

## Contents

<b>1</b>	<b>Origins and Concepts of Data Privacy</b>	<b>1</b>
1.1	Questions and Challenges of Data Privacy	2
1.1.1	But Cupid Turned Out to Be Not OK	3
1.2	The Conundrum of Voluntary Information	3
1.3	What Is Data Privacy?	5
1.3.1	Physical Privacy	5
1.3.2	Social Privacy Norms	5
1.3.3	Privacy in a Technology-Driven Society	5
1.4	Doctrine of Information Privacy	6
1.4.1	Information Sharing Empowers the Recipient	6
1.4.2	Monetary Value of Individual Privacy	7
1.4.3	“Digital Public Spaces”	7
1.4.4	A Model Data Economy	8
1.5	Notice-and-Choice versus Privacy-as-Trust	9
1.6	Notice-and-Choice in the US	9
1.7	Enforcement of Notice-and-Choice Privacy Laws	11
1.7.1	Broken Trust and FTC Enforcement	11
1.7.2	The Notice-and-Choice Model Falls Short	12
1.8	Privacy-as-Trust: An Alternative Model	13
1.9	Applying Privacy-as-Trust in Practice: The US Federal Trade Commission	14
1.9.1	Facebook as an Example	15
1.10	Additional Challenges in the Era of Big Data and Social Robots	16
1.10.1	What Is a Social Robot?	16
1.10.2	Trust and Privacy	17
1.10.3	Legal Framework for Governing Social Robots	17

1.11	The General Data Protection Regulation (GDPR)	18
1.12	Chapter Overview	19
	Notes	21
<b>2</b>	<b>A Brief History of Data Privacy</b>	<b>23</b>
2.1	Privacy as One's Castle	23
2.1.1	Individuals' "Castles" Were Not Enough	24
2.2	Extending Beyond the "Castle"	24
2.3	Formation of Privacy Tort Laws	24
2.3.1	A Privacy Tort Framework	25
2.4	The Roots of Privacy in Europe and the Commonwealth	25
2.5	Privacy Encroachment in the Digital Age	26
2.5.1	Early Digital Privacy Laws Were Organic	27
2.5.2	Growth in Commercial Value of Individual Data	27
2.6	The Gramm-Leach-Bliley Act Tilted the Dynamic against Privacy	28
2.7	Emergence of Economic Value of Individual Data for Digital Businesses	29
2.7.1	The Shock of the 9/11 Attacks Affected Privacy Protection Initiatives	29
2.7.2	Surveillance and Data Collection Was Rapidly Commercialized	30
2.7.3	Easing of Privacy Standards by the NSA Set the Tone at the Top	30
2.8	Legislative Initiatives to Protect Individuals' Data Privacy	31
2.9	The EU Path	33
2.9.1	The Internet Rights Revolution	34
2.9.2	Social Revolutions	34
2.10	End of the Wild West?	37
2.11	Data as an Extension of Personal Privacy	37
2.12	Cambridge Analytica: A Step Too Far	39
2.13	The Context of Privacy in Law Enforcement	39
	Summary	41
	Notes	41
<b>3</b>	<b>GDPR's Scope of Application</b>	<b>45</b>
3.1	When Does GDPR Apply?	45
3.1.1	"Processing" of Data	46
3.1.1.1	Manual Processing	46
3.1.2	"Personal Data"	47
3.1.2.1	Relative Criteria for Identifiability	47
3.1.2.2	Individual Circumstances	48
3.1.2.3	Special Cases	48
3.1.2.4	Anonymization	50

	3.1.2.5 Pseudonymization	51
	3.1.3 Exempted Activities under GDPR	51
3.2	The Key Players under GDPR	52
3.3	Territorial Scope of GDPR	54
	3.3.1 Physical Presence in the EU	54
	3.3.2 Processing Done in the Context of the Activities	55
	3.3.3 Users Based in the EU	56
	3.3.4 “Time of Stay” Standard	57
3.4	Operation of Public International Law	57
	Notes	57
<b>4</b>	<b>Technical and Organizational Requirements under GDPR</b>	<b>61</b>
4.1	Accountability	61
4.2	The Data Controller	62
	4.2.1 Responsibilities of the Controller	63
	4.2.1.1 Demonstration	63
	4.2.1.2 Data Protection Policies	64
	4.2.1.3 Adherence	64
	4.2.2 Joint Controllers and Allocating Liability	65
	4.2.2.1 Additional Obligations Placed on Joint Controllers	65
	4.2.2.2 Joint and Several Liabilities	65
	4.2.2.3 Controllers Outside of the EU	67
	4.2.3 The Duty to Cooperate with the SA	68
4.3	Technical and Organizational Measures	69
	4.3.1 Maintain a Data-Protection Level	69
	4.3.2 Minimum Requirements for Holding a Data Protection Level	69
	4.3.3 Weighing the Risks	70
	4.3.3.1 Risk to the Business	70
	4.3.3.2 Risk to Consumers	70
	4.3.3.3 Risks Caused by Third Parties	71
	4.3.4 The Network and Information Systems Directive	71
4.4	Duty to Maintain Records of Processing Activities	72
	4.4.1 Content of Controller’s Records	72
	4.4.2 Content of Processor’s Records	73
	4.4.3 Exceptions to the Duty	73
4.5	Data Protection Impact Assessments	73
	4.5.1 Types of Processing That Require DPIA	74
	4.5.2 Scope of Assessment	75
	4.5.2.1 Determining the Risk	75
	4.5.2.2 Contents of the DPIA	76
	4.5.2.3 Involvement of the DPO	76
	4.5.2.4 Prior Consultation	77
	4.5.3 Business Plan Oversight	78

4.6	The Data Protection Officer	80
4.6.1	Designation of DPO	80
4.6.2	Qualifications and Hiring a DPO	81
4.6.3	Position of the DPO	81
4.6.4	Tasks of the DPO	82
4.6.5	An Inherent Conflict of Interest?	83
4.6.6	DPO Liability	84
4.7	Data Protection by Design and Default	84
4.7.1	Data Protection at the Outset	84
4.7.2	Balancing the Amount of Protection	85
4.7.3	Applying Data Protection by Design	86
4.7.4	Special Case: Blockchain Technology and GDPR	91
4.8	Data Security during Processing	92
4.8.1	Data Security Measures	93
4.8.2	Determining the Risk Posed	94
4.8.3	Data Protection Management Systems: A “Technical and Organizational Measure”	94
4.9	Personal Data Breaches	94
4.9.1	Overview of Data Breaches	95
4.9.1.1	Types of Data Breaches	95
4.9.1.2	Damage Caused by Data Breaches	96
4.9.1.3	Degrees of Data Breaches	97
4.9.1.4	Types of Cyber-Threats	99
4.9.1.5	Practically Implementing Cyber-Security	100
4.9.1.6	Combating Cyber-Security Threats	100
4.9.1.7	Breach Response Plan	101
4.9.1.8	Manual versus Automated Cyber-Security	102
4.9.1.9	Cyber-Security Insurance	102
4.9.2	The Controller’s Duty to Notify	103
4.9.2.1	Excusable Delays	104
4.9.2.2	Contents of Notification	104
4.9.2.3	Exception	105
4.9.3	Controller’s Duty to Communicate the Breach to Data Subjects	106
4.9.3.1	A Timely Communication	106
4.9.3.2	Contents of the Communication	106
4.9.3.3	Exceptions	107
4.10	Codes of Conduct and Certifications	107
4.10.1	Purpose and Relationship under GDPR	107
4.10.2	Codes of Conduct	108
4.10.2.1	Codes of Conduct by Associations	108
4.10.2.2	Monitoring Approved Codes of Conduct	109
4.10.3	Certification	110
4.10.3.1	Certification Bodies	110
4.10.3.2	Factors for Granting Accreditation to Certification Bodies	110

	4.10.3.3	Responsibilities of Certification Bodies	111
	4.10.3.4	The Certification Mechanisms	111
4.11		The Data Processor	112
	4.11.1	Relationship between Processor and Controller	112
	4.11.2	Responsibilities of Controller in Selecting a Processor	113
	4.11.2.1	Sufficient Guarantees	113
	4.11.2.2	Maintaining Processing Contracts	113
	4.11.2.3	Standard Contractual Clauses	114
	4.11.3	Duties of the Processor	114
	4.11.4	Subprocessors	116
		Notes	116
<b>5</b>		<b>Material Requisites for Processing under GDPR</b>	<b>125</b>
5.1		The Central Principles of Processing	125
	5.1.1	Lawful, Fair, and Transparent Processing of Data	126
	5.1.2	Processing Limited to a “Purpose”	127
	5.1.2.1	Restriction on Processing and Exceeding the Purpose	128
	5.1.2.2	The “Compatibility” Test	128
	5.1.2.3	Processing That Does Not Require Identification	129
	5.1.3	Data Minimization and Accuracy	130
	5.1.4	Storage of Data	131
	5.1.5	Integrity and Confidentiality of the Operation	131
5.2		Legal Grounds for Data Processing	132
	5.2.1	Processing Based on Consent	132
	5.2.1.1	What Constitutes Consent?	132
	5.2.1.2	Consent of a Child	134
	5.2.1.3	NYOB.eu versus Google, Facebook, Whatsapp, and Instagram: A Case Study on Consent	135
	5.2.2	Processing Based on Legal Sanction	144
	5.2.2.1	Formation or Performance of a Contract	144
	5.2.2.2	Compliance with a Legal Obligation	145
	5.2.2.3	Protection of Vital Interests	145
	5.2.2.4	Public Interest and Exercise of Official Authority	145
	5.2.2.5	Exercising Legitimate Interests	146
	5.2.3	Changing the Processing “Purpose”	148
	5.2.4	Special Categories of Data	149
	5.2.4.1	What Is “Special” Data?	150
	5.2.4.2	Location and Behavioral Data	150

	5.2.4.3	Processing Data Relating to Criminal Convictions	151
	5.2.4.4	The Exceptions to the Rule	152
	5.2.4.5	New Technologies Involving Special Data	157
	5.2.4.6	Developing the Law Further	160
5.3		International Data Transfers	161
	5.3.1	Adequacy Decisions and “Safe” Countries	162
	5.3.1.1	Determining Adequacy	162
	5.3.1.2	Application of the Factors	163
	5.3.1.3	Revocation of the Adequacy Decision	165
	5.3.2	Explicit Consent	166
	5.3.3	Standard Contractual Clauses	166
	5.3.3.1	Overview of Commission Decisions	166
	5.3.3.2	Content of SCCs	167
	5.3.3.3	Consequences of Breaching the Conditions of SCCs	168
	5.3.4	The EU–US Privacy Shield	169
	5.3.5	Binding Corporate Rules	172
	5.3.5.1	Legally Mandated Clauses	172
	5.3.5.2	Conditions for Approval	174
	5.3.6	Transfers Made with or without Authorization	175
	5.3.6.1	International Data Transfers without the SA’s Authorization	175
	5.3.6.2	International Data Transfers with SA’s Authorization	176
	5.3.6.3	Implementing Appropriate Safeguards	177
	5.3.7	Derogations	177
	5.3.7.1	Permitted Derogations	177
	5.3.7.2	Unauthorized Derogations	178
	5.3.7.3	Transfers Not Authorized by EU	179
	5.3.8	Controllers Outside of the EU	180
5.4		Intragroup Processing Privileges	182
5.5		Cooperation Obligation on EU Bodies	183
5.6		Foreign Law in Conflict with GDPR	184
		Notes	185

## 6 Data Subjects’ Rights 193

6.1		The Controller’s Duty of Transparency	194
	6.1.1	Creating the Modalities	194
	6.1.2	Facilitating Information Requests	195
	6.1.3	Providing Information to Data Subjects	195
	6.1.4	The Notification Obligation	196
6.2		The <i>Digital Miranda</i> Rights	197
	6.2.1	Accountability Information	197
	6.2.2	Transparency Information	198

6.2.3	Timing	200
6.2.4	Defenses for Not Providing Information	200
6.3	The Right of Access	201
6.3.1	Accessing Personal Data	201
6.3.2	Charging a “Reasonable Fee”	202
6.4	Right of Rectification	203
6.4.1	Inaccurate Personal Data	204
6.4.2	Incomplete Personal Data	204
6.4.3	Handling Requests	204
6.5	Right of Erasure	205
6.5.1	Development of the Right	205
6.5.2	The Philosophical Debate	206
6.5.3	Circumstances for Erasure under GDPR	209
6.5.4	Erasure of Personal Data Which Has Been Made Public	211
6.5.5	What Is “Erasure” of Personal Data?	212
6.5.6	Exceptions to Erasure	212
6.6	Right to Restriction	214
6.6.1	Granting Restriction	215
6.6.2	Exceptions to Restriction	216
6.7	Right to Data Portability	216
6.7.1	The Format of Data and Requirements for Portability	217
6.7.2	Business Competition Issues	218
6.7.3	Intellectual Property Issues	219
6.7.4	Restrictions on Data Portability	220
6.8	Rights Relating to Automated Decision Making	221
6.8.1	The Right to Object	221
6.8.2	Right to Explanation	223
6.8.3	Profiling	224
6.8.4	Exceptions	225
6.8.5	Special Categories of Data	225
6.9	Restrictions on Data Subject Rights	226
6.9.1	Nature of Restrictions Placed	226
6.9.2	The Basis of Restrictions	227
	Notes	228
<b>7</b>	<b>GDPR Enforcement</b>	<b>233</b>
7.1	In-House Mechanisms	233
7.1.1	A Quick Review	234
7.1.2	Implementing an Internal Rights Enforcement Mechanism	235
7.1.2.1	Step 1: Getting the Information Across	235
7.1.2.2	Step 2: The Privacy Policy	236
7.1.2.3	Step 3: Create the “Technical” Measures	237

	7.1.2.4	Step 4: Implement the “Organizational” Measures	239
	7.1.2.5	Step 5: Create a Dispute Resolution Policy	239
7.2		Data Subject Representation	240
	7.2.1	Standing of NPOs to Represent Data Subjects	240
	7.2.2	Digital Rights Activism	241
7.3		The Supervisory Authorities	241
	7.3.1	Role of Supervisory Authority	241
	7.3.2	The Members of the Supervisory Authority	242
	7.3.3	An Independent Body	243
	7.3.4	Professional Secrecy	243
	7.3.5	Competence of the Supervisory Authority	244
	7.3.5.1	The Lead Supervisory Authority	245
	7.3.5.2	Local Competence	246
	7.3.6	Tasks of the Supervisory Authority	246
	7.3.6.1	Advisory Duties	246
	7.3.6.2	Promoting Knowledge and Compliance	247
	7.3.6.3	Investigative Duties	247
	7.3.6.4	Cooperation	247
	7.3.6.5	Regulating Compliance	247
	7.3.6.6	Internal Responsibilities	248
	7.3.7	Powers of the SA	248
	7.3.7.1	Investigative Powers	248
	7.3.7.2	Corrective Powers	249
	7.3.7.3	Authorization and Advisory Powers	250
	7.3.7.4	Appropriate Safeguards	250
	7.3.8	Cooperation and Consistency Mechanism	250
	7.3.8.1	EU Data Protection Board	251
	7.3.8.2	The Cooperation Mechanism	251
	7.3.8.3	The Consistency Mechanism	252
	7.3.9	GDPR Enforcement by Supervisory Authorities	252
7.4		Judicial Remedies	253
	7.4.1	Judicial Action against the Controller or Processor	253
	7.4.2	Courts versus SA; Which Is Better for GDPR Enforcement?	254
	7.4.3	Judicial Action against the Supervisory Authority	254
	7.4.4	Controller Suing the Data Subject?	256
	7.4.5	Suspending the Proceedings	257
7.5		Alternate Dispute Resolution	258
	7.5.1	Is an ADR Arrangement Allowed under GDPR?	260
	7.5.2	ADR Arrangements	260
	7.5.3	Key Hurdles of Applying ADR to GDPR	261
	7.5.4	Suggestions for Implementing ADR Mechanisms	263



7.6	Forum Selection Clauses	265
7.7	Challenging the Existing Law	266
	Notes	267
<b>8</b>	<b>Remedies</b>	<b>271</b>
8.1	Allocating Liability	271
8.1.1	Controller Alone Liable	271
8.1.2	Processor Alone Liable	272
8.1.3	Joint and Several Liabilities	272
8.2	Compensation	273
8.2.1	Quantifying “Full Compensation”	273
8.2.2	Conflict in the Scope of “Standing” in Court	274
8.3	Administrative Fines	275
8.3.1	Fines for Regulatory Infringements	275
8.3.2	Fines for Grave Infringements	276
8.3.3	Determining the Quantum of the Fine	276
8.4	Processing Injunctions	279
8.4.1	Domestic Law	279
8.4.2	The EU Injunction Directive	280
8.4.3	The SA’s Power to Restrain Processing	281
8.5	Specific Performance	283
	Notes	284
<b>9</b>	<b>Governmental Use of Data</b>	<b>287</b>
9.1	Member State Legislations	287
9.2	Processing in the “Public Interest”	291
9.2.1	What Is Public Interest?	291
9.2.2	Public Interest as a “Legal Basis” for Processing	292
9.2.3	State Use of “Special” Data	292
9.2.4	Processing Relating to Criminal Record Data	294
9.3	Public Interest and the Rights of a Data Subject	294
9.3.1	Erasure and Restriction of Data Processing	294
9.3.2	Data Portability	295
9.3.3	Right to Object	296
9.3.4	Right to Explanation	296
9.4	Organizational Exemptions and Responsibilities	297
9.4.1	Representatives for Controllers Not within the EU	297
9.4.2	General Impact Assessments in Lieu of a Data Protection Impact Assessment (DPIA)	297
9.4.3	Designation of a Data Protection Office (DPO)	298

	9.4.4	Monitoring of Approved Codes of Conduct	299
	9.4.5	Third-Country Transfers	299
9.5		Public Documents and Data	301
	9.5.1	The Network and Information Systems Directive	301
	9.5.2	Telemedia Data Protection	302
	9.5.3	National Identification Numbers	303
9.6		Archiving	304
9.7		Handling Government Subpoenas	305
9.8		Public Interest Restrictions on GDPR	305
9.9		Processing and Freedom of Information and Expression	306
	9.9.1	Journalism and Expression under GDPR	306
	9.9.2	Combating “Fake News” in the Modern Age	307
9.10		State Use of Encrypted Data	308
9.11		Employee Data Protection	309
	9.11.1	The Opening Clause	310
	9.11.2	Employment Agreements	311
	9.11.3	The German <i>Betriebsrat</i>	312
	9.11.4	The French “Comité d’entreprise”	313
		Notes	314

## 10 Creating a GDPR Compliance Department 319

10.1		Step 1: Establish a “Point Person”	319
10.2		Step 2: Internal Data Audit	321
10.3		Step 3: Budgeting	322
10.4		Step 4: Levels of Compliance Needed	323
	10.4.1	Local Legal Standards	323
	10.4.2	Enhanced Legal Standards for International Data Transfers	324
	10.4.3	International Legal Standards	324
	10.4.4	Regulatory Standards	324
	10.4.5	Contractual Obligations	324
	10.4.6	Groups of Undertakings	325
10.5		Step 5: Sizing Up the Compliance Department	325
10.6		Step 6: Curating the Department to Your Needs	326
	10.6.1	“In-House” Employees	326
	10.6.2	External Industry Operators	326
	10.6.3	Combining the Resources	327
10.7		Step 7: Bring Processor Partners into Compliance	327
10.8		Step 8: Bring Affiliates into Compliance	328
10.9		Step 9: The Security of Processing	328
10.10		Step 10: Revamping Confidentiality Procedures	329
10.11		Step 11: Record Keeping	329
10.12		Step 12: Educate Employees on New Protocols	330

10.13	Step 13: Privacy Policies and User Consent	331
10.14	Step 14: Get Certified	331
10.15	Step 15: Plan for the Worst Case Scenario	331
10.16	Conclusion	332
	Notes	332
<b>11</b>	<b>Facebook: A Perennial Abuser of Data Privacy</b>	<b>335</b>
11.1	Social Networking as an Explosive Global Phenomenon	335
11.2	Facebook Is Being Disparaged for Its Data Privacy Practices	335
11.3	Facebook Has Consistently Been in Violation of GDPR Standards	336
11.4	The Charges against Facebook	336
11.5	What Is Facebook?	337
11.6	A Network within the Social Network	337
11.7	No Shortage of “Code of Conduct” Policies	338
11.8	Indisputable Ownership of Online Human Interaction	339
11.9	Social Networking as a Mission	339
11.10	Underlying Business Model	340
11.11	The Apex of Sharing and Customizability	341
11.12	Bundling of Privacy Policies	341
11.13	Covering All Privacy Policy Bases	342
11.14	Claims of Philanthropy	343
11.15	Mechanisms for Personal Data Collection	344
11.16	Advertising: The Big Revenue Kahuna	346
11.17	And Then There Is Direct Marketing	347
11.18	Our Big (Advertiser) Brother	347
11.19	A Method to Snooping on Our Clicks	348
11.20	What Do We Control (or Think We Do)?	349
	11.20.1 Ads Based on Data from FB Partners	350
	11.20.2 Ads Based on Activity on FB That Is Seen Elsewhere	350
	11.20.3 Ads That Include Your Social Actions	351
	11.20.4 “Hiding” Advertisements	351
11.21	Even Our Notifications Can Produce Revenue	352
11.22	Extent of Data Sharing	353
11.23	Unlike Celebrities, We Endorse without Compensation	354
11.24	Whatever Happened to Trust	355
11.25	And to Security of How We Live	355
11.26	Who Is Responsible for Security of Our Life Data?	356
11.27	And Then There Were More	359
11.28	Who Is Responsible for Content?	359
11.29	Why Should Content Be Moderated?	360
11.30	There Are Community Standards	361

11.31	Process for Content Moderation	369
11.31.1	Identifying and Determining Content Removal Requests	369
11.32	Prospective Content Moderation “Supreme Court”	370
11.33	Working with Governmental Regimes	370
11.34	“Live” Censorship	371
11.35	Disinformation and “Fake” News	372
11.35.1	“Disinformation”	372
11.35.2	False News Policy	374
11.35.3	Fixing the “Fake News” Problem	375
11.36	Conclusion	380
	Notes	386
<b>12</b>	<b>Facebook and GDPR</b>	<b>393</b>
12.1	The Lead Supervisory Authority	393
12.2	Facebook nicht spricht Deutsch	393
12.3	Where Is the Beef? Fulfilling the <i>Information Obligation</i>	394
12.4	Data Processing <i>Purpose Limitation</i>	395
12.5	Legitimate Interests Commercial “Restraint” Needed	396
12.6	Privacy by Design?	398
12.7	Public Endorsement of Personalized Shopping	398
12.8	Customizing Data Protection	399
12.9	User Rights versus Facebook’s Obligations	400
12.10	A Digital Blueprint and a GDPR Loophole	401
12.11	Investigations Ahead	402
12.12	Future Projects	403
	Notes	404
<b>13</b>	<b>The Future of Data Privacy</b>	<b>407</b>
13.1	Our Second Brain	407
13.2	Utopian or Dystopian?	409
13.3	Digital Empowerment: Leveling the Playing Field	410
	Notes	412
	<b>Appendix: Compendium of Data Breaches</b>	<b>413</b>
	<b>About the Authors</b>	<b>467</b>
	<b>Index</b>	<b>469</b>