

Digitalisierte Verwaltung Vernetztes E-Government

Herausgegeben von

Priv.-Doz. Dr. Margrit Seckelmann

Bearbeitet von

Prof. Dr. Marion Albers, Prof. Dr. Nadja Braun Binder,
Dr. Alfred G. Debus, Dr. Wolfgang Denkhäus,
Prof. Dr. Daniela Heinemann, Manuel J. Heinemann,
Dr. Thorsten Hennrich, Priv.-Doz. Dr. Tobias Herbst,
Melanie Horster, Prof. Dr. Constanze Janda,
Dr. Markus Kaulartz, Kai-Niklas Knüppel,
Prof. Dr. Dieter Kugelman, Prof. Dr. Kai von Lewinski,
Prof. Dr. Jörn von Lucke, Prof. Dr. Andreas Mann,
Prof. Dr. Veith Mehde, Manuel Misgeld,
Prof. Dr. Ralf Müller-Terpitz, Dr. Conrad Neumann,
Priv.-Doz. Dr. Jakob Julius Nolte, Prof. Eike Richter,
Prof. Dr. Utz Schliesky, Dr. Sönke E. Schulz,
Dr. Stephan Schwarz, Priv.-Doz. Dr. Margrit Seckelmann,
Prof. Dr. Thorsten Siegel, Prof. Dr. Christoph Sorge,
Dr. Mike Weber, Maria Wilhelm, Markus Wojtczak

Begründet von

Prof. Dr. Frank Bieler und Prof. Dr. Gunnar Schwarting

2., völlig neu bearbeitete Auflage

ERICH SCHMIDT VERLAG

Inhaltsverzeichnis

Geleitwort	5
Vorwort	7
Inhaltsübersicht	9
Autorenverzeichnis	35
Abkürzungsverzeichnis	41
Einleitung	45

Teil I

E-Government, Open und Smart Government und Digitalisierung: Begriffe, Probleme und Chancen

Kapitel 1: Vom E-Government zur Digitalisierung (Wolfgang Denkhaus)	51
A. Einleitung	51
B. Digitalisierung als Herausforderung an Politik und Verwaltung ..	53
I. Europäische Union	53
II. Bund	54
III. Länder und Kommunen	55
C. Schritte auf dem Weg zur digitalen Verwaltung	55
I. Der Auf- und Ausbau des IT-gestützten Verwaltens	56
1. IT-gestütztes Verwalten: Rechenzentren, Verwaltungsnetze, EDV in den Amtsstuben	56
2. IT-Recht der öffentlichen Verwaltung als Datenschutzrecht und Verwaltungsprivatrecht	57
II. E-Government und Verwaltungsmodernisierung	58
1. E-Government als „Leitbild und Projekt“ zur Verwaltungs- modernisierung	58
2. Verfassungsrechtliche Verankerung in Art. 91c GG	59
3. Punktuelle Regelungen im Verwaltungsrecht	60
4. E-Government-Gesetzgebung	60
5. Zwischenbilanz	61
III. Verwaltung im digitalen Wandel	62
1. Verwaltung unter Bedingungen von Digitalisierung	62
2. „Digitalisierung der Verwaltung“: Neue Mittel und technische Instrumente	63
3. „Verwaltung der Digitalisierung“: Neue Aufgaben und Handlungsfelder	65

4.	Data Policies – Regulierung persönlichkeitsrechtlich sensitiver digitaler Märkte	66
D.	Entwicklungstendenzen und Herausforderungen an das Recht der digitalen Verwaltung	66
I.	Die Organisation der digitalen Verwaltung zwischen Ausdifferenzierung, Zentralisierung und Konzentration	67
1.	Zentralisierung: Das Beispiel der Reform der föderalen IT-Koordinierung gem. Art. 91c GG	67
2.	Konzentration: Vom CIO zum CDO zum Digitalministerium? ...	68
II.	Weiterentwicklung digitaler Verwaltungsangebote und Verwaltungsverfahren	69
1.	Von der Ermöglichungs- zur „Aktivierungsfunktion“ des Verwaltungsrechts	69
2.	Online Zugang zu digitalen Verwaltungsangeboten: Verwaltungsportale, Portalverbund, Single Gateway und einheitliche Servicekonten	71
3.	Nutzung vorhandener Daten in Verwaltungsverfahren: „Once-Only“ oder doch „Only-Once“	73
4.	Vollautomatisierte Verwaltungsverfahren	74
III.	Gewährleistung von Transparenz und Open Government	74
1.	Bereitstellung von Open (Government) Data	75
2.	Elektronische Bürgerbeteiligung und e-Voting	75
IV.	IT-Sicherheit und Persönlichkeitsrechtsschutz als Determinanten des Rechts der elektronischen Verwaltung	76
1.	IT-Sicherheit	76
2.	Persönlichkeitsrechtsschutz	76
3.	Verhältnis von IT-Sicherheit und Datenschutz	77
4.	Digitale Souveränität und Eigentumsrechte an Nutzerdaten	77
E.	Fazit und Ausblick	78
Kapitel 2: Smart Government (Jörn von Lucke)		81
A.	Einführung: Smart Government	81
I.	„Smart“ bedeutet „Intelligente Vernetzung“!	82
II.	Vision: Von Industrie 4.0 zur Verwaltung 4.0	84
B.	Smart Government: Intelligent vernetztes Regierungs- und Verwaltungshandeln	87
I.	Erste Szenarien zu Smart Government	91
1.	Smarte Feuerwehr	92
2.	Smarte Gerichte	92
3.	Smarte Bauverwaltung	93

II.	Erste Umsetzungen in der Verwaltungspraxis	94
C.	Sorgen am Horizont: Dystopie einer smarten Politik	97
D.	Forschungsagenda Smart Government	99
E.	Auf dem Weg zu einer intelligent vernetzten Verwaltung	104

Kapitel 3: Datenbanken sowie Ordnungs- und Personenkenneichen

	(Kai von Lewinski)	107
A.	Allgemeines	107
I.	Geschichte und Entwicklung	107
II.	Funktion und Einsatzfelder von Datenbanken der Öffentlichen Hand	109
	1. Bürokratisches Abbild der Wirklichkeit	109
	2. Eindeutige Referenzierung der Datensätze	109
III.	Gefahren	110
	1. Individuelle Verdattung	110
	2. Codierung der Gesellschaft	111
IV.	Datenbankenstrukturen als Rechtsproblem auch jenseits des Datenschutzes	111
B.	Rechtliche Problemfelder und einzelne Regelungen	112
I.	Errichten eines logischen Raums	112
	1. Gesetzesvorbehalt für Datenbankstrukturen	112
	a) Kein allgemeiner Gesetzesvorbehalt	113
	b) Kein ausdrücklicher Gesetzesvorbehalt	113
	c) Grundrechtlicher Gesetzesvorbehalt?	113
	2. Kompetenzordnung	114
	3. Leistungsdimension	114
II.	Einrichten eines logischen Raums	115
	1. Zweckmäßigkeit der Einrichtung	115
	a) Eindeutige Referenzierbarkeit	115
	b) Codierung	115
	c) Größe	116
	d) Zeit	116
	e) Übernahme bestehender Datenstrukturen	116
	2. Zuschnitt	117
	a) Erforderlichkeit und Geeignetheit	117
	b) Namens- und Allgemeines Persönlichkeitsrecht	117
	c) Informationelle Selbstbestimmung	118
	aa) Grenze des Persönlichkeitsprofils	118
	bb) Sprechende und nicht-sprechende Codierung	119
	d) Diskriminierungsverbote	119
	3. Technisch-organisatorischer Datenschutz	120

III.	Einordnung in logischen Raum und Zuteilung von Kennzeichen	120
1.	Einordnung und Nichteinordnung	121
2.	Modus	121
3.	Technisch-organisatorische Absicherung	122
IV.	Einsatz	122
1.	Verwaltungsverfahrenrecht	122
2.	Datenschutzrecht	123
V.	Öffnung des logischen Raums	123
1.	Zugangsrestriktion	123
a)	Datenbankschutz	123
b)	Datensatzschutz	124
aa)	Datenschutz	124
bb)	Geheimnisschutz	124
2.	Zugangsermöglichung	124
a)	Grenze der informationellen Amtshilfe	124
b)	Nichtdiskriminierung	124
c)	Keine Datenportabilität zugunsten des Betroffenen	125
d)	Recht an Kennzeichen	125
C.	Logischer Raum der Verwaltungsdatenbanksysteme als offenes Regelungsfeld	126
	Kapitel 4: Big Data Analytics (Mike Weber)	127
A.	Grundlagen und Konzepte	127
I.	Was ist Big Data: Die V-Aspekte	127
II.	Weiterentwicklungen und Auswertungsmöglichkeiten	130
B.	Die Kunst des Fragens: Beschränkungen von Big Data	131
I.	Von Daten zu Wissen	132
II.	Gütekriterien der Datenauswertung	133
III.	Aussagekraft der Ergebnisse	134
C.	Beispielhafte Anwendungsfelder im öffentlichen Sektor	135
I.	Wahlkampfunterstützung	135
II.	Polizeiarbeit	136
III.	Kulturverwaltung	137
IV.	Grundschulplanung	137
D.	Big Data Analytics zwischen Anspruch und Wirklichkeit	138
	Kapitel 5: Transparenz und Open Government (Manuel J. Heinemann) ..	141
A.	Transparenz und Open Government	141
B.	Transparenz	143
C.	Hintergründe	144

D. Begriff der Transparenz und Abgrenzung zur Informationsfreiheit und zum Datenschutz	146
E. Kulturwandel	149
F. Transparenz in der gesetzlichen Umsetzung	150
I. Gesetzeszweck	150
II. Bezugsobjekt der Transparenz	151
III. Beteiligte	151
IV. Bereichsausnahmen	152
V. Entgegenstehende Belange	153
1. Entgegenstehende öffentliche Belange	153
2. Entgegenstehende Belange des behördlichen Entscheidungsprozesses	153
3. Entgegenstehende Belange durch geistiges Eigentum, Betriebs- und Geschäftsgeheimnisse	154
4. Entgegenstehende Belange des Datenschutzes	155
5. Entgegenstehende Belange sonstiger Art	156
VI. Informationszugang auf Antrag	156
VII. Informationszugang über die jeweilige Transparenzplattform	157
VIII. Kosten	157
IX. Rechtsweg	158
G. Landesbeauftragte	158
H. Besondere Initiativen	158
I. Missbrauch des Informationszugangs	158
J. Open Government	159
1. Ziele von Open Government	160
2. Gegenstand von Open Government	162
3. Adressaten des Open Government	163
4. Die Kernbereiche des Open Government	164
a) Transparenz	164
b) Partizipation	164
c) Kollaboration	166
5. Teilbereiche und Aspekte des Open Government	167
a) Austausch von Daten und Informationen innerhalb der Verwaltung	168
b) Offenlegung von Vermögensverhältnissen der Verwaltung	168
c) Korruptionsbekämpfung	169
d) Bewältigung von politischen und gesellschaftlichen Herausforderungen	169
e) Rechenschaftslegung der Verwaltung	170
f) Kontrolle der Verwaltung	170
g) Open Data	171

6. Internationale Entwicklung	172
7. Europarechtliche Grundlagen	173
8. Aktuelle gesetzliche Entwicklungen	174
9. Praktische Umsetzungen und Entwicklungen des Open Government in Deutschland	175
a) Das Datenportal GovData	175
b) Die Modellkommunen	176
c) Digitale Strategien und digitale Dialoge	177
d) Weitere Portale	177
K. Vorteile und Chancen – Risiken und Nachteile	178
I. Vorteile und Chancen	178
II. Risiken und Nachteile	179
L. Ausblick	182
Kapitel 6: Elektronisch unterstützte Partizipationsverfahren und e-Voting (Nadja Braun Binder)	185
A. Einleitung	185
B. Verfahren	186
I. Elektronisch unterstützte bzw. online durchgeführte Partizipationsverfahren	186
II. Kategorien von Partizipationsverfahren	187
C. Elektronisch unterstützte Partizipationsverfahren	188
I. Top-down: Staatlich organisierte Konsultation, Involvierung und Kollaboration	188
1. Informelle Konsultation	188
2. Involvierung (formelle Konsultation)	191
3. Kollaboration	192
II. Bottom-up: Zivilgesellschaftliche Partizipation	192
1. E-Petitionen	192
2. Europäische Bürgerinitiative	195
D. E-Voting	196
E. Fazit	198

Teil II
Organisation und E-Government-Gesetze

Kapitel 7: Der unionale Rahmen von E-Government (Veith Mehde)	203
A. Ausgangslage	203
B. Faktische und rechtliche Handlungsmöglichkeiten der EU-Organe	203
I. Konkrete kompetenzrechtliche Situation	204
II. Programme/Soft Law	205
1. Erklärung von Tallinn	206
2. Aktionspläne	206
3. Strategien	207
III. Finanzielle Absicherung	208
IV. Organisatorische Absicherung	209
C. Ausgestaltungsnotwendigkeiten und -prinzipien	210
I. Interoperabilität	210
II. Einheitlicher Zugang	213
III. Medienbruchfreiheit	214
IV. Datenoffenheit/Transparenz	214
V. Cybersicherheit/Datenschutz	214
VI. Einmalige Erfassung	215
D. Spezielle Referenzgebiete	217
I. E-Rechnung	217
II. E-Vergabe	218
III. Dienstleistungsrichtlinie	219
E. Schluss	219
Kapitel 8: Der bundesrechtliche Rahmen und die Kooperationstatbestände (Utz Schliesky)	221
A. Einleitung	221
B. Verfassungsrechtlicher Rahmen des E-Government in Deutschland	222
I. IT und das Verbot der Mischverwaltung	222
II. Art. 91c GG als neuer Ordnungsrahmen	224
1. Hintergrund	224
2. Charakter der Vorschrift	225
3. Inhaltliche Aussagen von Art. 91c GG	226
a) Zusammenwirken von Bund und Ländern bei informations- technischen Systemen (Art. 91c Abs. 1 GG)	226
b) Vereinbarungen über Standards und Sicherheitsanforderungen (Art. 91c Abs. 2 GG)	229

c) Ländervereinbarung über Betrieb informationstechnischer Systeme und Errichtung von dazu bestimmten Einrichtungen (Art. 91c Abs. 3 GG)	230
d) Verbindungsnetz (Art. 91c Abs. 4 GG)	230
4. Zwischenfazit zu Art. 91c GG	231
5. Art. 91c Abs. 5 GG und Onlinezugangsgesetz	231
III. Bestehender einfach-gesetzlicher Rahmen des E-Governments	233
1. Bezüge des Verwaltungsverfahrensgesetzes zum E-Government ...	233
2. Das E-Government-Gesetz des Bundes	235
3. De-Mail-Gesetz	236
4. Elektronischer Personalausweis (PAuswG)	237
5. SigG, SigV, eIDAS und Vertrauensdienstegesetz	238
IV. Schluss	241

Kapitel 9: Der landesrechtliche Rahmen von E-Government

(Sönke E. Schulz)

A. Einleitung	243
B. E-Government-Recht als Verfahrensrecht	245
C. Vorrang des Landesrechts (§ 1 Abs. 3 VwVfG) auch beim E-Government-Recht	246
D. Simultangesetzgebung hindert Innovation im Bereich elektronischer Verwaltungskommunikation	247
E. Impulsgesetzgebung des Bundes als taugliches Element?	249
F. E-Government im Landesverwaltungsverfahrenrecht	251
I. Zulässigkeit elektronischer Kommunikation und Schriftformäquivalente	252
II. Zugangseröffnung	253
III. Elektronischer Verwaltungsakt	254
IV. Elektronische Nachweise	255
V. Identifizierung von Antragstellern	256
VI. Elektronische Aktenführung und Vorgangsbearbeitung	256
VII. Ersetzendes Scannen	257
VIII. Akteneinsicht	257
IX. Elektronische Bezahlverfahren	258
X. Elektronische Rechnungen	258
G. Organisatorische Folgen des ebenenübergreifenden E-Governments	260

Kapitel 10: Die digitale Stadt – Chancen und Herausforderungen der Digitalisierung für die lokale Gemeinschaft (Eike Richter)	265
A. Digitalisierung als Chance und Herausforderung für Städte und Gemeinden	265
B. Politische Konzepte der Digitalen Stadt und der Smart City	267
I. Digitalisierung als Aufgabe der politischen Gestaltung	267
II. Prozeduralisierung, Beteiligung und Kooperation	269
III. Querschnittscharakter, Handlungsmaximen und Erprobung	270
IV. Elemente und Handlungsfelder der kommunalen Digitalisierungsstrategien	271
1. Digitalisierung der gesellschaftlichen und staatlichen Lebensbereiche	271
2. Digitalisierung von Geschäftsprozessen, Verfahren und Organisation	272
3. Digitalisierung der Infrastruktur und digitale Infrastruktur	273
C. Herausforderungen an die kommunalrechtlichen und -strukturellen Rahmenbedingungen	274
I. Unterstützung durch Private	275
II. Anforderungen an die kommunale Dateninfrastruktur	278
III. Digitalisierung gemeindlicher Wahlen und anderer Beteiligungsformen	280
IV. Erprobung	280

Teil III

Kommunikation und Verfahren

Kapitel 11: Rechtssichere elektronische Kommunikation (Maria Wilhelm)	285
A. Aktuelle Entwicklung, Desiderate und Perspektiven	285
I. Bestehende Systeme und Ziele	286
II. Besonderes elektronisches Behördenpostfach (beBPO)	288
B. Kommunikationsbegriff und Gestaltungsziel der Bürgerorientierung	288
C. Rechtsgrundlagen	289
I. Vorgaben auf europäischer Ebene	290
II. Vorgaben im deutschen Recht	292
1. Verfassungsrecht	292
2. Bundesrechtliche Regelungen	292
3. Landesgesetze	293
III. Anforderungen an Auslegung und Anwendung der Gesetze	294

D.	Verfügbarkeit und Verkehrsfähigkeit als Grundvoraussetzung	295
I.	Vorzuhaltende Einrichtungen	295
II.	Anschlussfähigkeit für andere Systeme	296
E.	Rechtssicherheit durch Authentizität	296
I.	Elektronische Signaturen	296
1.	Einfache E-Signaturen	297
2.	Qualifizierte E-Signaturen	297
II.	Sichere Übermittlungswege	298
III.	Elektronische Siegel, Zertifikate und weitere Konzepte	298
IV.	Identitätszuordnung nach dem De-Mail-Gesetz	299
F.	Rechtssicherheit durch Vertraulichkeit	300
I.	Datenschutz, Aktengeheimnis und weitere besondere Anforderungen	300
II.	Vertraulichkeit durch Sicherheit	301
G.	Verbindlichkeit und Integrität	301
I.	Konkrete Anforderungen an die IT-Sicherheit	302
1.	Schutz der Hardware	302
2.	Anwendung von Verschlüsselungstechniken	303
II.	Anforderungen an ein Fehlermanagementsystem	303
H.	Rechtssicherheit im und durch das Verwaltungsverfahren	304
I.	Allgemeine Beweiswirkungen im Mehrebenensystem	304
II.	Rechts- und Pflichtenkreis des Absenders elektronischer Nachrichten und Wiedereinsetzungsanträge	305
III.	Rechts- und Pflichtenkreis des Nachrichtempfängers	306
I.	Anforderungen an die konkrete Form von Ausgestaltung und Umsetzung elektronischer Kommunikationssysteme	307
I.	Organisatorisch-funktionale Begrenzung durch Behördenaufbau und Aufgabenverteilung	307
II.	Einheitlichkeit des gesamten elektronischen Rechtsverkehrs	308
III.	Effizienz vs. Rechtssicherheit?	308
J.	Bewertung und Ausblick	309
	Kapitel 12: Vollautomatisierte Verwaltungsverfahren, vollautomatisiert erlassene Verwaltungsakte und elektronische Aktenführung (Nadja Braun Binder)	311
A.	Einleitung	311
B.	Vollautomatisierte Verwaltungsverfahren	312
I.	Definition	312
II.	Rechtlicher Rahmen	313
1.	Regelung in der AO	314
2.	Regelung im VwVfG	315

3. Regelung im SGB X	316
4. Vergleich der drei Regelungen	317
III. Potenziale und rechtliche Grenzen	318
1. Potenziale	318
2. Grenzen	318
IV. (Voll-)Automatisiert erlassene und elektronische Verwaltungsakte ...	321
C. Elektronische Aktenführung	321
I. Definition	321
II. Rechtlicher Rahmen	322
1. Pflicht zur Führung elektronischer Akten (§ 6 Satz 1 EGovG) ...	322
2. Übertragung von Papierdokumenten in die elektronische Form (§ 7 EGovG)	323
3. Recht auf Akteneinsicht (§ 8 EGovG)	324
III. Vor- und Nachteile einer E-Akte	324
D. Fazit	325
Kapitel 13: E-Vergabe (Thorsten Siegel)	327
A. Begriff	327
B. Vorzüge und Risiken	327
C. Entwicklung	328
I. Die Öffnung für die E-Vergabe	328
II. Die fakultative E-Vergabe	329
III. Die obligatorische E-Vergabe	329
D. Rechtsgrundlagen	330
I. Die Zweiteilung des Vergaberechts	330
II. Kartellvergaberecht	331
1. Das Kaskadenprinzip	331
2. Relevanz der Vergabeordnungen	332
3. Bedeutsame Regelungen zur E-Vergabe	332
III. Haushaltsvergaberecht	333
1. Rechtsgrundlagen	333
2. Bedeutung der Vergabeordnungen	333
a) Wirkungsweise im Unterschwellenbereich	333
b) Von der VOL/A zur Unterschwellenvergabeordnung (UVgO) .	334
3. Bedeutsame Regelungen zur E-Vergabe	334
E. Die E-Vergabe im Kartellvergaberecht	335
I. Die Hinwendung zur obligatorischen E-Vergabe	335
1. Grundsatz	335
2. Ausnahmen	335

II.	Elektronische Kommunikationsmittel	336
1.	Begriff und technische Anforderungen	336
2.	Anforderungen an den Einsatz	336
III.	Einzelne Verfahrensschritte	337
1.	Bekanntmachung	337
2.	Abrufbarkeit der Vergabeunterlagen	337
3.	Abgabe von Angeboten und anderen Erklärungen	338
4.	Elektronische Rechnungsstellung	338
IV.	Besondere Methoden und Instrumente	339
1.	Übersicht	339
2.	Einzelne Instrumente nach § 120 GWB	339
3.	e-Certis	340
F.	Die E-Vergabe im Haushaltsvergaberecht	340
I.	Bisherige Rechtslage	340
II.	Künftige Rechtslage	341
Kapitel 14: Barrierefreiheit (Daniela Heinemann)		343
A.	Einführung	343
I.	Begriff und Historie	343
II.	Anwendungsbereiche	344
1.	Internet	344
2.	Schriftverkehr	344
3.	Telefonate	344
4.	Barrierefreies Bauen und Wohnen	345
5.	Mobilität	346
III.	Schwerbehinderung/Behinderung/Beeinträchtigung	346
B.	Umsetzung in der Praxis	348
I.	Technische Anforderungen an barrierefreies Internet	348
II.	Leichte Sprache	348
III.	Gebärdensprache	349
IV.	Digitales Vorlesen	350
V.	Blindenschrift	350
C.	Rechtliche Hintergründe	351
I.	Europarecht	351
II.	UN-Konvention über die Rechte von Menschen mit Behinderung	353
III.	Das Behindertengleichstellungsgesetz	355
IV.	Konkretisierung durch Rechtsverordnungen und technische Regelungen	357
D.	Ausblick	358

Kapitel 15: Elektronische Kommunikation mit den Verwaltungsgerichten (Jakob Nolte)	359
A. Einführung	359
B. Einheitliche Regelung für alle Gerichtsbarkeiten	360
I. Anwendungsbereich	361
II. Technische Anforderungen an die Kommunikation und Übermittlungswege nach § 55a Abs. 2 bis 4 VwGO	362
III. Eingang elektronischer Kommunikationsakte bei Gericht	365
IV. Kommunikationsakte des Gerichts	366
V. Förmliche Zustellung gerichtlicher Dokumente	367
VI. Elektronische Formulare	368
VII. Verpflichtende Teilnahme an der elektronischen Kommunikation ...	368
C. Fazit	371

Teil IV

Datenschutz und Datensicherheit

Kapitel 16: Die Datenschutz-Grundverordnung der EU (Tobias Herbst)	375
A. Einleitung	375
I. Zielsetzung der DSGVO	376
II. Struktur der DSGVO	377
B. Anwendungsbereich der DSGVO	378
I. Sachlicher Anwendungsbereich	378
II. Territorialer Anwendungsbereich	379
C. Voraussetzungen der Rechtmäßigkeit der Verarbeitung personenbezogener Daten	380
D. Anforderungen an die Einwilligung der betroffenen Person	380
E. Die Zweckbindung	381
F. Die Rechte der betroffenen Personen	382
I. Informationspflichten und Auskunftsrechte	383
II. Recht auf Berichtigung	384
III. Recht auf Löschung („Recht auf Vergessenwerden“)	385
IV. Recht auf Einschränkung der Verarbeitung (vormals „Sperrung“) ...	386
V. Recht auf Datenübertragbarkeit	387
VI. Widerspruchsrecht	387
VII. Rechte bei automatisierter Einzelfallentscheidung	388
G. Datenschutz durch technische und organisatorische Maßnahmen und durch datenschutzfreundliche Voreinstellungen	389
H. Auftragsverarbeitung	390

I.	Dokumentationspflichten	391
J.	Melde- und Benachrichtigungspflichten bei Datenlecks und Datenpannen	392
K.	Aufsichtsbehörden	393
I.	Organisatorische Struktur und Zusammenarbeit der Aufsichtsbehörden	393
II.	Aufgaben und Befugnisse der Aufsichtsbehörden	394
L.	Behördliche und betriebliche Datenschutzbeauftragte	395
M.	Selbstregulierung der Verantwortlichen	396
N.	Datenübermittlung in Drittstaaten	397
I.	Genehmigungsfreie Übermittlungen	397
II.	Übermittlungen mit Genehmigung	398
III.	Als Ausnahmen zulässige Übermittlungen	399
O.	Regelungen zu Spezialfällen	399
I.	Besondere Kategorien personenbezogener Daten („sensible“ Daten) ..	399
II.	Medienprivileg	399
III.	Zugang der Öffentlichkeit zu amtlichen Dokumenten	400
IV.	Nationale Kennziffer	400
V.	Beschäftigtendatenschutz	400
VI.	Archive, Forschung und Statistik	401
VII.	Berufsgeheimnis	402
VIII.	Kirchliche Datenschutznormen	402
P.	Schadensersatz und Geldbußen	403
 Kapitel 17: Bundesrechtliche datenschutzrechtliche Spielräume und das neue BDSG (Melanie Horster)		405
A.	Einleitung	405
I.	Ausgangslage	405
II.	Rechtscharakter der DSGVO	406
III.	Gegenüberstellung der bisherigen bundesgesetzlichen Regelung (BDSG-alt) und des neuen BDSG	408
B.	Videüberwachung öffentlich zugänglicher Räume	409
I.	Regelungen zur Videüberwachung	409
1.	Vergleich der Regelungen zur Videüberwachung im BDSG-alt und BDSG-neu	409
2.	Öffnungsklausel zur Schaffung nationaler Regelungen im Bereich der Videüberwachung öffentlich zugänglicher Räume	410
3.	Zulässigkeitsvoraussetzungen der Videüberwachung	411
4.	Bekanntmachung der Beobachtung	412
5.	Speicherung und Verwendung von im Rahmen der Videüberwachung erhobenen Daten	413

6. Informationspflicht gegenüber betroffenen Personen	413
7. Löschung von im Rahmen der Videoüberwachung erhobenen Daten	413
II. Zusammenfassung der Ausführungen zur Videoüberwachung	414
C. Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses ..	414
I. Regelungen zum Beschäftigtendatenschutz	414
1. Vergleich der Regelungen zum Beschäftigtendatenschutz im BDSG-alt und BDSG-neu	415
2. Öffnungsklausel zur Schaffung nationaler Regelungen	415
3. Zulässigkeitsvoraussetzungen für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses	415
4. Einwilligung zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses	416
5. Verarbeitung besonderer Kategorien personenbezogener Daten .	417
6. Datenverarbeitung auf Grundlage von Kollektivvereinbarungen für Zwecke des Beschäftigungsverhältnisses	418
7. Grundsätze für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses	418
8. Berücksichtigung der Beteiligungsrechte von Interessensvertretungen	418
9. Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses unabhängig von der Speicherung in einem Dateisystem	419
10. Definition des Begriffs Beschäftigte	420
II. Zusammenfassung der Ausführungen zum Beschäftigtendatenschutz	421
D. Auswirkungen der DSGVO auf datenschutzrechtliche Spielräume des nationalen Gesetzgebers	421
Kapitel 18: Anwendungsbereich und Spielräume der Landesdatenschutzgesetze (Dieter Kugelmann)	423
A. Der Landesgesetzgeber in der regulatorischen Klemme	423
I. Europarecht	423
II. Bundesrecht	424
III. Bereichsspezifisches Landesrecht	425
B. Landesdatenschutzgesetz und Richtlinie zu Polizei und Justiz	425
I. Die Richtlinie und ihre Umsetzung	425
II. Anwendungsbereich	427
C. Regelungsmöglichkeiten des Landesgesetzgebers	430
I. Öffnungsklauseln und Beibehalten von vorhandenen Regelungen ...	430
II. Wiederholungsverbot	430
III. Notwendiges Schweigen des Landesdatenschutzgesetzes	431
D. Schwerpunkte eines Landesdatenschutzgesetzes	432

I.	Materielle Regeln	432
II.	Technisch-organisatorische Regeln	434
III.	Die Stellung des Landesdatenschutzbeauftragten	435
IV.	Sanktionen gegenüber Behörden	436
E.	Funktionen des Landesdatenschutzgesetzes	437
I.	Freiheitssicherung	437
II.	Rechtssicherheit und Lückenfüllung	437
Kapitel 19: Sichere Informationstechnik (Christoph Sorge)		439
A.	Einleitung: Zur Bedeutung sicherer Informationstechnik	439
B.	Schutzziele	440
C.	Vorgehensweisen	441
I.	Standards der IT-Sicherheit	441
II.	Maßnahmen	441
D.	Elektronische Dokumente und elektronische Akten	443
I.	Signaturen und Siegel	444
II.	Langzeitaufbewahrung	446
E.	Schnittstellen nach außen	448
I.	E-Mail	448
II.	Personalausweis	448
III.	Ersetzendes Scannen	450
F.	Elektronische Gesetzesverkündung	451
G.	Fazit	452

Teil V
Einsatzfelder

Kapitel 20: Möglichkeiten des Einsatzes von Cloud Computing durch die öffentliche Verwaltung (Thorsten Henrich)		455
A.	Einleitung	455
B.	Cloud Computing – Begriff und Erscheinungsformen	456
I.	Begriffsdefinition	456
II.	Abgrenzung zu konventionellen IT-Outsourcing-Szenarien, Virtualisierung	457
III.	„IT as a Service“ – Die Cloud-Service-Modelle	458
1.	Infrastructure as a Service (IaaS)	458
2.	Platform as a Service (PaaS)	459
3.	Software as a Service (SaaS)	459
4.	Everything/IT as a Service (XaaS)	459

IV.	Betriebs- & Bereitstellungsmodelle	460
1.	Public Cloud	460
2.	Private Cloud	460
3.	Hybrid Cloud	460
4.	Community Cloud	461
C.	Cloud Computing durch die öffentliche Verwaltung	461
I.	Typische IT-Outsourcing-Szenarien der öffentlichen Verwaltung	462
II.	Möglichkeiten, Chancen und Vorteile	463
III.	Gefahren und Risiken	464
IV.	Rechtsrahmen	464
1.	Verfassungsrecht	465
a)	Funktionsvorbehalt nach Art. 33 Abs. 4 GG	465
b)	Verbot der Mischverwaltung (Art. 83 ff. GG)	466
2.	Datensicherheit	467
a)	Komplexität der Sicherheit einer Cloud-Architektur	467
b)	Virtualisierung	468
c)	Zertifizierungen und Audits	469
d)	Datenschutzreform	469
3.	Datenschutz	469
D.	Fazit	472
Kapitel 21: Verwaltung und soziale Medien (Alfred G. Debus)		473
A.	Begriff, Arten und Funktionsweisen der sozialen Medien	473
I.	Begriff der sozialen Medien	473
II.	Arten und Funktionsweisen der sozialen Medien	473
1.	Foren	473
2.	Ideen- oder Beschwerdemanagementplattformen	473
3.	Wikis	474
4.	(We-)Blogs	474
5.	Microblogging/Informationsdienste	475
6.	Instant Messaging Dienste	475
7.	Podcasts und Multimediaportale	475
8.	Befragungs-/Bewertungsportale, insbes. Bürgerhaushalte	475
9.	Social Bookmarking	476
10.	Soziale Netzwerke	476
11.	Sonstige Formen	477
B.	Nutzungsanlässe, Chancen und Risiken	477
I.	Verwaltung	477
1.	Unterscheidung von dienstlicher, privater und sonstiger Nutzung .	477
2.	Erfüllung von klassischen staatlichen Aufgaben	478

3. Transparenz und Open Government	479
4. Fachlicher Diskurs	479
5. Presse- und Öffentlichkeitsarbeit bzw. Social Media Marketing und Social Relations	479
6. Interne Arbeitsprozesse	481
7. Social-Media-Monitoring/-Analytics	481
8. Chancen	482
9. Risiken	483
II. Politikerinnen und Politiker	483
III. Bürgerinnen und Bürger	484
Kapitel 22: Einsatz bei der Polizei: Twitter-Nutzung, Online-Streifen, Trojaner, Facebook-Fahndung, Biometricsoftware, (intelligente) Videoüberwachung, Predictive Policing, Body-Cams und Fotodrohnen (Margrit Seckelmann)	485
A. Einleitung: Die Polizei als Grenzstellenmanagerin im Kampf um Informations- und Deutungshoheit	485
B. Nutzung von Social Media durch die Polizei (informierend, präventiv und repressiv)	487
I. Twitternutzung durch die Polizei	489
1. Neuvermessung der Grenzstelle in der Kommunikation zwischen Staat und Bürgern	489
2. Fragen von Privacy und Datenschutz	490
a) (Quasi-)Monopole bestimmter Unternehmen	490
b) Die Datenschutzgrundverordnung der EU und das „Privacy Shield“	491
II. Online-Streifen, Trojaner und Facebook-Fahndung	492
1. Online-Streifen	492
2. Quellen-Telekommunikationsüberwachung/„Trojaner“	494
3. Facebook-Fahndung	495
a) „Steckbrief 2.0“	495
b) Das „Recht auf Vergessenwerden“	496
4. Spezialproblem Hate Speech	497
C. Bild und Tonaufzeichnungen durch die Polizei	497
I. Intelligente Videoüberwachung von Kriminalitätsschwerpunkten	497
1. Videobeobachtung und Videoaufzeichnung	498
a) Abgrenzung zwischen beiden Instrumenten	498
b) Zentrale verfassungsrechtliche Anforderungen	500
aa) Bestimmtheit/Erkennbarkeit	500
bb) Beurteilung von doppelfunktionalen Maßnahmen	501
cc) Verhältnismäßigkeit	501

2. Kombination mit Biometriesoftware zur „Intelligenten Videoeobachtung“	502
II. Predictive Policing	505
III. Body-Cams	506
IV. Kameradrohnen	507
D. Fazit	508
Kapitel 23: Sicherheitsbehördliche Vernetzung und Datenschutz (Marion Albers)	509
A. Einleitung	509
B. Grundlagen: Vernetzung und Digitalisierung	511
I. Vernetzung, Netze und Netzwerke als konkretisierungsbedürftige Paradigmata	511
II. Digitalisierung sicherheitsbehördlicher Arbeit	515
C. Datenschutz vor neuen Herausforderungen	518
D. Informationelle Vernetzung der Sicherheitsbehörden	522
I. Datenübermittlung und Datenempfang	524
II. Zentraldateien und Verbunddateien	525
III. Gemeinsame Dateien von Polizeien und Nachrichtendiensten	529
IV. Gemeinsame Abwehrzentren	532
E. Fazit	533
Kapitel 24: Geodaten – Anwendungsfeld und Pionier des E-Government (Conrad Neumann)	535
A. Einleitung	535
B. Nutzung von Geodaten	535
I. Begriff	535
II. Geodaten in der öffentlichen Verwaltung	537
1. Vermessungswesen	537
2. Umweltbereich	539
3. Gefahrenabwehr und Landesverteidigung	539
4. Statistik und Meldewesen	539
5. Soziale Infrastruktur, übrige Daseinsvorsorge	540
III. Geodaten in der Bundesverwaltung	540
C. Rechtsrahmen für Geodaten	540
I. Europäische Ebene	541
1. INSPIRE-RL	542
2. Umweltinformationsrichtlinie	543
3. PSI-RL	544
4. Transparenzverordnung	545

II.	Bundesebene	546
	1. GeoZG	547
	2. BGeoRG	549
	3. EGovG	551
	4. Weitere Bundesgesetze	553
III.	Länderebene	553
	1. L-VermKatG	553
	2. LGDIG/LGeoZG	554
	3. L-EGovG	555
IV.	Kommunalebene	556
D.	Koordinierung des Geoinformationswesens im Föderalismus	556
I.	IMAGI	556
II.	Geofortschrittsberichte der Bundesregierung	557
III.	IT-Planungsrat	557
IV.	LG und GKst. GDI-DE	559
E.	Entwicklungen im Geoinformationswesen	559
I.	GeoGovernment	559
II.	NGIS	560
III.	Open Data	561
	1. Definition und Rechtliches	561
	2. Initiativen	561
F.	Zusammenfassung	562
Kapitel 25: Apps (Stephan Schwarz)	565	
A.	Mobile Apps und M-Government	566
B.	Beispiele für Apps der öffentlichen Verwaltung	568
I.	App „Zoll und Reise“ des Bundesministeriums der Finanzen	568
II.	„Service App Berlin“ des Landes Berlin	569
III.	App „Ludwig II. – Auf den Spuren des Märchenkönigs“ der Bayerischen Staatsbibliothek	570
C.	Problematischer Datenschutz im App-Bereich	571
D.	Begriffsbestimmung und Charakteristika mobiler Apps	572
E.	Native Apps und Web-Apps	573
F.	Datenschutzrechtliche Aspekte mobiler Apps	574
I.	Anwendbares Recht	574
II.	Im App-Kontext relevante Daten	578
III.	Informationspflichten	580
IV.	Einwilligungen	580
V.	Datensicherheit: Technische und organisatorische Maßnahmen	581

VI. Datenschutz durch Technikgestaltung: „Privacy bei Design“ und „Privacy bei Default“	582
VII. Apps mit Standortdatenerhebung (Location-Based-Services)	583
G. Zusammenfassung	584

Kapitel 26: Smart Grids (Ralf Müller-Terpitz und Kai-Niklas Knüppel) .. 587

A. Einleitung	587
B. Begrifflichkeiten	588
I. Smart Grids	588
II. Smart Metering	589
C. Gegenwärtige Rechtslage	589
I. Smart Grids	589
II. Smart Metering	591
1. Einführung des Messstellenbetriebsgesetzes	591
2. Smart Metering unter dem Messstellenbetriebsgesetz	592
a) Begriff des intelligenten Messsystems	592
b) Einbaupflicht und Betrieb des intelligenten Messsystems	592
c) Vorgaben an die einzelne Messstelle	594
d) Regulierung	595
e) Zwischenfazit	596
D. Datenschutz und Datensicherheit in Smart Grids	596
I. Datenschutz	597
1. Anknüpfungspunkt und Adressaten der Datenverarbeitung	597
2. Konkurrenz zu anderen datenschutzrechtlichen Regelungen	599
3. Voraussetzungen der Datenerhebung, -verarbeitung und -nutzung	600
a) Zweckbindung	601
b) Datensparsamkeit	603
c) Transparenz und Informationsrechte der Anschlussnutzer	605
d) Zwischenergebnis	605
II. Daten- und Informationssicherheit	605
E. Fazit	607

Teil VI
Personal

Kapitel 27: Elektronische Personalaktenführung (Constanze Janda)	611
A. Begriff der Personalakte	612
B. Allgemeine Grundsätze der Personalaktenführung	613
I. Vollständigkeit und Wahrheit	613

II.	Transparenz	615
III.	Vertraulichkeit	616
IV.	Löschen von Daten	617
C.	Zulässigkeit der Datenerhebung in der digitalisierten Personalakte	618
I.	Anwendungsbereich des BDSG	618
	1. Sachlicher Anwendungsbereich	618
	2. Personeller Anwendungsbereich	618
	3. Datenerhebung durch öffentliche vs. nicht-öffentliche Stellen	619
II.	Verbot mit Erlaubnisvorbehalt	620
	1. Individuelle Einwilligung	620
	2. Zulässigkeit der Datenerhebung kraft Rechtsnorm	622
III.	Vorgaben zur Zulässigkeit der Datenerhebung	623
	1. Datenerhebung für Zwecke des Beschäftigungsverhältnisses, § 26 BDSG	624
	2. Erhebung von Daten über den Gesundheitszustand	625
	a) Schutz der Gesundheitsdaten von Beschäftigten vor Inkrafttreten der DSGVO	625
	aa) Gesundheitsdaten der Beschäftigten in der Privatwirtschaft ..	625
	bb) Gesundheitsdaten der Beschäftigten im öffentlichen Dienst ..	626
	b) Erhebung von Gesundheitsdaten nach § 26 Abs. 3 BDSG n.F. ...	627
	3. Datenverarbeitung durch den Arbeitgeber für andere als beschäftigungsbezogene Zwecke	628
	a) Rechtslage vor Neufassung des BDSG	628
	b) Rechtslage nach Neufassung des BDSG	630
D.	Beteiligungsrechte von Betriebs- und Personalrat	630
I.	Mitbestimmung	630
II.	Einsichtsrechte	632
III.	Überwachungspflichten	632
Kapitel 28: Führung in der Netzwerkverwaltung		
	(Manuel Misgeld und Markus Wojtczak)	635
A.	Einleitung	635
B.	Ein föderal-vernetztes E-Government zwischen Anspruch und Wirklichkeit	637
I.	Das Leitbild der Netzwerkverwaltung	637
II.	Mögliche Auswirkungen digitaler Arbeit	639
III.	Kritische Bestandsaufnahme des föderalen E-Governments	642
IV.	Das föderale E-Government als vertracktes Problem	643
C.	Neue Führungsansätze	645
I.	Transformationale Führung	645
II.	Agile Führung	650

III.	Digitale Führung – veränderte Anforderungen und empirische Belege	652
1.	Neue Arbeit – neue Personalführung?	652
2.	Evidenzen digitaler Führung	654
D.	Fazit und Ausblick	656

Teil VII
Akzeptanz und Visionen

Kapitel 29: Bürgerseitige Akzeptanz des E-Government (Andreas Mann)	659	
A. Akzeptanz als Grundlage für ein erfolgreiches E-Government	659	
B. Konzeptionelle Grundlagen der Akzeptanz	660	
I.	Akzeptanz – ein vielschichtiger Begriff	660
II.	Konzepte zur Erklärung der Akzeptanzgenese und -wirkung	664
III.	Ein integriertes Prozessmodell der Akzeptanzentwicklung	668
1.	Objektbezogene Akzeptanzdeterminanten	670
2.	Nutzerbezogene Akzeptanzdeterminanten und Moderatorgrößen	672
3.	Umweltbezogene Akzeptanzdeterminanten	676
C. Grundlegende Ansatzpunkte zur Steigerung der bürgerseitigen Akzeptanz des E-Government	677	
I.	Analyse von Bürgererwartungen und -verhaltensweisen als Grundlage segmentbezogener E-Government-Leistungen	678
II.	Gezielte Bürgerkommunikation und spezifische Nutzungsanreize zur Steigerung des Nutzenbewusstseins und Vertrauens	680
III.	Sicherheit und Usability bei der Websitenutzung gewährleisten	683
IV.	Implementierung eines Akzeptanz-Controlling	685
D.	Fazit	687

Kapitel 30: Die Blockchain in der öffentlichen Verwaltung (Markus Kaulartz)	689	
A. Die Innovation hinter den Blockchain-Technologien	689	
I.	Verzicht auf zentrale Intermediäre	689
II.	Beispiel Bitcoins	691
III.	Transaktionen als Wesensmerkmal von Blockchains	691
IV.	Miteinander verkettete Blöcke	692
V.	Blockchain-Typen	693
B. Charakteristika von Blockchains	694	
C. Anwendungsbeispiele in der öffentlichen Verwaltung	694	
I.	Register (Grundbuch, Handelsregister etc.)	694
II.	Wahlen – E-Voting	696
III.	Identity Management – E-Identity	696

Inhaltsverzeichnis

IV.	Verifizierung	697
V.	Automatisiertes Verwaltungshandeln mittels Smart Contracts – RegTech	698
	1. Technischer Hintergrund und Definition	698
	2. Charakteristika von Smart Contracts	698
	3. Anwendungsfall	699
	4. Wertung	699
D.	Vor der Nutzung von Blockchains zu lösende Herausforderungen .	699
E.	Fazit	702
	Ausgewählte Literatur	703
	Stichwortverzeichnis	733