

Inhaltsverzeichnis

Vorwort	5
Inhaltsübersicht	7
Abkürzungsverzeichnis	13
I. Grundlagen der Gesundheitstelematik	17
A. Einführung	17
1. Begriffsbestimmung	17
2. Gesundheitstelematik vs Telemedizin und ELGA	18
2.1. Telemedizin	18
2.2. ELGA	19
B. Rechtlicher Rahmen der Gesundheitstelematik	22
1. Grundlagen des DSGVO 2000	22
1.1. Grundrecht auf Datenschutz	22
1.2. Personenbezogene Daten	23
1.3. Akteure des DSGVO	24
1.4. Anwendungsbereich - persönlich/geografisch/sachlich	25
1.5. Zulässigkeit und Grundsätze der Datenverwendung / Geheimhaltungsinteressen	26
1.6. Datenverkehr mit dem Ausland	27
1.7. Datenverarbeitungsregister	28
2. Grundprinzipien des TKG 2003	30
2.1. Einführung	30
2.2. Kommunikationsgeheimnis	31
2.3. Technische Überwachungseinrichtungen - Lawful Interception	34
2.3.1. Grundlagen	34
2.3.2. Schnittstellenspezifikation	36
2.3.3. IP-basierte Lawful Interception	38
2.4. Schlussfolgerungen	39
3. Grundprinzipien des GTelG 2012	39
3.1. Grundlagen	39
3.2. Gesundheitsdaten	41
3.3. Datenweitergabe und Datenverwendung	42
3.4. Die Gesundheitsdiensteanbieter	44
C. Datensicherheitsaspekte in der Gesundheitstelematik	45
1. Datensicherheit im DSGVO 2000	45
1.1. Datensicherheitsmaßnahmen	46
1.1.1. Allgemeine Datensicherheitsmaßnahmen	46
1.1.2. Konkrete Datensicherheitsmaßnahmen	48
1.2. Datengeheimnis	52

1.3.	Datensicherheit gem deutschem Bundesdatenschutzgesetz (BDSG).....	52
2.	Datensicherheit im TKG 2003.....	53
3.	Datensicherheit im GTeIG 2012.....	55
3.1.	Grundsätze.....	56
3.2.	Identität.....	56
3.3.	Rollenkonzept.....	58
3.4.	Vertraulichkeit.....	59
3.4.1.	Cloud Computing.....	61
3.4.2.	Mögliche Netzwerkinfrastruktur und Vertraulichkeit.....	63
3.4.2.1.	LAN-Infrastruktur.....	63
3.4.2.2.	WLAN-Infrastruktur.....	63
3.4.2.3.	WAN-Infrastruktur.....	64
3.4.2.4.	BSI-Empfehlung.....	64
3.4.2.5.	Firewall Infrastruktur.....	65
3.4.3.	Mögliche Applikationsinfrastruktur und Vertraulichkeit.....	66
3.5.	Datenintegrität.....	67
3.5.1.	Elektronisches Signaturrecht.....	68
3.5.1.1.	Signatur-RL.....	68
3.5.1.2.	Signaturgesetz.....	71
3.5.1.3.	Signaturverordnung.....	72
3.5.1.4.	Elektronische Kommunikation im öffentlichen Bereich.....	75
3.6.	IT-Sicherheitskonzept.....	75
3.6.1.	Checklist - IT-Datensicherheitskonzept.....	78
3.7.	Die GTeIG-Privilege.....	85
3.7.1.	Inhouse-Privileg.....	85
3.7.2.	GDA-Privileg.....	86

II. Bedarfsorientierte Dienste / Cloud Computing..... 89

A.	Technische Grundlagen.....	90
1.	Einführung.....	90
2.	Begriffsbestimmung.....	91
2.1.	Zugänglichkeit des Cloud-Dienstes – Rollout/Betriebs-Modelle.....	93
2.2.	Cloud-Servicekategorien/-modelle und Funktionalitäten.....	95
2.3.	Funktionsweise.....	98
3.	Technische und organisatorische Aspekte.....	99
4.	Spezifische Schutzziele bei IaaS, PaaS, SaaS.....	103
4.1.	IaaS.....	103
4.2.	PaaS.....	104
4.3.	SaaS.....	106
5.	Schlussfolgerungen.....	108
B.	Bedarfsorientierte Dienste aus europäischer / europarechtlicher Sicht.....	110

1. Grundlagen und Risiken	110
2. EU-Rechtsrahmen	113
2.1. Anwendbares Recht	114
2.2. Akteure und Verantwortlichkeiten	115
2.3. Datenschutzgrundprinzipien in der Cloud	119
2.3.1. Verfügbarkeits-, Integritäts- und Vertraulichkeitstrias (VIV-Trias)	121
2.3.2. Transparenz und Isolierung/Zweckgebundenheit	123
2.3.3. Intervenierbarkeit, Portabilität und Rechenschaftspflicht	123
3. Datentransfer in Drittstaaten	124
3.1. Safe-Harbor USA, Kanada, Israel	125
3.2. EuGH Entscheidung zum US Safe-Harbor	128
3.3. Sichere Drittstaaten	130
3.4. EU-Standardvertragsklauseln / interner Verhaltenskodex	130
3.5. Verhaltenskodex für Unterauftragsnehmer/ Sub-Dienstleister	132
4. Datennutzung im hoheitlichen Bereich	133
C. Rechtsgrundlagen in Österreich	135
1. Akteure	135
2. Datenweitergabe - zivilrechtliche Dimension	136
3. Datenweitergabe ins Ausland – öffentlich-rechtliche Dimension	137
4. Datenweitergabe an Subdienstleister	139
5. Verschlüsselte Daten	141
D. Datensicherheit	144
1. Regelungen im DSG 2000	144
2. Regelungen im TKG 2003	144
3. Regelungen im GTeIG 2012	144
3.1. Grundlegendes	144
3.2. Bedarfsorientierte Dienste	145
3.3. Datensicherheit bei Cloud Computing	145
4. Sicherheitsnormen/Technische Standards	147
5. ISO 2700x	148
5.1. Grundlagen	149
5.2. ISO 27001 und 27002	151
5.3. ISO 27017 (DIS) und 27018	153
5.3.1. ISO 27017 (DIS)	154
5.3.2. ISO 27018	157
5.3.3. DIS 27017 : ISO 27018	160
6. BSI IT-Grundschutz	160
7. Abgeleitete Sicherheitsmaßnahmen	162
7.1. Informationssicherheitsleitlinie	162
7.2. Datenschutzrichtlinie	164
7.3. Datensicherungskonzept	165

7.4.	Sicherstellung der Vertraulichkeit	167
7.5.	Sicherstellung der Integrität der Daten	169
7.6.	Zugriffskontrolle	170
7.7.	Zutrittsschutz	171
7.8.	Protokollierung	172
7.9.	Fazit.....	174
III. Zusammenfassung und Ausblick.....		175
IV. Anhang.....		177
DSG 2000.....		177
GTeIG 2012		180
GTeIV 2013		185
SigV 2008.....		187
Literaturverzeichnis		195
Stichwortverzeichnis.....		197