

Sabine Stollhof

Datenschutzgerechtes E-Government

Eine Untersuchung am Beispiel
des Einheitlichen Ansprechpartners nach der
Europäischen Dienstleistungsrichtlinie



Nomos

Inhaltsverzeichnis

Abbildungsverzeichnis	15
Einleitung	17
Teil 1: E-Government und die Europäische Dienstleistungsrichtlinie	22
A Entwicklung des E-Government in Deutschland	22
I. Der Begriff	22
II. Ursprung und Ziele	27
1. Ursprung	27
2. Ziele	28
a) Interaktionspartner	28
b) Interaktionsstufen	29
III. Die bisherigen Projekte	30
1. Europäische Ebene	31
a) eEurope	31
b) i2010	33
c) Digitale Agenda für Europa	34
2. Nationale Ebene	35
a) Bundesebene	35
aa) BundOnline 2005	35
bb) E-Government 2.0	36
b) Landesebene	39
c) Kommunale Ebene	41
aa) <i>MEDIA@Komm</i> , <i>MEDIA@Komm-Transfer</i> , <i>MEDIA@Komm-Innovation</i>	41
bb) Sonstige Projekte	42
d) Gemeinsame Projekte	42
aa) Deutschland Online	42
bb) IT-Zusammenarbeit nach Art. 91c GG	44
cc) Nationale E-Government-Strategie	45
3. Zusammenfassung	46
IV. Status quo	47

1.	Stagnation des Fortschritts	47
2.	Datenschutz als Akzeptanzfaktor für ein erfolgreiches E-Government	49
B	Europäische Dienstleistungsrichtlinie (DL-RL)	53
I.	Hintergrund	54
II.	Wesentliche Inhalte	56
1.	Anwendungsbereich	56
2.	Verwaltungsvereinfachung, Art. 5 ff. Dienstleistungsrichtlinie	57
3.	Weitere Regelungen	60
III.	Potenzial und mögliche Auswirkungen der Dienstleistungsrichtlinie	61
C	Der Einheitliche Ansprechpartner	64
I.	Bestimmungen der Dienstleistungsrichtlinie und Anforderungsprofil	64
1.	Die Bestimmungen der Dienstleistungsrichtlinie	64
2.	Das Anforderungsprofil	66
a)	Aufgaben des Einheitlichen Ansprechpartners	66
b)	Befugnisse des Einheitlichen Ansprechpartners	70
c)	Elektronische Lösung?	74
II.	Anpassung des Verfahrensrechts - Das Vierte Verwaltungsverfahrenänderungsgesetz	75
III.	Die institutionelle Verortung des Einheitlichen Ansprechpartners	79
1.	Die Diskussion in Deutschland	79
a)	Abgelehnte Modelle	80
b)	Gewählte Modelle	81
2.	Die Entscheidungen der Länder	83
D	Potenzielle Gefahren bei E-Government im Hinblick auf Datenschutz und Datensicherheit	86
I.	Allgemeine Bedrohungen bei elektronischer Kommunikation	87
1.	Unsichtbarkeit und Flüchtigkeit elektronischer Informationen	87
2.	Zunahme personenbezogener Daten	88
a)	Inhaltsdaten	88
b)	Bestandsdaten	89
c)	Nutzungsdaten	89
d)	Verkehrsdaten	90

e) Risiko	90
II. Unsicherheit auf dem Transportweg	91
III. Bedrohungen in der Sphäre des Einheitlichen Ansprechpartners	91
IV. Bedrohungen in der Sphäre des Nutzers	92
Teil 2: Datenschutz	94
A Datenschutzrechtliche Vorgaben des Verfassungsrechts für die Tätigkeit des Einheitlichen Ansprechpartners	94
I. Das informationelle Selbstbestimmungsrecht	95
1. Herleitung	95
2. Grundrechtsqualität	96
II. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	97
III. Die verfassungsrechtlichen Datenschutzgrundsätze und die Konflikte mit der Dienstleistungsrichtlinie	100
1. Grundsatz der Zweckbindung	100
2. Grundsatz der informationellen Gewaltenteilung	102
3. Grundsatz der Erforderlichkeit	104
4. Grundsatz der Transparenz	105
5. Grundsatz der Datenvermeidung und der Datensparsamkeit	106
6. Grundsatz der Erforderlichkeit gesetzlicher Regelung	107
7. Ergebnis	107
B Restriktion europarechtlicher Vorgaben durch deutsches Recht?	108
I. Verhältnis des europäischen Rechts zum nationalen Recht	108
1. Die Rechtsprechung des Europäischen Gerichtshofs	108
2. Die Rechtsprechung des Bundesverfassungsgerichts	109
3. Der Vertrag von Lissabon	110
II. Anwendbarkeit des deutschen Verfassungsrechts im vorliegenden Fall	112
C Datenschutzrechtliche Vorgaben des Europäischen Rechts für die Tätigkeit des Einheitlichen Ansprechpartners	117
I. Europäisches Grundrecht zum Schutz personenbezogener Daten	118

1.	Rechtsquellen des Grundrechts auf Datenschutz	119
2.	Inhalt des Grundrechts auf Datenschutz	120
3.	Vergleich mit nationalem Verfassungsrecht	122
II.	Die europäische Datenschutzrichtlinie	122
III.	Ergebnis	123
D	Datenschutzrechtliche Vorgaben des einfachen nationalen Rechts für die Tätigkeit des Einheitlichen Ansprechpartners	124
I.	Die Datenschutzgesetze des Bundes und der Länder	124
1.	Anwendungsbereich	126
a)	Öffentliche Stelle	126
b)	Personenbezogene Daten	128
c)	Verarbeitung	131
aa)	Formen der Verarbeitung personenbezogener Daten	131
(1)	Erhebung	132
(2)	Speicherung	132
(3)	Übermittlung	133
(4)	Nutzung	134
bb)	Verarbeitungsformen bei der Tätigkeit des Einheitlichen Ansprechpartners	134
(1)	Verarbeitung bei der Bereitstellung von Informationen	134
(2)	Verarbeitungsformen bei der Tätigkeit als Verfahrenskoordinator	135
cc)	Auftragsdatenverarbeitung?	137
2.	Zulässigkeit der Verarbeitung	141
a)	Erhebung	141
b)	Speicherung und Nutzung	142
aa)	Erforderlichkeit	143
bb)	Zweckbindung	146
cc)	Dauer der Speicherung, Löschung	149
c)	Übermittlung	153
d)	Einwilligung	156
e)	Datenvermeidung und Datensparsamkeit	159
f)	Ergebnis	160
3.	Sonstige Pflichten	161
a)	Informationspflichten	161
b)	Technisch-organisatorische Maßnahmen nach § 9 LDSG BW	162
c)	Verfahrensverzeichnis	163

II.	Telemedienrecht	164
1.	Der Begriff »Telemedien« und die Abgrenzung zum Telekommunikationsrecht	165
a)	Der Begriff Telemedien	165
b)	Abgrenzung zum Telekommunikationsrecht	167
2.	Anwendungsbereich des Telemediengesetzes	168
3.	Datenschutzanforderungen an Telemediendienste	169
a)	Bestandsdaten, § 14 TMG	170
b)	Nutzungsdaten, § 15 TMG	175
c)	Weitere Anforderungen	181
III.	Telekommunikationsrecht	182
IV.	Ergebnis	183
E	Modernisierung des Datenschutzrechts?	184
I.	Modernisierung der Datenschutzgrundsätze?	185
1.	Grundsatz der Zweckbindung	185
a)	Zweckvereinbarkeit statt Zweckidentität	186
b)	Subjektive Zweckbestimmung durch den Betroffenen	188
c)	Rechtsgemäße Technikgestaltung	191
d)	Ergebnis	193
2.	Grundsatz der informationellen Gewaltenteilung	193
3.	Grundsatz der Erforderlichkeit	196
4.	Grundsatz der Transparenz	197
5.	Grundsatz der Datenvermeidung und der Datensparsamkeit	201
6.	Ergebnis	202
II.	Weitere Modernisierungskonzepte	203
1.	»Datenschutz durch Technik« und »Privacy by Design«	204
2.	Datenschutzmanagement	207
3.	Datenschutzaudit	211
a)	Datenschutzaudit als Wettbewerbsfaktor	212
b)	Geeignetheit eines Datenschutzaudits für den Einheitlichen Ansprechpartner als öffentliche Stelle	212
c)	Geltende Rechtslage	214
d)	Konzeption und Ziele eines Datenschutzaudits	217
e)	Ergebnis zum Datenschutzaudit	220
4.	Ergebnis	221

Teil 3: Datensicherheit	222
A Datensicherheitsrechtliche Vorgaben für die Tätigkeit des Einheitlichen Ansprechpartners	222
I. § 9 LDSG BW: Technische und organisatorische Maßnahmen	223
1. Allgemeines zum Regelungsgehalt	223
2. Maßnahmen nach § 9 Abs. 3 LDSG BW	226
a) Zutrittskontrolle (Nr. 1)	226
b) Datenträgerkontrolle (Nr. 2)	228
c) Speicherkontrolle (Nr. 3)	229
d) Benutzerkontrolle (Nr. 4)	230
e) Zugriffskontrolle (Nr. 5)	231
f) Übermittlungskontrolle (Nr. 6)	232
g) Eingabekontrolle (Nr. 7)	234
h) Auftragskontrolle (Nr. 8)	235
i) Transportkontrolle (Nr. 9)	235
j) Verfügbarkeitskontrolle (Nr. 10)	237
k) Organisationskontrolle (Nr. 11)	238
3. Hilfestellung	239
4. Kritik	241
5. Ergebnis	243
II. §13 Abs. 4 TMG	244
1. Jederzeitige Beendigung der Dienstenutzung (Nr. 1)	245
2. Löschung oder Sperrung von Nutzungsdaten (Nr. 2)	245
3. Geschützte Inanspruchnahme von Telemedien (Nr. 3)	247
4. Trennung von Nutzungsdaten (Nr. 4)	248
5. Zusammenführung nur für Abrechnungszwecke (Nr. 5)	249
6. Separierung von Nutzungsprofilen (Nr. 6)	249
7. Ergebnis	250
III. Signaturrecht	250
1. §3a(L)VwVfG	251
2. Qualifizierte elektronische Signatur	253
a) Die Signaturtypen nach dem Signaturgesetz	253
b) Funktionsweise	256
3. Ausländische elektronische Signaturen	257
4. Zusammenfassung	262
B Elektronische Kommunikation ohne qualifizierte elektronische Signatur?	262
I. Lockerung der gesetzlichen Schriftformerfordernisse	263

1.	Der Grundsatz der Nichtöffentlichkeit des Verwaltungsverfahrens, § 10 (L)VwVfG	264
2.	Funktionen der Schriftform	264
3.	Alternativen zur Schriftform bzw. zur qualifizierten elektronischen Signatur	266
	a) Die Textform im Privatrecht	267
	b) Anforderungen an die Textform	268
4.	Ersatz von Schriftformerfordernissen durch die Textform	270
5.	Einzelfallbetrachtung	271
6.	Ergebnis	272
II.	Wahl eines niedrigeren Sicherheitsniveaus - Beispiel ELSTER	273
1.	Funktionsweise des ELSTER-Verfahrens	274
2.	Unterschied zur qualifizierten elektronischen Signatur	275
3.	Stellungnahme der Datenschützer	277
4.	Übertragbarkeit auf andere E-Government-Anwendungen?	278
5.	Ergebnis	281
III.	Einsatz von elektronischen Identitätskarten	282
1.	Funktionalitäten des neuen elektronischen Personalausweises	282
	a) Biometriefunktion	282
	b) Authentifizierungsfunktion	283
	c) Signaturfunktion	284
2.	Bedeutung und Einsatzmöglichkeit im E-Government	284
3.	Grenzüberschreitender Einsatz von elektronischen Identitätskarten	288
4.	Ergebnis	290
IV.	De-Mail-Dienste	291
1.	Funktionalitäten der De-Mail-Dienste	291
2.	Perspektiven für E-Government und den Einheitlichen Ansprechpartner	296
3.	Ergebnis	299
V.	Abschließende Betrachtung	300
	Teil 4: Zusammenfassung und Ausblick	304
	Literaturverzeichnis	309