

CONTENTS

Introduction	1
The purpose of the GDPR.....	2
Structure of the Regulation	3
Impact on the EU	4
Implementing the GDPR.....	6
A note on the UK and Brexit	8
Key definitions.....	9
Part 1: Core considerations for the GDPR	13
Chapter 1: Scope, controllers and processors	15
Scope of the GDPR.....	15
Controller and processor	17
Data controllers	17
Joint controllers.....	20
Data processors	20
Controllers that are processors.....	22
Controllers and processors outside the EU	22
Records of processing	24
Demonstrating compliance	28
Chapter 2: Data processing principles	31
Principle 1: Lawfulness, fairness and transparency	33
Principle 2: Purpose limitation.....	40
Principle 3: Data minimisation	41
Principle 4: Accuracy.....	43
Principle 5: Storage limitation	45
Principle 6: Integrity and confidentiality	47
Accountability and compliance.....	48
Chapter 3: Data subjects' rights	53
Fair processing	54
The right to access	56
The right to rectification	58

Contents

The right to be forgotten	58
The right to restriction of processing	61
The right to data portability	63
The right to object.....	65
Rights in relation to automated decision-making	66
Part 2: Building compliance.....	69
Chapter 4: Privacy compliance frameworks.....	71
Material scope	75
Territorial scope	76
Governance	78
Objectives	80
Key processes.....	82
Personal information management systems.....	87
ISO/IEC 27001:2013	91
Selecting and implementing a compliance framework	98
Implementing the framework.....	100
Chapter 5: Information security as part of data protection	105
Personal data breaches	107
Anatomy of a data breach	108
Sites of attack.....	109
Securing your information	110
ISO 27001	111
NIST standards.....	112
Ten Steps to Cyber Security	113
Cyber Essentials.....	114
The information security policy	115
Assuring information security.....	116
Governance of information security	117
Information security beyond the organisation's borders.....	119
Chapter 6: Lawfulness and consent	121

Contents

Consent in a nutshell	122
Withdrawing consent	125
Alternatives to consent.....	126
Practicalities of consent	129
Children.....	131
Special categories of personal data	134
Data relating to criminal convictions and offences.....	135
Chapter 7: Subject access requests	137
Receiving a request	138
The information to provide	138
Data portability	140
Responsibilities of the data controller.....	141
Processes and procedures.....	142
Options for confirming the requester's identity	144
Records to examine.....	147
Time and money	148
Dealing with bulk subject access requests	149
Right to refusal.....	149
The process flow	150
Chapter 8: Role of the data protection officer	153
Voluntary designation of a data protection officer	159
Undertakings that share a DPO.....	160
DPO on a service contract.....	161
Publication of DPO contact details	163
Position of the DPO	164
Necessary resources	166
Acting in an independent manner	167
Protected role of the DPO	169
Conflicts of interest.....	170
Specification of the DPO	171
Duties of the DPO	174
The DPO and the organisation.....	178
The DPO and the supervisory authority.....	180

Contents

Data protection impact assessments and risk management	181
In-house or contract	182
Chapter 9: Data mapping.....	185
Objectives and outcomes	186
Four elements of data flow	187
Data mapping, DPIAs and risk management.....	188
Part 3: Data protection impact assessments and risk management.....	195
Chapter 10: Requirements for data protection impact assessments.....	197
DPIAs.....	199
Consulting with stakeholders.....	210
Who needs to be involved?.....	211
Data protection by design and by default	213
Chapter 11: Risk management and DPIAs	217
DPIAs as part of risk management	218
Risk management standards and methodologies	218
Risk responses.....	229
Risk relationships.....	231
Risk management and personal data.....	233
Chapter 12: Conducting DPIAs.....	235
Five key stages of the DPIA	236
Identify the need for the DPIA.....	236
Objectives and outcomes	238
Consultation	240
Describe the information flow	243
Identify privacy and related risks.....	244
Identify and evaluate privacy solutions	247
Sign off and record the outcome.....	250
Integrating the DPIA into the project plan.....	252
Part 4: International transfers and incident management.....	253

Contents

Chapter 13: Managing personal data internationally	255
Key requirements	257
Adequacy decisions	258
Safeguards.....	260
Binding corporate rules.....	263
Standard contractual clauses	263
Limited transfers	265
Cloud services.....	265
Chapter 14: Incident response management and reporting	267
Notification	268
Events vs incidents.....	271
Types of incident.....	272
Cyber security incident response plans.....	273
Key roles in incident management.....	275
Prepare	276
Respond.....	277
Follow up	279
Part 5: Enforcement and transitioning to compliance	283
Chapter 15: GDPR enforcement	285
The hierarchy of authorities	285
One-stop-shop mechanism.....	287
Duties of supervisory authorities	288
Powers of supervisory authorities	289
Duties and powers of the European Data Protection Board	290
Data subjects' rights to redress	291
Administrative fines.....	292
The Regulation's impact on other laws	296
Chapter 16: Transitioning and demonstrating Compliance	299

Contents

Transition frameworks	299
Using policies to demonstrate compliance	301
Codes of conduct and certification mechanisms.....	306
Appendix 1: Index of the Regulation	309
Appendix 2: EU/EEA national supervisory authorities	317
Appendix 3: Implementation FAQ.....	321
IT Governance resources	385
Publishing services.....	385
Certified GDPR training and staff awareness.....	387
IT Governance training centre	387
Professional services and consultancy	389
Newsletter	390