

Inhaltsverzeichnis

Geleitwort	5
Autoren	7
Executive Summary	13
A. Einleitung:	
Elektronische Kommunikation durch Berufsgeheimnisträger	17
B. Kommunikationssicherheit – Definition eines Sicherheitsniveaus geheimnisbezogener Kommunikation	21
I. Verfassungsrechtliche Grundlagen der Kommunikations- sicherheit	21
1. Allgemeines	21
2. Kommunikationsfreiheit, Art. 5 GG	21
3. Brief-, Post- und Fernmeldegeheimnis, Art. 10 GG	24
a) Briefgeheimnis	24
b) Postgeheimnis	25
c) Fernmeldegeheimnis	27
4. Informationelle Selbstbestimmung und Privatheit, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	29
a) Allgemeines Persönlichkeitsrecht	29
b) Recht auf informationelle Selbstbestimmung	30
c) Recht auf Vertraulichkeit und Integrität informa- tionstechnischer Systeme (IT-Grundrecht)	32
5. Grundrechtliche Schutzpflichten	35
II. Einfachgesetzliche Grundlagen der Kommunikationssicher- heit	37
1. Telekommunikationsgesetz (TKG)	38
2. Telemediengesetz (TMG)	39
3. Bundesdatenschutzgesetz (BDSG)	41
4. Signaturgesetz, De-Mail-Gesetz	42
a) Signaturgesetz (SigG)	42
b) De-Mail-Gesetz (De-MailG)	43
5. Postgesetz (PostG)	44
6. IT-Planungsrat-Staatsvertrag (ITPRStV)	46
7. Sonstige Vorgaben (IT-Compliance)	46
8. Strafrechtliche Vorschriften	47

III. Prinzip der Formenwahlfreiheit bei (elektronischer) Kommunikation	49
1. Verfassungsrechtliche Kommunikationsmittelwahlfreiheit	49
2. Elektronische Kommunikation	49
IV. Allgemeine Grenzen der Kommunikationswahlfreiheit	50
1. Begrenzung durch Form- und Verfahrensvorschriften	50
a) Form- und Verfahrensvorschriften als tradierter Kommunikationsrahmen	50
b) Elektronische Form	51
c) Bereichsspezifische Form- und Verfahrensvorschriften	52
2. Begrenzung durch Anforderungen an eine vertrauliche Kommunikation (§ 9 BDSG)	52
a) Bestimmung eines angemessenen Schutzniveaus für vertrauliche Kommunikation	52
b) Maßnahmenkatalog zu § 9 BDSG	54
V. IT-Sicherheit als variable, kontext- und einzelfallabhängige Größe	57
1. Terminologie	57
2. Sicherheit in der Rechtsordnung – Maß an Sicherheit	59
a) Sicherheit und Schutzmaßnahmen am Beispiel des Immissionsschutzrechts und des Atomrechts	59
(1) Bundesimmissionsschutzgesetz (BImSchG)	59
(2) Atomgesetz (AtG)	61
b) Sicherheit in der elektronischen Kommunikation	62
VI. Ausreichendes Sicherheitsniveau – kein verhältnismäßiger Gewinn an IT-Sicherheit durch die Ende-zu-Ende-Verschlüsselung	65
1. Verschlüsselungstechnologien	65
2. Ende-zu-Ende-Verschlüsselung ist keine conditio sine qua non für sichere Kommunikation	67
3. Aufwändige Installation der Ende-zu-Ende-Verschlüsselung	68
4. Keine Schutzpflicht des Staates zur Normierung der Ende-zu-Ende-Verschlüsselung	71
VII. (Kommunikations-)Sicherheitsnivellierungskraft des Faktischen	73
VIII. Berücksichtigung der Verkehrsanschauungen der beteiligten Verkehrskreise	74
IX. Rechtsbegriff der Kommunikationssicherheit	74
X. Zwischenergebnis	75

C. Geheimnisschutz	77
I. Geheimhaltungsbedürftige Bereiche	77
II. Berufsgeheimnisse	77
1. Anwaltsgeheimnis	77
2. Arztgeheimnis	78
3. Steuergeheimnis	79
4. Sozialgeheimnis	80
5. Beichtgeheimnis/Seelsorgegeheimnis	81
6. Bankgeheimnis	81
III. Maß an Geheimnisschutz und Kommunikationssicherheit	82
1. Verletzung von Privatgeheimnissen, § 203 StGB	82
a) Schutzzweck des § 203 StGB	83
b) Schutzobjekt: „Anvertrautes fremdes Geheimnis“	84
c) Täterkreis des § 203 StGB: Berufsgeheimnisträger	85
d) Tathandlung: Unbefugtes Offenbaren	86
e) Subjektiver Tatbestand des § 203 StGB	88
f) Betrachtung der herkömmlichen, unverschlüsselten E-Mail	88
g) Betrachtung des E-Postbriefs	90
(1) E-Postbrief mit elektronischer Zustellung	90
(2) E-Postbrief mit klassischer Zustellung	91
h) Zwischenergebnis	92
2. Anwaltsgeheimnis	92
3. Arztgeheimnis	93
4. Steuergeheimnis	93
5. Sozialgeheimnis	94
6. Beichtgeheimnis/Seelsorgegeheimnis	94
7. Bankgeheimnis	95
IV. Befund: Geheimnisschutz hat keine Garantiefunktion	95
V. Checkliste: Wahl eines sicheren Kommunikationsmittels	96
D. Einsatz des E-Postbriefs durch Berufsgeheimnisträger	97
I. Steigerung des Sicherheitsniveaus durch den E-Postbrief	97
1. Gewährleistung der Vertraulichkeit	97
2. Gewährleistung der Integrität	99
3. Gewährleistung der Authentizität	100
4. Gewährleistung des Zugangs	101
5. Gewährleistung der Kommunikationssicherheit beim Hybridbrief	102
6. Zwischenergebnis	102
II. Begrenzung des E-Postbriefs durch Form- und Verfahrensvorschriften	102

III.	Die funktionelle Äquivalenz des E-Postbriefs mit anderen Kommunikationsmitteln	103
1.	Akzeptanz der Briefpost	103
2.	Risiken der Briefpost	103
3.	Risiken des E-Postbriefs	104
4.	Normativer Schutz des E-Postbriefs	104
5.	Äquivalenz des E-Postbriefs zur Briefpost	105
IV.	Befund: Kommunikationssicherheitszuwachs durch den E-Postbrief bei Berufsheimnisträgern	106
E.	Gesamtbewertung und Handlungsempfehlungen	107
I.	Höherer Geheimnisschutz durch den E-Postbrief in der Praxis	107
II.	Gesamtbewertung und Fazit aus rechtswissenschaftlicher Sicht	108
III.	Handlungsempfehlungen aus rechtswissenschaftlicher Sicht	109
	Literaturverzeichnis	111