

**Studien zu Information, Kommunikation, Medien und Recht**  
Beiträge der Forschungsstelle für Informationsrecht an der Universität St. Gallen

**Studies in Information, Communication, Media and Law**  
Contributions of the Research Center for Information Law at the University of St. Gallen

**Patrick Kos**

Dr. iur., Rechtsanwalt, Executive M.B.L. HSG

**Rechtliche Anforderungen an die  
elektronische Schriftgutverwaltung  
in der Privatwirtschaft und  
Zertifizierungen nach ISO 15489-1  
und ISO/IEC 27001**

---

# Inhaltsverzeichnis

Zusammenfassung	XXIII
Résumé	XXIV
Abstract	XXV
Abbildungen	XXVI
Abkürzungen	XXVII
Literatur	XXXIII
Materialien	XLV
<b>Teil 1: Einleitung</b>	<b>1</b>
<b>A. Ausgangslage und Zielsetzung</b>	<b>3</b>
I. Ausgangslage	3
1. Dynamische Informations- und Dokumentenflut	3
2. Zwecke	4
3. Risiken und Herausforderungen	5
a) Wirtschaftlichkeit	6
b) Technische Aspekte	6
c) Rechtliche Aspekte	7
II. Zielsetzung	8
<b>B. Aufbau der Untersuchung</b>	<b>10</b>
<b>Teil 2: Grundlagen</b>	<b>13</b>
<b>A. Elektronische Schriftgutverwaltung</b>	<b>15</b>
I. Begriffe	15
1. Angelsächsischer Einfluss	15
2. Uneinheitliche Terminologie	15
3. Daten und Informationen	15
4. Dokument und Schriftgut	17
5. Elektronische Schriftgutverwaltung	17
6. Metadaten	18
7. Information Lifecycle Management (ILM)	19
8. Electronic / Enterprise Content Management (ECM)	19
II. Gegenstand der Untersuchung	20
III. Abgrenzung	20
<b>B. Informationssicherheit</b>	<b>21</b>
I. Einleitung	21
II. Begriffe	22
1. Informationssicherheit / IT-Sicherheit / Datensicherheit	22

2.	Grundwerte / Schutzziele der Informationssicherheit	24
a)	Vertraulichkeit	24
b)	Verfügbarkeit	24
c)	Integrität	25
d)	Authentizität	26
e)	Nichtabstreitbarkeit (Non-Repudiation)	27
f)	Verbindlichkeit	27
III.	Umfang	28
1.	Teilgebiete	28
2.	Physische Sicherheit	28
3.	Logische Sicherheit	29
IV.	Daten- und Informationssicherung	30
V.	Ergebnisse	31
<b>C.</b>	<b>Akkreditierungs- und Zertifizierungswesen</b>	<b>32</b>
I.	Übersicht	32
II.	Akkreditierungen	33
1.	Rechtlicher Rahmen	33
2.	Akkreditierungsverfahren im Allgemeinen	34
3.	Akkreditierungsverfahren für Qualitätsmanagementsysteme	35
III.	Zertifizierungen von Public Key Infrastructures (PKI)	36
1.	Übersicht	36
2.	Anerkennungsverfahren (Zertifizierung)	36
IV.	Ergebnisse	38
	<b>Teil 3: Rechtliche Anforderungen</b>	<b>41</b>
<b>A.</b>	<b>Übersicht</b>	<b>43</b>
<b>B.</b>	<b>Spezialgesetze</b>	<b>45</b>
<b>C.</b>	<b>Bundesgesetz über die elektronische Signatur (ZertES)</b>	<b>46</b>
I.	Entstehung	46
1.	EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EU-Signaturrichtlinie)	46
2.	Zertifizierungsdienstverordnung	49
II.	Übersicht	51
1.	Struktur und Konzept	51
2.	Ziel, Zweck und Gegenstand	51
a)	Ziel	51
b)	Zweck und Gegenstand	52
III.	Begriffe – Kategorien elektronischer Signaturen	53
1.	Übersicht	53
2.	Elektronische Zertifikate – einfache elektronische Signaturen	54
3.	Fortgeschrittene elektronische Signaturen / Qualifizierte elektronische Zertifikate nicht anerkannter Zertifizierungsdiensteanbieter	55

4.	Qualifizierte elektronische Zertifikate anerkannter Zertifizierungsdiensteanbieter	55
IV.	Ergebnisse	57
<b>D.</b>	<b>Obligationenrecht – Die kaufmännische Buchführung (Art. 957 ff. OR)</b>	61
I.	Einleitung – Aufbewahrungspflicht	61
II.	Elektronische Aufbewahrung	62
1.	Grundsatz	62
2.	Eingesetzte Technologie	63
3.	Aufzubewahrende Dokumente und Beweiskraft	63
a)	Geschäftsbücher	64
b)	Geschäftskorrespondenz	64
(i)	Übersicht	64
(ii)	E-Mails	65
4.	Digitalisierung – Original und elektronische Kopie	65
a)	Ausgangslage und Problematik	65
b)	Zulässigkeit	66
5.	Dauer und Ort der Aufbewahrung	68
<b>E.</b>	<b>Geschäftsbücherverordnung (GeBüV)</b>	71
I.	Übersicht	71
II.	Aufbewahrungspflichten für elektronische Daten	72
1.	Allgemeine Grundsätze – Ordnungsmässigkeit, Integrität und Dokumentation	72
a)	Ordnungsmässigkeit	72
b)	Integrität	73
c)	Dokumentation	74
2.	Grundsätze der ordnungsgemässen elektronischen Aufbewahrung	75
a)	Allgemeine Sorgfaltspflicht und Verfügbarkeit	75
b)	Organisation	75
c)	Archiv	76
3.	Informationsträger	77
a)	Zulässige Informationsträger	77
b)	Digitale Signaturverfahren	78
(i)	Herausforderungen	78
(ii)	Elektronische Signaturen und Geschäftsbücherverordnung	79
c)	Überprüfung und Datenmigration	82
III.	Rechtsfolgen	83
IV.	Ergebnisse	83
1.	Allgemeines	83
2.	Terminologie, Regelungsansatz und -umfang	84
3.	Praktische Themen	85

<b>F. Mehrwertsteuerrecht</b>	<b>87</b>
I. Übersicht	87
II. Verordnung des Eidgenössischen Finanzdepartements über elektronisch übermittelte Daten und Informationen (EIDI-V)	88
1. Anforderungen	88
2. Elektronische Signatur	89
a) Problemstellung	89
b) Fortgeschrittene elektronische Signaturen	89
3. Übergangsbestimmungen – Ersatz bestehender Zertifikate	91
4. Anforderungen an die Aufbewahrung der Daten	92
5. Dauer und Ort der Aufbewahrung	93
III. Rechtsfolgen	94
IV. Ergebnisse	95
1. Allgemeines	95
2. Terminologie, Regelungsansatz und -umfang	95
<b>G. Datenschutzrecht</b>	<b>97</b>
I. Einleitung	97
II. Übersicht	97
III. Datensammlungen	99
IV. Grundsatz der Datensicherheit	100
V. Technische und organisatorische Massnahmen	101
1. Einleitung	101
2. Besondere technische und organisatorische Massnahmen	103
3. Protokollierung	105
4. Bearbeitungsreglement	106
a) Übersicht	106
b) Nutzen	107
c) Vorgehen	107
d) Kritische Bereiche	108
VI. Bearbeitungsreglement – Struktur und Inhalt	109
1. Allgemeines	109
a) Änderungskontrolle	110
b) Prüfung/Genehmigung	110
c) Referenzierte Dokumente	110
d) Verwendete Abkürzungen	110
2. Präambel	110
3. Herkunft der Daten	111
4. Verwendungszweck für die Daten	111
5. Kontrollverfahren – technische und organisatorische Massnahmen	111
a) Zugangskontrolle	112
b) Datenträgerkontrolle	112
c) Transportkontrolle	112
d) Speicherkontrolle	112
e) Change Management	112

f)	Benutzerkontrolle	113
g)	Eingabekontrolle	113
6.	Beschreibung des Systems	113
a)	Aufbau und Datenherkunft	113
b)	Datenbank	113
c)	Software	114
d)	Sicherheitsaspekte	114
e)	Datenfelder Strukturen	114
f)	Daten, Systeme und Zugriffe / Schnittstellen	115
g)	Löschen	115
h)	Backup	115
i)	Reporting / Datenselektion und -anonymisierung	115
7.	Art und Umfang der Zugriffsberechtigungen	116
a)	Anonymisierung	116
b)	Archivierung	116
c)	Vernichtung und Löschung der Daten	116
8.	Informatikmittel (Hardware, Software, Netzwerk)	116
9.	Auskunftsrecht	117
VII.	Rechtsfolgen	117
VIII.	Datenschutz Zertifizierungen	117
1.	Einleitung	117
2.	Zertifizierungsstellen	118
3.	Gegenstand – Datenschutzmanagementsystem	119
4.	Richtlinien für Datenschutzmanagementsysteme	119
a)	Übersicht	119
b)	Datenvertraulichkeit	121
c)	Datenintegrität	121
d)	Datenverfügbarkeit	121
5.	Erteilung und Gültigkeit der Datenschutzzertifizierung	122
6.	Nutzen und Bedeutung von Datenschutzzertifizierungen	123
IX.	Ergebnisse	125
1.	Allgemeines	125
2.	Terminologie, Regelungsansatz und -umfang	126
<b>H.</b>	<b>Prozessrecht</b>	<b>128</b>
I.	Einleitung	128
II.	Zivilprozess	129
1.	Einleitung	129
2.	Gegenstand und Prozessmaximen	130
3.	Grundlagen des Beweisrechts	132
a)	Recht auf Beweis – Zulässigkeit der Beweisführung	132
b)	Beweiserbringung	133
c)	Beweisgegenstand	134
d)	Beweismass	134
e)	Beweislast – Behauptungslast und Substantiierungslast	135
(i)	Allgemeines	135
(ii)	Beweislast und elektronische Schriftgutverwaltung	138
f)	Beweisabnahme und Beweiswürdigung	139

g)	Beweismittel	140
(i)	Übersicht	140
(ii)	Herausgabepflicht von Urkunden (Editionspflicht)	142
4.	Beweisführung mit elektronischen Dokumenten	143
a)	Recht auf Beweis – Zulässigkeit der Beweisführung	144
b)	Elektronische Dokumente als Beweismittel	144
(i)	Urkundenbeweis de lege lata	145
(ii)	Urkundenbeweis de lege ferenda	146
(iii)	Augenscheinbeweis	148
(iv)	Sachverständigenbeweis (Gutachten, Expertise)	150
c)	Beweiskraft	154
(i)	Allgemeines	154
(ii)	Elektronische Dokumente auf überschreibbaren Datenträgern	155
(iii)	Elektronische Dokumente auf nicht überschreibbaren Datenträgern	156
(iv)	Elektronische Dokumente mit elektronischen Signaturen	156
(v)	Digitalisierte Informationen	157
(a)	Allgemeines	157
(b)	Fallgruppen	158
(c)	Formvorschriften	159
d)	Einbringung in den Prozess	160
5.	Rechtsmittelweg	161
a)	Allgemeines	161
b)	Arten von Rechtsmitteln	162
(i)	Ordentliche und ausserordentliche Rechtsmittel	162
(ii)	Vollkommene und unvollkommene Rechtsmittel	162
c)	Allgemeine Voraussetzungen der Rechtsmittel	162
d)	Neue Tatsachen, Beweismittel und Rechtsbegehren – kantonaler Instanzenzug	163
(i)	De lege lata	163
(ii)	De lege ferenda	164
e)	Neue Tatsachen, Beweismittel und Rechtsbegehren – bundesrechtliche Rechtsmittel	166
6.	Ergebnisse	168
III.	Verwaltungsverfahren und Verwaltungsrechtspflege	170
1.	Einleitung	170
2.	Gegenstand, Verfahrensgrundsätze und -garantien	171
a)	Allgemeines	171
b)	Verfahrensgrundsätze	172
(i)	Übersicht	172
(ii)	Anwendungsbereich	173
c)	Anspruch auf rechtliches Gehör	174
d)	Recht auf gerichtliche Beurteilung – Rechtsweggarantie	175
3.	Rechtsmittelweg	175
a)	Verwaltungsinterne Verwaltungsrechtspflege	175
(i)	Übersicht	175
(ii)	Beschwerde oder Rekurs	176
(iii)	Einsprache	177
(iv)	Revision und Wiedererwägung	177

b)	Verwaltungsgerichtsbarkeit	178
(i)	Übersicht	178
(ii)	Beschwerde an das Bundesverwaltungsgericht	179
(iii)	Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht	182
4.	Ergebnisse	185
<b>I.</b>	<b>Ergebnisse und Würdigung</b>	<b>187</b>
I.	Allgemeines	187
II.	Rechtliche Anforderungen – Terminologie und Regelungsansatz und -umfang de lege lata und de lege ferenda	187
1.	Übersicht	187
2.	Informationssicherheit	191
3.	Terminologie	191
4.	Regelungsansatz und -umfang	191
5.	Würdigung	192
III.	Elektronische Signaturen de lege ferenda	193
1.	Übersicht	193
2.	Würdigung	194
IV.	Elektronische Schriftgutverwaltungssysteme – Umsetzung der rechtlichen Anforderungen	195
1.	Allgemeines	195
2.	Systemerneuerungen – Migration von Daten	196
<b>Teil 4:</b>	<b>Internationale und nationale Normen</b>	<b>197</b>
<b>A.</b>	<b>Einleitung</b>	<b>199</b>
<b>B.</b>	<b>Fachverbände und Normenorganisationen</b>	<b>200</b>
<b>C.</b>	<b>Normen</b>	<b>202</b>
I.	Übersicht	202
1.	Wesen und Aufbau	202
2.	Entstehung von Normen	203
II.	Schweizer Fachempfehlungen und Normen	205
1.	Schweizer Fachempfehlungen	205
a)	Wirtschaftsprüfungshandbuch und CobiT	205
b)	eCH Standard	206
2.	Schweizer Normen	207
III.	Internationale Normen und elektronische Schriftgutverwaltung	209
1.	Einleitung	209
2.	Norm ISO 15489	211
a)	Entstehung	211
(i)	Australische Norm AS 4390	211
(ii)	Prinzipien von AS 4390	212
(iii)	Norm ISO 15489	213
b)	Allgemeines	215
(i)	Zweck und Geltungsbereich	215

(ii)	Aufbau und Prinzipien	215
c)	Inhalt – Übersicht	216
(i)	Norm ISO 15489-1	216
(ii)	Norm ISO/TR 15489-2	217
d)	Einzelne Bestimmungen	218
(i)	Regelungsumfeld	218
(ii)	Anforderungen an die Schriftgutverwaltung	219
(a)	Grundsätze der Programme zur Schriftgutverwaltung	219
(b)	Merkmale von Schriftgut	220
(iii)	Konzeption, Entwicklung und Einsatz von Schriftgutverwaltungssystemen	221
(a)	Merkmale von Schriftgutverwaltungssystemen	221
(b)	Konzeption, Entwicklung und Implementierung von Schriftgutverwaltungssystemen	223
(c)	Ablösung von Schriftgutverwaltungssystemen	226
(iv)	Prozesse und Steuerung der Schriftgutverwaltung	226
(a)	Festlegung der Aufbewahrungsdauer von Schriftgut	226
(b)	Schriftguterfassung	227
(c)	Aufbewahrung und Handhabung	228
(d)	Zugang	228
(e)	Nachvollziehbarkeit	229
(f)	Durchführung der Aussonderung	230
e)	Normative Referenzen	231
(i)	Physische Schriftgutverwaltung	231
(ii)	Elektronische Schriftgutverwaltung	232
3.	Normen ISO/IEC 27002 und ISO/IEC 27001	234
a)	Entstehung	234
(i)	Norm BS 7799	234
(ii)	Normenserie ISO/IEC 27000	235
b)	Zweck und Inhalt	237
(i)	Norm ISO/IEC 27002	237
(ii)	Norm ISO/IEC 27001	238
(a)	Grundsätze	238
(b)	Spezifikationen	239

**D. Ergebnisse** 241

I.	Internationale Normen	241
II.	Internationale Normen und elektronische Schriftgutverwaltung	241
III.	Norm ISO 15489	242
IV.	Corporate und IT Governance	243

**Teil 5: Zertifizierungen nach ISO 15489-1 und ISO/IEC 27001** 245

**A. Übersicht** 247

I.	Allgemeines	247
II.	Ziel einer Zertifizierung	248

III.	Zertifizierungsvereinbarung und Zertifizierungsprozess im Überblick	248
1.	Zertifizierungsvereinbarung	249
2.	Zertifizierungsprozess	250
<b>B.</b>	<b>Zertifizierungsvereinbarung und Zertifizierungsprozess</b>	<b>252</b>
I.	Einleitung	252
II.	Zertifizierungsvereinbarung	252
1.	Hintergrund	252
2.	Leistungsumfang der Zertifizierungsstelle – Zertifizierungsprozess im Detail	253
a)	Erstmaliges Audit (Hauptaudit)	253
(i)	Preaudit: Überblick und generelle Kontrollen	254
(ii)	Phase 1: Dokumentationsaudit nach ISO 15489-1 / ISO/IEC 27001	254
(iii)	Phase 2: Implementierungsaudit nach ISO 15489-1 / ISO/IEC 27001	255
(iv)	Abstimmung von Prozessphasen beim Hauptaudit	256
b)	Überwachungsaudit	256
c)	Wiederholungsaudit	257
d)	Verfahren bei Abweichungen von den Kontrollzielen	258
3.	Geltungsbereich der Zertifizierung	259
a)	Bereiche der Zertifizierung	259
b)	Referenzierte Normen	260
4.	Abgrenzung	260
III.	Berichterstattung	260
IV.	Pflichten und Verantwortlichkeit der Organisation	261
V.	Einschränkungen	263
VI.	Auditteam	263
VII.	Zeitplan und Honorar	264
VIII.	Bedingungen der Zertifizierung	265
1.	Erteilung	265
2.	Aufrechterhaltung	265
3.	Erweiterung oder Einschränkung	265
4.	Aussetzung	266
5.	Entzug	267
6.	Verwendung und Veröffentlichung von Zertifikaten und Zeichen	267
IX.	Einsprüche, Beschwerden und Streitfälle	269
1.	Allgemeine Meinungsverschiedenheiten zwischen der Organisation und der Zertifizierungsstelle	269
a)	Zuständigkeit	269
b)	Verfahren	270
c)	Korrekturen – Massnahmen	270
d)	Endentscheid	270
e)	Überprüfung – Nachhaltigkeit	270
(i)	Qualitätsmanagement der Zertifizierungsstelle	270
(ii)	ISMS der Organisation	271

2.	Meinungsverschiedenheiten bei Aussetzung und Entzug des Zertifikates	271
a)	Zuständigkeit	271
b)	Bestellung des Schiedsgerichtes	271
c)	Sitz des Schiedsgerichtes	271
d)	Verfahrensbestimmungen	271
e)	Verfahrenssprache	272
f)	Schriftsätze und andere Mitteilungen der Parteien	272
3.	Beschwerden von Drittparteien	272
<b>C.</b>	<b>Ergebnisse</b>	273
I.	ISO 15489 und nationales Recht	273
II.	Zertifizierungsvereinbarung	273
III.	Nutzen und Bedeutung von Zertifizierungen	274
<b>Teil 6:</b>	<b>Ausgewählte Einzelthemen</b>	279
<b>A.</b>	<b>Elektronische Schriftgutverwaltung, rechtliche Anforderungen und internationale Standards</b>	281
<b>B.</b>	<b>Rechtsprechung</b>	283
I.	Schweiz	283
1.	Bundesgerichtliche Rechtsprechung	283
2.	Kantonale Rechtsprechung – Steuerrekurskommission Zürich	284
a)	Ausgangslage	284
b)	Erwägungen	285
(i)	Elektronisches Kassensystem	285
(ii)	Elektronisch geführtes Kassenbuch	286
3.	Ergebnisse und Würdigung	287
II.	USA	290
1.	Einleitung	290
2.	Civil law vs common law	291
a)	Rechtssysteme	291
b)	Zivilprozess – Merkmale	292
(i)	Schweiz	292
(ii)	USA	293
(a)	Gerichtssystem	293
(b)	Prozessbeteiligte	294
(c)	Kostenerstattung	295
(d)	Zuständigkeit (Jurisdiction)	297
(e)	Prozessordnungen	298
3.	Zivilprozess vor US Bundesgerichten	300
a)	Übersicht	300
b)	Discovery	302
(i)	Übersicht	302
(ii)	Ziele	303
(iii)	Aufbewahrungspflicht	304
(iv)	Umfang	306

(v)	Dokumente	307
(a)	Übersicht	307
(b)	Physische Dokumente	308
(c)	Elektronisch Gespeicherte Informationen (ESI)	308
(vi)	Durchgriff auf ausländische Konzerngesellschaften	311
(vii)	Sanktionen und Ausnahmen	311
(a)	Sanktionen	311
(b)	Ausnahmen	313
(viii)	Kostenverlegung	314
c)	Hauptverhandlung (trial)	315
d)	Beweisrecht	316
(i)	Beweislast, Beweismittel und Beweisführung	316
(ii)	Beweiswürdigung	317
(a)	Einleitung	317
(b)	E-Mail	318
(c)	Website Postings, Text Messaging und Chat Room Inhalte	318
(d)	Auf Computern gespeichertes Schriftgut und Datenbasen	319
4.	Ergebnisse und Würdigung	320
a)	Allgemeines	320
b)	Risiken	320
c)	Verteidigungsstrategien	322
d)	Elektronische Schriftgutverwaltung	323
e)	E-Mail und New Social Media	325
f)	E-Discovery und europäischer Datenschutz	327
III.	Ergebnisse und Würdigung	328
<b>C.</b>	<b>Wettbewerbsrecht</b>	<b>331</b>
I.	Einleitung	331
1.	Allgemeines	331
2.	Untersuchungsmassnahmen	332
3.	Sanktionen	332
II.	Praxis der Wettbewerbsbehörden	333
1.	Hausdurchsuchungen	333
2.	Sanktionen	335
III.	Ergebnisse und Würdigung	336
1.	Allgemeines	336
2.	Massnahmen	336
a)	Compliance System	336
b)	Bereitschaftsplan	337
c)	Siegelung von Dokumenten	338
d)	Elektronisches Schriftgutverwaltungssystem	338
<b>D.</b>	<b>Fazit in Thesen</b>	<b>339</b>
<b>Anhänge</b>		<b>345</b>
I.	Übersicht Erlasse DSMS	345

II.	Control Objective Domain ISO 15489-1 / ISO/IEC 27001	346
III.	Certification Audit Approach ISO 15489-1 / ISO/IEC 27001	349
IV.	Risiko Management Prozess ISO/IEC 27001	351
V.	Implementierungsaudit – Sektoraudits	353
VI.	Audit Plan	354
VII.	Lebenslauf	355

# Abbildungen

Abbildung 1: Schalenmodell Informationssicherheit.....	30
Abbildung 2: Akkreditierungs- und Anerkennungsablauf für PKI.....	38
Abbildung 3: Zertifizierungszyklus DSMS.....	122
Abbildung 4: Synoptische Darstellung rechtliche Anforderungen.....	189
Abbildung 5: IT-Normen und allgemeine Normen (Standards).....	211
Abbildung 6: Zertifizierung ISO 15489-1 und ISO/IEC 27001 .....	234
Abbildung 7: PDCA Modell für ISMS Prozesse .....	238
Abbildung 8: Übersicht US Zivilprozess .....	301
Abbildung 9: Übersicht Discovery .....	303