

Table of Contents

Disclaimer	vii
About the Author	ix
CHAPTER 1	
Data Protection Projects: Building an Inventory	1
1.1 Introduction	1
1.2 How This Book Helps Enterprises in GDPR Projects	2
1.2.1 The Risk-Based Approach in the GDPR	3
1.3 Topics Covered and Purposes of the Book	4
1.4 Building an Inventory and the Key Documentation	7
1.5 Material and Territorial Scope of the GDPR	8
1.5.1 Article 2: Material Scope	8
1.5.2 Article 3: Territorial Scope	9
1.6 The Establishment Criterion: Article 3(1)	10
1.7 The Targeting Criterion: Article 3(2)	13
1.7.1 Position of Processors When Not Established in the EU	15
1.7.2 Appointing Representatives under Article 27	16
1.8 How to Achieve a Minimum Level of Compliance	18
1.9 GDPR the Terminology and Common Problems in Completing an Inventory	20
1.10 Content and Format of an Inventory	22
1.11 Personal Data	22
1.12 Names as Identifiers	27
1.13 The Use of Unique Identifiers	28
1.14 IP Addresses	29
1.15 Pseudonymised Data	30
1.16 Anonymous Data	30
1.17 ECJ Case Law on What Constitutes Personal Data	33
1.18 Sensitive Data and Criminal Conviction Data	35

Table of Contents

1.18.1	Health Data	37
1.18.2	The Meaning of Racial or Ethnic Origin	38
1.19	Processing	41
1.20	List of Useful Documents	43
CHAPTER 2		
	Gap Analysis: Identifying the Enterprise's Gaps	45
2.1	Developing a Project Management Methodology	45
2.2	Implementation of the Gaps	47
2.3	Starting the Gap Analysis or Data Audit	48
2.4	Benefits of a Gap Analysis	48
2.5	High-risk Areas to Date for Enforcement by Regulators	49
2.6	Drafting a Project Plan for GDPR	50
2.7	The Role of the DPO	52
2.8	Policies, Procedures, Standards, and Guidelines	53
2.9	Building a Risk Analysis Framework	54
2.10	Individuals' Rights under the GDPR	56
2.11	Summary of Powers of the Supervisory Authorities	56
2.12	Direct Marketing under the ePrivacy Directive	57
2.13	ePrivacy Directive	58
CHAPTER 3		
	Legal Bases for Processing	59
3.1	The Lawful Basis Principle	59
3.2	The Categories of Data Determine the Legal Bases	60
3.3	The Six Legal Bases for Processing Personal Data	60
3.4	Sensitive/Special Category Personal Data	62
3.5	Consent	64
3.6	Vital Interest	70
3.7	Contract with the Data Subject	73
3.8	Legal Obligation	74
3.9	Public Interest	75
3.10	Legitimate Interest: Purpose and Necessity	76
	3.10.1 Balancing of Rights	79
	3.10.2 Impact	80
	3.10.3 Assessment by Enterprise	80
3.11	Further Processing	81
CHAPTER 4		
	Article 30 Record Keeping	83
4.1	Records of Processing for Article 30	83
4.2	What Records Must a Controller Keep?	84
	4.2.1 Purposes of Processing	85
	4.2.2 Categories of Personal Data	85
	4.2.3 Technical and Organisational Safeguards	85

4.3	Who Is the Controller?	86
4.3.1	Factors in Determining Whether the Enterprise Is a Controller	86
4.3.2	Purposes and Means Test	88
4.3.3	Factors in Determining Whether the Enterprise Is a Joint Controller	89
4.3.4	Jointly Determined Purpose(s)	90
4.3.5	Joint Controller Agreements	92
4.4	Who Is the Processor?	92
4.5	What Records Must Be Kept by Processors?	93
4.5.1	Categories of Processing Activity	94
4.5.2	Safeguards over Transfers	94
4.5.3	Retention Period	95
4.5.4	Categories of Recipients	96
4.5.5	Sub-processors in the GDPR Article 28	96
4.5.6	Technical and Organisational Safeguards	97
4.5.7	Factors in Determining Whether the Enterprise Is a Processor	98
4.5.8	EDPB Guidance on Processors	98
4.5.9	Article 28: Processing Agreement – What Is Included?	99
4.5.10	Clauses Which Should Be in Data Processing Agreements	102
CHAPTER 5		
Breaches, Incident Response, Security, and Controls		105
5.1	What Is a Breach?	105
5.2	Responding to Breaches	106
5.2.1	Most Common Breaches Attracting Enforcement Action	107
5.2.2	Accidental and Unlawful Destruction	108
5.2.3	When Does an Enterprise Need to Notify a Breach?	109
5.3	Notification to the Supervisory Authority	111
5.3.1	What Records Does an Enterprise Need to Keep?	111
5.4	Reporting	112
5.4.1	Breach Recording	112
5.4.2	Notification to the Supervisory Authority	113
5.4.3	Information to Be Provided to Supervisory Authorities	113
5.4.4	Delays in Notification and Notifying in Phases	114
5.5	Article 34: Notification to the Data Subject	114
5.5.1	Notifying the Data Subject	114
5.5.2	Information to Be Provided	114
5.5.3	When Is a Notification Not Required	115
5.6	Article 32 Security and Controls: Technical, Physical, and Organisational	116
5.6.1	Summary of Controls for Controllers	116
5.6.2	What Do Enterprises Need to Consider in Implementing Controls?	116
5.6.3	Technical Controls	117

Table of Contents

5.6.4	Organisational Measures	118
5.6.5	Physical Security	118
CHAPTER 6		
	Data Protection Impact Assessments	121
6.1	Asset Type	125
6.2	DPO Involvement	125
6.3	Stages	126
6.4	Identify Data Protection and Related Risks	127
CHAPTER 7		
	Retention of Data and the Right to Erasure	133
7.1	The Meaning of Storage in Processing	135
7.2	<i>Google Spain</i> and the Right to Be Forgotten	136
7.3	Principles of Data Protection and Data Retention	137
7.4	The Right to Erasure Explained	139
7.5	Writing a Data Storage, and Erasure: Retention Policy	141
	7.5.1 Scope	141
7.6	Classification	142
7.7	Purpose of Retention	143
7.8	Policy for Managing Personal Data in Record Keeping	145
7.9	Principles for Retaining Data	146
7.10	Record Creation	146
7.11	Record Retention and Maintenance	146
	7.11.1 Retention Based on One of the Five Exceptions in Article 17(3)	147
	7.11.2 Assessing the Value of Records	147
7.12	Data Retention Rules for Processors	147
7.13	Secure Disposal of Records	147
7.14	European Court of Human Rights Cases on Data Retention	149
CHAPTER 8		
	Data Protection by Design and Default	153
8.1	What Is Meant by Privacy by Design and by Default?	153
	8.1.1 The Ontario Principles	154
8.2	DPbDD: The Principles	156
	8.2.1 Demonstrate Compliance with the Principles: Accountability	159
8.3	Pseudonymising of Personal Data	160
8.4	Certification Mechanisms	160
8.5	Technical and Organisational Controls in Software Development	160
8.6	Software Design and Development: Our Experience	162
CHAPTER 9		
	Data Subject Rights	167
9.1	Introduction: Data Subject Rights Are Mandatory	167

9.2	Transparency in Articles 13 and 14	168
9.2.1	Transparency and Writing Privacy Notices	168
9.3	Subject Access Requests SARs and the Article 15 Requirements	171
9.3.1	Restricting Rights and Freedoms and Article 23	173
9.3.2	Opening a Request and Whether a Controller Can Reject a SAR	175
9.3.3	Receiving a SAR What to Do	176
9.3.4	Identifying the Data Subject for the SAR	176
9.3.5	Communication with the Data Subject	179
9.3.6	Searching and Communicating with Data Subjects	180
9.3.7	Requirements for Communication with Data Subjects	182
9.3.8	Making the Records Available to the Data Subject	183
9.3.9	Methods for Redacting Documents	184
9.4	Right to Portability	184
9.5	Article 16: Rectification	186
9.6	Erasure: Article 17 and the Right to Be Forgotten	187
9.7	Article 18: Restriction	188
9.8	Right to Object	189
CHAPTER 10		
	Automated Decision-Making and Profiling Technologies	191
10.1	Introduction to Big Data and Machine Learning	191
10.2	Big Data under GDPR	192
10.2.1	What Is Big Data?	193
10.2.2	Personal Data Processing in Research Falling under Article 89	193
10.2.3	Processing Big Data in Commercial Applications	194
10.3	What Is Artificial Intelligence?	195
10.4	Common Types of Algorithms	196
10.5	Designing Machine Learning, Data Mining and AI Processes	199
10.5.1	Stages in the Data Lifecycle	199
10.5.2	'Automated Decision-Making Including Profiling' under Article 22	201
CHAPTER 11		
	Children's Data under the GDPR	203
11.1	Introduction to Children's Rights	203
11.2	Why Are Children Considered Vulnerable under the GDPR?	209
11.3	General Rules for Processing Children's Data	211
11.4	Information Society Services	213
11.5	Schools	215
11.6	COVID-19 and Health Matters	216
11.7	Biometrics Cases on Children Before the ECHR	216
11.8	Regulators Focus on Processing Children's Data	218
11.8.1	CCTV and Home Learning	218

Table of Contents

11.9	Biometrics and Children	219
11.10	Facial Recognition and Children	220
11.11	Publishing Children's Photos and School Teachers' Personal Data Online	221
11.12	Apps Evaluating Teachers	224
11.13	Surveys Collecting Children's Personal Data	224
11.14	Data Breaches of Children's Data	225
CHAPTER 12		
	CCTV, Video, and IP Cameras	227
12.1	The Meaning of the Terms Necessary and Proportionate in EU Law	231
12.2	CCTV and Video	233
12.3	DPbDD in Video	233
12.4	When Does the GDPR Apply to Video Surveillance Devices?	234
12.5	Key Precedent in Processing CCTV Images: The <i>Rynes</i> Case	234
12.6	Is Processing Video Images a High-Risk Process Requiring a DPIA?	236
12.7	Interaction with the Right to Privacy under Article 8 of the ECHR	237
12.8	What Information Do Controllers Need to Provide to Data Subjects?	238
	12.8.1 Transparency	238
12.9	Making CCTV GDPR Compliant	240
12.10	Webcams and Web Conferencing Software	244
12.11	Spy Cameras	244
CHAPTER 13		
	Facial Recognition and Biometrics	247
13.1	Categories of Biometrics	250
13.2	Classifying Biometric Technology	251
13.3	Data Protection Risks when Processing Biometric Data	256
13.4	Facial Recognition	257
13.5	Emerging Use Cases for Facial Recognition Software	258
	13.5.1 Detection	260
	13.5.2 Alignment	261
	13.5.3 Measurement	261
	13.5.4 Translation of Templates	261
	13.5.5 Matching	261
	13.5.6 Verification or Identification	261
	13.5.7 Principal Component Analysis	262
	13.5.8 Linear Discriminant Analysis	263
	13.5.9 Elastic Bunch Graph Matching	263
13.6	Data Protection Issues to Consider and Completing a DPIA When Deploying Facial Recognition	264
	13.6.1 Safeguards to Consider If Deploying Facial Recognition Technology	267

CHAPTER 14

Third-Country Transfers Outside the EEA	269
14.1 Transfers under an Adequacy Decision or to Inadequate Jurisdictions	269
14.2 Adequacy under the GDPR	270
14.3 Adequate Countries: Requirements	274
14.4 Non-adequate Jurisdictions the Options for Controllers	275
14.5 Binding Corporate Rules	276
14.6 Appropriate Safeguards for Transfers: Inadequate Jurisdictions <i>Pre-Schrems II</i>	278
14.7 Standard Contractual Clauses	278
14.8 <i>Schrems II</i> and European Essential Guarantees and Supplemental Measures	284
14.8.1 The <i>Schrems II</i> Decision: Judgment of the Court (Grand Chamber) of 16 July 2020	284
14.8.2 EDPB Recommendations on Supplementary Measures for International Data Transfers	287
14.8.3 The Six Steps Recommended by the EDPB	288
14.8.4 Annex II: Examples of Effective and Non-effective Transfers	290
14.8.5 Transfers for Which Supplementary Measures Are Unlikely to Be Effective	291
14.8.6 European Essential Guarantees	292
14.9 The Early Cases and DPA Decisions Based on <i>Schrems II</i>	293
14.9.1 Amazon AWS and the Conseil d'État	293
14.9.2 Microsoft and the Conseil d'État	294
14.9.3 Bavarian DPA and Mailchimp	295
14.10 Codes of Conduct and Certification Mechanisms	296
14.11 Derogations for Specific Situations	296
14.11.1 Explicit Consent	298
14.11.2 Contractual Exceptions	298
14.11.3 Important Public Interests	299
14.11.4 Legal Claims	299
14.11.5 Vital Interests	299
14.11.6 Register to Provide Information	299
14.11.7 Necessary for Compelling Legitimate Interests	299

CHAPTER 15

Data Protection of Employees in the Workplace	301
15.1 Data Protection Versus Privacy	301
15.2 Data Generated by the Employment Relationship	303
15.3 The Basics of an Employment Inventory	303
15.4 Building an Employee Inventory	306
15.5 The Impact of Article 88 of the GDPR	310
15.6 Legal Bases for Processing Employee Personal Data	312
15.7 Employee Capacity to Give Consent	313

Table of Contents

15.7.1	The ECHR on Privacy under the European Convention on Human Rights	314
15.7.2	The EDPB View on Using Consent to Process Employee Personal Data	316
15.8	Processing Is Necessary to Fulfil the Employment Contract Between the Employer and Employee	318
15.9	Processing Is Necessary for Compliance with a Legal Obligation to Which the Employer Is Subject	319
15.10	Impact of Charter of Fundamental Rights of the European Union on Legitimate Interest Assessments	320
15.11	Processing Is Necessary for the Employer's Legitimate Interests and Others	321
15.12	Processing Sensitive Employee Data	323
CHAPTER 16		
	Processing Employee Health Data	325
16.1	Processing Employees' Health Data and Working from Home	326
16.2	Temperature Control and Access Technology in the Workplace	327
16.3	Employees and Temperature Screening	328
16.4	How Temperature Screening Works	329
16.5	Risks That Should Be Considered in the DPIA	332
16.6	The EDPB Guidance for Employers on COVID-19	332
16.7	Member State Regulators Views on Temperature Checks	335
CHAPTER 17		
	Surveillance in the Workplace	337
17.1	Derogations for Employee Monitoring under Article 88 of the GDPR	338
17.2	The Council of Europe's Employment Data Recommendation	339
17.3	European Court of Human Rights Cases on Surveillance	339
17.4	Justifiable Use of Surveillance in an Employment Context	341
17.5	EDPS Guidelines on Assessing the Proportionality of Measures That Limit Fundamental Rights	343
17.6	Workplace Monitoring for Loss Prevention	344
17.7	Background Checks on Employees	345
17.8	Data Loss Prevention in the Workplace	346
17.9	Monitoring the Social Media of Prospective, Current, and Former Employees	347
17.10	Transparency and AUP of IT Resources	347
17.11	The Obligation to Provide Information to the Data Subject	349
17.12	Recommended Minimum Content for an Employers Policy on Monitoring Email	349
17.13	Recommended Minimum Content for a Policy on Monitoring Internet Use	350

17.14	Principles Relating to Internet Monitoring	350
17.15	Where Employee Monitoring May Not Be Legitimate	351
17.16	Bring Your Own Device Policies	352
	Table of Cases	355