

**E-Mail-Kommunikation von Rechtsanwälten
mit Mandanten und Gerichten**

von Dirk Lindloff

ISBN: 3-8288-8930-1

A.	Einführung	25
B.	Die E-Mail als elektronische Nachricht	27
I.	Die E-Mail	27
1.	Der Aufbau	28
2.	Adressierung	32
3.	Erscheinungsformen	32
a)	Reine Textmail	32
b)	HTML-Mail	32
c)	Nachrichtentext als Anhang	35
d)	E-Mail Web-Formular	35
e)	XJustiz / XML-Mail	35
4.	Zusatzfunktionen	37
a)	Empfangs- oder Lesebestätigung	37
b)	Verschlüsselung	39
aa)	Symmetrische Verfahren	40
bb)	Asymmetrische Verfahren	41
cc)	Kryptographische Sicherung von E-Mails	42
c)	Elektronische Signatur	42
aa)	Technische Funktion der Signatur	43
bb)	Organisatorische Sicherheit	44
(1)	Zuordnung eines öffentlichen Schlüssels	45
(2)	Vertrauen in die ausschließliche Verfügungsgewalt	45
cc)	Arten der Signaturen nach dem Signaturgesetz	45
(1)	(Einfache) elektronische Signatur	46
(2)	Fortgeschrittene elektronische Signatur	46
(3)	Qualifizierte elektronische Signatur	47
(4)	Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung	49
(5)	Anhang: Attribute	49
dd)	E-Mail und Signatur	50
II.	Übertragung	50
1.	E-Mail-Anwendung des Absenders	52
2.	Postausgangsserver	53
a)	Interner Server	53
b)	E-Mail-Server eines Dienstleisters (Provider)	53
3.	Vermittlungsrechner (Router)	53
4.	Posteingangsserver	56
a)	Externer Posteingangsserver	57
b)	Interner Posteingangsserver	58
5.	E-Mail-Anwendung des Empfängers	58
C.	Die technischen Risiken der E-Mail	59
I.	Verlustrisiken	59
1.	Technikimmanentes Übermittlungsrisiko	59
2.	Verlust durch (Spam-)Filter	59
a)	Arten der Filter	60
aa)	User-Negativliste	60
bb)	Server-Negativliste	60
cc)	User-Positivliste	60
dd)	Wortfilter	61
ee)	Massenfilter	61
ff)	Briefkopf-Analyse	61
gg)	Textmuster-Filter	61

Inhalt

b)	Zusammenfassende Betrachtung der Filterung	62
3.	Verlustrisiko durch Virenfiler	62
4.	Abschließende Bewertung des Verlustrisikos	62
II.	Risiko der Einsichtnahme	63
1.	Einsichtnahme auf dem Übermittlungsweg	63
a)	Zugriff an den Routern und Netzwerkleitungen	63
b)	Zugriff an den SMTP-Servern	65
2.	Einsichtnahme in die Mailbox des Empfängers	66
a)	Unternehmenseigene E-Mail-Server	66
b)	Neutrale Provider	67
3.	Abschließende Bewertung des Einsichtnahmerisikos	67
III.	Fälschungsrisiko	68
1.	Fälschung der Identität des Absenders	69
a)	Benutzerkonto auf fremden Namen	69
b)	Manipulation der Konfiguration des E-Mail-Programms	69
c)	Einschleusung in den Verkehr zwischen SMTP-Servern	70
2.	Angriff auf die Unversehrtheit einer Erklärung während der Übertragung	72
3.	Fälschung durch den Empfänger	73
4.	Fälschung durch den Absender	74
5.	Zusammenfassung	74
D.	Allgemeine Kommunikationsanforderungen	75
I.	Wahrung der Vertraulichkeit	75
1.	Zielkonflikt Sicherheit - Bequemlichkeit	75
2.	Bedeutung in der Mandatsbeziehung	76
3.	Historische Entwicklung der Verschwiegenheitspflicht	76
4.	Verschwiegenheitsregelungen neben § 43a BRAO	77
5.	Die Kernnormen der Verschwiegenheit im Einzelnen	78
a)	Strafrechtliche Verpflichtung	78
aa)	Rechtsgut	78
bb)	Tatbestand	80
b)	Berufsrechtliche Verpflichtung	81
c)	Strafrechtliche und berufsrechtliche Verpflichtung im Vergleich	83
6.	Tatsächliche Berührungspunkte von E-Mail und Vertraulichkeit	83
a)	E-Mail-Adresse	83
aa)	E-Mail-Adresse als vertrauliche Tatsache	84
bb)	Mandatsbeziehung	85
b)	Inhalt der E-Mail	86
aa)	Sonderfall: Ergebnis einer Hauptverhandlung	86
bb)	Informationen über Dritte	87
c)	Zeitliche Erstreckung der Verpflichtung	88
d)	Zwischenergebnis	88
7.	Vereinbarkeit von E-Mail und Vertraulichkeit	88
a)	Bestandsaufnahme	89
b)	Beurteilungsmaßstab	90
c)	Vergleich mit klassischen Kommunikationsmitteln	91
aa)	Postalischer Brief	92
bb)	Leitungsvermittelte Telefonie	95
cc)	Funkvermittelte Telefonie	97
dd)	Telefax	98
ee)	Zusammenfassende Wertung und weitere Zugangswege	98
d)	Schutz von E-Mail-Kommunikation durch die Rechtsordnung	100
aa)	Dem Fernmeldegeheimnis verpflichtete Personen	100
bb)	Drittzugriff auf die Kommunikation	103
cc)	Europarecht	105
e)	Pflicht zu aktiven Maßnahmen	105
f)	Sonderfall: Besondere Bedeutung eines Mandats	106
8.	Zusammenfassung E-Mail und Vertraulichkeit	107
II.	Gestaltung der E-Mail eines Rechtsanwaltes	107
1.	Anwendbarkeit der Vorschriften über Pflichtangaben	108
a)	Rechtsformabhängige Pflichten in Geschäftsbriefen	108
b)	Spezifische Pflichten der Rechtsberatung	111
2.	Anordnung der Pflichtangaben	114
3.	Disclaimer	115
4.	Zusammenfassung	116
III.	Virenfreiheit der versendeten E-Mails	116
IV.	Prüfung der Identität bei eingehenden E-Mails	116

Inhalt

1.	Einfache E-Mails	117
2.	Prüfung der elektronischen Signatur	117
V.	Eingangskontrolle durch automatisierte Filter	118
1.	Virentfilter	118
2.	Spamfilter	119
VI.	Pflicht zur Führung von Handakten	120
1.	Form der Handaktenführung bei E-Mails	120
2.	Aufbewahrung	121
3.	Herausgabe	122
E.	Kommunikationsvorgänge mit Mandanten	123
I.	Mandatserteilung und Vollmacht	124
1.	Vergütung	124
2.	Rechtsgeschäftliche Vollmachten	125
3.	Vollmachten gegenüber Behörden	126
4.	Prozessuale Vollmacht	126
a)	Vollmacht in arbeitsgerichtlichen, finanzgerichtlichen und zivilprozessualen Angelegenheiten	127
b)	Vollmacht in verwaltungsgerichtlichen Angelegenheiten	129
c)	Vollmacht in sozialgerichtlichen Angelegenheiten	129
d)	Vollmacht in strafprozessualen Angelegenheiten	129
5.	Zusammenfassung	130
II.	Reaktion auf Mandatsanfragen	130
1.	Eingangsbestätigung	131
2.	Identifizierung	131
3.	Entscheidungsbildung und Ablehnung des Mandats	132
a)	Art der Kenntnisnahme	132
b)	Reaktionszeit „unverzüglich“	133
aa)	Pflichtbeginn	133
(1)	Machtbereich des Rechtsanwalts bei E-Mails	133
(2)	Zugangszeitpunkt - Kenntnisnahmefiktion	134
bb)	Prüfungs- und Überlegungsfrist	135
c)	Reaktionsweg	137
4.	Annahme des Mandats	139
5.	Zusammenfassung	140
III.	Fernabsatzvertrag	140
1.	„Erzwungene“ E-Mail-Kommunikation	140
2.	Planmäßige Nutzung von E-Mail zur Kommunikation	141
3.	Konsequenzen	141
IV.	Rechnungsstellung	143
F.	Kommunikation mit dem Gericht	145
I.	Formgebundene Erklärungen an die Zivilgerichte	146
1.	Grundlagen des § 130a ZPO	146
a)	Grundlegendes Normverständnis	146
b)	Kommunikationsbezogener Anwendungsbereich	147
c)	Rechtsverordnung nach § 130a Abs. 2 ZPO	147
aa)	Zeitpunkt	148
bb)	Form	148
cc)	Gefährdung eines einheitlichen Rechtswesens	149
2.	Sorgfaltspflichten des Rechtsanwaltes im Umgang mit den Rechtsverordnungen	151
a)	Aktualisierungspflicht	151
b)	Übertragung auf Mitarbeiter	151
3.	Qualifizierte elektronische Signatur	152
a)	Qualifizierte elektronische Signatur als Ordnungsvorschrift	153
b)	Auslegung als „Muss“-Vorschrift für bestimmende Schriftsätze	153
aa)	Wortlaut	154
bb)	Systematische Auslegung	154
cc)	Historische Auslegung – Rechtsprechung	155
dd)	Historische Auslegung – Gesetzgeber	160
ee)	Verfassungsrechtliche Auslegung	162
ff)	Teleologische Auslegung	165
(1)	Abschlussfunktion	165
(2)	Identitätsfunktion	167
(3)	Eigenhandlungsfunktion	171
(4)	Ergänzende Aspekte	172
gg)	Zwischenergebnis	173

Inhalt

hh)	Weitere Folgerungen für die Auslegung der Ordnungsvorschrift.....	173
c)	Technische Fehler bei der Authentifizierung.....	174
aa)	Fehlerquellen.....	174
(1)	Signaturschlüssel und Verarbeitung.....	175
(2)	Zufällige Veränderungen der Nachricht.....	175
(3)	Technische Einrichtungen des Gerichts.....	175
bb)	Konsequenzen der fehlgeschlagenen Signaturprüfung.....	175
d)	Fazit.....	177
4.	Verschlüsselung als „Form“.....	177
a)	Verschlüsselung und Verarbeitung.....	177
b)	Hinweispflicht.....	180
c)	Wiedereinsetzung in den vorigen Stand.....	180
d)	Fazit.....	182
5.	Dateiformat.....	183
a)	Generelle Fragen der verwendbaren Dateiformate.....	183
b)	Konkrete Kompatibilitätsprobleme.....	185
c)	Prüfungspflicht des Gerichts.....	185
d)	Wiedereinsetzung in den vorigen Stand.....	186
6.	Zeitpunkt des Eingangs.....	186
a)	Bestimmte Empfangseinrichtung des Gerichts.....	186
aa)	Externer Posteingangsserver.....	186
bb)	Veröffentlichte E-Mail-Adresse.....	187
cc)	Eingänge an andere Adressen.....	187
b)	Aufzeichnung als maßgeblicher Zeitpunkt.....	189
7.	Unbestimmtheit der Laufzeit von E-Mails.....	190
a)	Indirekte Übertragung bei Einschaltung von Providern.....	190
aa)	Verweis auf den sichersten Übertragungsweg.....	191
bb)	Unverschuldete Laufzeit.....	191
cc)	Ausgangskontrolle des Rechtsanwaltes.....	194
b)	Direkte Übertragung.....	196
8.	Eingangsbestätigung.....	198
9.	Postalische Nachreichung von Abschriften.....	198
10.	Zusammenfassung.....	199
II.	Formfreie Erklärungen an das Gericht.....	199
1.	Anwendung von § 130a Abs. 2 ZPO.....	200
2.	Anforderungen der Rechtsverordnungen.....	200
III.	Zustellungen des Gerichts an den Rechtsanwalt.....	201
1.	Praktischer Anwendungsbereich.....	201
2.	Formelle Anforderungen.....	204
a)	Hinweis auf die Zustellung gegen Empfangsbekanntnis.....	204
b)	Elektronische Signatur.....	205
aa)	Art der Signatur.....	205
bb)	Elektronisches Dokument und Doppelsignatur.....	205
c)	Verschlüsselung.....	206
aa)	Generelle Kritik.....	206
bb)	Gerichtliche Probleme des Schlüsselmanagements.....	206
cc)	Anwaltliche Probleme des Schlüsselmanagements.....	207
3.	Zustellungsadressat.....	208
4.	Verarbeitung beim Empfänger.....	208
5.	Empfangsbekanntnis.....	209
a)	Abgrenzung zu Empfangsbekanntnissen.....	210
b)	Anwendung von § 130a ZPO auf das Empfangsbekanntnis.....	211
6.	Fazit.....	211
IV.	Elektronische Akteneinsicht.....	211
1.	Verfassungsrechtliche Verankerung der Akteneinsicht.....	212
2.	Akteneinsichtsgesuch.....	212
3.	Entscheidung des Gerichts.....	213
4.	Durchführung.....	214
a)	Übermittlung der Dokumente.....	214
aa)	Verfügungen.....	215
bb)	Dokumentenformate.....	216
cc)	Ordnung der elektronischen Akte.....	216
b)	Datenvolumen.....	217
c)	Vollständigkeit.....	218
d)	Verschlüsselung.....	218
e)	Elektronische Signatur.....	219
5.	Annex: Weitergabe an den Mandanten.....	220

Inhalt

V.	Formfreie Erklärungen des Gerichts an den Rechtsanwalt.....	220
VI.	Andere Gerichte	221
1.	Verwaltungs-, Finanz- und Sozialgerichtsbarkeit	221
a)	Vergleich § 130a ZPO und § 55a VwGO.....	222
b)	Elektronische Akteneinsicht.....	222
2.	Arbeitsgerichtsbarkeit.....	223
3.	Strafgerichtsbarkeit.....	224
4.	Andere Gerichte oder Verfahrensarten.....	224
G.	Abschließendes Fazit.....	225
	Literaturverzeichnis.....	227
	Sachregister	251