

Inhaltsverzeichnis

1	<i>Verträge im elektronischen Geschäftsverkehr</i>	1
1.1	Vertragsschluss im Netz.....	1
1.1.1	Angebot und Annahme	1
1.1.2	Beweisschwierigkeiten	3
1.1.3	Zugang der Willenserklärungen, insbesondere von E-Mails.....	8
1.1.4	Fazit.....	13
1.2	Online-AGB.....	13
1.2.1	Kriterien wirksamer Einbeziehung	14
1.2.2	Einbeziehungsnachweis	15
1.2.3	Gesetzliche Inhaltskontrolle	16
1.2.4	Besonderheiten bei Unternehmen/Kaufleuten	16
2	<i>Digitale Signatur und elektronische Form</i>	19
2.1	Erweiterung der Formvorschriften.....	19
2.2	Probleme des E-Commerce.....	20
2.3	Die elektronische Form	21
2.4	Technische Voraussetzungen nach dem Signaturgesetz.....	22
2.5	Die Textform.....	23
2.6	Beweisführung mit der elektronischen Form	26
2.7	Übermittlung von Schriftsätzen im Gerichtsverfahren	28
3	<i>Online-Handel</i>	31
3.1	Allgemeine Informationspflichten	31
3.1.1	Impressumpflicht.....	31
3.1.2	Besondere Informationspflichten bei kommerzieller Kommunikation	36
3.1.3	Pflichten im elektronischen Geschäftsverkehr	36
3.1.4	Pflichtangaben in E-Mails	37
3.2	Fernabsatzbestimmungen.....	40
3.2.1	Gesetzliche Grundlagen	40

Inhaltsverzeichnis

3.2.2	Persönlicher Anwendungsbereich	40
3.2.3	Sachlicher Anwendungsbereich	41
3.2.4	Verhältnis zu anderen Verbraucherschutzbestimmungen	44
3.2.5	Spezielle Informationspflichten gegenüber dem Verbraucher	45
3.2.6	Widerrufsrecht	47
3.2.7	Beweislast	50
3.2.8	Praktische Umsetzung	50
3.3	Rechtsfragen bei Online-Auktionen	53
3.3.1	Verbraucher oder Unternehmer	53
3.3.2	Zustandekommen des Vertrages	54
3.3.3	Scheingebote	55
3.3.4	Zulässigkeit von Hilfsmitteln	56
3.3.5	Minderjährige Geschäftspartner	56
3.3.6	Widerrufsrecht nach Fernabsatzrecht	57
3.3.7	Gewährleistungsansprüche	58
3.3.8	Kollision mit Marken- und Schutzrechten	59
3.3.9	Transportrisiko	59
3.3.10	Zahlungsmodalitäten	60
3.3.11	Missbrauchsfälle	61
3.4	Das neue Telemediengesetz (TMG)	62
4	<i>Haftungsfragen</i>	67
4.1	Problemstellung – haftungsrelevante Inhalte	67
4.2	Das Haftungsszenario	68
4.3	Die Haftung nach dem TDG	70
4.3.1	Gesetzliche Regelung	71
4.3.2	Haftungsprivilegierung	71
4.3.3	Teledienste	72
4.4	Haftung für eigene Inhalte	73
4.5	Haftung für Fremdinhalte	74
4.5.1	Kenntnis als Voraussetzung	74
4.5.2	Aktive Nachforschung	75
4.5.3	Evidenzhaftung für Schadensersatz	76

4.5.4	Kenntniszurechnung.....	77
4.5.5	Weisungsverhältnisse.....	78
4.5.6	Zumutbarkeit der Sperrung.....	79
4.5.7	Absolute Haftungsprivilegierung.....	81
4.5.8	Persönliche Haftung von Mitarbeitern.....	82
4.5.9	Allgemeine Störerhaftung.....	83
4.6	Verkehrssicherungspflichten und Organisationsverschulden.....	84
4.7	Haftung für Links.....	87
4.8	Haftung für Viren.....	89
4.8.1	Erscheinungsformen.....	89
4.8.2	Deliktische Ansprüche.....	91
4.8.3	Umfang der Verkehrspflichten.....	92
4.8.4	Vertragliche Ansprüche.....	95
4.8.5	Einwendungen gegen Schadensersatzansprüche.....	95
4.8.6	Verantwortlichkeit der Mitarbeiter.....	97
4.9	Haftungsausschlüsse.....	97
4.9.1	Disclaimer.....	97
4.9.2	Allgemeine Geschäftsbedingungen.....	98
4.10	Das IT-Sicherheitskonzept.....	99
4.10.1	Ganzheitliche IT-Sicherheit.....	99
4.10.2	Maßnahmen zur Haftungsprävention.....	102
5	<i>Internetnutzung am Arbeitsplatz.....</i>	107
5.1	Private oder dienstliche Internetnutzung.....	107
5.2	Erlaubte oder verbotene Privatnutzung.....	108
5.2.1	Ausdrückliche Erlaubnis.....	108
5.2.2	Konkludente Erlaubnis.....	109
5.2.3	Betriebliche Übung (Betriebsübung).....	110
5.2.4	Beseitigung der Erlaubnis.....	112
5.2.5	Umfang der Erlaubnis.....	114
5.3	Missbrauch und Pflichtverstöße.....	116
5.4	Arbeitsrechtliche Sanktionen bei Pflichtverstößen.....	119
5.4.1	Unverbindlicher Hinweis und Abmahnung.....	119

Inhaltsverzeichnis

5.4.2	Fristgebundene Kündigung.....	121
5.4.3	Fristlose Kündigung.....	123
5.4.4	Verdachtskündigung.....	125
5.5	Zivilrechtliche Folgen – Schadensersatz.....	126
5.5.1	Schadensersatzpflicht des Arbeitnehmers.....	126
5.5.2	Haftungsmilderung wegen gefahrgeneigter Tätigkeit.....	128
5.6	Rundfunkgebühren auf Computer.....	131
5.6.1	Neuartige Rundfunkgeräte.....	131
5.6.2	Herkömmliche Rundfunkgeräte.....	132
5.6.3	GEZ-Filter.....	133
5.6.4	Gebühren und Zweitgerätebefreiung.....	133
5.6.5	Verschiedene Standorte.....	134
5.6.6	Telearbeit, Freiberufler.....	135
5.6.7	Sanktionen bei Verstoß.....	136
5.6.8	Fallbeispiele.....	136
6	<i>Datenschutz und Kontrolle.....</i>	139
6.1	Datenschutz – Grundbegriffe.....	139
6.1.1	Datenschutzgesetze.....	139
6.1.2	Rechtsprechung.....	140
6.1.3	Personenbezogene Daten.....	141
6.1.4	Gebot der Zweckbindung.....	143
6.1.5	Präventives Verbot mit Erlaubnisvorbehalt.....	143
6.1.6	Datenschutzverletzungen.....	145
6.1.7	Der Datenschutzbeauftragte.....	147
6.2	Erlaubte Privatnutzung – Datenschutz nach TK-Recht.....	151
6.2.1	Grundvoraussetzungen des TKG-Datenschutzes.....	151
6.2.2	Anwendbarkeit auf den Arbeitgeber.....	151
6.3	Datenschutzpflicht nach TK-Recht.....	154
6.3.1	Reichweite des Fernmeldegeheimnisses.....	155
6.3.2	Zulässige Kontrolle trotz Fernmeldegeheimnis.....	156
6.3.3	Modifizierende Vereinbarungen.....	158
6.3.4	TKÜV und Vorratsdatenspeicherung.....	160

6.4	Anwendbarkeit des Teledienstedatenschutzgesetzes (TDDSG)	162
6.5	Unerlaubte oder dienstliche Nutzung – Datenschutz nach dem Bundesdatenschutzgesetz (BDSG)	164
6.5.1	Anwendungsbereich des BDSG	164
6.5.2	Anwendungsvoraussetzungen des BDSG	165
6.6	Vorgaben und Datenschutzpflichten aus dem BDSG	166
6.6.1	Vertraglicher Zweck	167
6.6.2	Das Abwägungsgebot	167
6.6.3	Verhältnismäßigkeitsprinzip	169
6.6.4	Allgemein zugängliche Daten	171
6.6.5	Andere Rechtsvorschriften	171
6.6.6	Einwilligung des Betroffenen	171
6.6.7	Benachrichtigung, Auskunft, Löschung	172
6.7	Datenschutzkonforme Mitarbeiterkontrolle	173
6.8	Richtige Reaktion auf Missbrauch	178
6.9	Beweisverwertungsverbote	180
6.10	Rechtliche Gestaltung des Datenschutzes	181
6.10.1	Die Betriebs- bzw. Dienstvereinbarung – Voraussetzungen und Wirkung	182
6.10.2	Betriebs- bzw. Dienstvereinbarung für die Internetnutzung – Mitbestimmungsrechte	184
6.10.3	Checkliste: Notwendige Regelungspunkte einer Betriebsvereinbarung	185
6.10.4	Formulierungsbeispiel einer Betriebsvereinbarung	186
7	<i>Rechtmäßige Filtersysteme</i>	203
7.1	Rechtliche Zulässigkeit des Spammings	204
7.1.1	Deutsche Rechtslage	204
7.1.2	EU-Rechtslage	205
7.1.3	Juristische Abwehrmöglichkeiten	206
7.1.4	Wer kann gegen Spammer vorgehen?	207
7.1.5	Schadensersatz	207
7.1.6	Gegen wen macht ein Vorgehen Sinn?	208
7.1.7	Kostentragung	209

Inhaltsverzeichnis

7.2	Rechtsaspekte des Spam-Filters	209
7.2.1	Reine Markierung.....	210
7.2.2	Mailunterdrückung durch Aussortieren und Löschen	210
7.2.3	Einsichtnahme in den Spamordner.....	213
7.2.4	Verantwortlichkeit des Administrators.....	213
7.2.5	Zugang der „false positives“	214
7.2.6	Kaufmännisches Bestätigungsschreiben	215
7.2.7	Fazit.....	216
7.3	Haftungsfragen des Spamfilters	217
7.3.1	Filterpflicht des E-Mail-Providers	217
7.3.2	Filtern durch den Provider	217
7.3.3	Filtern durch den Empfänger	218
7.3.4	Filterpflicht des Empfängers.....	219
7.4	Rechtliche Leitlinien https-Scanning.....	220
7.4.1	Konstellationen in der Praxis	220
7.4.2	Technisches Verfahren	222
7.4.3	Mögliche Straftatbestände.....	222
7.4.4	Datenschutzrechtliche Zulässigkeit.....	224
7.4.5	Best Practice Beispiel.....	225
8	<i>Anwendbares Recht und Gerichtszuständigkeit.....</i>	227
8.1	Problemstellung	227
8.2	Gerichtsstand im Zivilrecht	228
8.2.1	Wohnsitz und Niederlassung	228
8.2.2	Vertragliche Ansprüche	229
8.2.3	Unerlaubte Handlungen	230
8.3	Anwendbares Recht – unerlaubte Handlungen.....	231
8.3.1	Tatortprinzip und Deliktsstatut	231
8.3.2	Marken- und Domainrecht	233
8.3.3	Wettbewerbsrecht	233
8.3.4	Produkt- oder Produzentenhaftung	235
8.3.5	Datenschutz.....	235
8.4	Anwendbares Recht – Vertragsbeziehungen	236

8.4.1	Rechtswahl	236
8.4.2	Prinzip der engsten Verbindung	237
8.4.3	Verbraucherschutz	237
9	<i>Risikomanagement, Standards und Zertifizierung.....</i>	241
9.1	Verpflichtungen zur IT-Sicherheit.....	241
9.1.1	Privat- und Geschäftsgeheimnisse	241
9.1.2	Personenbezogene Daten.....	244
9.2	Risikomanagement nach KonTraG.....	244
9.2.1	Ziele und Zweck des KonTraG.....	245
9.2.2	Lage- und Risikobericht	245
9.2.3	Anwendungsbereich des KonTraG.....	248
9.2.4	Risikomanagement – Überwachungssystem	249
9.2.5	Haftung der Geschäftsleitung.....	251
9.2.6	Beweislast.....	253
9.2.7	Prüfung durch Aufsichtsrat und Abschlussprüfer	254
9.3	SOX – Sarbanes Oxley Act.....	256
9.3.1	Zweck von SOX.....	256
9.3.2	Anwendungsbereich	257
9.3.3	Section 404 und internes Kontrollsystem	257
9.3.4	Behördliche Überwachung und Regelwerke	259
9.3.5	SOX in der EU.....	260
9.4	Zertifizierung von IT-Sicherheit	260
9.4.1	Vorteile und Standards	261
9.4.2	IT-Grundschutz nach BSI	262
9.5	Vorgaben nach Basel II	264
9.5.1	Ratingverfahren für den Kreditnehmer.....	264
9.5.2	Anforderungen an den Kreditgeber.....	265
9.5.3	MaRisk – gesetzliches Regelwerk für Informationssicherheit	265
9.6	Juristische Sicherheit.....	270
9.6.1	Rechtliche Gestaltung	270
9.6.2	Risikomanagement.....	271
9.6.3	Datenschutzkonzept	271

Inhaltsverzeichnis

9.6.4	Beratung, Schulung, Workshops.....	272
10	<i>Outsourcing von IT-Dienstleistungen.....</i>	273
10.1	Ausgangslage	273
10.2	Was ist Outsourcing?	274
10.3	Rangliste der Outsourcing-Vorteile.....	275
10.4	Rangliste der ausgelagerten Bereiche.....	275
10.5	Erscheinungsformen	275
10.6	Vorbereitungsphase und Entscheidung.....	277
10.7	Anbieterauswahl	278
10.8	Vertragsgestaltung.....	279
10.8.1	Service Level Agreements.....	279
10.8.2	Das Erfolgskriterium: Werk- oder Dienstvertrag.....	281
10.8.3	Gemischter Vertrag	282
10.8.4	Gewährleistung	283
10.8.5	Schadensersatz	284
10.9	Berichtswesen/ Reporting	285
10.10	Rechtsfolgen	285
10.11	Rahmenvertrag	285
10.12	Transitionsphase	286
10.13	Ausstiegsszenario, Vertragsbeendigung	287
10.14	Die häufigsten Outsourcing-Fehler.....	289
11	<i>Archivierungspflichten, Storage, Backup.....</i>	291
11.1	Handelsrechtliche Aufbewahrungspflichten	291
11.1.1	Einsetzbare Datenträger (verwendbare Speichermedien)	292
11.1.2	Aufbewahrungsfristen nach Handelsrecht.....	293
11.2	Steuerrechtliche Aufbewahrungspflichten.....	293
11.2.1	Einsetzbare Datenträger (verwendbare Speichermedien)	294
11.2.2	Außenprüfung	294
11.2.3	Rechnungen und Vorsteuerabzug.....	295
11.2.4	Aufbewahrungsfristen nach Steuerrecht.....	295
11.3	Gesetzliche Aufbewahrungspflichten aufgrund sonstiger Vorschriften	296

11.4	Vorlegungspflichten und Beweislast im Prozess	296
11.5	Strafrechtliche Sanktionen.....	298
11.6	Kollision mit dem Datenschutz, insbesondere die E-Mail-Archivierung....	299
12	<i>Hacker, Phishing, Spyware</i>	303
12.1	Phishing.....	303
12.1.1	Zivilrechtliche Haftung	304
12.1.2	Haftung ohne Verschulden	305
12.1.3	Verschuldensabhängige Haftung	305
12.1.4	Strafbarkeit des Phishing	309
12.2	Hacker-Strafrecht	311
12.2.1	Ausspähen von Daten, § 202a StGB	311
12.2.2	Datenveränderung, § 303a StGB	313
12.2.3	Computersabotage, § 303b StGB.....	314
12.2.4	Strafbarkeit von Hacker-Tools.....	314
13	<i>Voice over IP, Internettelefonie</i>	317
13.1	Überblick: Gefahren von Voice over IP.....	318
13.2	Angriffe auf Voice over IP	318
13.2.1	Viren und Trojaner	318
13.2.2	VoIP-Spoofing	319
13.2.3	Möglichkeiten der Sicherung	319
13.3	Rechtliche Sicherheit bei VoIP.....	320
13.3.1	Eckpunkte zur VoIP-Regulierung	320
13.3.2	Notrufverpflichtung.....	321
13.3.3	Telekommunikations-Überwachung, TKÜV	321
13.3.4	Sicherheitsanforderungen an VoIP	322
13.3.5	Fernmeldegeheimnis.....	323
13.3.6	Betriebsverfassungsrecht	324
13.3.7	VoIP-Spamming, SPIT.....	324
13.3.8	Regulierung von VoIP	324

Inhaltsverzeichnis

14	<i>IT-Rechts-Leitfaden</i>	327
14.1	Mit Rechtssicherheit zur Informationssicherheit	327
14.2	Haftungsfragen – Alles was Recht ist!	328
14.2.1	Strafverfolgung und Auskunftspflichten	328
14.2.2	Verkehrssicherungspflichten	329
14.2.3	Störerhaftung für ungesicherte Netzwerke, offene W-LAN	332
14.2.4	Haftungsszenario	333
14.2.5	Rechtsfolgen	333
14.2.6	Eigenhaftung der Mitarbeiter	334
14.2.7	Haftung nach TDG	336
14.3	Compliance und Risikomanagement	336
14.3.1	Haftung der Geschäftsleitung nach KonTraG	336
14.3.2	Anerkannte Standards und Zertifizierung	337
14.3.3	Vorgaben nach Basel II	338
14.3.4	Compliance nach SOX	340
14.4	Archivierungspflichten – mit Sicherheit Recht behalten!	342
14.4.1	Handelsrechtliche Pflichten	342
14.4.2	Steuerrechtliche Pflichten	343
14.4.3	Ordnungsgemäße Buchführung nach GoBS	343
14.4.4	Elektronische Betriebsprüfung nach GDPdU	344
14.4.5	Digitale Rechnungen	345
14.4.6	Archivierung im Eigeninteresse	346
14.5	Rechtssichere https-Scanserver	346
14.5.1	Zulässigkeitsvoraussetzungen	347
14.5.2	Best Practice-Beispiel	348
14.6	Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis?	348
14.6.1	Private Nutzung, Fernmeldegeheimnis	348
14.6.2	Dienstliche Nutzung, unerlaubte Privatnutzung	349
14.6.3	Interessenausgleich durch rechtliche Gestaltung	350
14.6.4	Mitbestimmung der Betriebs- und Personalräte	351
14.6.5	Betriebs- oder Dienstvereinbarungen	351
14.7	Checkliste	353
	<i>Sachwortverzeichnis</i>	355