

CONTENTS

Guiding Points for Data Protection Officers	xix
Abbreviations	xxv

SECTION 1 A NEW PROFESSION

1

New Role: New Impact	3
Introduction	3
The Parties	3
Personal Data Use and Compliance	4
What Data Protection Is	5
Need for Data Protection	7
Growing Importance of Data Protection	8
Data Protection Regime	15
Outward-Facing Data Protection Compliance	15
Inward-Facing Data Protection Compliance	16
A Rights-Based Regime	16
Supervisory Authority	16
Data Protection Issues	17
General Criteria for Data Processing	19
Data Protection Overview	19
Legitimate Processing	24
Key/Topical Issues, Cases, and Legislation	24
Categories of Personal Data	31
General Personal Data	32
Sensitive Personal Data	32
Conclusion	36

2	New Profession	37
	Introduction	37
	Designation of the Data Protection Officer	39
	Independence	39
	Cannot Be Dismissed or Penalized for Doing Job	40
	Reporting Line	41
	Data Protection Officer	42
	Qualifications and Expertise of the Data Protection Officer	44
	Independent in Role and Functions	45
	Resources	45
	Description	45
3	New Role in Organizations	47
	Introduction	47
	Data Protection Officer	47
	Position of the Data Protection Officer	48
	Tasks of the Data Protection Officer	49

SECTION 2 THE REGULATION

4	New Data Protection Regime	53
	General Data Protection Regulation Sections	53
	General Data Protection Regulation Chapters	54
	General Provisions	55
	Principles	55
	Rights of the Data Subject	55
	Controller and Processor	57
	Transfer to Third-Party Countries or International Organizations	59
	Independent Supervisory Authorities	59
	Cooperation and Consistency	60
	Cooperation	60
	Consistency	61
	European Data Protection Board	61
	Remedies, Liability, and Sanctions	62
	Provisions for Specific Data Processing Situations	62
	Delegated Acts and Implementing Acts	63
	Final Provisions	63

SECTION 3 ROLE

5	Role, Obligations, and Position	67
	Introduction	67
	New Role of Data Protection Officer	67
	Role and Position	68
	Independent in Role and Tasks	68
	Resources	69
	Group Data Protection Officer	69
	Contact Details	70
	Reporting	70
6	Independence Needed	71
	Independence	71
	Instructions Regarding Tasks	71
	Cannot Be Dismissed or Penalized for Performing Tasks and Functions	72
	Report to Highest Management Level	72
7	Relationship with the Management Board	75
	The Management Board in General	75
	Reporting to Management Level	75
	Promoting Data Protection to the Management Board	76
8	Relationship with Management Director Responsible for Data Protection	81
	Management Director	81
9	Relationship with Information Technology	83
	Data Protection Officer and the Information Technology Function	83
10	Relationship with Product Development	89
	Product Development	89

11	Relationship with Human Resources	91
	Human Resources	91
12	Obligation to Maintain Records and Documentation	93
13	Staff Training Guides	97
	Staff Training	97

SECTION 4 TASKS

14	Tasks	101
	Tasks under the New Regulation	101
	Tasks Required by the New Regulation	103
	Explicit Required Tasks under the New Regulation	103
	Implicit Required Tasks under the New Regulation	104
	Further Implicit Required Tasks	107
15	Tasks in Detail	119
	Explicit Required Tasks	119
	Advising on Obligations	119
	Inform and Advise the Controller of Their Data Protection Obligations	119
	Inform and Advise the Processor of Their Data Protection Obligations	120
	Inform and Advise Employees of Their Data Protection Obligations	121
	Monitor Compliance	123
	Monitor Compliance with Data Protection Rules	123
	Monitor Compliance of with Other EU Data Protection Rules	123
	Monitor Compliance with National Data Protection Rules	124
	Monitor Compliance of the Policies with Data Protection	124
	Monitor Assignment of Responsibilities	125
	Awareness-Raising of the Controller/Processor	126

Awareness-Raising of Staff	126
Training of the Controller/Processor	127
Training of Controller/Processor Employees Involved in Processing Operations	127
Internal Audits	127
Advising on Data Protection Impact Assessments	129
Provide Advice on Data Protection Impact Assessments	129
Cooperate with the Supervisory Authority	129
Cooperate with the Supervisory Authority	129
Contact for the Supervisory Authority	130
Being the Contact Point for the Supervisory Authority on Personal Data	130
Being the Contact Point for the Supervisory Authority on Prior Consultation	131
Consulting with Supervisory Authority on Any Other (Data Protection) Matters	131
Consulting on Any Other (Data Protection) Matters	131
Due Regard to the Risk Associated with Processing	132
Implicit Required Tasks of the New Regulation	132
All Data Protection Issues	132
Maintain Proper and Timely Involvement in All Data Protection Issues	132
Champion and Ensure Adequate Resources	133
Performing Tasks with Resources Necessary to Carry Out These Tasks	133
Accessing Personal Data and Processing Operations	133
Access to Personal Data and Processing Operations	133
Maintaining Expertise	134
Maintain Expert Knowledge	134
Contact Point for Data Subjects	134
Be the Contact Point for Data Subjects on All Issues Related to the Processing of the Data Subject's Data	134
Be the Contact Point for Data Subjects on All Issues Related to the Exercise of Their Rights	134
Avoiding Instructions on Tasks	135
Ensure That No Instructions Regarding the Exercise of Tasks Are Received	135
Avoiding Dismissal/Discipline on Tasks	135
Ensuring That Any Dismissal or Similar Actions Do Not Relate to Data Protection Officer Tasks (Which Are Protected)	135
Report Directly to Highest Management	136
Ensure Direct Reporting to the Highest Management Level of the Controller/Processor	136

xii Contents

Risk Issues	136
Avoid Conflicts	137
Ensure No Conflict of Interest between Data Protection Tasks and Any Other Tasks and Duties	137
Further Implicit Required Tasks	138
Compliance with the Data Protection Principles	138
Compliance with the Rights of Data Subjects:	
Transparency and Modalities	139
Transparent Information and Communication	139
Compliance with Rights of Data Subjects: Information and Access to Data	142
Information to the Data Subject	142
Right of Access for the Data Subject	142
Compliance with Rights of Data Subjects: Rectification and Erasure	146
Right to Rectification	146
Right to Erasure (Right to Be Forgotten)	146
Right to Data Portability	149
Compliance with Rights of Data Subjects: Right to Object and Profiling	149
Right to Object	149
Measures Based on Automated Decisions and Profiling	150
Compliance with Rights of Data Subjects: Restrictions	151
Restrictions	151
Compliance with Controller and Processor: General Obligations	151
Responsibility of the Controller	151
Data Protection Principles	157
Data Protection by Design and by Default	159
Joint Controllers	165
Representatives of Controllers or Processors Not Established in the Union	165
Processor	165
Processing under the Authority of the Controller and Processor	167
Records	168
Cooperation with the Supervisory Authority	170
Compliance with the Controller and Processor: Data Security	170
Security of Processing	170
Notification of a Personal Data Breach to the Supervisory Authority	171
Communication of a Personal Data Breach to the Data Subject	172

Compliance with Controller and Processor: Data Protection Impact Assessment and Prior Authorization	174
Data Protection Impact Assessments	174
Prior Consultation	182
Compliance with the Controller and Processor: Data Protection Officer	183
Compliance with the Controller and Processor: Codes of Conduct and Certification	183
Compliance with Transfer of Personal Data to Third-Party Countries or International Organizations	185
Compliance with Remedies, Liability, and Sanctions	186
Compliance with Provisions Relating to Specific Data Processing Situations	187
Additional and/or More Specific Tasks	188
Training	188
Policies	189
Drafting Data Protecting Policies	189
Implementing Data Protection Policies	189
Updating Data Protection Policies	189
Reviewing Other Policies in Relation to Data Protection Sections and Issues	189
Contracts, Terms, and So On	190
Reviewed Data Protection Terms, References and Clauses in the Organization's Contracts, Terms, and So On	190
Existing IT Projects and Processing	190
Reviewing and Engaging in Existing IT Projects as Regards the Impact on Personal Data and Data Processing Compliance Issues and Risks	190
New IT Projects and Processing	191
Reviewing and Engaging in New IT Projects as Regards the Impact on Personal Data and Data Processing Compliance Issues and Risks	191
Access Requests (Additional)	191
Queries	192
Being the Point of Contact for Data Access Queries and Requests	192
Point of Contact	193
Communications	193
Audits (Internal)	194
Audits	194
Audits (By Supervisory Authorities)	195
Audits	195
Audits (Of New Proposed Products and Services)	195

Audits	195
Employment Contract of the Data Protection Officer	196
Recitals on the GDPR	196
Main Articles of the GDPR	197
European Data Protection Supervisor	198
Adequate Staff and Resources	199
Information and Awareness-Raising Function	199
Advisory Function	199
Organizational Function	200
Cooperative Function	200
Monitoring of Compliance	201
Handling Queries and Complaints	201
Guaranteeing Independence	202
No Conflict of Interest between Duties	202
Staff and Resources to Carry Out Duties	203
No Receipt of Instructions Regarding the Performance of Duties	203
Access to Information and to Offices and Data-Processing Installations	203
Ensuring Compliance	204
Keeping Controllers and Data Subjects Informed of Rights and Obligations	204
Access to Data	205
Prior Notice of Processing	205

SECTION 5 TOOLS OF THE DATA PROTECTION OFFICER

16	Tools of the Data Protection Officer	209
	Introduction	209
	Advantages of Data Protection Officers	209
	Significant Cost of Getting Data Protection Wrong	211
	Fines and Penalties	213
	Director and Officer Responsibility	216
	Data Subject Actions	216
	Organizational Data Subject Groups	220

17	Accessing the Data Sources	221
	Sources and Locations of Personal Data	221
	Sample Audit Inventory Queries	221

Customers/Clients	222
Employees	222
Sensitive Personal Data	223
Service Application Forms	223
Third-Party Requests for Disclosure	224
Staff Training and Awareness	224
Marketing	225
Customers	225
Prospective Customers	225
Project Management Activities	226
Information and Knowledge Management Practices	226
Contracts with Data Processors	226
Access Requests	226
Computer Systems and Security	227
Personal Computers of Employees	227
Removable Media	227
Network Security	228
Biometrics	228
CCTV	228
Personal Data Inventory Tool	229

18

Tools and Access Rights 233

Access Right	233
Confirmation Right Regarding Personal Data	234
Access Rights Regarding Personal Data	235
Considering an Access Request	236
Dealing with Access Requests	236
Response to Access Request	237

19

Records and Documentation Issues 241

Records and Documentation	241
---------------------------	-----

20

Engaging Processors 247

Processors	247
------------	-----

21

Tools and Data Protection by Design and by Default 257

Data Protection by Design and by Default	257
Sample Tools	261
Recommendations	263

22	Security and Data Breach Tools	265
	Data Breach	265
	Notification Processes	265
	Security Standards	268
	Incident Response	270
	Breach and Security	271
23	Data Protection Impact Assessment Tools	273
	Data Protection Impact Assessment Obligation	273
	Identifying When to Undertake a Data Protection Impact Assessment	274
	Key Characteristics of Data Protection Impact Assessment	279
	Key Elements of Data Protection Impact Assessment Report	281
	Some Key Steps and Methodologies	281
	Some Data Protection Impact Assessment Issues	282
	Regular Monitoring	283
24	Prior Consultation	285
25	Data Breach	289
	Data Breaches	289
	Be Prepared	291
	Why Being Prepared and Aware Is Important	292
	Team	292
	Lead Coordinator	292
	Reporting	293
	Board Level Responsibility	293
	IT/IT Security	293
	Legal and Privacy	294
	Public Relations	294
	Customer Relations	295
	Employees and Human Resources	295
	Police and Law Enforcement	295
	Providers of Breach Resolution Services	296
	Training and Preparing for Breach Incidents	296
26	Sample Data Protection Officer Datasets	299
	Sample Data Protection Officer Datasets	299

27

Model Tips and Guidelines for the Role and Tasks	303
Model Tips and Guidelines	303
Data Protection Officers: Preparing for the New GDPR Legal Regime	311
New Data Protection Officers	312
Appendix	315
Index	363



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>