Inhaltsverzeichnis

1 Einführung 1
1.1 Haben wir etwas zu verbergen? 2
1.2 Säulen des Datenschutzes 3
1.3 Themen dieses Buchs und Lernziele 4

Teil I Technischer Datenschutz

2 Einführung in den Technischen Datenschutz 9
2.1 Schutzziele 9
2.1.1 „Klassische" IT-Sicherheits-Schutzziele 10
2.1.2 „Neue" Datenschutz-Schutzziele 10
2.2 Begriffsbestimmungen 11
2.2.1 Begriff des Datenschutzes 11
2.2.2 Begriffe zum technischen Datenschutz 12
2.3 Grundlegende kryptographische Verfahren 15
2.3.1 Verschlüsselung 15
2.3.2 Digitale Signatur 18
2.3.3 Blinde Signatur 18
2.3.4 Kryptographische Hash-Funktionen 19
2.3.5 Diffie-Hellman-Verfahren 20
2.4 Grundlegende Verfahren aus der IT-Sicherheit 22
2.4.1 Transport Layer Security 23
2.4.2 Virtual Private Networks 25
2.5 Fazit 26
2.6 Übungsaufgaben 26
Literatur 26

Bibliografische Informationen
https://d-nb.info/1264668074

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3 Anonymitätsmaße 29
3.1 Überblick 29
3.1.1 Anonymitäts-Modelle 30
3.1.2 Quasi-Identifikatoren 32
3.2 k-Anonymität 34
3.2.1 Generalisierung von Daten 35
3.2.2 Angriffe auf k-Anonymität 36
3.2.3 l-Diversität 39
3.3 Differential Privacy 40
3.4 Anonymisierung in der Praxis 42
3.5 Fazit 43
3.6 Übungsaufgaben 44
Literatur 45

4 Anonymität im Internet 47
4.1 Verkehrsflussanalyse 48
4.1.1 Angreiferklassifikation 48
4.1.2 Beispiel: Ablauf der Ticketbestellung 49
4.1.3 Beispiel: Mögliche Gegenmaßnahme 50
4.2 Mixes 51
4.2.1 Verfahren 52
4.2.2 Analyse 52
4.3 Mix-Kaskaden 53
4.3.1 Verfahren 53
4.3.2 Analyse 55
4.3.3 Antwort-Nachrichten 55
4.4 Onion Routing/Tor 57
4.4.1 Grundkonzept von Tor 58
4.4.2 Tor-Zellen 58
4.4.3 Aufbau eines Circuits 59
4.4.4 Leaky Pipe 61
4.4.5 Missbrauch von Tor 62
4.4.6 Hidden Services 62
4.4.7 Angriffe auf Tor 62
4.4.8 Zensurresistenz mit Tor 65
4.5 Fazit 65
4.6 Übungsaufgaben 66
Literatur 67

5 Identitätsmanagement 69
5.1 Überblick 70
5.1.1 Schwerpunkte und Sichtweisen im Identitätsmanagement 70
5.2 OpenID 71
5.2.1 Ablauf der Authentifizierung 72
5.2.2 Analyse 72
5.3 OAuth 73
5.3.1 Verfahren 74
5.3.2 Analyse 75
5.4 OpenID Connect 76
5.5 Geprüfte Identitäten in der Praxis 77
5.6 Fazit 78
5.7 Übungsaufgaben 78
Literatur 79

6 Anonymes Bezahlen 81
6.1 Anforderungen an ein anonymes Bezahlverfahren 82
6.2 Anonymes Bezahlen nach Chaum 83
6.2.1 Verfahren im Überblick 83
6.2.2 Bewertung 86
6.3 Bitcoin 86
6.3.1 Anonymität von Bitcoin 89
6.4 Anonymisierungskonzepte für Kryptowährungen 90
6.4.1 Mixcoin 91
6.4.2 Monero 92
6.5 Anonymes Bezahlen in der Praxis 95
6.5.1 Prepaid-Karten 95
6.6 Fazit 96
6.7 Übungsaufgaben 97
Literatur 97

7 Datenschutz im World Wide Web 99
7.1 Tracking im Web 99
7.1.1 Cookies 100
7.1.2 Tracking-Pixel 102
7.1.3 Device Fingerprinting 104
7.1.4 History Hijacking 104
7.1.5 P3P 104
7.2 Social Plugins 105
7.3 Fazit 106
7.4 Übungsaufgaben 106

8 Instant Messaging 107
8.1 Abgrenzung des Instant Messagings von E-Mail 107
8.1.1 Schutzziele bei der E-Mail-Sicherheit 108
8.1.2 Schutzziele beim Instant Messaging 108
8.2 Off-the-record Messaging 109
8.2.1 Protokoll 109
8.2.2 Implementierung 111
8.2.3 Angriffe auf OTR Messaging 111
8.2.4 SIGMA-Protokoll 112
8.3 WhatsApp 113
8.3.1 Signal-Protokoll 114
8.3.2 Medien-Verschlüsselung 115
8.3.3 Sichere Telefonie 116
8.3.4 Schlüssel-Verifikation 116
8.3.5 Datenschutzrechtliche Probleme 116
8.4 Fazit 116
8.5 Übungsaufgaben 117
Literatur 117

9 Elektronische Ausweisdokumente 119
9.1 Elektronischer Reisepass 120
9.1.1 Passive Authentication 120
9.1.2 Basic Access Control 120
9.1.3 Extended Access Control 122
9.2 Elektronischer Personalausweis 126
9.2.1 PACE 127
9.2.2 Extended Access Control Version 2 128
9.2.3 Restricted Identification 130
9.2.4 Weitere Anwendungen 132
9.2.5 Exkurs: Elektronische Signaturen 133
9.3 Fazit 135
9.4 Übungsaufgaben 136
Literatur 136

10 Weitere kryptographische Verfahren für PETs 137
10.1 Weitere Signaturverfahren 137
10.1.1 Gruppensignatur 138
10.1.2 Ringsignatur 139
10.2 Secure Multiparty Computation 139
10.2.1 Klassische MPC-Protokolle 140
10.2.2 Anwendungen der Secure Multiparty Computation 141
10.3 Zero-Knowledge Proof 142

10.4 Anonyme Berechtigungsnachweise 143
10.4.1 Probleme 143
10.4.2 Verfahren 144
10.5 Fazit 145
10.6 Übungsaufgaben 145
Literatur 145

Teil II Datenschutzrecht

11 Einführung in das Datenschutzrecht 149

12 Die Rechtsordnung im Allgemeinen 151
12.1 Die Quellen des Rechts – Rechtsquellen 151
12.2 Ähnlichkeiten zwischen der Rechtsordnung und Software 152
12.3 Überblick über die Rechtsordnung 154
12.3.1 Die Bundesebene 155
12.3.2 Die Landesebene 158
12.3.3 Die Ebene der Europäischen Union bzw. des Europäischen Wirtschaftsraums 159
12.3.4 Der Europarat 161
12.3.5 Die allgemeinen Regeln des Völkerrechts 162
12.3.6 Die Hierarchie des Rechts 162

13 Grundlagen des Datenschutzrechts 165
13.1 Entwicklung des Datenschutzes 165
13.1.1 Punktuelle Diskretionsregelungen 166
13.1.2 Allgemeine Datenschutzgesetze 167
13.1.3 Das Volkszählungsurteil des BVerfG 168
13.2 Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich 169
13.3 Zweck des Datenschutzes 170
13.4 Wichtige Gesetze 173
13.4.1 Wichtige Rechtsakte auf Ebene der Europäischen Union 173
13.4.2 Wichtige Gesetze auf Ebene der Bundesrepublik Deutschland 176
13.4.3 Wichtige Gesetze auf Ebene der deutschen Bundesländer 179
13.5 Wichtige Begriffe des Datenschutzes 180
13.5.1 Personenbezogene Daten 181
13.5.2 Verarbeitung, Verarbeitungsschritte 184
13.5.3 Pseudonymisierung 186
13.5.4 Dateisystem 187
13.5.5 Verantwortlicher 188

13.5.6 Auftragsverarbeiter ... 190
13.5.7 Dritter ... 191
13.5.8 Besondere Kategorien personenbezogener Daten ... 191

14 Welche Daten darf man wofür verarbeiten? ... 193
14.1 Gilt ein „Verbot mit Erlaubnisvorbehalt"? ... 193
14.1.1 Das präventive Verbot mit Erlaubnisvorbehalt im Allgemeinen ... 193
14.1.2 Ein präventives Verbot mit Erlaubnisvorbehalt im Datenschutzrecht? ... 194
14.2 Rechtsgrundlagen ... 195
14.2.1 Art. 6 Abs. 1 UAbs. 1 lit b DSGVO – Vertragserfüllung ... 196
14.2.2 Art. 6 Abs. 1 UAbs. 1 lit c DSGVO – Rechtliche Verpflichtung ... 197
14.2.3 Art. 6 Abs. 1 UAbs. 1 lit d DSGVO – Lebenswichtige Interessen ... 198
14.2.4 Art. 6 Abs. 1 UAbs. 1 lit e DSGVO – Öffentliches Interesse, öffentliche Gewalt ... 198
14.2.5 Art. 6 Abs. 1 UAbs. 1 lit f DSGVO – Berechtigtes Interesse ... 200
14.2.6 Art. 6 Abs. 1 UAbs. 1 lit a DSGVO – Einwilligung ... 202
14.3 Allgemeine Voraussetzungen für die Rechtmäßigkeit von Datenverarbeitungen ... 209
14.3.1 Art. 5 Abs. 1 lit a DSGVO – Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ... 210
14.3.2 Art. 5 Abs. 1 lit b DSGVO – Zweckbindung ... 211
14.3.3 Art. 5 Abs. 1 lit c DSGVO – Datenminimierung ... 212
14.3.4 Art. 5 Abs. 1 lit d DSGVO – Richtigkeit ... 213
14.3.5 Art. 5 Abs. 1 lit e DSGVO – Speicherbegrenzung ... 213
14.3.6 Art. 5 Abs. 1 lit f DSGVO – Integrität und Vertraulichkeit ... 213
14.3.7 Art. 5 Abs. 2 DSGVO – Rechenschaftspflicht ... 213
14.4 Dauer der Datenverarbeitung – Löschung ... 213
14.4.1 Grundsatz: Löschverpflichtung ... 214
14.4.2 Pflicht zur Nachberichtigung ... 215
14.4.3 Ausnahmen von der Lösch- und Nachbrichtigungs-verpflichtung ... 215
14.5 Übermittlungen von Daten in Drittstaaten ... 217
14.5.1 Angemessenheitsbeschluss der EU-Kommission ... 218
14.5.2 Geeignete Garantien, Standardvertragsklauseln ... 219
14.5.3 Verbindliche interne Datenschutzvorschriften ... 219
14.5.4 Sonstige Drittlandsübermittlungen in Einzelfällen ... 219

14.6 Die Bedeutung zivilrechtlicher Nutzungsrechte für den Datenschutz ... 219

15 Rechenschaftspflicht ... 221
15.1 Verzeichnis der Verarbeitungstätigkeiten ... 222
15.1.1 Verarbeitungstätigkeiten ... 223
15.1.2 Enthaltene Angaben ... 224
15.1.3 Entbehrlichkeit eines Verzeichnisses der Verarbeitungstätigkeiten ... 226
15.2 Datenschutz-Folgenabschätzung ... 228
15.2.1 Zweck einer Datenschutz-Folgenabschätzung ... 228
15.2.2 Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung ... 229
15.2.3 Ohne Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung ... 230
15.2.4 Inhalt einer Datenschutz-Folgenabschätzung ... 230
15.2.5 Ergebnis der Datenschutz-Folgenabschätzung ... 231
15.3 Datenpannen ... 231
15.3.1 Was sind Datenpannen? ... 231
15.3.2 Was tut man mit Datenpannen? ... 232
15.4 Informationspflichten ... 235
15.5 Zu schließende Verträge ... 239
15.5.1 Vereinbarung zur gemeinsamen Verantwortung ... 239
15.5.2 Auftragsverarbeitungsvertrag ... 240

16 Technische und organisatorische Maßnahmen – toMs ... 243

17 Betroffenenrechte ... 247
17.1 Wichtige Betroffenenrechte ... 247
17.1.1 Auskunft ... 247
17.1.2 Berichtigung ... 249
17.1.3 Löschung ... 251
17.1.4 Einschränkung der Verarbeitung ... 251
17.1.5 Nachberichtigung ... 252
17.1.6 Widerspruch ... 253
17.1.7 Datenübertragbarkeit ... 254
17.1.8 Recht auf Entscheidung durch Menschen ... 255
17.1.9 Beschwerde bei einer Datenschutz-Aufsichtsbehörde ... 256
17.2 Allgemeine Anforderungen an die Reaktion des Verantwortlichen ... 256
17.3 Gesetzliche Beschränkungen von Betroffenenrechten ... 257

18 Ausgewählte Verarbeitungssituationen 259
18.1 Videoüberwachung 259
18.2 Aufnahme und Veröffentlichung von Fotos 260
18.2.1 Rechtslage vor Wirksamwerden der DSGVO – das KUG 260
18.2.2 Rechtslage seit Wirksamwerden der DSGVO – das KUG? 261
18.2.3 Urheberrecht 262
18.3 Websites und Apps 262
18.3.1 Impressumspflicht 263
18.3.2 Informationspflicht 263
18.3.3 Rechtsgrundlage 263
18.4 E-Mail 267
18.5 Elektronische Kalender 267
18.6 Messenger 268
18.7 Cloud Computing, Software as a Service 268

19 Zertifizierung, Akkreditierung 271

20 Der (betriebliche oder behördliche) Datenschutzbeauftragte 273
20.1 Benennpflicht 273
20.1.1 Benennpflicht aus Art. 37 DSGVO 273
20.1.2 Benennpflicht aus § 38 BDSG 276
20.2 Stellung des Datenschutzbeauftragten 278
20.3 Aufgaben 278
20.3.1 Unterrichtung und Beratung – lit a 278
20.3.2 Überwachung – lit b 279
20.3.3 Beratung und Überwachung bei Datenschutz-Folgenabschätzung – lit c 280
20.3.4 Verhältnis zur Aufsichtsbehörde – lit d und e 280

21 Rolle der der Datenschutz-Aufsichtsbehörde 283
21.1 Beratung 283
21.2 Kontrolle und Sanktion 284
21.3 Zertifizierung, Akkreditierung 284
21.4 Informationsquellen 284

22 Zusammenfassung und Ausblick 287

Stichwortverzeichnis 289