



Publikationen aus dem Zentrum für Informations- und
Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Annette Willi

IT-Sicherheit und Recht

**Grundlagen eines integrativen
Gestaltungskonzepts**

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIX
Literaturverzeichnis	XXVII
Materialienverzeichnis	XLI
Abbildungsverzeichnis	XLV

§ 1 Einleitung	1
-----------------------------	----------

§ 2 IT-Sicherheit als technisches und organisatorisches Phänomen	3
A. Begriffliche Grundlagen der IT-Sicherheit	3
I. Ausgangslage	3
II. Definitionen und Grundlagen	4
1. Information	4
2. Sicherheit	5
3. Informationstechnik	6
4. IT-Sicherheit	6
a) Wesenselemente und Definition	6
b) Abgrenzung zur Informationssicherheit	7
III. Elemente der IT-Sicherheit	8
1. Bedrohung	8
2. Risiko	11
3. Sicherheitsanforderungen	12
a) Verfügbarkeit	12
b) Vertraulichkeit	13
c) Integrität	13
4. Erweiterung der Sicherheitsanforderungen	13
a) Authentizität	13
b) Rechtsverbindlichkeit	14
5. Klassifizierung von Information und informationsverarbeitenden Systemen	14
B. IT-Sicherheitsprozess	15
I. Ausgangslage	15
II. Übersicht	17
III. Phasen des Sicherheitsprozesses	18
1. Vorgabe von Zielen	18
2. Durchführung einer Sicherheitsanalyse	19
a) Begriffliche Grundlagen	19
b) Baseline-Ansatz	19
c) Vorgehensschritte im Rahmen einer Sicherheitsanalyse	21
aa) Festlegung der Risikoanalysemethode	21

bb)	Bedarfsanalyse und Bestimmung des Analysebereichs	21
cc)	Bedrohungsanalyse	22
dd)	Risikobewertung	22
ee)	Risikobeurteilung	23
3.	Planung und Umsetzung von Massnahmen	23
4.	Überprüfung und Weiterentwicklung des Sicherheits- prozesses	24
IV.	Konkretisierung des Sicherheitsprozesses	24
C.	Massnahmen zur Sicherung von Informationen und IT-Systemen	25
I.	Rahmenbedingungen	25
II.	Systemtheoretische Grundlagen	26
III.	Übersicht über die Arten und Wirkungsweisen der Massnahmen	28
IV.	Gliederung der Massnahmen	31
1.	Präventive Wirkung	31
a)	Technische Massnahmen	31
aa)	Firewalls	31
bb)	Berechtigungsverwaltung	31
cc)	Datenverschlüsselung	32
dd)	Anonymisierung	32
ee)	Verifikation der Systemkomponenten	32
b)	Administrative Massnahmen	33
aa)	Definition von Verantwortlichkeiten und Vorgehensweisen	34
bb)	Dokumentation der Massnahmen	34
cc)	Einbindung der Vertragspartner	34
c)	Personelle Massnahmen	34
aa)	Fachliche und persönliche Anforderungen an Mitarbeiter	34
bb)	Schaffung einer Sicherheitskultur und eines Sicherheitsbewusstseins der Mitarbeitenden	35
cc)	Regelung des Arbeitsverhältnisses	35
2.	Detektive Wirkung	35
a)	Technische Massnahmen	36
aa)	Automatische Angriffserkennung	36
bb)	Firewalls mit zusätzlicher Malicious Code detection	36
cc)	Installation von Audit Trails	36
b)	Personelle Massnahmen	36
3.	Reaktive Wirkung	36
a)	Technische Massnahmen	37
aa)	Intrusion Prevention	37
bb)	Data-Recovery	37
b)	Administrative Massnahmen	37
aa)	Notfallplanung und -behandlung	37
bb)	Versicherungsschutz	37
cc)	Vertragliche Ausfallsvereinbarungen	37

§ 3 IT-Sicherheit als Gegenstand des Rechts	37
A. Rechtliche Steuerungselemente im Überblick	37
I. Rechtliche Erfassung der IT-Sicherheit	37
II. Regulatorische Konzepte	39
1. Internationales Recht	40
2. Nationalstaatliches Recht	40
3. Selbstregulierung	41
B. Recht der IT-Sicherheit im internationalen und europäischen Kontext	43
I. Globale Regulierungsansätze	43
1. World Summit on the Information Society (WSIS)	43
a) Vision und Herausforderung einer globalen Informationsgesellschaft	43
b) IT-Sicherheit als Element der Informationsgesellschaft	44
c) Plan of Action	44
d) Ergänzungen durch den Weltgipfel in Tunis (2005)	45
2. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security	46
II. Recht der Europäischen Union	47
III. Übereinkommen des Europarates	50
1. Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten	50
2. Übereinkommen über Computerkriminalität des Europarates	51
C. Staatliches Recht (Schweiz)	52
I. Gliederungsansatz	52
II. Bereichsübergreifende (horizontale) Regelungen der IT-Sicherheit	53
1. Datenschutzrecht	53
a) Stellung der IT-Sicherheit im Datenschutzrecht	53
b) Pflicht zur Datensicherung (Art. 7 DSG)	54
c) Spezifische technische Kontrollziele	55
d) Pflicht zur Erstellung eines Protokolls und einer Systemdokumentation	57
e) Stärkung der Datensicherheit im Entwurf zur Änderung des Datenschutzgesetzes	58
2. Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)	58
3. Strafrechtliche Sicherung von Daten und Datenverarbeitungssystemen gegen unbefugten Zugriff	59
III. Bereichsspezifische (vertikale) Regelungen der IT-Sicherheit	59
1. Bereichsspezifische Sicherungspflichten	59
a) Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz)	59

b)	Entwurf des Bundesgesetzes über geographische Information.....	60
2.	Bereichsspezifische Geheimnisschutzregeln.....	60
a)	Fernmeldegeheimnis (Art. 43 FMG).....	60
b)	Strafrechtlicher Schutz des Fernmeldegeheimnisses (Art. 321 ^{ter} StGB).....	60
c)	Strafrechtliche Geheimnisschutzregeln.....	61
d)	Vertragliche Geheimnisschutzregeln.....	61
3.	Bereichsspezifische Aufbewahrungs- und Nachweispflichten.....	62
a)	Buchführungsvorschriften (Art. 957–963 OR).....	62
b)	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV).....	62
c)	Verordnung zum Bundesgesetz über die Mehrwertsteuer (MWSTGV).....	62
d)	Verordnung des EFD über elektronisch übermittelte Daten und Informationen (EIDI-V).....	63
4.	Verletzung von Sicherungspflichten als Haftungs- und Gewährleistungsvoraussetzung.....	64
5.	IT-Sicherheit in der Bundesverwaltung.....	65
a)	Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz.....	65
b)	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV).....	66
c)	Weisungen des Informatikrats des Bundes (IRB) über die Informatiksicherheit in der Bundesverwaltung.....	67
D.	Selbstregulierung.....	67
I.	Technische IT-Sicherheitsstandards.....	68
1.	IT-Grundsatz des BSI.....	68
2.	BS 7799 (Information Security Management System)/ISO 17799-2 (Code of Practice for Information Security Management).....	68
3.	Common Criteria/ISO 15408 (Evaluation Criteria for IT-Security).....	69
4.	COBIT (Control Objectives for Information and Related Technology).....	70
5.	IT Infrastructure Library (ITIL).....	70
II.	Normative Standards.....	71
1.	Eigenmittelanforderungen von Basel II.....	71
2.	Rundschreiben der Eidgenössischen Bankenkommission (EBK) zur Auslagerung von Geschäftsbereichen (Outsourcing).....	71
3.	Corporate Governance Regelwerke.....	72
III.	Relevanz selbstregulativer Normenkomplexe in der Praxis.....	72
1.	Bedeutungszuwachs.....	72

2. Evaluation und Zertifizierung von IT-Produkten und IT-Systemen.....	73
Z. Private und staatliche Organisationen zur Förderung der IT-Sicherheit	74
I. Internationale und europäische Organisationen zur Förderung der IT-Sicherheit	74
1. Information Systems Security Association (ISSA).....	74
2. Institute of Electric and Electronics Engineers (IEEE)	75
3. Forum of Incident Response and Security Teams (FIRST)	75
4. Information Systems Audit and Control Association (ISACA).....	75
5. Agentur für Netz- und Informationssicherheit (ENISA) der EU.....	75
6. Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland.....	76
II. Internationale und europäische Normierungsinstanzen	76
1. Internationale Standardisierungsinstanzen	77
2. ETSI (European Telecommunications Standards Institute).....	77
3. National Institute of Standards and Technology (NIST)	77
III. Organisationen zur Förderung der IT-Sicherheit in der Schweiz	78
1. InfoSurance.....	78
2. Informatikstrategieorgan Bund (ISB)	78
3. Switch (Netzwerk Security).....	78
4. Melde- und Analysestelle Informationssicherung (MELANI)	79
5. Bundesamt für wirtschaftliche Landesversorgung (BWL).....	79
6. SICTA/ASIT	79
7. Fachgruppe Security (FGSec)/iss	80
8. CLUSIS	80
F. Würdigung	80
§ 4 Grundlagen einer IT-Sicherheitsinfrastruktur	83
A. Einleitung.....	83
B. Kryptographie.....	84
I. Grundlagen	84
II. Verschlüsselungsverfahren	85
1. Funktionsweise kryptographischer Verschlüsselungsverfahren	85
2. Symmetrische Verfahren	86
3. Asymmetrische Verfahren	87
4. Umsetzung in der Praxis	88
III. Regulierung kryptographischer Verschlüsselungsverfahren	89
1. Regulierungstypen.....	89
a) Verbot	89
b) Erlaubnis mit Vorbehalt des staatlichen Zugriffs (key recovery-Verfahren).....	89

c)	Erlaubnis mit Hinterlegungspflicht der Schlüssel bei einer vertrauenswürdigen Stelle (key escrow-Verfahren)	90
d)	Keine staatliche Beschränkung	90
2.	Sicherheitsregulierungen in der Praxis (Krypto-Policies)	90
a)	Internationale Krypto-Politik: OECD-Guidelines	90
b)	Europäische Union	91
c)	Schweiz	91
3.	Handelsregulierungen (Export- und Importkontrolle)	91
a)	Wassenaar-Abkommen	92
b)	Exportregulierung der Vereinigten Staaten	93
c)	EU Dual Use-Verordnung	94
d)	Regulierung in der Schweiz	95
aa)	Güterkontrollverordnung	95
bb)	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)	95
cc)	Verordnung über Frequenzmanagement und Funkkonzessionen (VFK)	96
C.	Elektronische Signatur	96
I.	Definition und Ausgangslage	96
II.	Technische Grundlagen	96
1.	Erzeugung der Signatur	96
2.	Public Key Infrastructure (PKI)	98
III.	Internationale Harmonisierungsbestrebungen	98
1.	Rechtliche Rahmenbedingungen	98
2.	UNCITRAL	99
3.	Europäische Union	101
a)	Zertifizierungsdiensteanbieter	101
b)	Anerkennung der elektronischen Signatur	103
IV.	Bundesgesetz über die elektronische Signatur (ZertES)	104
1.	Entstehungsgeschichte und Konzeption	104
2.	Regulierungsansatz	106
3.	Organisation der Zertifizierungsdienste	106
4.	Haftung	107
5.	Rechtswirkungen der elektronischen Signatur	110
a)	Beweiseignung	110
b)	Materiellrechtliche Anerkennung	112
D.	Identifizierungs- und Authentifizierungsverfahren	112
I.	Ausgangslage und begriffliche Grundlagen	112
II.	Bedeutung der Access Control	114
1.	Authentifikationsverfahren als Element der IT-Sicherheitsinfrastruktur	114
2.	Rechtliche Perspektiven der Access Control	116
III.	Übersicht über die Authentifizierungsarten und -verfahren	117
1.	Authentifizierungsarten	117
2.	Authentifikationsverfahren	118

a)	Wissensbasierte Authentifizierung.....	118
b)	Authentifizierung mittels Besitz.....	119
c)	Authentifizierung mittels physischer Merkmale (Biometrie).....	119
IV.	Aktuelle Verfahren der Personenauthentifikation in der Praxis.....	121
1.	Einführung des biometrischen Passes in der Schweiz.....	121
2.	Automatisches Fingerprint-Identifikationssystem (Swiss AFIS).....	123
3.	Pilotprojekt «Secure Check».....	124
4.	Gesichtserkennung bei der Euro 2008.....	125
§ 5	Angewandte IT-Sicherheit im rechtlichen Kontext.....	127
A.	Einleitung.....	127
B.	IT-Sicherheit bei Netzinfrastrukturen.....	129
I.	IT-Sicherheit als organisationsübergreifende Aufgabe.....	129
II.	Eigenschaften und Ausprägungen kritischer Infrastrukturen.....	132
1.	Begriffsverwendungen.....	132
2.	IT-sicherheitsrelevante Ausprägung einzelner Infrastruktur- sektoren.....	133
a)	Informations- und Kommunikationsinfrastruktur.....	133
b)	Energieinfrastruktur.....	135
c)	Finanzinfrastruktur.....	136
III.	Informationstechnologisches Risikopotenzial von kritischen Infrastrukturen.....	137
1.	Vorgehen zur Ermittlung und Einschätzung der Bedrohungs- lage.....	138
2.	Analyse der IT-spezifischen Bedrohungssituation von kritischen Infrastrukturen.....	139
a)	Angriffsziel.....	139
b)	Angriffsmethode.....	140
c)	Schwachstelle.....	140
d)	Angreifer.....	141
3.	Beurteilung IT-spezifischer Risiken.....	142
IV.	Konzepte zum Schutz kritischer Infrastrukturen.....	143
1.	Bisherige Entwicklungen.....	143
2.	Konzeptionelle Ansätze im internationalen Vergleich.....	143
V.	Verfassungsrechtliche Analyse des Infrastrukturschutzes.....	145
1.	Einleitung.....	145
2.	Innere und äussere Sicherheit und Gefahrenabwehr.....	145
a)	Verfassungsrechtliche Grundlagen.....	145
b)	Kompetenzordnung.....	146
3.	Infrastrukturelle Grundversorgung.....	147
a)	Begriffliche Grundlagen.....	147

b)	Horizontale Vorgaben zur Gewährleistung der Grundversorgung	148
c)	Vertikale Bestimmungen in der Telekommunikationsinfrastruktur	148
d)	Vertikale Bestimmungen in der Energieinfrastruktur	149
e)	Vertikale Bestimmungen in der Finanzinfrastruktur	150
4.	Verantwortlichkeitsordnung	150
VI.	Regulierungskonzepte	152
1.	Sektorübergreifende Regulierungsbestrebungen zum Schutz kritischer Infrastrukturen	152
a)	Bundesgesetz über die wirtschaftliche Landesversorgung	152
b)	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit	153
c)	Sicherheitspolitischer Bericht 2000	154
d)	Bericht des Bundesrates zur Grundversorgung in der Infrastruktur	154
2.	Sektorspezifische Regulierungsbestrebungen zum Schutz kritischer Infrastrukturen	155
a)	Telekommunikationsinfrastruktur	155
b)	Energieinfrastruktur	161
c)	Finanzinfrastruktur	162
3.	Kooperationsformen zwischen privater und öffentlicher Hand	165
VII.	Aktivitäten zum Schutz kritischer Infrastrukturen in der Schweiz	167
1.	Schutzkonzept	167
a)	Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz	167
b)	Konzept «Information Assurance»	167
2.	Institutionen	169
a)	Aktivitäten von Bundesbehörden	169
b)	Aktivitäten von privaten Institutionen	170
3.	Entwicklungstendenzen in der Schweiz	171
4.	Internationale Aktivitäten und Institutionen zum Schutz kritischer Infrastrukturen	173
C.	IT-Sicherheit in Organisationen	176
I.	IT-Sicherheit als organisationspezifische Aufgabe	176
1.	Ausgangslage	176
2.	Herausforderungen einer unternehmensweiten Sicherheitsgestaltung	176
3.	Unternehmensspezifische Risikosituation	177
4.	Governance der IT-Sicherheit im Unternehmen	179
II.	Funktionale Anforderungen an die IT-Sicherheit im Unternehmen	180
1.	Gewährleistungsfunktion	181
2.	Schutzfunktion	181
3.	Wertschöpfungsfunktion	182

4. Überblick	182
III. Informationsschutz im Unternehmen	183
1. Information als schützenswertes Gut	183
2. Rahmenbedingungen des Informationsschutzes	184
a) Rechtliche Vorgaben	184
b) Strategische Komponenten	184
c) Ökonomische Rahmenbedingungen	185
3. Etablierung eines Management-Informationssystems	186
IV. Konzeptioneller Ansatz eines unternehmensweiten IT-Sicherheitsmanagements	188
1. IT-Sicherheits-Policy	188
a) Inhalt	188
b) Zuständigkeit	189
2. IT-Sicherheitskonzept	191
a) Inhalt	191
b) Zuständigkeit	191
c) Prozess zur Erstellung eines Sicherheitskonzepts	192
3. IT-Sicherheitsrichtlinien	192
a) Inhalt	192
b) Umsetzung der Richtlinien	193
c) Zuständigkeit	193
4. Zuständigkeitsordnung im Unternehmen	193
a) Anforderungen	193
b) Unternehmensspezifische Anpassungen	194
c) Schnittstellen mit anderen Zuständigkeitsbereichen im Unternehmen	195
d) Übersicht	195
V. Verantwortlichkeit der Unternehmensorgane für IT-Sicherheit	197
1. Ausgangslage	197
2. Allgemeine Haftungsvoraussetzungen von Art. 754 OR	197
3. Widerrechtlichkeit im Besonderen	198
a) Oberleitung der Gesellschaft (Art. 716a Abs. 1 Ziff. 1 OR)	198
b) Festlegung der Organisation (Art. 716a Abs. 1 Ziff. 2 OR)	199
c) Oberaufsicht (Art. 716a Abs. 1 Ziff. 5 OR)	200
d) Sorgfaltspflichtverletzung (Art. 717 OR)	201
4. Weitere Rechtsgrundlagen	202
a) Corporate Governance-Empfehlungen	202
b) Revision des Aktien- und Rechnungslegungsrechts	203
c) Verordnung über die Banken und Sparkassen (BankV)	203
d) Sarbanes-Oxley Act	204
e) Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (Deutschland)	204

VI.	Begrenzung der persönlichen Haftung der Unternehmensorgane	205
1.	Delegation an die IT-Revision?	205
2.	Versicherung von IT-Risiken	205
3.	Evaluation und Zertifizierung der IT-Sicherheit	206
4.	Beurteilung eines Vorgehens nach dem Best Practice-Ansatz im Unternehmen	206
5.	Ausblick	207
VII.	Elektronische Aufbewahrung und Archivierung	208
1.	Ausgangslage	208
2.	Neues Buchführungsrecht	208
a)	Art. 957–963 OR	208
b)	Geschäftsbücherverordnung (GeBüV)	209
c)	Verordnung des Eidg. Finanzdepartements über elektronische übermittelte Daten und Informationen (EIDI-V)	209
3.	Technikneutralität und internationale Standardisierung	210
4.	System- und organisationsbezogene Kriterien der Aufbewah- rung und Archivierung	212
5.	Integrität der Informationen im Besonderen	213
6.	Organisation und Verfahren	215
7.	Vorgehen im Rahmen der Archivierung	218
8.	Datenschutzrechtliche und beweisrechtliche Heraus- forderungen	220
9.	Elektronische Aufbewahrung und Archivierung in der öffentlich-rechtlichen Körperschaft	222
a)	Anforderungen	222
b)	Rechtsgrundlagen	222
c)	Zugänglichkeit des Archivguts und Datenschutz	223
d)	Projekte auf Bundesebene	224
VIII.	Outsourcing	224
1.	Datenschutzproblematik	224
2.	Security Outsourcing	226
3.	Bankenbereich im Besonderen	227
4.	IT-Outsourcing in der Verwaltung	228
IX.	Weitere ausgewählte Sicherheitsaspekte des elektronischen Geschäftsverkehrs	230
1.	IT-Sicherheit als Voraussetzung des elektronischen Geschäftsverkehrs	230
2.	Sicheres E-Mail	230
a)	Sicherheitsrelevante Vorgaben	230
b)	Rechtliche Anforderungen	231
c)	Praktische Umsetzung	232
3.	IT-Sicherheit bei elektronischen Bezahlvorgängen	233
a)	Einführung	233

b)	Anforderungen an elektronische Zahlungssysteme im Allgemeinen.....	234
c)	Sicherheitsanforderungen im Besonderen.....	236
d)	Übersicht über verschiedene elektronische Zahlungsüberweisungssysteme.....	237
aa)	Internet Keyed Payment Protocols.....	237
bb)	Secure Transaction Technology.....	238
cc)	Secure Electronic Payment Protocol.....	239
dd)	Secure Electronic Transaction.....	239
ee)	3D-Secure/SPA/UCAF.....	239
ff)	CyberCash.....	240
gg)	Click&buy.....	241
hh)	Easyp@y.....	241
ii)	PayPal.....	242
e)	Bedeutung elektronischer Zahlungsüberweisungssysteme in der Praxis.....	242
D.	IT-Sicherheit im Spannungsfeld von Individuum und Kollektiv.....	243
I.	Ausgangslage.....	243
II.	IT-Sicherheit und Datenschutz bei der automatischen Identifizierung über Funk (RFID).....	245
1.	Einführung.....	245
2.	Bedrohungslage.....	247
a)	Schwachstellen/Angriffsziele.....	247
b)	Angriffsmethoden.....	248
3.	Sicherheitsmassnahmen.....	249
4.	RFID und Datenschutzrecht.....	250
a)	Beteiligte Interessengruppen.....	250
b)	Mobile und allgegenwärtige Datenverarbeitung.....	251
c)	Anpassungsbedarf der bestehenden Datenschutzkonzepte.....	252
d)	Entwicklungsperspektiven.....	253
III.	IT-Sicherheit bei elektronischen Wahl- und Abstimmungsverfahren.....	253
1.	Ausgangslage.....	253
a)	Bisherige Entwicklungen.....	253
b)	Begriffliche Grundlagen.....	255
2.	Rechtsgrundlagen.....	255
a)	Art. 34 BV.....	255
b)	Art. 8a des Bundesgesetzes über die politischen Rechte.....	257
c)	Art. 27a–27q der Verordnung über die politischen Rechte.....	257
aa)	Pilotversuche mit elektronischer Stimmabgabe (Art. 27a–27c VPR).....	257
bb)	Genehmigungsvoraussetzungen (Art. 27d VPR).....	258

3.	Chancen und Risiken des E-Voting (Interessenabwägungsprozess).....	258
a)	Einführung von E-Voting als Chance für die demokratischen Prozesse.....	259
b)	IT-Sicherheit als massgebliches Risiko von E-Voting.....	260
c)	Herausforderungen bei der Einführung von E-Voting.....	260
d)	Beurteilung und Akzeptanz von E-Voting in der Bevölkerung.....	261
e)	Akzeptanz des Restrisikos.....	261
4.	Sicherheitsaspekte bei elektronischen Abstimmungsverfahren.....	262
a)	Rechtliche Anforderungen an die Umsetzung von E-Voting.....	262
aa)	Kontrolle der Stimmberechtigung (Art. 27d Abs. 1 lit. a VPR).....	263
bb)	Einmaligkeit der Stimmabgabe (Art. 27d Abs. 1 lit. b VPR).....	263
cc)	Zuverlässige Wiedergabe unverfälschter Willenskundgabe (Art. 27d Abs. 1 lit. c VPR).....	263
dd)	Wahrung des Stimmgeheimnisses (Art. 27d Abs. 1 lit. d VPR).....	264
ee)	Vertrauenswürdigkeit der Ergebnisermittlung (Art. 27d Abs. 1 lit. e VPR).....	265
ff)	Regelkonformität des Urnengangs (Art. 27d Abs. 1 lit. f VPR).....	265
b)	Technische Mindestanforderungen zur Sicherstellung der rechtlichen Vorgaben für E-Voting.....	266
5.	Realisierung von E-Voting in der Schweiz.....	268
a)	Bisherige Entwicklungen in der Schweiz.....	268
b)	Übersicht über die Pilotprojekte und Projektorganisation.....	269
c)	Organisation und Systemarchitektur des Zürcher Pilotprojekts.....	270
aa)	Schaffung eines virtuellen Stimmregisters in dezentralen Strukturen.....	270
bb)	Sicherheitselemente des neuen Stimmrechtsausweises.....	271
cc)	Elektronische Stimmabgabe und Urnendienst.....	272
dd)	Architektur des E-Voting Systems.....	272
d)	Beurteilung des Standes der Umsetzung unter sicherheitsspezifischen Gesichtspunkten.....	272
e)	Einschätzung der bestehenden Risiken der kantonalen Umsetzung.....	273
6.	Ausblick und künftige Entwicklungsschritte.....	275
IV.	IT-Sicherheit bei E-Health.....	278
1.	Ausgangslage.....	278
2.	Chancen und Risiken von E-Health.....	279

3.	Rechtsgrundlagen von E-Health	281
4.	Überblick über die Anwendungsbereiche von E-Health	284
a)	Interne Prozesse und telemedizinische Übermittlungsvorgänge	284
aa)	Informations-/Kommunikationssysteme	284
bb)	Patientenchipkarte und -dossier	284
cc)	Weitere Dienstleistungen	286
b)	Telemedizin	287
aa)	Telemonitoring und Disease Management	287
bb)	Internet-Hotline und Call-Center	287
cc)	Telediagnostik	288
dd)	Telechirurgie	288
ee)	Weitere Dienstleistungen	289
5.	Einführung der Versicherten- bzw. Gesundheitskarte in der Schweiz	289
a)	Rechtsgrundlage	289
b)	Vorgesehene Funktionen und Anwendungen der Versichertenkarte	291
c)	Sicherheit und Datenschutz	293
d)	Vorgehen und Ausblick	294
6.	Schutzvorgehen	294
a)	Interdisziplinarität des Regelungsansatzes	295
b)	Datensicherheits- und Infrastruktursicherheitskonzepte	295
c)	Interne Organisation und Audit	297
d)	Zugangsregelungen	297
e)	Prozedurale Aspekte	298
V.	Identitätsmanagement	299
1.	Zunahme digitaler Identitäten	299
2.	Identitätsmanagement und Datenschutz	300
3.	eCard-Strategie der Bundesregierung in Deutschland	302
4.	Identitätsmanagement mittels multifunktionaler Chipkarten?	303
5.	Entwicklungstendenzen	304
VI.	Herausforderungen an den Datenschutz	305
1.	Proaktiver Datenschutz	305
a)	Technikgestaltung	305
b)	Datenschutz-zertifizierung	306
2.	Internationale Standardisierungstendenzen im Datenschutzrecht	308
3.	Modernisierung des Datenschutzes	309
§ 6	Ausblick	313