

Inhaltsverzeichnis

Vorwort	V
Inhaltsverzeichnis	VII
Abkürzungsverzeichnis	XIII
Literaturverzeichnis	XV

A. Einleitung	1
B. Entwicklung der gesetzlichen Grundlagen des ERV	2
I. Einleitung	2
II. Vereinfachungsnovelle	2
III. Signaturgesetz	3
1. Grundbegriffe des Signaturrechts	3
2. Technische Grundlagen der elektronischen Signatur	4
IV. Zustellungsreformgesetz	6
V. Formvorschriftenanpassungsgesetz	6
1. Überblick über die Regelungen	6
a) Einleitung	6
b) ERV nach § 130a ZPO <i>de lege lata</i>	7
aa) Eröffnung durch Rechtsverordnung und Festlegung der Rahmenbedingungen	7
bb) Qualifizierte elektronische Signatur als zwingende Wirksamkeitsvoraussetzung	8
cc) Art und Weise der Verbindung von Dokument und elektronischer Signatur	9
dd) Festlegung weiterer Rahmenbedingungen durch Rechtsverordnung	10
2. Elektronische Form und Textform	12
VI. Justizkommunikationsgesetz	12
VII. Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG)	12
VIII. Gesetz zur Neuregelung des Rechtsberatungsrechts	13
IX. De-Mail-Gesetz	13
X. Gesetz zur Förderung der elektronischen Verwaltung	14
XI. Gesetz zur Förderung des elektronischen Rechtsverkehrs (ERV-Gesetz)	14
1. Einleitung	14
2. Anlass für das Tätigwerden des Gesetzgebers	14
a) Lückenhafte und uneinheitliche Eröffnung des ERV	14
b) Qualifizierte elektronische Signatur als Hemmschuh?	15
3. Entstehung des Gesetzes	15

C. Rechtslage nach dem ERV-Gesetz und dessen Änderungen und Ergänzungen	17
I. Einleitung	17
II. Öffnung der Gerichte für den elektronischen Rechtsverkehr	17
III. Elektronische Einreichung mit qualifizierter elektronischer Signatur oder auf einem sicheren Übermittlungsweg	18
1. Einleitung	18
2. Einreichung aus dem besonderen elektronischen Anwaltspostfach (beA)	20
a) Das beA als sicherer Übermittlungsweg	20
b) Einrichtung aufgrund von § 31a BRAO	21
c) Postfachinhaber	22
d) Mögliche Kommunikationspartner	26
3. Einreichung mittels absenderbestätigter De-Mail	27
4. Einreichung aus dem besonderen elektronischen Behördenpostfach (beBPO)	28
5. Weitere Verfahren als sichere Übermittlungswege	29
6. Ergänzende Regelungen zur elektronischen Einreichung	29
a) Bestätigung des Zeitpunkt des Eingangs	29
b) Übermittlung in ungeeignetem Format	30
IV. Elektronische Zustellungen	31
1. Einleitung	31
2. Besonderheiten des Gesetzgebungsverfahrens	31
3. Pflicht zur Bereithaltung eines sicheren Übermittlungsweges	32
4. Empfangsbekenntnis als strukturierter Datensatz	33
V. Aktive Nutzungspflicht für den ERV	34
VI. Empfangsbereitschaft und Nutzungspflicht des beA	35
1. Einleitung	35
2. Entwicklung der Diskussion	36
3. Empfangsbereite Einrichtung des beA	38
a) Einleitung	38
b) Grammatische Auslegung	38
c) Systematische Auslegung hinsichtlich der Position der Vorschrift in der BRAO	39
d) Historische und teleologische Auslegung	40
e) Auslegung hinsichtlich der Regelungssystematik des ERV-Gesetzes	40
f) § 31a BRAO als Rechtsgrundlage der empfangsbereiten Einrichtung des beA	41
4. Folge der empfangsbereiten Einrichtung – »Nutzungspflicht«?	43
a) Einleitung	43
b) Förmliche Zustellungen gegen Empfangsbekenntnis	43
c) Eingang sonstiger Nachrichten	44
d) Bedeutung eines fehlenden Annahmewillens	45
5. Übergangsregelung und Konsequenzen für die Praxis	46

VII. Schutzschriftenregister	49
1. Einleitung	49
2. Einführung des Schutzschriftenregisters 2016	49
3. Technische Rahmenbedingungen der Hinterlegung von Schutzschriften	50
4. Nutzungspflicht	51
a) Berufsrechtliche Pflicht zur Nutzung	51
b) Verfahrensrechtliche Pflicht zur Nutzung	51
VIII. Sonstige Regelungen	53
1. Ausfertigungen	53
2. Formulare	53
3. Scannen und Ersetzen des Papieroriginals	54
4. Beweisregel für mittels De-Mail versandte Dokumente	55
5. Maschinelles Mahnverfahren und beA	55
IX. Überblick über Zeitpunkte des Inkrafttretens und verschiedene Rechtszustände	57
X. Überblick über mögliche Fehler und Haftungsrisiken	60
1. Einleitung	60
2. Einbeziehung von anderen Personen	60
3. Haftungsrisiko durch Nichtnutzung des beA	61
4. Versand an ein nicht für den ERV eröffnetes Gericht	61
a) Rechtslage	61
b) Urteil des OLG Düsseldorf vom 24.07.2013	62
c) Folgen für die Praxis	63
d) Einsatz von Mitarbeitern	63
5. Nichtbeachtung der für den ERV geltenden technischen Rahmenbedingungen	64
6. Materiell-rechtliche Erklärungen in Schriftsätzen	65
XI. Ausblick auf zukünftige gesetzliche Änderungen	65
1. Einleitung	65
2. E-Akte und elektronischer Rechtsverkehr in Strafsachen	66
3. eIDAS-Verordnung und ihre Umsetzung in nationales Recht	67
4. E-Justice 2	68
D. Die technische Infrastruktur des elektronischen Rechtsverkehrs	69
I. Die Organisationsstrukturen in der Justiz	69
1. Einleitung	69
2. Sichere Identitäten für den elektronischen Rechtsverkehr = SAFE	72
3. Sichere Kommunikation für den ERV = EGVP-Infrastruktur	73
4. Automatisierter Datenaustausch = XJustiz	73
5. Ressortübergreifende Koordination des ERV	73
II. Überblick über die technische Infrastruktur des ERV	74
III. Das Elektronische Gerichts- und Verwaltungspostfach (EGVP)	74

1.	Einleitung	74
2.	Der Protokollstandard OSCI-Transport	75
3.	OSCI und EGVP	76
4.	Der EGVP Classic Client und andere EGVP-Sendekomponenten	77
5.	EGVP auf Seiten der Justiz	78
6.	Der EGVP-Nutzerkreis	78
7.	Abkündigung des EGVP-Classic-Clients	79
IV.	SAFE	80
1.	Einleitung	80
2.	Grundprinzipien	81
3.	Anwendungsszenarien	82
4.	Akteneinsichtsportal	83
	a) Hintergrund	83
	b) Funktionsweise des Akteneinsichtsportals	83
V.	XJustiz	84
1.	Einleitung	84
2.	XML	85
3.	XJustiz	85
E.	Das besondere elektronische Anwaltspostfach (beA)	86
I.	Überblick über die Entwicklung des Projektes	86
1.	Gesetzliche Vorgaben und Anforderungen der Nutzer an die Entwicklung	86
	a) Gesetzliche Vorgaben an die Entwicklung des beA	86
	b) Anforderungen der Nutzer an die Entwicklung	87
	aa) Einleitung	87
	bb) Workshops	87
	cc) Online-Umfragen	88
	c) Praktische Umsetzung der Anforderungen	89
	aa) Vergabe und Beauftragung	89
	bb) Umsetzungsphase – Realisierung und Tests	89
	cc) beA-Betrieb	90
	aaa) Einrichtung	90
	bbb) Betriebsumgebungen	90
	ccc) Hilfefunktion und Anwendersupport	91
	d) Start des beA	91
II.	Technische und organisatorische Grundlagen	93
1.	beA-Architektur	93
	a) Einleitung	93
	b) Webanwendung	93
	c) Kanzleisoftware-Schnittstelle	94
	d) Sicherer Verzeichnisdienst	94
	e) Qualifizierte elektronische Signatur bzw. sicherer Übermittlungsweg	97
	f) Journale	97

g)	Strukturdaten	98
h)	Barrierefreiheit	98
i)	Abwickler, Vertreter und Zustellungsbevollmächtigte	98
2.	beA-Sicherheit	99
a)	Einleitung	99
b)	Ende-zu-Ende-Verschlüsselung	100
c)	Client Security als Nutzungs-Voraussetzung im beA	102
aa)	Begriffserläuterung	102
bb)	Hinweise zur Installation der Client Security	103
d)	Sichere Anmeldung	103
e)	Sicherheits-Token	104
III.	Erstregistrierung	108
1.	Erstregistrierung durch den Postfachbesitzer	108
2.	Erstregistrierung für Benutzer ohne eigenes Postfach	109
IV.	Mitarbeiter und Berechtigungen verwalten	109
1.	Einleitung	109
2.	Feste und optionale Rechte	110
3.	Liste der Berechtigungen	111
4.	Rechteabstufungen	113
5.	Absicherung der Rechtevergabe	114
6.	Vorüberlegungen	115
7.	Erläuterung zu einigen Berechtigungen	117
a)	Empfangsbekenntnis	117
b)	»persönlich/vertraulich«	117
8.	Vergabe von Rechten im beA	118
a)	Benutzer mit/ohne Postfach	118
b)	Rechtevergabe an einen Mitarbeiter	118
aa)	Vorüberlegung	118
bb)	Anlegen eines Mitarbeiters	119
cc)	Berechtigung eines Mitarbeiters, der bereits angelegt ist	120
dd)	Weitere Rechte vergeben	120
c)	Rechtevergabe an einen anderen Rechtsanwalt	121
d)	Rechte entziehen	121
e)	Sicherheitsüberlegungen bei der Vergabe von Rechten und der Zuordnung von Sicherheits-Token	121
V.	Funktionen im beA	123
1.	Einleitung	123
2.	Nachrichtenübersicht	123
3.	Senden und Empfangen	125
a)	Einleitung	125
b)	Qualifizierte elektronische Signatur bzw. sicherer Übermittlungsweg	126
c)	Erforderliche Berechtigungen	127

d) Auszufüllende Felder	128
4. Sonstige Nachrichtenfunktionen im Überblick	132
F. Praktische Anleitungen	135
I. Erstregistrierung	135
1. Erstregistrierung für Benutzer mit eigenem Postfach	135
2. Erstregistrierung für Benutzer ohne eigenes Postfach	140
a) Einleitung	140
b) Praktische Anleitung	141
II. Anmelden im Postfach	144
III. Sicherheits-Token	144
1. Hardware-Token als Sicherheits-Token hinzufügen	144
2. Software-Token als Sicherheits-Token hinzufügen	145
3. Sicherheits-Token löschen	146
IV. Rechtevergabe	147
1. Mitarbeiter anlegen	147
2. Berechtigung eines Mitarbeiters, der bereits angelegt ist	149
3. Weitere Rechte vergeben	150
4. Rechtevergabe an einen anderen Rechtsanwalt	151
5. Absicherung der Rechtevergabe	152
6. Rechte entziehen	152
V. Nachrichtenfunktionen	154
1. Nachrichten empfangen	154
2. Nachrichten drucken und exportieren	155
3. Nachrichten erstellen	155
4. Nachrichten versenden oder speichern	162
5. Antworten und Weiterleiten	164
6. Nachrichten löschen	165
7. Nachrichten organisieren	165
a) Nachrichten verschieben	165
b) Etiketten verwalten	166
c) Nachrichten markieren	167
d) Spaltenauswahl	168
e) Unterordner	169
Stichwortverzeichnis	171