Das NAVO-Portal mit dem nPA als Identitätsmanagement-Infrastruktur.....	317
III. Nutzerverantwortlichkeit	317
IV. Penetrationstests der Anwendung durch die Verwaltung und Audits als Umsetzung der Schutzpflicht	318
V. De-Mail als Rückkanal für Bescheide.....	318
VI. Verantwortliche Stelle	318
VII. Besondere Bedeutung von Bezahldiensten.....	319
VIII. Fazit: Komplexe Vertragslandschaft für den Nutzer.....	319
C. Anonyme und pseudonyme Nutzung von Diensten	319
D. Die Rolle der datenschutzrechtlichen Einwilligung im E-Government	321
E. Datenschutzakteure im E-Government	325
I. Ausschuss De-Mail-Standardisierung	325
II. Weiterentwicklung technischer und organisatorischer Anforderungen	325
III. Grundrechtsschutz durch den Datenschutzbeauftragten	326
IV. Systemdatenschutz als Aufgabe der Gremien	328
V. Wirksame Durchsetzung datenschutzrechtlicher Bestimmungen	328
VI. Das Bundesamt für Sicherheit (BSI) in der Informationstechnik als „Warnungs- und Beratungsinstanz“	328
1. Aufgaben des BSI nach dem BSIG	328
2. Das Nationale Cyber-Abwehrzentrum beim BSI	329
F. Vollzugsoptimierung und -ergänzung durch Datenschutzaudits.....	330
G. Vollzugsoptimierung durch Aufklärung	332
Teil 6: Zusammenfassung der Ergebnisse von Teil 2 bis 5 in Thesen	333
Ergebnisse Teil 2	333
Ergebnisse Teil 3	334
Ergebnisse Teil 4	336
Ergebnisse Teil 5	337
Literaturverzeichnis	339