

Datenschutzrecht

Dr. iur. Sandra Husi-Stämpfli, LL.M., Executive MPA

Dr. iur. Anne-Sophie Morand, LL.M., Rechtsanwältin

Prof. iur. Ursula Sury, Rechtsanwältin

Inhaltsverzeichnis

Vorwort der Herausgeber	V
Vorwort der Autorinnen	VII
Inhaltsübersicht	IX
Abkürzungsverzeichnis	XXIX
Allgemeines Literaturverzeichnis	XXXVII
Allgemeines Materialienverzeichnis	XXXIX
1. Kapitel: Datenschutz – allgegenwärtig, aber um was geht es eigentlich?	1
A. Einstieg	2
B. Einführungsfall	4
C. Weshalb ist Datenschutz (noch immer) wichtig?	5
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
3. Exkurs: Dynamische Entwicklungen auf EU-Ebene – Wegweiser für die Schweiz	11
2. Kapitel: Rechtliche Einordnung	17
A. Einstieg	18
B. Einführungsfall	20
C. Verfassungs- und grundrechtlicher Persönlichkeitsschutz ...	21
I. Überblick	21
II. Art. 10 und 13 BV	22
1. Recht auf Leben und persönliche Freiheit (Art. 10 BV)	22

2. Recht auf Schutz der Privatsphäre (Art. 13 BV)	23
III. Subjekte des Persönlichkeitsschutzes	24
D. Zivilrechtlicher Persönlichkeitsschutz	25
I. Überblick	25
II. Schutz der Persönlichkeit gegen Verletzungen von Dritten (Art. 28 ZGB)	26
1. Inhalt und Schutzzweck	27
2. Verletzung der Persönlichkeit	28
3. Rechtfertigungsgründe einer Persönlichkeits- verletzung	29
a) Einwilligung	29
b) Überwiegendes privates oder öffentliches Interesse	29
c) Gesetz	30
4. Rechtsbehelfe im zivilrechtlichen Persönlichkeits- schutz, nicht-vermögensrechtliche und vermögens- rechtliche Ansprüche	31
E. Datenschutzrechtlicher Persönlichkeitsschutz	32
I. Föderale Kompetenzordnung	32
II. «Allgemeines» und «besonderes» Datenschutzrecht	32
1. «Allgemeines» Datenschutzrecht	33
2. «Besonderes» Datenschutzrecht	33
a) Öffentliche Organe	33
b) Privatpersonen	34
3. Kapitel: Zweck und Geltungsbereich des DSG	35
A. Einstieg	36
B. Einführungsfall	37
C. Zweck	37
D. Persönlicher Geltungsbereich	38
E. Sachlicher Geltungsbereich	39
I. Daten natürlicher Personen	39
II. Ausnahmen und Abgrenzungen	40
1. Ausnahmen vom Geltungsbereich des DSG	40

2. Abgrenzungen	40
a) Verfahrensrecht	40
aa) Begriff der Gerichtsverfahren und der bundesrechtlichen Verfahren	41
bb) Anknüpfungspunkt	41
b) Öffentliche Register des Privatrechtsverkehrs	43
c) Abgrenzung Persönlichkeitsschutz nach DSGVO und StGB	43
F. Räumlicher Geltungsbereich (Kollisionsrecht)	44
4. Kapitel: Begriffe	47
A. Einstieg	48
B. Einführungsfall	49
C. Überblick – Begriffe von Art. 5 DSGVO	51
D. Personendaten (lit. a)	52
I. Definition	52
II. «Anonymisierte Daten»	53
III. «Pseudonymisierte Daten»	54
E. Betroffene Person (lit. b)	55
F. Besonders schützenswerte Personendaten (lit. c)	55
I. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten (Ziff. 1) ..	56
II. Daten über die Gesundheit (Ziff. 2)	57
III. Daten über die Intimsphäre (Ziff. 2)	57
IV. Zugehörigkeit zu einer Rasse oder Ethnie (Ziff. 2)	57
V. Genetische Daten (Ziff. 3)	58
VI. Biometrische Daten (Ziff. 4)	58
VII. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Ziff. 5)	59
VIII. Daten über Massnahmen der sozialen Hilfe (Ziff. 6)	59
G. Bearbeiten (lit. d)	60
H. Bekanntgeben (lit. e)	62
I. Profiling (lit. f)	63
I. Begriff	63

II. Risikobasierter Ansatz: Profiling mit hohem Risiko (lit. g)	64
J. Verletzung der Datensicherheit (lit. h)	65
K. Bundesorgan (lit. i)	66
I. Begriff	66
II. Anknüpfungspunkt «öffentliche Aufgabe des Bundes»	67
L. Verantwortlicher (lit. j)	70
M. Auftragsbearbeiter (lit. k)	72
I. Definition	72
II. Abgrenzung zum Verantwortlichen	74
III. Nicht jeder Dienstleister ist ein Auftragsbearbeiter	75
IV. Auftragsdatenbearbeitungsvertrag (ADV)	76
5. Kapitel: Bearbeitungsgrundsätze	79
A. Einstieg	80
B. Einführungsfall	81
C. Generelles	82
D. Die Bearbeitungsgrundsätze im Einzelnen	84
I. Grundsatz der Rechtmässigkeit	84
II. Grundsatz von Treu und Glauben	86
III. Grundsatz der Verhältnismässigkeit	87
1. Geeignete, notwendige und zumutbare Datenbearbeitung	87
2. Praktische Umsetzung	90
IV. Grundsatz der Zweckbindung	91
1. Datenbeschaffung für einen bestimmten Zweck	91
2. Vernichtung und Anonymisierung bei Wegfall des Zwecks	95
V. Datenrichtigkeit	96
6. Kapitel: <i>privacy by design</i> und <i>privacy by default</i>	99
A. Einstieg	100
B. Einführungsfall	100
C. Hintergrund	102

D. Normzweck und allgemeine Aspekte	103
I. Persönlicher Geltungsbereich	104
II. Sachlicher Geltungsbereich	105
E. Datenschutz durch Technik (<i>privacy by design</i>)	106
I. Zielsetzung	106
II. Mittel: Technologie und Organisation im Dienst des Datenschutzes	106
1. Technische und organisatorische Massnahmen	107
a) Technische Massnahmen	108
b) Organisatorische Massnahmen	108
2. Beurteilungskriterien	109
F. Datenschutz durch datenschutzfreundliche Voreinstellungen (<i>privacy by default</i>)	111
I. Zielsetzung	111
II. Mittel: Geeignete Voreinstellungen	111
7. Kapitel: Datensicherheit	113
A. Einführung	114
B. Einführungsfall	114
C. Vorbemerkungen	115
D. Begriff der Datensicherheit	116
I. Keine Definition im Gesetz	116
II. Nuancierung des Begriffs der Datensicherheit in der DSV	116
III. Internationale Standards und <i>best practices</i>	117
E. Persönlicher Geltungsbereich von Art. 8 DSGVO	119
F. Schutzziele	120
I. Vertraulichkeit	120
II. Verfügbarkeit	120
III. Integrität	121
IV. Nachvollziehbarkeit	121
G. Vorgehen zur Festlegung der geeigneten technischen und organisatorischen Massnahmen	121
I. Methodik	121
1. Erster Schritt: Beurteilung des Schutzbedarfs	123

a. Art der bearbeiteten Daten	123
b. Zweck, Art, Umfang und Umstände der Datenbearbeitung	123
2. Zweiter Schritt: Beurteilung des Risikos	124
a. Risikoursachen	124
b. Die hauptsächlichen Gefahren	124
c. Getroffene oder geplante Massnahmen zur Risikominimierung	125
d. Wahrscheinlichkeit und Auswirkungen einer Verletzung der Datensicherheit trotz getroffener Massnahmen	128
3. Dritter Schritt: Wahl der technischen und organisatorischen Massnahmen	129
II. Dynamischer Prozess	130
8. Kapitel: Verhaltenskodizes	133
A. Einstieg	134
B. Einführungsfall	134
C. Verhaltenskodizes	135
I. Zweck von Verhaltenskodizes	135
II. Normadressaten	136
III. Inhalt von Verhaltenskodizes	136
IV. Freiwilligkeit von Verhaltenskodizes	137
V. Stellungnahme des EDÖB zu Verhaltenskodizes	137
9. Kapitel: Zertifizierungen	139
A. Einstieg	140
B. Einführungsfall	140
C. Zertifizierungen	141
I. Vorbemerkungen	141
II. Normadressaten	141
III. Was kann zertifiziert werden?	142
IV. Massstäbe für die Zertifizierung	142

V. Wer zertifiziert?	143
VI. Verfahren und Aufsicht des EDÖB	143
10. Kapitel: Datenbearbeitung durch Private	145
A. Einstieg	146
B. Einführungsfall	147
C. Verantwortlichkeit im Unternehmen	148
D. Widerrechtliche Persönlichkeitsverletzungen durch bestimmte Datenbearbeitungen	150
I. Persönlichkeitsverletzungen	150
II. Rechtfertigungsgründe	151
1. Einwilligung	152
2. Überwiegendes öffentliches oder privates Interesse	154
3. Gesetzliche Grundlage	157
E. Klagen zum Schutz der Persönlichkeit	157
F. Datenbearbeitung durch private Verantwortliche mit Sitz oder Wohnsitz im Ausland	158
I. Vertretung (Art. 14 DSGVO)	158
II. Pflichten der Vertretung (Art. 15 DSGVO)	159
11. Kapitel: Datenbearbeitung durch öffentliche Organe	161
A. Einstieg	162
B. Einführungsfall	163
C. Vorab: Mehrere Datenbearbeitende – eine Verantwortung ...	164
D. Rechtsgrundlagen	165
I. Verankerung des verfassungsmässigen Legalitäts- prinzips	165
II. Rechtsgrundlage für das Bearbeiten «gewöhnlicher» Personendaten	166
III. Rechtsgrundlage für das Bearbeiten besonders schützenswerter Personendaten	166
IV. Ausnahme: Regelungskompetenz des Bundesrats	168
V. Ausnahme: Bearbeiten ohne materiell- oder formell-gesetzliche Grundlage	168

E. Pilotversuche	169
I. Rechtsstaatliche Notwendigkeit einer Pilotversuchs- Regelung	169
II. Kumulative Voraussetzungen für einen Pilotversuch	170
1. Vorab: Nur Pilotversuche mit besonders schützens- werten Personendaten?	171
2. Aufgabennorm in einem Gesetz im formellen Sinne	171
3. Massnahmen zur Begrenzung von Persönlichkeits- verletzungen auf ein Mindestmass	172
4. Unentbehrlichkeit der Testphase	172
III. Modalitäten vor und während der Testphase	173
1. Regelung des Pilotprojekts in einer Verordnung	173
2. Bewilligung durch den Bundesrat, Einbezug des EDÖB	174
3. Keine unendliche Geschichte: Evaluation und Befristung der Pilotphase	175
F. Bearbeiten für nichtpersonenbezogene Zwecke	176
I. Erfordernis einer Regelung	176
II. Der «nichtpersonenbezogene» Zweck	177
III. Bearbeitungsvoraussetzungen	178
G. Privatrechtliche Tätigkeit eines Bundesorgans	179
12. Kapitel: Datenbekanntgabe	181
A. Einstieg	182
B. Einführungsfall	183
C. Bekanntgabe von Daten im Generellen	185
D. Durch öffentliche Organe	185
I. Grundsatz des Legalitätsprinzips	185
II. Ausnahmen: Bekanntgabe ohne gesetzliche Grundlage	186
1. Unentbehrlichkeit für die Erfüllung einer gesetzlichen Aufgabe	187
2. Einwilligung der betroffenen Person	187
3. Dringender Schutz von Leib und Leben	188
4. Veröffentlichung der Personendaten durch die betroffene Person	188

5. Bekanntgabe zur Durchsetzung von Rechtsansprüchen der Empfängerin bzw. des Empfängers	188
III. «Personalien-Bekanntgabe»	189
IV. Bekanntgabe mittels Informations- und Kommunikationsdiensten	190
V. Einschränkungsgünde	190
VI. Widerspruchsrecht	191
VII. Spezialfall «Bekanntgabe» nach Öffentlichkeitsprinzip (BGÖ)	192
E. Datenbekanntgabe ins Ausland	193
I. Was ist ein Datentransfer ins Ausland?	193
II. Was ist kein Datentransfer ins Ausland?	194
III. Grundsätze (Art. 16 DSGVO)	195
1. Länder mit angemessenem Datenschutzniveau	195
2. Länder ohne angemessenes Datenschutzniveau	197
a) Standardvertragsklauseln (SCC) im Spezifischen	198
b) Weitere Garantien	201
IV. Ausnahmen (Art. 17 DSGVO)	203
13. Kapitel: Bearbeiten durch Auftragsbearbeiter	205
A. Einstieg	206
B. Einführungsfall	207
C. Bearbeiten durch Auftragsbearbeiter	208
I. Outsourcing von Aufgaben	208
II. Zur Erinnerung: Auftragsbearbeiter, Verantwortung und Bekanntgabeprivileg	208
III. Voraussetzungen einer Auftragsbearbeitung	210
1. Auftragsbearbeitung gestützt auf eine gesetzliche Grundlage oder einen Vertrag	210
2. Cura in eligendo, in instruendo et in custodiendo	210
3. Kein Verbot der Auftragsbearbeitung	212
IV. Unterauftragsbearbeitung	213
V. Auslagerung ins Ausland	213

14. Kapitel: (Governance-)Pflichten des Verantwortlichen und des Auftragsbearbeiters	215
A. Einstieg	216
B. Einführungsfall	217
C. Informationspflicht (inkl. Ausnahmen)	218
I. Informationspflicht bei der Beschaffung von Personendaten (Art. 19 DSGVO)	218
1. Allgemeines	218
2. Zweck der Informationspflichten	219
3. Mindestinformationen	219
4. Zeitpunkt der Information	221
5. Formvorschriften	221
6. Datenschutzerklärungen	221
II. Ausnahmen von der Informationspflicht und Einschränkungen (Art. 20 DSGVO)	224
III. Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 21 DSGVO)	225
1. Wann liegt eine automatisierte Einzelentscheidung vor?	226
2. Möglichkeit zur Stellungnahme durch die betroffene Person	227
3. Überprüfung durch eine natürliche Person	227
4. Ausnahmen	228
5. Automatisierte Einzelentscheidungen durch Bundesorgane	228
D. Governance-Pflichten	229
I. Allgemeines	229
II. Bearbeitungsverzeichnis	229
1. Pflicht zur Führung eines Bearbeitungsverzeichnisses	229
2. Inhalt des Bearbeitungsverzeichnisses	230
3. Formvorgaben	231
4. Ausnahmen von der Pflicht zur Führung eines Bearbeitungsverzeichnisses	231
5. Folgen bei unterlassener Erstellung eines Bearbeitungsverzeichnisses	233

III.	Weitere Dokumentationspflichten	233
1.	Protokollierungspflicht	233
a)	Vorab: Datensicherheit oder <i>privacy by design</i> ? ..	233
b)	Verpflichtete	234
c)	Umfang der Protokollierungspflicht	234
d)	Aufbewahrung und Zugänglichkeit der Protokolle	235
2.	Das Bearbeitungsreglement	235
a)	Verpflichtete	235
b)	Inhalt und Form	236
3.	Interne Datenschutzrichtlinie	236
IV.	Datenschutz-Folgenabschätzung	237
1.	Vorgehen und Inhalt	238
2.	Form und Aufbewahrungsdauer	239
3.	Ausnahmen	239
4.	Folgen bei Vorliegen eines hohen Risikos	239
E.	Meldung von Verletzungen der Datensicherheit	240
I.	Normzweck	240
II.	Normadressat	240
III.	Definition «Verletzung der Datensicherheit»	240
IV.	Meldepflicht	241
1.	Gegenüber dem EDÖB	241
2.	Gegenüber der betroffenen Person	242
a)	Grundsatz	242
b)	Einschränkungen der Meldepflicht gegenüber der betroffenen Person	242
3.	Inhalt der Meldepflicht	243
4.	Dokumentation	243
5.	Exkurs: Meldepflicht vs. Selbstanzeige und Rechte des Angeschuldigten	244
F.	Ausblick: Meldung von Cyberangriffen auf kritische Infrastrukturen	244
I.	Verpflichtete Bereiche	245
II.	Zu meldende Angriffe	247
III.	Inhalt der Meldung	247

IV. Meldefrist	247
V. Einordnung der vorgeschlagenen Regelungen aus Datenschutzsicht	248
15. Kapitel: Rechte der Betroffenen	249
A. Einstieg	250
B. Einführungsfall	251
C. Betroffenenrechte im Allgemeinen	252
D. Das Recht auf Auskunft	253
I. Auskunftsrecht als zentrales Instrument der informationellen Selbstbestimmung	253
II. Zuständigkeit	254
III. Umfang des Auskunftsrechts	254
IV. Modalitäten, Kosten und Fristen	255
1. Modalitäten	255
2. Kosten	256
3. Fristen	256
V. Einschränkungen des Auskunftsrechts	257
1. Einschränkung im Gesetz im formellen Sinn und bei überwiegenden Interessen	257
2. Einschränkung bei rechtsmissbräuchlichen Gesuchen	257
3. Einschränkungsgründe für private Verantwortliche	258
4. Einschränkungsgründe für Bundesorgane	258
5. Folgen bei der Missachtung des Auskunftsrechts	259
6. Medienprivileg	259
VI. Exkurs: Abgrenzung zum Akteneinsichtsrecht	259
E. Das Recht auf Datenherausgabe und -übertragung	260
I. Zweck	260
II. Voraussetzungen	260
III. Umfang	261
IV. Gängiges elektronisches Format	261
V. Kosten	262
VI. Löschung nach der Übertragung	263

VII. Einschränkungen des Rechts auf Datenportabilität	263
VIII. Folgen bei der Missachtung des Rechts auf Datenportabilität	263
F. Berichtigungs- und Widerspruchsrecht gegenüber Privaten	264
G. Ansprüche gegen Bundesorgane: Unterlassung, Beseitigung, Feststellung der Widerrechtlichkeit	265
16. Kapitel: Beratungs- und Aufsichtsorgane	269
A. Einstieg	270
B. Einführungsfall	270
C. Datenschutzberater/innen	271
I. Sinn und Zweck dieser Funktion	271
II. Datenschutzberater/innen in Unternehmen (Art. 10 DSGVO, Art. 23 DSV)	272
III. Datenschutzberater/innen in Bundesorganen (Art. 10 DSGVO, Art. 25 ff. DSV)	274
D. Eidgenössischer Datenschutz- und Öffentlichkeits- beauftragter	276
I. EDÖB – Amt oder Person?	276
II. Organisation	277
1. Organisatorische, fachliche und finanzielle Unabhängigkeit	277
2. Persönliche Voraussetzungen	277
3. Amtsdauer	278
III. Aufgaben und Befugnisse	279
1. Beratungs- und Sensibilisierungstätigkeit	279
2. Anhörung zu Erlassen und Massnahmen des Bundes	279
3. Erarbeitung von Empfehlungen zu <i>best practices</i>	280
4. Register der Bearbeitungstätigkeiten	281
5. Funktionen nach BGÖ	281
6. Untersuchung von Verstössen gegen Datenschutz- vorschriften	281
7. Amtshilfe	284

8. Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC; Art. 41 DSV)	286
9. Auch beim EDÖB können Personendaten bearbeitet werden	286
17. Kapitel: Sanktionen	287
A. Einstieg	288
B. Einführungsfall	289
C. Vorbemerkungen	289
I. Verpasste Chance?	289
II. Gemeinsamkeiten aller Tatbestände	290
III. Anwendbarkeit der allgemeinen Bestimmungen des StGB	291
IV. Zuständigkeit	291
D. Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten	291
E. Verletzung von Sorgfaltspflichten	292
F. Verletzung der beruflichen Schweigepflicht	294
G. Missachtung einer Verfügung	295
18. Kapitel: Praxis<i>Inside</i>	297
A. Einstieg	298
B. Digitale Transformation, das Phänomen der Stunde	301
I. Worum geht es?	301
II. Achtung Stolperfallen!	302
1. Digitalisierungsprojekte sind nicht nur «Projekte der IT-Abteilung»	302
2. Digitalisierung von Prozessen: Keine 1:1-Übernahme aus der analogen Welt	304
3. Digitalisierungsprojekte bringen auch rechtliche Fragestellungen mit sich	305
C. Staatliche digitale Souveränität	305
I. Digitale Souveränität – worum geht es?	305

II.	Überlegungen im Verwaltungsalltag – gerade beim Gang in die Cloud	306
III.	Staatliche digitale Souveränität, ein Auslaufmodell?	307
D.	Wenn der Staat in die Cloud will – rechtliche Überlegungen	309
E.	Datenschutzmanagementsystem	313
I.	Um was geht es?	313
II.	Warum ein Datenschutzmanagementsystem?	313
III.	Inhaltliche Anforderungen an ein Datenschutzmanagementsystem	314
IV.	Weitere Anforderungen	316
F.	Online Collaboration – alles kein Problem?	317
I.	Worum geht es?	317
II.	Rechtliche Fragestellungen	317
III.	Risikobasierte Überlegungen bei der Wahl eines Online Collaboration Tools	319
G.	Online-Plattformen und Social Media	321
I.	Aktualität	321
II.	Was ist eine Online-Plattform?	322
III.	Datenschutzrechtliche Aspekte	323
1.	Allgemeine datenschutzrechtliche Vorgaben	323
2.	Die Frage der Verantwortlichkeit	324
a)	Grundsatzproblematik	324
b)	Verantwortlichkeiten bei Bewertungsplattformen	324
3.	Die Big-Data-Frage	325
4.	Das Social-Media-Paradox	325
H.	Cookies	326
I.	Herausforderung: Die Krümelspur im Internet	326
II.	Rechtliche Regelungen	328
1.	In der Schweiz	328
2.	In der EU	328
III.	Tipps zum Einsatz von Cookies	329
I.	Governance in Blockchain und DLT	330
I.	Kleine Blockchain-Kunde	330
1.	Was ist eine Blockchain?	330

2.	Drei Kerneigenschaften der Blockchain	331
3.	Wie funktioniert eine Blockchain?	331
4.	Ausgestaltungsformen	332
II.	Datenschutzrechtliche Aspekte	332
1.	Einwilligung?	332
2.	Notwendigkeit der «Veröffentlichung»?	332
3.	Wahrung der Betroffenenrechte	333
4.	Die Frage der Verantwortung und des anwendbaren Rechts	333
5.	Governance der Blockchain	334
III.	Blockchain: Eine datenschutzrechtliche <i>Mission impossible?</i>	335
J.	Internet of Things (IoT)	336
I.	Um was geht es?	336
II.	Regulierung von IoT	339
III.	Governance von IoT	339
IV.	Datenschutzrechtliche Herausforderungen	339
1.	Grundsätzliches	339
2.	Daten- und Informationssicherheit	340
K.	Metaverse	341
I.	Was ist das Metaverse?	341
1.	Annäherung	341
2.	Versuch einer Definition	341
3.	Wie gelangt man «ins Metaverse»?	342
II.	Arten von Metaverse-Plattformen	342
III.	Wirtschaftsraum Metaverse	344
IV.	Metaverse – ein Hype oder eine längerfristige Revolution?	344
V.	Rechtliche Aspekte des Metaverse	345
1.	Grundsätzliches	345
2.	Das anwendbare Recht	345
3.	Die Verantwortlichkeiten	346
4.	Sicherheit im Metaverse	346
5.	Datenschutz im Metaverse	347

L. Self-Sovereign Identity	347
I. Um was geht es?	347
II. Was ist eine Self-Sovereign Identity?	348
III. Wie funktioniert eine Self-Sovereign Identity?	350
IV. Datenschutzrechtliche Aspekte	351
M. Immersive Reality, VR, AR und MR	353
I. Um was geht es?	353
II. Varianten der virtuellen Realitäten (VR, AR, MR)	353
III. Einsatzmöglichkeiten	355
1. Allgemein	355
2. Einsatzmöglichkeit «Digital Twin»	356
IV. Rechtliche Fragestellungen	356
1. Allgemeines	356
2. Datenschutzrechtliche Aspekte	357
a) Rechtmässigkeit der Datenbearbeitung?	358
b) Aufbewahrungsort und -dauer, Zugriffsberechtigungen	358
c) Datensicherheit	358
d) Datenschutzrechtlicher Handlungsbedarf?	359
Sachregister	361