

Handbücher für die Anwaltspraxis

Datenschutzrecht

Beraten in Privatwirtschaft
und öffentlicher Verwaltung

herausgegeben von

Nicolas Passadelis

Rechtsanwalt in Zürich

David Rosenthal

**Konsulent, Lehrbeauftragter an der
Universität Basel und an der ETH Zürich**

Hanspeter Thür

**Eidg. Datenschutz- und
Öffentlichkeitsbeauftragter (EDÖB)**

Helbing Lichtenhahn Verlag

Inhaltsübersicht

Erster Teil: Grundlagen

§ 1	Geschichte und Zukunft des Datenschutzrechts	3
	Rainer J. Schweizer	
§ 2	Grund- und menschenrechtlicher Datenschutz	41
	Rainer J. Schweizer/David Rechsteiner	
§ 3	Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden	73
	Stefan Gerschwiler/Astrid Epiney/Daniela Nüesch/Hussein Noureddine/ Claudia Leonie Wasmer	
§ 4	Informations- und Meldepflichten bei der Bearbeitung von Personendaten	121
	Michael Widmer	
§ 5	Rechte der Datenschutzsubjekte	149
	Michael Widmer	
§ 6	Rechtsanwendung bei internationaler Datenbearbeitung durch Private	167
	Nicolas Passadelis	
§ 7	Sanktionierung von Datenschutzverstößen	203
	David Rosenthal	
§ 8	Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten	245
	Yvonne Jöhri	

Zweiter Teil: Datenschutzrechtliche Herausforderungen in einzelnen Branchen

§ 9	Datenschutz in der Telekommunikationsbranche	281
	Nicole Beranek Zanon/Carmen De la Cruz Böhringer	
§10	Datenschutz im Gesundheitswesen	323
	Ursula Uttinger	

§ 11	Datenschutz im Finanzwesen	355
	Werner W. Wyss	
§ 12	Datenschutz in der Privatversicherung	407
	Niggi Zittel	
§ 13	Datenschutz im Sozialversicherungswesen	431
	Yvonne Prieur	
§ 14	Datenschutz im Medienbereich	487
	Peter Studer	
§ 15	Datenschutz bei Geodäten	513
	Meinrad Huser	
§ 16	Datenschutz im Handel mit Bonitätsdaten	557
	Christoph Hofer	
Dritter Teil: Datenschutz im privatwirtschaftlichen Unternehmen		
§ 17	Datenschutz im Personalwesen	577
	Roberta Papa/Thomas Pietruszak	
§ 18	Datenschutz in Compliance und Rechtsverfahren	613
	Mark Livschitz	
§ 19	Marketing und Internet – datenschutzrechtliche Aspekte	681
	Lukas Bühlmann/Michael Schüepp	
§ 20	Datenschutz und Outsourcing	759
	Ralph Gramigna	
§ 21	Organisatorische und technische Datenschutzmassnahmen	787
	Matthias Bossardt	
§ 22	Organisation und Aufgaben des betrieblichen Datenschutzbeauftragten	819
	Maria Winkler	
§ 23	Datenschutz-Zertifizierung	843
	Caroline Gloor Scheidegger	

§ 24 Datenschutz bei Veräußerung und Zusammenschluss von Unternehmen	869
Dieter Gericke/Christof Burri	

Vierter Teil: Datenschutz in der öffentlichen Verwaltung

§ 25 Öffentlichkeitsgesetz und Datenschutz	
Reto Ammann/Renate Lang	
§ 26 Datenschutz im Ausländer- und Asylbereich	943
Hanspeter Thür	
§ 27 Datenschutz im Sozialbereich	973
Peter Mösch Payot	
§ 28 eGovernment und Datenschutz	987
Christian Laux	
§ 29 Datenschutz in Justiz und Polizei	1053
Franz Riklin	
§ 30 Datenschutz in Statistik und Forschung	1079
Karin Koç;	

Fünfter Teil: Datenschutz im Ausland

§ 31 Entwicklungen im internationalen Datenschutzrecht	1101
Tobias Fasnacht	
§ 32 Datenschutzrecht der Europäischen Union	1123
Jürgen Härtung	
§ 33 Datenschutzrecht in den USA	1157
Lothar Determann	
§ 34 Datenschutzrecht in Drittstaaten	1175
Yvonne Schleiss/Ivan Dunjic	

Sachregister	1195
---------------------	------

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Autorenverzeichnis	XXXIII
Abkürzungsverzeichnis	XXXV
Materialienverzeichnis	LV
Erster Teil: Grundlagen	i
§ 1 Geschichte und Zukunft des Datenschutzrechts	3
I. Zur Entwicklung des Datenschutzrechts in der Schweiz	6
1. Einleitung	6
2. Vorbemerkung: Bisherige Darstellungen	7
3. Die Frühzeit des Datenschutzrechts im Ausland und in der Schweiz	8
4. Datenschutz in Europa und Auswirkungen auf die Schweiz	9
5. Die föderalistische Ordnung des Datenschutzrechts	13
6. Das Bundesgesetz über den Datenschutz von 1992 und seine Fortentwicklung	15
7. Kantonale Datenschutzgesetzgebung	19
8. Legislatorisches Konzept	20
9. Der Beitrag der Gerichte, insbesondere des Bundesgerichts, der Eidgenössischen Datenschutzkommission und des Bundesverwaltungsgerichts	25
10. Die Bedeutung der Praxis der eidgenössischen und der kantonalen Kontrollbehörden	26
11. Der Beitrag der Lehre	26
II. Was hat sich verändert? Was hat sich bewährt? Wo erscheint das Datenschutzrecht heute als ungenügend?	27
III. Die heutigen Bedrohungen und der von diesen bewirkte Verlust an Vertrauen in die Freiheit der Kommunikation und die Garantien des Datenschutzrechts	31
IV. Reformvorschläge in Europa und in der Schweiz	35
V. Eigene Vorschläge	36
1. Grundrecht auf Datenschutz ausbauen!	36
2. Stärkung der individuellen Autonomie gegenüber den datenbearbeitenden Personen, Unternehmen und öffentlichen ~ Stellen	37
3. Die Abwehrrechte und die Prozessrechte der betroffenen Personen müssen massiv verbessert werden	38

4.	Stärkung der Grundsätze der fairen Datenbearbeitung	39
5.	Stärkung der öffentlichen Aufsicht über die privaten Datenbearbeiter	39
6.	Technikbezogene und bereichsspezifische Vorschriften ausbauen, aber unter Wahrung des Vorrangs der allgemeinen Gesetze und der allgemeinen Rechte der betroffenen Personen	40
§2 Grund- und menschenrechtlicher Datenschutz		4i
I.	Einleitung	43
II.	Der grundrechtliche Datenschutz	43
1.	Die Tragweite des Grundrechtsschutzes	43
2.	Besonderer datenschutzrechtlicher Grundrechtsschutz	45
3.	Persönlicher Schutzbereich	45
4.	Sachlicher Schutzbereich	45
5.	Einschränkungen	47
6.	Horizontalwirkung und Schutzpflichten	52
7.	Einwilligung und Grundrechtsverzicht	55
III.	Der menschenrechtliche Datenschutz	56
1.	Allgemeine Erklärung der Menschenrechte	56
2.	UN-Pakt II	56
3.	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK)	58
4.	Europäische Grundrechtecharta	65
5.	Datenschutzkonvention des Europarates von 1981 und Zusatzprotokoll von 2001	68
IV.	Ausblick	68
V.	Checkliste	71
§3 Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden		73
I.	Inhaltsübersicht	74
II.	Verankerung in der Rechtsordnung	74
1.	Völkerrecht	74
2.	Bundesverfassung	76
3.	Einfaches Bundesrecht	77
4.	Kantonales Recht	79
III.	Begriffliches	81
1.	Bearbeiten von Personendaten	81
2.	Besonders schützenswerte Personendaten und Persönlichkeitsprofile	84

3.	Bekanntgabe an Dritte, Auftragsdatenbearbeitung	87
4.	Datensammlungen und deren Inhaber	87
IV.	Allgemeine Grundsätze der Datenbearbeitung	88
1.	Grundlagen	88
2.	Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 DSGVO)	89
3.	Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSGVO)	90
4.	Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSGVO)	91
5.	Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSGVO)	93
6.	Grundsatz der Transparenz (Art. 4 Abs. 4 DSGVO)	95
7.	Grundsatz der Datenrichtigkeit und Datensicherheit (Art. 5 und 7 DSGVO)	96
V.	Besondere Bestimmungen der Datenbearbeitung durch Privatpersonen	98
1.	Erleichterter Nachweis einer persönlichkeitsverletzenden Datenbearbeitung	99
2.	Der Umgang mit öffentlich zugänglichen Personendaten	102
3.	Rechtfertigungsgründe	104
4.	Prüfschema	107
VI.	Datenbearbeitung durch Bundesorgane	108
1.	Art. 16 DSGVO: Grundlage	108
2.	Legalitätsprinzip	110
3.	Beschaffen von Personendaten	113
4.	Informationspflicht beim Beschaffen von Personendaten	114
5.	Bekanntgabe von Personendaten	116
§4	Informations- und Meldepflichten bei der Bearbeitung von Personendaten	121
I.	Vorbemerkung	121
II.	Informationspflichten bei der Beschaffung von Daten	122
1.	Vorbemerkung	122
2.	Bei Beschaffung durch private Personen	123
3.	Bei Beschaffung durch Bundesorgane	127
III.	Informationspflicht bei grenzüberschreitender Bekanntgabe	131
1.	Grundlagen	131
2.	Zweck und Voraussetzungen	131
3.	Verpflichtete	132
4.	Zeitpunkt und Aktualisierung der Information	132
5.	Inhalt	133
6.	Modalitäten/Form	134
7.	Folgen bei Unterlassen der Information	134
IV.	Meldepflicht betreffend Datensammlungen	134
1.	Grundlagen und Zweck	134

2.	Führung und Inhalt des Registers	135
3.	Öffentlichkeit des Registers und Registerauskünfte	135
4.	Geografischer und sachlicher Anwendungsbereich	135
5.	Meldepflicht privater Personen	136
6.	Meldepflicht der Bundesorgane	139
7.	Ausnahmen	140
8.	Meldung betreffend Datenschutzverantwortlichen oder Datenschutz-Qualitätszeichen	144
9.	Fristansetzung und Abklärungen durch den EDÖB	145
10.	Folgen bei Unterlassen der Anmeldung	145
V.	Checklisten	146
1.	Informations- und Meldepflichten privater Personen	146
2.	Informations- und Meldepflichten von Bundesorganen	147
§5	Rechte der Datenschutzsubjekte	149
I.	Einleitung	149
II.	Auskunftsrecht	150
1.	Funktionen	150
2.	Voraussetzungen	150
3.	Berechtigte	151
4.	Verpflichtete	152
5.	Modalitäten und Form	152
6.	Inhalt der Auskunft	156
7.	Gesundheitsdaten	158
8.	Verzicht auf das Auskunftsrecht	158
9.	Einschränkung des Auskunftsrechts (Art. 9 und 10 DSGVO)	159
10.	Verletzung des Auskunftsrechts	161
III.	Weitere Rechte und Ansprüche	161
1.	Bearbeitung durch Private	161
2.	Bearbeitung durch Bundesorgane	163
§6	Rechtsanwendung bei internationaler Datenbearbeitung durch Private	167
I.	Einleitung	167
II.	Feststellung des anwendbaren Rechts	170
1.	Internationaler Bezug der Datenbearbeitung	170
2.	Räumlicher Anwendungsbereich im Datenschutzrecht	170
III.	Rechtsanwendung bei internationaler Datenbearbeitung durch Private	176
1.	Datenbearbeitung in der Schweiz	176
2.	Grenzüberschreitende Datenbekanntgabe aus der Schweiz	182
3.	Datenbearbeitung im Ausland	195

4.	Grenzüberschreitende Datenbekanntgabe in die Schweiz	198
5.	Grenzüberschreitende Datenbekanntgabe durch die Schweiz (Datentransit)	199
IV.	Schlussbetrachtungen	200
V.	Checkliste	201
§ 7	Sanktionierung von Datenschutzverstößen	203
I.	Einleitung	203
II.	Überblick	204
III.	Möglichkeiten der Sanktionierung	205
1.	Zivilrechtlicher Rechtsschutz	205
2.	Vertragsrechtliche Sanktionierung	212
3.	Strafrechtliche Sanktionierung	217
4.	Verwaltungsrechtliche Sanktionierung	225
5.	Andere Formen der Sanktionierung	232
6.	Konkurrenzen	236
IV.	Sanktionierung nach ausländischem Recht?	236
V.	Schlussfolgerungen und Ausblick	237
VI.	Checkliste zur Abklärung möglicher Sanktionen als Folge von Datenschutzverstößen durch private Datenbearbeiter	240
§ 8	Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten	245
I.	Öffentliche Datenschutzbeauftragte	246
1.	Institution der Datenschutzgesetze	247
2.	Zuständigkeit der Aufsichtsstelle	252
II.	Aufgaben der öffentlichen Datenschutzbeauftragten	255
1.	Aufsicht (Überwachung und Kontrolle)	255
2.	Beratung	263
3.	Information und Berichterstattung	266
4.	Stellungnahmen	268
5.	Zusammenarbeit mit in- und ausländischen Datenschutzbehörden	268
6.	Registerführung über Datensammlungen	269
7.	Weitere Aufgaben	270
III.	Bedeutung der öffentlichen Datenschutzbeauftragten	273
1.	Wirksamer Datenschutz ...	273
2.	... im Rahmen der Möglichkeiten	274
3.	Quo vadis?	276

Zweiter Teil: Datenschutzrechtliche Herausforderungen in einzelnen Branchen	279
§9 Datenschutz in der Telekommunikationsbranche	28i
I. Ausgangslage	282
II. Telekommunikationsbranche	282
1. Anbieterinnen von Fernmeldediensten	282
2. Andere Anbieterinnen von Dienstleistungen im Telekommunikationsumfeld	284
III. Rechtsgrundlagen	285
1. Relevanz der Qualifikation als Fernmeldedienstanbieterin	285
2. Verfassungsrechtliche Grundlagen	286
3. Gesetzliche Grundlagen	290
IV. Datenschutzrechtliche Aspekte in der Telekommunikationsbranche	295
1. Persönlicher Anwendungsbereich des DSGVO	295
2. Sachlicher Anwendungsbereich im Allgemeinen	296
3. Datensicherheit	306
V. Fernmelderechtliche Datenschutzbestimmungen	308
1. Grundlagen im FMG	308
2. Spezifische fernmelderechtliche Datenschutzverpflichtungen	309
VI. Technologische Weiterentwicklungen und Trends	320
1. Im Allgemeinen	320
2. Schlüsselfunktion der Fernmeldedienstanbieterin	320
3. Integration neuer Dienste in die Wertschöpfungskette	321
4. Datenschutz in der Telekommunikationsbranche als dauernde Herausforderung	322
§10 Datenschutz im Gesundheitswesen	323
I. Einleitung	323
II. Patientenrechte und Behandlungsvertrag	324
1. Grundsätze Datenschutz	324
2. Datenweitergabe	326
3. Einsichtsrecht und Auskunftsrecht	328
4. Praxisadministration und Datenschutz	329
III. Amts- und Berufsgeheimnis	331
1. Problemstellung	331
2. Amtsgeheimnis	331
3. Berufsgeheimnis nach Art. 321 StGB	332
4. Berufsgeheimnis nach Art. 35 DSGVO	334

IV.	eHealth	334
	1. Versichertenkarte	334
	2. Elektronisches Patientendossier	336
V.	Datenschutz in der medizinischen Forschung	338
VI.	Genetische Untersuchung	341
	1. Allgemeines	341
	2. Genetische Untersuchungen im Arbeitsbereich	343
	3. Genetische Untersuchungen im Versicherungsbereich	344
	4. Klärung der Abstammung oder zur Identifikation	345
	5. Strafandrohung	346
	6. Personalisierte Medizin	346
VII.	Case Management	347
	1. Definition von Case Management	347
	2. Case Management im Gesundheitswesen	348
	3. Datenschutzrechtliche Angelpunkte im Case Management	350
VIII.	Muster für eine Einwilligungsklausel «Case Management»	354
§ 11 Datenschutz im Finanzwesen		355
I.	Einführung	356
II.	Implementierung der Fachstelle Datenschutzberatung	357
	1. Funktion der Fachstelle Datenschutzberatung	357
	2. Organisation der Fachstelle Datenschutzberatung	360
	3. Enge Einbindung in Unternehmensabläufe	362
	4. Unternehmensinterne Regelung der Fachstelle Datenschutzberatung	364
III.	Typische Verantwortlichkeiten der Fachstelle Datenschutzberatung	365
	1. Führen des Datensammlungsinventars	365
	2. Auskunftsbegehren nach Art. 8 DSGVO	367
	3. Einsatz in besonders sensiblen unternehmensinternen Verfahren	375
IV.	Weitere ausgewählte Herausforderungen in der Praxis	383
	1. Bekanntgabe von Daten an ausländische Behörden	383
	2. Auslagerung (Outsourcing)	390
	3. Bearbeitung von Daten in sog. Clouds	396
	4. Herausforderungen beim sog. Mobile Computing	398
	5. Bedeutung des Datenmanagements für einen wirksamen Datenschutz	400
V.	Checklisten	402
	1. Anforderungen an eine Fachstelle Datenschutzberatung	402
	2. Anforderungen an ein effizientes Datensammlungsinventar	403
	3. Anforderungen an effiziente Abläufe bei Auskunftersuchen	403
	4. Anforderungen an effiziente Whistleblowing-Verfahren	404

5. Unternehmensinterne Überwachungen und Untersuchungen	404
6. Bekanntgabe von Personendaten an ausländische Behörden	404
7. Anforderungen an eine Outsourcing-relevante Auslagerung	405
8. Anforderungen an die Bearbeitung von Daten in sog. Clouds	405
9. Anforderungen an Mobile Computing	406
10. Anforderungen an das Datenmanagement	406
§12 Datenschutz in der Privatversicherung	407
I. Allgemeines zum Datenschutz in der Privatversicherung	407
1. Bearbeitungszweck in der Privatversicherung	407
2. Anwendbarkeit des DSGVO in der Privatversicherung	407
II. Datenschutz beim Abschluss des Versicherungsvertrages	408
1. Datenschutzrechtliche Grundsätze beim Abschluss privatrechtlicher Versicherungsverträge	408
2. Einwilligungsklausel	409
3. Widerruf der Einwilligung	414
4. Anfragen beim Vorversicherer	416
5. Nicht zustande gekommener und beendeter Versicherungsvertrag	417
III. Datenschutz im Schadenfall	418
1. Begründung des Versicherungsanspruches	418
2. Interne Datenbekanntgabe	420
3. Interne Datenbekanntgabe im Schadenfall	423
4. Weitergabe von Schadendaten an andere Versicherer	425
5. Herausverlangen von Spital- und Operationsberichten	426
6. Observationen zur Bekämpfung von Versicherungsmissbrauch	427
§13 Datenschutz im Sozialversicherungswesen	431
I. Problemübersicht	431
II. Verfassungs- und Rechtsgrundsätze	432
III. Institutioneller und organisatorischer Datenschutz	434
1. Bundesrecht und kantonales Recht	434
2. Verschiedene Versicherungen unter einem Dach	435
IV. ATSG und spezifische Normen in Einzelgesetzen	436
1. Übersicht	436
2. Mitwirkungs- und Auskunftspflicht beim Vollzug	436
3. Meldung bei veränderten Verhältnissen	441
4. Amts- und Verwaltungshilfe	443
5. Schweigepflicht	446
6. Aktenführung	447
7. Akteneinsicht	449

V.	Bearbeitung von Personendaten	452
	1. Allgemeines	452
	2. Alters- und Hinterlassenenversicherung	454
	3. Invalidenversicherung	455
	4. Ergänzungsleistungen	455
	5. Berufliche Vorsorge	456
	6. Krankenversicherung	458
	7. Unfallversicherung	459
	8. Militärversicherung	460
	9. Erwerbsersatzordnung	460
	10. Familienzulagen	461
	11. Arbeitslosenversicherung	462
VI.	Mittel und Verfahren	463
	1. Die Datenbekanntgabe	463
	2. Einwilligung	472
	3. Abrufverfahren	473
	4. Interinstitutionelle Zusammenarbeit	475
	5. Versicherungsmissbrauch	477
VII.	Strafnormen bei Schweigepflichtverletzung	479
VIII.	Übersicht	480
	§ 14 Datenschutz im Medienbereich	487
I.	Medienschaffende zwischen Medienfreiheit, Schutz der Privatsphäre und Datenschutz	487
	1. Medienfreiheit (Art. 17 Abs. 1 BV)	487
	2. Schutz der Privatsphäre (Art. 13 BV)	488
	3. Grundrechtskonkurrenzen zwischen Medienfreiheit und Schutz der Privatsphäre	489
II.	Besondere Regelungsversuche gegenüber aktuellen medialen Gefährdungen der Privatsphäre	490
	1. Das Bundesgericht zu den Google-Diensten «Street View» und zum Recht am Bild (BGE 138 II 346)	490
	2. Das Amtsgericht Luzern-Land zum «Recht auf Vergessen» und zur Pflicht, Archivdaten nachzuführen	495
	3. Schranken der Internet-Fahndung	497
	4. Der «Shitstorm» als Versuchung der Medien	498
III.	Sonderbestimmungen für Medien im Datenschutzgesetz	502
IV.	Bundesgesetz über das Öffentlichkeitsprinzip und seine Auswirkungen auf die Medienpraxis	503
	1. Grundsätze, Zeit- und Kostenhürden	503

2.	<www.Öffentlichkeitsgesetz.ch>	504
3.	Einsichtsgesuche und Zugangsgesuche: Aus Urteilen des Bundesgerichts und des Bundesverwaltungsgerichts	506
V.	Die Folgen der «Snowden-Affäre» für die Medien	510
VI.	Suchmaschinenbetreiber und die Privatsphäre – ein Urteil des Europäischen Gerichtshofs vom 13. Mai 2014	511
§15 Datenschutz bei Geodäten		513
I.	Einleitung	514
II.	Die Datenschutzrelevanz von Geodäten	515
1.	Geodäten und Datenschutzgesetz	515
2.	Datenschutzrechtliche Sonderregelungen	524
3.	Geodäten und öffentliches Recht	527
4.	Folgerungen für das anwendbare Recht	530
III.	Bearbeiten von Geodäten	531
1.	Einleitung	531
2.	Widerrechtliche Persönlichkeitsverletzung (Art. 12 DSGVO)	532
3.	Rechtfertigungsgründe	537
IV.	Bearbeiten von Geobasisdaten	541
1.	Einleitung	541
2.	Bearbeiten nach dem Datenschutzrecht	542
3.	Bearbeiten nach dem Geoinformationsrecht	546
4.	Bearbeiten nach Grundbuchrecht im Speziellen	548
V.	Rechtsschutz	550
1.	Auskunftsrecht	550
2.	Sperrrecht	550
3.	Rechtsschutz bei Verletzung der Persönlichkeitsrechte durch Private	552
4.	Rechtsschutz bei Verletzung der Persönlichkeitsrechte durch Organe der öffentlichen Hand	553
VI.	Checkliste	555
§16 Datenschutz im Handel mit Bonitätsdaten		557
I.	Einführung	557
1.	Begriffe	557
2.	Wirtschaftliche Bedeutung	557
3.	Legitimation der Wirtschaftsauskunfteien	558
II.	Rechte der betroffenen Personen	559
1.	Auskunftsrecht	559
2.	Sperr- und Löschrecht	561

3.	Korrekturrecht	564
4.	Schadenersatz und Genugtuung für Persönlichkeitsverletzungen	566
III.	Grenzen der Bearbeitung von Wirtschaftsinformationen	567
1.	Rahmenbedingungen von Art. 13 Abs. 2 lit. c DSGVO	567
2.	Verhältnismässigkeit	568
IV.	Liste von Auskunfteien	573
Dritter Teil: Datenschutz im privatwirtschaftlichen Unternehmen		575
§ 17 Datenschutz im Personalwesen		577
I.	Rechtliche Grundlagen	578
1.	Art. 328b OR als lex specialis zum DSGVO	578
2.	Art. 328 Abs. 2 OR und Art. 26 ArGV 3	583
3.	Arbeitsvermittlungsgesetz	584
4.	Bundesgesetz über genetische Untersuchungen beim Menschen	585
5.	Internationale Verhältnisse	585
6.	Entwicklungen in der EU	587
II.	Beschaffung von Arbeitnehmerdaten	588
III.	Überwachung der Arbeitnehmer	591
1.	Grundsätzliche Schranken	591
2.	Einzelne Überwachungsmaßnahmen im Besonderen	594
IV.	Führung des Personaldossiers	598
1.	Begriff	598
2.	Bearbeitungsmodalitäten	599
3.	Auskunftsrecht	601
4.	Aufbewahrung und Vernichtung	603
5.	Auslagerung an Dritte (Outsourcing)	605
6.	Keine Registrierungspflicht	605
V.	Bekanntgabe von Arbeitnehmerdaten an Dritte	605
1.	Allgemeines	605
2.	Referenzen	606
3.	Bekanntgabe von Arbeitnehmerdaten an Versicherungen	607
4.	Anordnung von ärztlichen Untersuchungen	610
§ 18 Datenschutz in Compliance und Rechtsverfahren		613
I.	Datenschutz in Compliance	614
1.	Begriffsbestimmung und Elemente von Compliance	614
2.	Rechtliche Relevanz von Datenschutz bei Compliance-Aktivitäten	617
3.	Praktische Relevanz von Datenschutz bei Compliance-Aktivitäten	620
4.	Internationaler Anwendungsbereich schweizerischer Datenschutzbestimmungen im Zusammenhang mit Compliance	622

5. Datenbearbeitung bei präventiver Compliance	623
6. Datenbearbeitung bei reaktiver Compliance	626
7. Datenbearbeitung durch Beauftragte und Datenübertragung ins Ausland	649
8. Datenbearbeitung bei Whistleblowing	653
9. Rechte des Datensubjektes	656
10. Exkurs: Art. 271 und 273 StGB	661
II. Datenschutz in Rechtsverfahren	675
§ 19 Marketing und Internet – datenschutzrechtliche Aspekte	681
I. - Einleitung	685
II. Datenschutz im Internet und im Online-Marketing	686
1. Grundbegriffe und Datenspuren im Internet	686
2. Datenschutz beim Betrieb einer Website	696
3. Datenschutz im Online-Marketing	713
4. Datenschutz und soziale Netzwerke (am Beispiel von Facebook)	719
III. Datenschutz im E-Mail-Marketing	730
1. E-Mail-Adressen als Personendaten	731
2. Beschaffung der E-Mail-Adressen und Einwilligung in den Versand von Werbung	732
3. Inhaltliche Vorgaben für E-Mail-Werbung	738
4. Messung der Reaktionen auf Werbe-E-Mails	739
5. Checkliste	741
IV. Datenschutz im Offline-Marketing	742
1. Telefonmarketing	742
2. Postwerbesendungen («Briefkastenwerbung»)	747
3. Adresshandel	751
4. Checkliste	753
V. Datenschutz im Customer Relationship Management	755
1. Definitionen und Funktionsweise	755
2. Datenschutzrechtliche Beurteilung	755
3. Checkliste CRM	757
§ 20 Datenschutz und Outsourcing	759
I. Übersicht	760
1. Einleitung	760
2. Outsourcing und seine Erscheinungsformen	761
3. Begriff des Outsourcings	764
II. Datenschutzrechtlicher Rahmen des Outsourcings	766
1. Anwendbarkeit des Datenschutzgesetzes	766

2.	Auftragsbearbeitung i.S.v. Art. 10a DSGVO und eigenverantwortliche Bearbeitung	769
3.	Grenzüberschreitende Bekanntgabe	775
4.	Die datenschutzrechtlichen Prinzipien, Sicherheit und Audit	778
5.	Die Rechte betroffener Personen sowie die Pflicht zur Registrierung	780
6.	Zusammenfassende Übersicht	781
III.	Umsetzung der Vorgaben für das Outsourcing: Überblick und Checkliste	782
1.	Überblick	782
2.	Checkliste: Umsetzung der Vorgaben	783
§21	Organisatorische und technische Datenschutzmassnahmen	787
I.	Einleitung	787
II.	Gesetzliche Anforderungen	788
1.	Datensicherheit: Ziele und Anwendbarkeit	788
2.	Besondere Massnahmen	789
3.	Überprüfung der Massnahmen	790
4.	Protokollierung	791
5.	Bearbeitungsreglement	791
6.	Massnahmen vor Bekanntgabe der Daten	791
7.	Bestimmungen für Bundesorgane	791
8.	Vollständigkeit und Mindestanforderungen	792
III.	Schutzmassnahmen	792
1.	Datensicherheit als Grundlage des Datenschutzes	792
2.	Elemente der Governance	793
3.	Bedrohungen und Risiken	798
4.	Wirkungsweise von Schutzmassnahmen	799
5.	Auswahl von Schutzmassnahmen	800
6.	Beurteilung der Angemessenheit von Massnahmen	809
7.	Überprüfung von Massnahmen	811
IV.	Normen und Leitfäden in der Datensicherheit	812
1.	ISO/IEC 27000 Normenfamilie	813
2.	EDÖB – Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem	813
3.	FINMA – Rundschreiben 08/21 «Operationelle Risiken – Banken»	815
4.	EuroPriSe-Kriterien	816
5.	COBIT 5	816
6.	BSI – IT-Grundschutz-Kataloge	816
V.	Checklisten	817
1.	Datenschutz-Governance	817
2.	Angemessene organisatorische und technische Schutzmassnahmen	818

§ 22	Organisation und Aufgaben des betrieblichen Datenschutzbeauftragten	819
I.	Einleitung	819
II.	Rechtsgrundlagen	821
	1. Schweiz	821
	2. Europäische Union, Deutschland, Österreich und Liechtenstein	821
III.	Die Stellung des betrieblichen Datenschutzbeauftragten im Unternehmen	824
	1. Bezeichnung und Mitteilung an den EDÖB	824
	2. Fachliche Anforderungen	826
	3. Unabhängigkeit	828
IV.	Aufgaben	832
	1. Vorbemerkung	832
	2. Aufgaben	833
V.	Verantwortung	838
VI.	Checkliste: Pflichtenheft des betrieblichen Datenschutzbeauftragten '1	840
§ 23	Datenschutz-Zertifizierung	843
I.	Allgemeine Bemerkungen	843
	1. Vorbemerkung und gesetzliche Grundlagen	843
	2. Grundideen	844
	3. Auswirkungen einer Zertifizierung nach DSGVO	845
	4. Vergleichender Ausblick	846
II.	Beteiligte	849
	1. Schema	849
	2. Schweizerische Akkreditierungsstelle – SAS	850
	3. Zertifizierungsstellen	850
	4. Zertifizierte Stellen	852
	5. EDÖB	853
III.	Gegenstand und Verfahren der Zertifizierung im Allgemeinen	853
	1. Gegenstand der Zertifizierung	853
	2. Erteilung und Gültigkeit der Zertifizierung	853
	3. Anerkennung von ausländischen Zertifizierungen	854
	4. Mitteilung des Ergebnisses des Zertifizierungsverfahrens	854
	5. Sanktionen	855
IV.	Zertifizierung von Organisation und Verfahren – DSMS-Zertifizierung	858
	1. Gegenstand der DSMS-Zertifizierung	858
	2. Datenschutzmanagement – DSMS	860
V.	DSMS-Zertifizierung der Datenannahmestelle	864

VI.	Produktezertifizierung und Frage der Dienstleistungszertifizierung	865
VII.	Zusammenfassung	867
§ 24	Datenschutz bei Veräußerung und Zusammenschluss von Unternehmen	869
I.	Einleitung	870
	1. Gegenstand und Terminologie	870
	2. Entwicklung der Lehre und Rechtspraxis	871
	3. Abgrenzung	871
II.	Datenschutzrechtliche Grundlagen im Kontext von M&A-Transaktionen	872
	1. Anwendbarkeit des DSGVO auf Unternehmen und ihre Daten	872
	2. Zweck und Rechtstechnik des privatrechtlichen Datenschutzes	873
	3. Persönlichkeitsverletzende Datenbearbeitung	874
	4. Datenschutz in der M&A-Praxis	875
III.	Die Relevanz des DSGVO in den verschiedenen Phasen einer M&A-Transaktion	875
	1. Transaktionsphasen und ihre Bedeutung bezüglich Datenbekanntgabe	875
	2. Annäherungsphase	876
	3. Due Diligence	878
	4. Verpflichtungsgeschäft und Vorbereitung des Vollzugs	892
	5. Vollzug von M&A-Transaktionen	892
IV.	Zusammenfassung	896
V.	Checkliste	896
	Vierter Teil: Datenschutz in der öffentlichen Verwaltung	90i
§ 25	Öffentlichkeitsgesetz und Datenschutz	903
I.	Einleitung zum Öffentlichkeitsgesetz	903
II.	Grundzüge des Öffentlichkeitsgesetzes	905
	1. Das amtliche Dokument (Art. 5 BGÖ)	905
	2. Persönlicher Geltungsbereich (Art. 2 BGÖ)	907
	3. Sachlicher Geltungsbereich (Art. 3 BGÖ)	909
	4. Zeitlicher Geltungsbereich (Art. 23 BGÖ)	910
	5. Vorbehalt von Spezialbestimmungen (Art. 4 BGÖ)	911
III.	Das Zugangsverfahren	912
	1. Das Zugangsgesuch (Art. 10 BGÖ)	912
	2. Stellungnahme der Behörde (Art. 12 BGÖ)	913
	3. Beschränkung des Rechts auf Zugang (Art. 7 ff. BGÖ)	914
IV.	Zugang zu amtlichen Dokumenten mit Personendaten	917
	1. Grundrechtliche Aspekte zum Verhältnis von BGÖ und DSGVO	917

2.	Amtliche Dokumente mit Personendaten des Gesuchstellers (Art. 3 Abs. 2 BGÖ)	918
3.	Zugang zu amtlichen Dokumenten mit Personendaten (Art. 9 BGÖ)	919
4.	Interessenabwägung zwischen Schutz der Privatsphäre Dritter und öffentlichem Interesse am Zugang (Art. 7 Abs. 2 BGÖ)	925
s.	Anhörung (Art. 11 BGÖ)	930
6.	Würdigung	932
V.	Das Schlichtungs- und Beschwerdeverfahren	932
1.	Das Schlichtungsverfahren (Art. 13 f. BGÖ)	932
2.	Verfügung und Beschwerdeverfahren (Art. 15 f. BGÖ)	936
VI.	Gebühren (Art. 17 BGÖ)	936
1.	Grundsatz der Gebührenpflicht und Gebührenbemessung	937
2.	Information über voraussichtliche Gebühren	937
3.	Gebührenerhebung gegenüber Medien	938
4.	Gebührenstreitigkeiten	939
VII.	Praktische Hinweise und Links	940
§ 26	Datenschutz im Ausländer- und Asylbereich	943
I.	Einleitung	943
II.	Die gesetzlichen Regelungen	944
1.	Die relevanten internationalen Abkommen	944
2.	Die schweizerischen Gesetze	947
III.	Datenschutz im Ausländerrecht	949
1.	Vorbemerkung	949
2.	Die Datenbearbeitung	949
3.	Überwachungs- und Kontrollmassnahmen	951
4.	Meldepflichten und Datenweitergabe	952
IV.	Datenschutz im Schengen-Raum	955
1.	Das Schengen Durchführungübereinkommen (SDÜ) und die Richtlinie 95/46/EG	955
2.	Das Schengen-Informationssystem (SIS)	956
3.	Das zentrale Visa-Informationssystem	962
4.	Eurodac	965
V.	Datenschutz im Asylbereich	967
1.	Grundsätze	967
2.	Datenbearbeitung im Rahmen der Dublin-Assoziierungsabkommen	969
VI.	Checkliste	971

§ 27	Datenschutz im Sozialbereich	973
I.	Einleitung	973
II.	Rechtliche Grundlagen und -prinzipien für den Datenschutz im Sozialbereich	974
	1. Grundsatz des Datenschutzes als Persönlichkeitsschutz	974
	2. Grundsätze zu Informationsbeschaffung sowie Meldung, Auskunft und Informationsweitergabe im Besonderen	976
III.	Besondere Bedeutung und typische Herausforderungen des Datenschutzes im Sozialbereich	980
IV.	Aktuelle Entwicklungen der Gesetzgebung	981
	1. Entwicklung der Informationsnormen in der Sozialhilfegesetzgebung	981
	2. Entwicklung der Informationsnormen im Kindes- und Erwachsenenschutzrecht	982
	3. Offene Fragen rund um die erweiterten Informationsaustauschnormen im Sozialwesen	983
V.	Fazit	984
VI.	Checklisten	985
	1. Datenbearbeitung	985
	2. Informationsweitergabe	985
§ 28	eGovernment und Datenschutz	987
I.	Begriffe	988
	1. eGovernment	988
	2. Datenschutzrecht	988
II.	Herangehensweise und Gang der Darstellung	989
	1. Abgrenzung	989
	2. Gang der Darstellung	989
III.	Datenverarbeitung im eGovernment	990
	1. «eGovernment» als Aspekt des Verwaltungshandelns	990
	2. Regelungsgegenstand: Daten	991
	3. Drei Interessengruppen (A2C, A2B, A2A)	994
	4. Aufgabenstellungen des eGovernment	996
	5. eGovernment-Infrastruktur	997
	6. Der Begriff des Datenherrn	1000
	7. Ausblick: Öffentliche Basisdaten?	1002
IV.!	Gesetzliche Grundlagen	1004
	1. Bundesverfassung	1004
	2. Regierungs- und Verwaltungsorganisationsgesetz und Ausführungserlasse	1005
	3. Verfahrensgesetze und Ausführungserlasse	1007

4.	Datenschutzgesetz	1007
5.	ZertES und VZertES	1008
6.	Registerharmonisierungsgesetz	1008
7.	Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI)	1008
8.	Öffentlichkeitsgesetz (BGÖ)	1009
9.	Spezialgesetze	1010
10.	Kantonale Erlasse	1012
11.	Rahmenvereinbarung eGovernment	1012
V.	Ableitungen	1013
1.	Datenschutzrechtliche Grundprinzipien	1013
2.	Datenschutz beim Beizug von externen Dritten	1014
3.	Das RVOG als Auffangregelung im Bund	1014
4.	Zielkonflikt zwischen eGovernment und Datenschutz	1016
5.	Informationszugang und Öffentlichkeitsprinzip	1018
VI.	Empfehlungen für eGovernment Projekte	1019
1.	Vorgehensfragen	1019
2.	Sachdaten mit Personenbezug	1021
3.	Systemdatenschutz: Die Antwort liegt im IT-System	1024
4.	Sicherheitsanforderungen	1025
5.	Authentisierung und Autorisierung	1026
6.	Gestaltung des Web-Angebots	1030
7.	Insbesondere: Registerwesen	1033
8.	Hinweise für Private und kantonale Stellen zum Umgang mit der AHVN13	1039
VII.	Checklisten	1041
1.	Gesetzliche Grundlage	1041
2.	Empfohlene Schritte zur Klärung der gesetzlichen Rahmenbedingungen	1041
3.	Anforderungen an gesetzliche Grundlagen für Informationssysteme im eGovernment-Umfeld	1043
4.	Was gehört in die Organisationsvorschriften für das GEVER-System	1044
5.	Festlegung geeigneter Authentisierungsmethoden	1047
6.	OGD-Prinzipien	1050
§29 Datenschutz in Justiz und Polizei		1053
I.	Einleitung	1053
II.	Rechtsquellen	1056
III.	Gliederung	1056
IV.	Daten(schutz)vorschriften in der StPO	1057
1.	Allgemeines	1057

2. Datenbearbeitung	1057
3. Bearbeitung und Aufbewahrung von Personendaten nach Abschluss des Verfahrens/Archivierung von Akten	1065
V. Daten(schutz)vorschriften in andern eidgenössischen Erlassen (bezogen auf Datensammlungen)	1066
1. Strafregister und DNA-Register	1066
2. Weitere Register	1068
VI. Regelungen für kantonale Datenbearbeitungs- und Informationssysteme	1074
VII. Schlussbemerkungen	1075
1. Aspekt Auskunftsrecht	1075
2. Aspekt Datenlöschung	1076
3. Aspekt Datensicherheit	1077
§30 Datenschutz in Statistik und Forschung	1079
I. Einleitung	1079
II. Der Persönlichkeitsschutz im Allgemeinen	1080
1. Die Rechtsgrundlagen des Persönlichkeitsschutzes auf Verfassungsebene	1080
2. Gesetzliche Grundlagen im DSG	1080
III. Die Datenbearbeitung zum nicht personenbezogenen Zweck in der Statistik	1087
1. Aus dem Kompetenzbereich des EDÖB: Die Bundesstatistik und die Statistik von Privaten	1088
2. Ausgewählte Probleme	1094
Fünfter Teil: Datenschutz im Ausland	1099
§31 Entwicklungen im internationalen Datenschutzrecht	1101
I. Einleitende Bemerkungen	1102
II. Die Revision der Datenschutzkonvention des Europarates	1103
1. Hauptäschliche Ziele der Revision	1104
2. Begriffsbestimmungen	1104
3. Anwendungsbereich	1106
4. Prinzipien der Bearbeitung von Personendaten	1107
5. Besonders schützenswerte Personendaten	1108
6. Datensicherheit – Notifikationspflicht bei «Datenpannen»	1110
7. Rechte der Betroffenen	1111
8. Zusätzliche Verpflichtungen	1113
9. Grenzüberschreitender Datenverkehr	1114
III. Die Revision der OECD Guidelines	1115
1. Einleitende Bemerkungen	1115
2. Revisionsarbeiten und die neuen OECD Guidelines 2013	1116

3.	(Kurz-)Überblick über die normativen Inhalte der neuen OECD-Richtlinie 2013	1118
4.	Zu den einzelnen Neuerungen der OECD-Richtlinie 2013	1118
IV.	Abschliessende Bemerkungen	1121
§32	Datenschutzrecht der Europäischen Union	1123
I.	Allgemeines und Überblick	1124
1.	Rechtsgrundlagen	1124
2.	Reformvorhaben	1125
3.	Internationale Anwendbarkeit	1126
4.	Datenschutzaufsicht	1128
II.	Grundbegriffe	1130
1.	Personenbezogene Daten	1130
2.	Verarbeitung	1132
3.	Verantwortliche Stelle, Dritte, Auftragsverarbeiter	1133
III.	Erlaubnistatbestände	1135
1.	Grundregel	1135
2.	Einwilligung	1136
3.	Allgemeine Erlaubnistatbestände	1139
4.	Zusätzliche Anforderungen an Erlaubnistatbestände	1142
IV.	Allgemeine Prinzipien und interne Organisation	1145
1.	Zweckbindung	1145
2.	Technisch-organisatorische Massnahmen	1146
3.	Betroffenenrechte	1147
4.	Melde- und Genehmigungspflichten	1147
V.	Internationale Datenübermittlung	1149
1.	Grundsätze	1149
2.	Gesetzliche Ausnahmen	1149
3.	Sichere Drittstaaten	1150
4.	SafeHarbor	1151
5.	Standard-Verträge	1152
6.	Binding Corporate Rules	1153
VI.	Folgen bei Verstössen	1154
1.	Aufsichtsbehörden	1154
2.	Zivilrecht	1155
VII.	Checkliste	1155
§33	Datenschutzrecht in den USA	1157
I.	Einführung	1157
II.	Was es im US-Datenschutzrecht nicht gibt	1158

III. US-Datenschutzrecht im Überblick	1158
IV. Verfassung der USA	1160
V. Bundesgesetze	1161
1. Telekommunikationsgeheimnis (ECPA)	1161
2. Gesundheitswesen (HIPAA)	1162
3. Finanzwesen (Graham-Leach-Bliley-Act)	1164
4. Bonitätsdaten (Fair Credit Reporting Act)	1164
5. Werbe-E-Mails (CAN-SPAM Act)	1164
6. Kinder (COPPA)	1165
7. Computer-Schutz gegen Hacking	1166
VI. Recht der US-Einzelstaaten	1167
1. Verfassungsrecht	1167
2. Common Law Invasion of Privacy	1167
3. Datensicherheit	1168
VII. Beispiele von Spezialgesetzen	1169
1. Datenerhebung von Kreditkartenbenutzern	1169
2. Datenübermittlung zu Werbezwecken	1170
VIII. Datenschutz am Arbeitsplatz	1171
IX. Datenschutz gegenüber dem Staat	1172
X. Safe Harbor – EU, Schweiz, USA	1172
XI. Checklisten	1173
1. Wer ist in Ihrer Organisation für US-Datenschutz verantwortlich?	1173
2. Was unternimmt Ihre Organisation, um Daten sicher zu bewahren?	1173
3. Sind alle Belehrungen und Einwilligungen akkurat und erteilt worden?	1173
4. Sind US-Spezialgesetze auf Ihr Vorhaben, Unternehmen oder Marktsegment anwendbar?	1174
5. Erhalten oder senden Sie Daten über Ländergrenzen?	1174
6. Überwachen Sie Mitarbeiter mittels Whistleblower-Hotline oder Technologien?	1174
7. Halten Sie Datenschutz- und Wettbewerbsrecht im Zusammenhang mit Werbemaßnahmen ein?	1174
 §34 Datenschutzrecht in Drittstaaten	 1175
I. Einleitung	1175
II. Australien	1177
1. Rechtlicher Rahmen	1177
2. Frage der Angemessenheit	1178

III.	Brasilien	1179
	1. Rechtlicher Rahmen	1179
	2. Frage der Angemessenheit	1182
IV.	China	1183
	1. Rechtlicher Rahmen	1183
	2. Frage der Angemessenheit	1184
V.	Indien	1184
	1. Rechtlicher Rahmen	1184
	2. Frage der Angemessenheit	1186
VI.	Japan	1187
	1. Rechtlicher Rahmen	1187
	2. Frage der Angemessenheit	1189
VII.	Russland	1189
	1. Rechtlicher Rahmen	1189
	2. Frage der Angemessenheit	1191
VIII.	Türkei	1191
	1. Rechtlicher Rahmen	1191
	2. Frage der Angemessenheit	1193
IX.	Fazit	1194
	Sachregister	1195