

Inhaltsverzeichnis

Einladung zur Lektüre	VII
Vorwort	IX
Vorwort der 1. Auflage	XIII
Abbildungsverzeichnis und Glossar	XXI
Abkürzungsverzeichnis	XXIII
Literaturverzeichnis	XXVII

§1 Hintergründe zur schwierigen Digitalisierung des Justizstandorts Deutschland – eine kritische Einführung

§2 Der elektronische Rechtsverkehr (ERV)

I. Begriffsbestimmung	23
II. Weichenstellung durch Justizkommunikationsgesetz	23
III. Digitalisierungsprozess durch das E-Justiz-Gesetz	24
IV. Materiell- und verfahrensrechtliche Verbote und Gebote des E-Justiz-Gesetzes	28
1. Rechtsrahmen und -entwicklung	28
2. Digitalisierungsprozesse bei Unternehmen	31
a) Eingehende Dokumente	31
b) Gewohnte Arbeitsweise	31
c) Bedenken wegen Beweiskraftverlust	32
d) Kosten der Umstellung	32
3. Verwaltung	33
a) Elektronische Kommunikation mit der Verwaltung in Europa	33
b) Digitalisierungsprozesse in der Verwaltung	35
V. Praxisrelevante Neuregelungen des E-Justiz-Gesetzes	36
1. Anschluss-und-Benutzerzwang	36
2. Telefax	37
3. Das E-Dokument, das beA und die sicheren Übermittlungs- wege	37
4. beA – das besondere elektronische Anwaltspostfach	38
5. Eingang eines elektronischen Dokuments bei Gericht	83
6. Normative Funktion von Formularen	83
7. Die Elektronische-Akte (E-Akte)	84

8. Die Barrierefreiheit	84
9. Die Verfahrensbeschleunigung und Effektivitätssteigerung	84
10. Die E-Zustellungen	85
11. Die Neuregelungen der Beweiskraft und das ersetzende Scannen	85
12. Kosteneinsparung durch ERV	87
13. Versendung elektronischer Rechnungen	88
14. Das elektronische Schutzschriftenregister	90
15. Das Online-Mahnverfahren mit eID und DE-Mail	91
16. Gestaffeltes Inkrafttreten mit Übergangszeit bis 2022	91
VI. Praxisrelevante Fallbeispiele und Haftungskonstellationen zum beA	93
Fallbeispiel 1: Formatfehler bei elektronischem Dokument – einmalige gerichtliche Hinweispflicht	94
Fallbeispiel 2: Haftungskonstellation Rechtsanwalts-Signatur/Unterschrift vergessen	95
Fallbeispiel 3: Mitarbeiter-Karte und beA-Postfachbedienung . . .	95
Fallbeispiel 4: Nutzung nicht personalisierter Benutzerkonten . . .	95
Fallbeispiel 5: Nutzung der Container-Signatur	96
Fallbeispiel 6: Signaturmissbrauch	97
Fallbeispiel 7: beA-Softwarezertifikat des mobilen Rechtsanwalts .	97
Fallbeispiel 8: Zustellung an Gericht, das den ERV nicht eröffnet hat	97
Fallbeispiel 9: Verkürzung der materiell-rechtlichen Schriftform durch beA und sicheren Übermittlungsweg	98
Fallbeispiel 10: Umgang mit dem Empfangsbekanntnis	98
Fallbeispiel 11: Dokumentenverlust nach Löschung von Nachrichten im beA durch BRAK gem. § 31 Abs. 4 BRAO	99
Fallbeispiel 12: beA allein und Auslaufmodell „Vorab per Fax“? . . .	99
Fallbeispiel 13: Vertiefung qualifizierte elektronische Signatur (qeS)	100
VII. Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs	106

§3 Die elektronische Verwaltung und das E-Government-Gesetz

I. Überblick	111
II. Gestaffeltes Inkrafttreten	113
1. Regelungen zum ersetzenden Scannen (1.8.2013)	113
2. Pflicht zur Zugangseröffnung (1.7.2014)	113
3. Nutzung des elektronischen Identitätsnachweises (1.1.2015) . . .	113
4. Erreichbarkeit per DE-Mail (24.3.2016)	114
5. Pflicht zur E-Aktenführung für Bundesbehörden (1.1.2020) . . .	114

III.	Änderung des Verwaltungsverfahrenrechts des Bundes und der Länder	114
1.	Zugangseröffnung mit digitalen Signaturen	114
2.	VwVfG des Bundes	114
3.	Beispiel Baden-Württemberg	117
a)	Verwaltungsverfahrensgesetz	117
b)	E-Government Gesetz Baden-Württemberg	118
4.	Beispiel Bayern	120
5.	Beispiel Mecklenburg-Vorpommern	120
6.	Weitere Bundesländer	124
IV.	Elektronisches Behördenpostfach und virtuelle Poststelle	126
1.	Bei den Gerichten	126
2.	Bei übrigen Behörden	127
 §4 Elektronische Form und Sichere Übermittlungswege		
I.	Allgemeine Regeln	129
1.	Schriftform und elektronischer Form	129
a)	Anforderungen an die gesetzliche Schriftform nach dem BGB	129
b)	Anforderungen an die elektronische Form nach dem BGB	130
c)	Anforderungen an die Schriftform im öffentlichen Recht	131
d)	Anforderungen an die Schriftform im Verfahrensrecht	131
2.	Fehlende Verbreitung der qeS für den flächendeckenden Einsatz	132
II.	Erfüllung der Schriftform durch elektronische Unterzeichnung auf einem Tablet oder Smartphone	133
III.	Rechtsverbindlichkeit und Beweisvorschriften bei der Nutzung von Tabletunterschriften für formfreie Verträge und Textform	133
IV.	Rechtliche Formvorschriften für wirksame Stellvertretung in elektronischer Form	135
V.	Formen elektronischer Signaturen und rechtswirksame Dokumentensignierung	136
1.	Einfache E-Signatur	137
2.	Fortgeschrittene E-Signatur	137
3.	Qualifizierte E-Signatur (qeS)	138
VI.	DE-Mail	142
1.	Varianten der DE-Mail-Sicherheit	142
2.	Rechtliche Bewertung	143

§5 Regeln für Anwälte und Gerichte

I.	Elektronisches Mahnverfahren	145
II.	Elektronisches Klageverfahren	146
	1. § 130a ZPO und Verwendung der Containersignatur	147
	2. Gerichtskostenvorschuss	149
	3. Elektronische Gerichtsbriefkästen	150
	4. beA	152
III.	Die elektronische Akte (E-Akte)	153
	1. Allgemein	153
	2. Aussortieren von Dokumenten mit höherem Beweiswert	153
	3. Prüfung der Anforderungen an die Identitätsprüfung zwischen schriftlichem Dokument und gescanntem E-Dokument	153
	4. Praxisbeispiele Arbeitsabläufe	154
	5. Elektronische Akteneinsicht	155
	6. Begriff des E-Dokuments	155

§6 Ersetzendes Scannen

I.	Begriff	157
II.	Rechtsgrundlagen und Zielgruppenanalyse	157
	1. Unternehmen	157
	2. Behörden	160
	3. Gerichte	161
III.	Pflicht zur Einführung des Ersetzenden Scannens?	162
	1. Bundesbehörden	162
	2. Landesbehörden	163
	3. Kommunalbehörden	165
	4. Gerichte	165

§7 Umsetzung und Muster-Workflow

I.	Vorbereitende Analyse zur Beweiswerterhaltung durch Datenschutz	167
	1. Technik und Verfahren der TR-ESOR des BSI (TR 3125) ...	169
	2. Digitale Signatur	170
	3. Hashbaum-Verfahren	171
	4. Langzeitsicherung mit Hilfe von Beweisdokumenten nach Evidence Record Syntax	174
	a) Abkündigung von Signaturalgorithmen	174
	b) Abkündigung des Hashalgorithmus	175
II.	Praxisbeispiele Arbeitsabläufe, IT-Infrastruktur, Software ..	175

III. Revisionssichere Langzeitarchivierung	177
1. Aufbewahrungspflichten	177
2. Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme und Grundsätze zum Datenzugriff und zur Prüfbarkeit originär digitaler Unterlagen	178
IV. Vertrauensdienste nach der eIDAS-Verordnung	179
1. eID-Verfahren	180
2. Vertrauensdienste	180
a) Elektronische Signaturen	182
b) Elektronisches Siegel	184
c) Bewahrungsdienste	184
d) Zeitstempeldienste	185
e) Validierungsdienste	186
f) Elektronische Einschreibe- bzw Zustelldienste	186
g) Websiteauthentifizierung	187

§ 8 Datenschutz und IT-Sicherheit

A. Rechtlicher Rahmen	189
I. EU-Datenschutzgrundverordnung (DSGVO)	189
1. Grundlagen	189
a) Europäischer Rechtsrahmen und Normadressaten	191
b) Anwendungsbereich für die öffentliche Hand	192
c) Rechtsänderungen durch die DSGVO Marktortprinzip, extraterritoriale Wirkung	192
d) Erweiterte Grundprinzipien: Nachweis und Rechenschaft	193
e) Rechtmäßigkeit der Datenverarbeitung/Verbot mit Erlaubnisvorbehalt	193
f) Gesetzliche Erlaubnistatbestände	193
g) Zweckbindungsgrundsatz	194
h) Technische und organisatorische Anforderungen	194
2. Mitarbeiterdatenschutz	195
3. Stärkung der individuellen Betroffenenrechte	195
4. Neujustierung der Auftragsdatenverarbeitung (Auftragsverarbeitung)	195
5. Datenübermittlung an Drittländer	196
6. Konzerndatenschutz	197
7. Verhaltensregeln, Datenschutzaudit, Zertifizierungen, Akkreditierung	197
8. Datenschutzaufsicht	197
9. Haftung, Rechtsbehelfe, Sanktionen	198
II. Handlungsempfehlungen, Haftungsvermeidung, Compliance	198
1. Datenschutzmanagement	198
2. Einstellung auf Marktveränderungen und Planung der Anpassungsprozesse	199

III. DSGVO: Erwartungen erfüllt?	200
IV. Umsetzungen bei Industrie, Mittelstand und Behörden	201
V. Umsetzungen bei KMU und Vereinen	202
VI. Rolle der Aufsichtsbehörden in Deutschland und der EU ...	203
VII. Geschwächte Autorität des Rechts	204
VIII. Ausblick	206
IX. Übersichten	208
X. BDSG	211
1. Allgemeines	211
2. Landesdatenschutzgesetze	212
3. Telemediengesetz	213
B. Technische Sicherheitsmaßnahmen im Bereich des ERV	214
I. Verschlüsselung und Schlüsselstärke	214
II. TLS-/SSL-Sicherheit	214
III. Verhinderung von Identitätstäuschung	216
IV. Arbeitsrichtlinien IT-Sicherheit und Datenschutz	219
V. Infrastruktur, Hardware, Software	220
VI. Cloud Computing	221
VII. Regelungen für Home-Office-Arbeitsplätze	221
VIII. Videokonferenzsysteme	223
IX. Anwaltliches Berufsrecht: Wahrung der Verschwiegenheitspflicht	225
C. Ausblick	236
Anhang 1	
Übersicht über die Umsetzungsverpflichtungen aus dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften	239
Anhang 2	
Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail*	253
Anhang 3	
Rechtsvorschriften des ERV und wichtige Links	259
Sachverzeichnis	261