

Inhaltsübersicht

1. Kapitel: Ursprünge und Entwicklungen des Datenschutz- rechts	1
2. Kapitel: Rechtliche Einordnung	25
3. Kapitel: Zweck und Geltungsbereich des DSG	43
4. Kapitel: Begriffe	55
5. Kapitel: Bearbeitungsgrundsätze	87
6. Kapitel: <i>privacy by design</i> und <i>privacy by default</i>	107
7. Kapitel: Datensicherheit	121
8. Kapitel: Verhaltenskodizes	141
9. Kapitel: Zertifizierungen	147
10. Kapitel: Datenbearbeitung durch Private	153
11. Kapitel: Datenbearbeitung durch öffentliche Organe	169
12. Kapitel: Datenbekanntgabe	189
13. Kapitel: Bearbeiten durch Auftragsbearbeiter	213
14. Kapitel: (Governance-)Pflichten des Verantwortlichen und des Auftragsbearbeiters	223
15. Kapitel: Rechte der Betroffenen	263
16. Kapitel: Beratungs- und Aufsichtsorgane	283
17. Kapitel: Sanktionen	303
18. Kapitel: Praxis <i>Inside</i>	313

Inhaltsverzeichnis

Vorwort der Herausgeber	V
Vorwort der Autorinnen zur 2. Auflage	VII
Vorwort der Autorinnen zur 1. Auflage	IX
Inhaltsübersicht	XI
Abkürzungsverzeichnis	XXXI
Allgemeines Literaturverzeichnis	XXXIX
Allgemeines Materialienverzeichnis	XLI

1. Kapitel: Ursprünge und Entwicklungen des Datenschutzrechts

.....	1
A. Einstieg	2
B. Einführungsfall	5
C. Weshalb ist Datenschutz (noch immer) wichtig?	6
D. Entwicklung des Schweizer Datenschutzrechts	7
I. Die Zeit zwischen 460 und 370 v.Chr.: Hippokrates macht den Anfang	7
II. 20. Jahrhundert: Das Datenschutzrecht hält Einzug in die Rechtsordnungen	7
III. 21. Jahrhundert: Datenschutz und Digitalisierung	9
1. Impuls: Datenschutzrevision in der EU	9
2. Der Schweizer Weg zu einem modernen Datenschutzgesetz	9
E. Blick über die Grenzen – Datenschutz ausserhalb der Schweiz	11
I. Europäische Union	11
1. Die Anfänge	11
2. Die Datenschutz-Grundverordnung der EU	12
3. EU-Digitalpolitik	14
II. USA	18
III. China	22

2. Kapitel: Rechtliche Einordnung 25

A. Einstieg 26

B. Einführungsfall 28

C. Verfassungs- und grundrechtlicher Persönlichkeitsschutz ... 29

 I. Überblick 29

 II. Art. 10 und 13 BV 30

 1. Recht auf Leben und persönliche Freiheit (Art. 10 BV) 30

 2. Recht auf Schutz der Privatsphäre (Art. 13 BV) 31

 III. Subjekte des Persönlichkeitsschutzes 32

D. Zivilrechtlicher Persönlichkeitsschutz 33

 I. Überblick 33

 II. Schutz der Persönlichkeit gegen Verletzungen von Dritten (Art. 28 ZGB) 34

 1. Inhalt und Schutzzweck 35

 2. Verletzung der Persönlichkeit 36

 3. Rechtfertigungsgründe einer Persönlichkeitsverletzung 37

 a) Einwilligung 37

 b) Überwiegendes privates oder öffentliches Interesse 37

 c) Gesetz 38

 4. Rechtsbehelfe im zivilrechtlichen Persönlichkeitsschutz, nicht vermögensrechtliche und vermögensrechtliche Ansprüche 39

E. Datenschutzrechtlicher Persönlichkeitsschutz 40

 I. Föderale Kompetenzordnung 40

 II. «Allgemeines» und «besonderes» Datenschutzrecht 40

 1. «Allgemeines» Datenschutzrecht 41

 2. «Besonderes» Datenschutzrecht 41

 a) Öffentliche Organe 41

 b) Privatpersonen 42

3. Kapitel: Zweck und Geltungsbereich des DSG	43
A. Einstieg	44
B. Einführungsfall	45
C. Zweck	45
D. Persönlicher Geltungsbereich	46
E. Sachlicher Geltungsbereich	47
I. Daten natürlicher Personen	47
II. Ausnahmen und Abgrenzungen	48
1. Ausnahmen vom Geltungsbereich des DSG	48
2. Abgrenzungen	48
a) Verfahrensrecht	48
aa) Begriff der Gerichtsverfahren und der bundesrechtlichen Verfahren	49
bb) Anknüpfungspunkt	49
b) Öffentliche Register des Privatrechtsverkehrs	51
c) Abgrenzung Persönlichkeitsschutz nach DSG und StGB	51
F. Räumlicher Geltungsbereich (Kollisionsrecht)	52
4. Kapitel: Begriffe	55
A. Einstieg	56
B. Einführungsfall	57
C. Überblick – Begriffe von Art. 5 DSG	59
D. Personendaten (lit. a)	60
I. Definition	60
II. «Anonymisierte Daten»	61
III. «Pseudonymisierte Daten»	62
E. Betroffene Person (lit. b)	63
F. Besonders schützenswerte Personendaten (lit. c)	63
I. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten (Ziff. 1)	64
II. Daten über die Gesundheit (Ziff. 2)	65
III. Daten über die Intimsphäre (Ziff. 2)	65

IV. Zugehörigkeit zu einer Rasse oder Ethnie (Ziff. 2)	65
V. Genetische Daten (Ziff. 3)	66
VI. Biometrische Daten (Ziff. 4)	66
VII. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Ziff. 5)	67
VIII. Daten über Massnahmen der sozialen Hilfe (Ziff. 6)	67
G. Bearbeiten (lit. d)	68
H. Bekanntgeben (lit. e)	70
I. Profiling (lit. f)	71
I. Begriff	71
II. Risikobasierter Ansatz: Profiling mit hohem Risiko (lit. g)	72
J. Verletzung der Datensicherheit (lit. h)	73
K. Bundesorgan (lit. i)	74
I. Begriff	74
II. Anknüpfungspunkt «öffentliche Aufgabe des Bundes»	75
L. Verantwortlicher (lit. j)	78
M. Auftragsbearbeiter (lit. k)	80
I. Definition	80
II. Abgrenzung zum Verantwortlichen	82
III. Nicht jeder Dienstleister ist ein Auftragsbearbeiter	83
IV. Auftragsdatenbearbeitungsvertrag (ADV)	84
5. Kapitel: Bearbeitungsgrundsätze	87
A. Einstieg	88
B. Einführungsfall	89
C. Generelles	90
D. Die Bearbeitungsgrundsätze von Art. 6 DSG im Einzelnen ...	92
I. Grundsatz der Rechtmässigkeit	92
II. Grundsatz von Treu und Glauben	94
III. Grundsatz der Verhältnismässigkeit	95
1. Geeignete, notwendige und zumutbare Datenbearbeitung	95
2. Praktische Umsetzung	98
IV. Grundsatz der Zweckbindung	99

1. Datenbeschaffung für einen bestimmten Zweck	99
2. Vernichtung und Anonymisierung bei Wegfall des Zwecks	103
V. Datenrichtigkeit	104
6. Kapitel: <i>privacy by design</i> und <i>privacy by default</i>	107
A. Einstieg	108
B. Einführungsfall	108
C. Hintergrund	110
D. Normzweck und allgemeine Aspekte	111
I. Persönlicher Geltungsbereich	112
II. Sachlicher Geltungsbereich	113
E. Datenschutz durch Technik (<i>privacy by design</i>)	114
I. Zielsetzung	114
II. Mittel: Technologie und Organisation im Dienst des Datenschutzes	114
1. Technische und organisatorische Massnahmen	115
a) Technische Massnahmen	116
b) Organisatorische Massnahmen	116
2. Beurteilungskriterien	117
F. Datenschutz durch datenschutzfreundliche Voreinstellungen (<i>privacy by default</i>)	119
I. Zielsetzung	119
II. Mittel: Geeignete Voreinstellungen	119
7. Kapitel: Datensicherheit	121
A. Einführung	122
B. Einführungsfall	122
C. Vorbemerkungen	123
D. Begriff der Datensicherheit	124
I. Keine Definition im Gesetz	124
II. Nuancierung des Begriffs der Datensicherheit in der DSV	124
III. Internationale Standards und <i>best practices</i>	125

.....

E. Persönlicher Geltungsbereich von Art. 8 DSGVO	127
F. Schutzziele	128
I. Vertraulichkeit	128
II. Verfügbarkeit	128
III. Integrität	129
IV. Nachvollziehbarkeit	129
G. Vorgehen zur Festlegung der geeigneten technischen und organisatorischen Massnahmen	130
I. Methodik	130
1. Erster Schritt: Beurteilung des Schutzbedarfs	131
a. Art der bearbeiteten Daten	131
b. Zweck, Art, Umfang und Umstände der Datenbearbeitung	131
2. Zweiter Schritt: Beurteilung des Risikos	132
a. Risikoursachen	132
b. Die hauptsächlichen Gefahren	133
c. Getroffene oder geplante Massnahmen zur Risikominimierung	133
d. Wahrscheinlichkeit und Auswirkungen einer Verletzung der Datensicherheit trotz getroffener Massnahmen	137
3. Dritter Schritt: Wahl der technischen und organisatorischen Massnahmen	137
II. Dynamischer Prozess	138
 8. Kapitel: Verhaltenskodizes	 141
A. Einstieg	142
B. Einführungsfall	142
C. Verhaltenskodizes	143
I. Zweck von Verhaltenskodizes	143
II. Normadressaten	144
III. Inhalt von Verhaltenskodizes	144
IV. Freiwilligkeit von Verhaltenskodizes	145
V. Stellungnahme des EDÖB zu Verhaltenskodizes	145

9. Kapitel: Zertifizierungen	147
A. Einstieg	148
B. Einführungsfall	148
C. Zertifizierungen	149
I. Vorbemerkungen	149
II. Normadressaten	149
III. Was kann zertifiziert werden?	150
IV. Massstäbe für die Zertifizierung	150
V. Wer zertifiziert?	151
VI. Verfahren und Aufsicht des EDÖB	151
10. Kapitel: Datenbearbeitung durch Private	153
A. Einstieg	154
B. Einführungsfall	155
C. Verantwortlichkeit im Unternehmen	156
D. Widerrechtliche Persönlichkeitsverletzungen durch bestimmte Datenbearbeitungen	158
I. Persönlichkeitsverletzungen	158
II. Rechtfertigungsgründe	159
1. Einwilligung	160
2. Überwiegendes öffentliches oder privates Interesse	162
3. Gesetzliche Grundlage	165
E. Klagen zum Schutz der Persönlichkeit	165
F. Datenbearbeitung durch private Verantwortliche mit Sitz oder Wohnsitz im Ausland	166
I. Vertretung (Art. 14 DSGVO)	166
II. Pflichten der Vertretung (Art. 15 DSGVO)	167
11. Kapitel: Datenbearbeitung durch öffentliche Organe	169
A. Einstieg	170
B. Einführungsfall	171
C. Vorab: Mehrere Datenbearbeitende – eine Verantwortung	172
D. Rechtsgrundlagen	173

I.	Verankerung des verfassungsmässigen Legalitätsprinzips	173
II.	Rechtsgrundlage für das Bearbeiten «gewöhnlicher» Personendaten	174
III.	Rechtsgrundlage für das Bearbeiten besonders schützenswerter Personendaten	174
IV.	Ausnahme: Regelungskompetenz des Bundesrats	176
V.	Ausnahme: Bearbeiten ohne materiell- oder formell-gesetzliche Grundlage	176
E.	Pilotversuche	177
I.	Rechtsstaatliche Notwendigkeit einer Pilotversuchs-Regelung	177
II.	Kumulative Voraussetzungen für einen Pilotversuch	178
	1. Vorab: Nur Pilotversuche mit besonders schützenswerten Personendaten?	179
	2. Aufgabennorm in einem Gesetz im formellen Sinne	179
	3. Massnahmen zur Begrenzung von Persönlichkeitsverletzungen auf ein Mindestmass	180
	4. Unentbehrlichkeit der Testphase	180
III.	Modalitäten vor und während der Testphase	181
	1. Regelung des Pilotprojekts in einer Verordnung	181
	2. Bewilligung durch den Bundesrat, Einbezug des EDÖB	182
	3. Keine unendliche Geschichte: Evaluation und Befristung der Pilotphase	183
F.	Bearbeiten für nicht personenbezogene Zwecke	184
I.	Erfordernis einer Regelung	184
II.	Der «nicht personenbezogene» Zweck	185
III.	Bearbeitungsvoraussetzungen	186
G.	Privatrechtliche Tätigkeit eines Bundesorgans	187
12. Kapitel: Datenbekanntgabe	189
A.	Einstieg	190
B.	Einführungsfall	191
C.	Bekanntgabe von Daten im Generellen	193

D. Durch öffentliche Organe	193
I. Grundsatz des Legalitätsprinzips	193
II. Ausnahmen: Bekanntgabe ohne gesetzliche Grundlage	194
1. Unentbehrlichkeit für die Erfüllung einer gesetzlichen Aufgabe	195
2. Einwilligung der betroffenen Person	195
3. Dringender Schutz von Leib und Leben	196
4. Veröffentlichung der Personendaten durch die betroffene Person	196
5. Bekanntgabe zur Durchsetzung von Rechtsansprüchen der Empfängerin bzw. des Empfängers	196
III. «Personalien-Bekanntgabe»	197
IV. Bekanntgabe mittels Informations- und Kommunikationsdiensten	198
V. Einschränkungsründe	198
VI. Widerspruchsrecht	199
VII. Spezialfall «Bekanntgabe» nach Öffentlichkeitsprinzip (BGÖ)	200
E. Datenbekanntgabe ins Ausland	201
I. Was ist ein Datentransfer ins Ausland?	201
II. Was ist kein Datentransfer ins Ausland?	202
III. Grundsätze (Art. 16 DSGVO)	203
1. Länder mit angemessenem Datenschutzniveau	203
2. Länder ohne angemessenes Datenschutzniveau	206
a) Standardvertragsklauseln (SCC) im Spezifischen	207
b) Weitere Garantien	210
IV. Ausnahmen (Art. 17 DSGVO)	211
13. Kapitel: Bearbeiten durch Auftragsbearbeiter	213
A. Einstieg	214
B. Einführungsfall	215
C. Bearbeiten durch Auftragsbearbeiter	216
I. Outsourcing von Aufgaben	216
II. Zur Erinnerung: Auftragsbearbeiter, Verantwortung und Bekanntgabeprivileg	216

III. Voraussetzungen einer Auftragsbearbeitung	218
1. Auftragsbearbeitung gestützt auf eine gesetzliche Grundlage oder einen Vertrag	218
2. Cura in eligendo, in instruendo et in custodiendo	218
3. Kein Verbot der Auftragsbearbeitung	220
IV. Unterauftragsbearbeitung	221
V. Auslagerung ins Ausland	221
 14. Kapitel: (Governance-)Pflichten des Verantwortlichen und des Auftragsbearbeiters	 223
A. Einstieg	224
B. Einführungsfall	226
C. Informationspflicht (inkl. Ausnahmen)	227
I. Informationspflicht bei der Beschaffung von Personendaten (Art. 19 DSGVO)	227
1. Allgemeines	227
2. Zweck der Informationspflichten	228
3. Mindestinformationen	228
4. Zeitpunkt der Information	230
5. Formvorschriften	230
6. Datenschutzerklärungen	230
II. Ausnahmen von der Informationspflicht und Einschränkungen (Art. 20 DSGVO)	232
III. Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 21 DSGVO)	234
1. Wann liegt eine automatisierte Einzelentscheidung vor?	235
2. Möglichkeit zur Stellungnahme durch die betroffene Person	236
3. Überprüfung durch eine natürliche Person	236
4. Ausnahmen	236
5. Automatisierte Einzelentscheidungen durch Bundesorgane	237
D. Governance-Pflichten	237
I. Allgemeines	237

II.	Bearbeitungsverzeichnis	238
1.	Pflicht zur Führung eines Bearbeitungsverzeichnisses	238
2.	Inhalt des Bearbeitungsverzeichnisses	239
3.	Formvorgaben	240
4.	Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses	240
5.	Folgen bei unterlassener Erstellung eines Bearbeitungsverzeichnisses	241
III.	Weitere Dokumentationspflichten	242
1.	Protokollierungspflicht	242
a)	Vorab: Datensicherheit oder <i>privacy by design</i> ?	242
b)	Verpflichtete	242
c)	Umfang der Protokollierungspflicht	243
d)	Aufbewahrung und Zugänglichkeit der Protokolle	243
2.	Das Bearbeitungsreglement	244
a)	Verpflichtete	244
b)	Inhalt und Form	244
3.	Interne Datenschutzrichtlinie	245
IV.	Datenschutz-Folgenabschätzung	245
1.	Vorprüfung: Liegt ein «hohes Risiko» vor?	246
2.	DSFA: Vorgehen und Inhalt	247
3.	Form und Aufbewahrungsdauer	249
4.	Ausnahmen	249
5.	Folgen bei Vorliegen eines hohen Risikos	249
E.	Meldung von Verletzungen der Datensicherheit	252
I.	Normzweck	252
II.	Normadressat	252
III.	Definition «Verletzung der Datensicherheit»	253
IV.	Meldepflicht	254
1.	Gegenüber dem EDÖB	254
2.	Gegenüber der betroffenen Person	254
a)	Grundsatz	254
b)	Einschränkungen der Meldepflicht gegenüber der betroffenen Person	255

3. Inhalt der Meldepflicht 255

4. Dokumentation 256

5. Exkurs: Meldepflicht vs. Selbstanzeige und Rechte
des Angeschuldigten 256

F. Meldung von Cyberangriffen auf kritische Infrastrukturen ... 257

 I. Verpflichtete Bereiche 257

 II. Zu meldende Angriffe 259

 III. Inhalt der Meldung 260

 IV. Meldefrist 260

 V. Einordnung aus Datenschutzsicht 260

15. Kapitel: Rechte der Betroffenen 263

A. Einstieg 264

B. Einführungsfall 265

C. Betroffenenrechte im Allgemeinen 266

D. Das Recht auf Auskunft 267

 I. Auskunftsrecht als zentrales Instrument
 der informationellen Selbstbestimmung 267

 II. Zuständigkeit 268

 III. Umfang des Auskunftsrechts 268

 IV. Modalitäten, Kosten und Fristen 270

 1. Modalitäten 270

 2. Kosten 270

 3. Fristen 270

 V. Einschränkungen des Auskunftsrechts 271

 1. Einschränkung im Gesetz im formellen Sinn
 und bei überwiegenden Interessen 271

 2. Einschränkung bei rechtsmissbräuchlichen Gesuchen 272

 3. Einschränkungsgründe für private Verantwortliche 272

 4. Einschränkungsgründe für Bundesorgane 273

 5. Folgen bei der Missachtung des Auskunftsrechts 273

 6. Medienprivileg 273

 VI. Exkurs: Abgrenzung zum Akteneinsichtsrecht 274

E. Das Recht auf Datenherausgabe und -übertragung 274

I. Zweck	274
II. Voraussetzungen	275
III. Umfang	275
IV. Gängiges elektronisches Format	276
V. Kosten	276
VI. Löschung nach der Übertragung	277
VII. Einschränkungen des Rechts auf Datenportabilität	277
VIII. Folgen bei der Missachtung des Rechts auf Datenportabilität	277
F. Berichtigungs- und Widerspruchsrecht gegenüber Privaten	278
G. Ansprüche gegen Bundesorgane: Unterlassung, Beseitigung, Feststellung der Widerrechtlichkeit	279
16. Kapitel: Beratungs- und Aufsichtsorgane	283
A. Einstieg	284
B. Einführungsfall	284
C. Datenschutzberater/innen	285
I. Sinn und Zweck dieser Funktion	285
II. Datenschutzberater/innen in Unternehmen (Art. 10 DSG, Art. 23 DSV)	286
III. Datenschutzberater/innen in Bundesorganen (Art. 10 DSG, Art. 25 ff. DSV)	288
D. Eidgenössischer Datenschutz- und Öffentlichkeits- beauftragter	291
I. EDÖB – Amt oder Person?	291
II. Organisation	291
1. Organisatorische, fachliche und finanzielle Unabhängigkeit	291
2. Persönliche Voraussetzungen	292
3. Amtsdauer	293
III. Aufgaben und Befugnisse	293
1. Beratungs- und Sensibilisierungstätigkeit	293
2. Anhörung zu Erlassen und Massnahmen des Bundes	294
3. Erarbeitung von Empfehlungen zu <i>best practices</i>	294

4. Register der Bearbeitungstätigkeiten	295
5. Funktionen nach BGÖ	295
6. Untersuchung von Verstößen gegen Datenschutz- vorschriften	296
7. Amtshilfe	298
8. Zusammenarbeit mit dem Bundesamt für Cyber- sicherheit (BACS; Art. 41 DSV)	300
9. Auch beim EDÖB können Personendaten bearbeitet werden	301
 17. Kapitel: Sanktionen	 303
A. Einstieg	304
B. Einführungsfall	305
C. Vorbemerkungen	305
I. Verpasste Chance?	305
II. Gemeinsamkeiten aller Tatbestände	306
III. Anwendbarkeit der allgemeinen Bestimmungen des StGB	307
IV. Zuständigkeit	307
D. Verletzung von Informations-, Auskunfts- und Mitwirkungs- pflichten	307
E. Verletzung von Sorgfaltspflichten	308
F. Verletzung der beruflichen Schweigepflicht	310
G. Missachtung einer Verfügung	311
 18. Kapitel: PraxisInside	 313
A. Einstieg	314
B. Digitale Transformation	316
I. Worum geht es?	316
II. Achtung Stolperfallen!	317
1. Digitalisierungsprojekte sind nicht nur «Projekte der IT-Abteilung»	317
2. Digitalisierung von Prozessen: Keine 1:1-Übernahme aus der analogen Welt	319

3. Digitalisierungsprojekte bringen auch rechtliche Fragestellungen mit sich	320
C. Staatliche digitale Souveränität	321
I. Digitale Souveränität – worum geht es?	321
II. Überlegungen im Verwaltungsalltag – gerade beim Gang in die Cloud	322
III. Staatliche digitale Souveränität, ein Auslaufmodell?	323
D. Rechtliche Überlegungen zum staatlichen Gang in die Cloud	324
E. Künstliche Intelligenz	328
I. Die Geburtsstunde der künstlichen Intelligenz	328
II. Was ist künstliche Intelligenz?	329
III. Funktionsweise der KI	330
IV. Anwendungen	333
V. Ethische und rechtliche Herausforderungen	335
F. Informationssicherheits- und Datenschutzmanagement-system	339
I. Um was geht es?	339
II. Warum ein gesamtheitlicher Ansatz?	341
1. Zwei Systeme, drei gemeinsame Perspektiven	341
2. Synergien nutzen	342
III. Konkret: Einsatzbereich und Inhalt der Management-systeme	344
G. Online Collaboration	347
I. Worum geht es?	347
II. Rechtliche Fragestellungen	347
III. Risikobasierte Überlegungen bei der Wahl eines Online-Collaboration-Tools	349
H. Online-Plattformen und Social Media	351
I. Aktualität	351
II. Was ist eine Online-Plattform?	352
III. Datenschutzrechtliche Aspekte	353
1. Allgemeine datenschutzrechtliche Vorgaben	353
2. Die Frage der Verantwortlichkeit	354
a) Grundsatzproblematik	354
b) Verantwortlichkeiten bei Bewertungsplattformen	354

3. Die Big-Data-Frage	355
4. Das Social-Media-Paradox	355
I. Cookies	356
I. Was sind Cookies?	356
II. Rechtliche Einordnung	358
1. In der Schweiz	358
2. In der EU	358
III. Tipps zum Einsatz von Cookies	359
J. Governance in Blockchain und DLT	360
I. Kleine Blockchain-Kunde	360
1. Was ist eine Blockchain?	360
2. Drei Kerneigenschaften der Blockchain	361
3. Wie funktioniert eine Blockchain?	361
4. Ausgestaltungsformen	362
II. Datenschutzrechtliche Aspekte	362
1. Einwilligung?	362
2. Notwendigkeit der «Veröffentlichung»?	362
3. Wahrung der Betroffenenrechte	363
4. Die Frage der Verantwortung und des anwendbaren Rechts	363
5. Governance der Blockchain	364
III. Blockchain: Eine datenschutzrechtliche <i>Mission impossible?</i>	365
K. Internet of Things (IoT)	366
I. Um was geht es?	366
II. Regulierung von IoT	369
III. Governance von IoT	369
IV. Datenschutzrechtliche Herausforderungen	369
1. Grundsätzliches	369
2. Daten- und Informationssicherheit	370
L. Self-Sovereign Identity	371
I. Um was geht es?	371
II. Was ist eine Self-Sovereign Identity?	372

III. Wie funktioniert eine Self-Sovereign Identity?	373
IV. Datenschutzrechtliche Aspekte	374
M. Immersive Reality, VR, AR und MR	376
I. Um was geht es?	376
II. Varianten der virtuellen Realitäten (VR, AR, MR)	376
III. Einsatzmöglichkeiten	378
IV. Rechtliche Fragestellungen	379
1. Allgemeines	379
2. Datenschutzrechtliche Aspekte	380
a) Rechtmässigkeit der Datenbearbeitung?	380
b) Aufbewahrungsort und -dauer, Zugriffs- berechtigungen	381
c) Datensicherheit	381
d) Datenschutzrechtlicher Handlungsbedarf?	382
Sachregister	383