

CONTENTS

Introduction.....	11
The purpose of the GDPR.....	12
Structure of the Regulation	13
Impact on the EU	14
Implementing the GDPR.....	15
Key definitions.....	18
Chapter 1: Privacy Compliance Frameworks.....	23
Material scope.....	27
Territorial scope	28
Governance	30
Objectives	32
Key processes.....	34
Personal information management systems.....	39
ISO/IEC 27001:2013	41
Selecting and implementing a compliance framework...48	
Implementing the framework.....	50
Chapter 2: Role of the Data Protection Officer	53
Voluntary designation of a Data Protection Officer	58
Undertakings that share a DPO.....	59
DPO on a service contract.....	61
Publication of DPO contact details	62
Position of the DPO	63
Necessary resources	64
Acting in an independent manner	66
Protected role of the DPO	67
Conflicts of interest.....	69
Specification of the DPO	71
Duties of the DPO.....	73
The DPO and the organisation.....	78
The DPO and the supervisory authority.....	79

Contents

Data protection impact assessments and risk management	80
In house or contract.....	81
Chapter 3: Common Data Security Failures.....	83
Personal data breaches	85
Anatomy of a data breach	86
Sites of attack.....	87
Securing your information	88
ISO 27001	89
Ten Steps to Cyber Security	90
Cyber Essentials.....	91
NIST standards.....	92
The information security policy	93
Assuring information security.....	94
Governance of information security	95
Information security beyond the organisation's borders	96
Chapter 4: Six Data Protection Principles.....	98
Principle 1: Lawfulness, fairness and transparency	100
Principle 2: Purpose limitation.....	108
Principle 3: Data minimisation	109
Principle 4: Accuracy.....	111
Principle 5: Storage limitation	113
Principle 6: Integrity and confidentiality	114
Accountability and compliance.....	116
Chapter 5: Requirements for Data Protection Impact Assessments	121
Data protection impact assessments.....	123
When to conduct a DPIA	131
Who needs to be involved.....	136
Data protection by design and by default	137
Chapter 6: Risk Management and DPIAs	142
DPIAs as part of risk management	143
Risk management standards and methodologies	143

Contents

Risk responses.....	154
Risk relationships.....	157
Risk management and personal data.....	158
Chapter 7: Data Mapping	159
Objectives and outcomes	160
Four elements of data flow	161
Data mapping, DPIAs and risk management	162
Chapter 8: Conducting DPIAs.....	170
Reasons for conducting a DPIA.....	171
Objectives and outcomes	172
Consultation	175
Five key stages of the DPIA	177
Integrating the DPIA into the project plan.....	186
Chapter 9: Data Subjects' Rights	189
Fair processing	190
The right to access	192
The right to rectification	194
The right to be forgotten	195
The right to restriction of processing	198
The right to data portability	200
The right to object.....	202
The right to appropriate decision making	203
Chapter 10: Consent	206
Consent in a nutshell.....	207
Withdrawing consent	210
Alternatives to consent.....	211
Practicalities of consent	214
Children.....	217
Special categories of personal data	220
Data relating to criminal convictions and offences.....	220
Chapter 11: Subject Access Requests	222
The information to provide	224
Data portability	225

Contents

Responsibilities of the data controller.....	227
Processes and procedures.....	228
Options for confirming the requester's identity.....	229
Records to examine.....	232
Time and money	233
Dealing with bulk subject access requests	234
Right to refusal.....	235
Chapter 12: Controllers and Processors.....	236
Data controllers.....	236
Joint controllers.....	238
Data processors	239
Controllers that are processors.....	240
Controllers and processors outside the EU	241
Records of processing.....	243
Demonstrating compliance	247
Chapter 13: Managing Personal Data Internationally	249
Key requirements	250
Adequacy decisions	252
Safeguards.....	254
Binding corporate rules.....	256
The EU-US Privacy Shield	257
Privacy Shield Principles	260
Limited transfers	262
Cloud services.....	262
Chapter 14: Incident Response Management and Reporting	265
Notification	266
Events vs incidents.....	269
Types of incident.....	270
Cyber security incident response plans.....	271
Key roles in incident management.....	273
Prepare	274

Contents

Respond.....	275
Follow up	277
Chapter 15: GDPR Enforcement	280
The hierarchy of authorities	280
One-stop-shop mechanism.....	282
Duties of supervisory authorities	283
Powers of supervisory authorities.....	284
Duties and powers of the European Data Protection Board	285
Data subjects' rights to redress	286
Administrative fines.....	288
The Regulation's impact on other laws	291
Chapter 16: Transitioning and Demonstrating Compliance	294
Transition frameworks	294
Transition – understanding the changes from DPD to GDPR.....	296
Using policies to demonstrate compliance	299
Codes of conduct and certification mechanisms.....	304
Appendix 1: Index of the Regulation	306
Appendix 2: EU/EEA National Supervisory Authorities	313
Appendix 3: Implementation FAQs	317
ITG Resources.....	377