

Contents

<i>Table of Cases</i>	xv
<i>Table of UK Legislation</i>	xvii
<i>Table of UK Secondary Legislation</i>	xxiii
<i>Table of European and International Legislation</i>	xxv
<i>Contributing Authors' Biographies</i>	xxvii
<i>List of Abbreviations</i>	xxxi
<i>Introduction</i>	xxxiii
1. Territorial Scope and Terminology	1
<i>Damien Welfare and Peter Carey</i>	
Introduction and Historical Perspective	2
Territorial Scope	5
Introduction to Terminology	7
Personal Data	8
Processing	15
Filing System	16
Controller	18
Processor	19
Special Categories of Personal Data	20
European Economic Area	21
Main Establishment	21
Data Subject	22
Pseudonymization	23
Profiling	23
Personal Data Breach	24
The Data Subject's Consent	24
Child	24
Genetic Data	25
Biometric Data	25
Recipient	25
Data Protection by Design	26
Data Protection by Default	26
Codes of Conduct	26
Joint Controllers	27
European Data Protection Board	27
Delegated Acts	28
Certification	28
One Stop Shop	29
Directive on Security of Network and Information Systems	30
Directive on Personal Data Processed for Criminal Law Enforcement	31

2. Data Protection Principles	32
<i>Peter Carey</i>	
Introduction	32
Lawfulness, Fairness, and Transparency	33
Purpose Limitation	34
Data Minimization	35
Data Accuracy	37
Storage Limitation	38
Integrity, Confidentiality, and Security	39
Exemptions	40
Accountability	40
Data Protection by Design and by Default	41
Processors	41
3. Fair, Lawful, and Transparent Processing	42
<i>Estelle Dehon and Peter Carey</i>	
Introduction	42
Obtaining Data—Duty Not to Mislead	43
Obtaining Data in a Transparent Manner—Information to Be Supplied to the Data Subject	44
Other Unfair Processing	50
The Lawfulness Conditions	50
Other Unlawful Processing	59
Cases of Significance	61
Summary	65
4. Special Categories of Data	66
<i>Nicola Fulford and Peter Carey</i>	
Introduction	66
The Conditions for Processing	69
Personal Data Relating to Criminal Convictions and Offences	81
Advice on Processing Special Category Personal Data	83
5. Data Security and Breach Notifications	88
<i>Ann Bevitt and Peter Carey</i>	
Introduction	88
Obligations of the Controller and Processor	91
Privacy by Design and Privacy by Default	95
Pseudonymization	96
Privacy Enhancing Technologies	97
ISO 27001	97
Security and Outsourcing	98
Security and Exports	98
Security Breaches	98
Notifying Security Breaches	100
Advice on Breach Notification	104

6. International Data Transfers	105
<i>Eduardo Ustaran</i>	
Introduction	105
Examples of International Transfers	107
Scope of Data Transfers	108
Adequate Level of Protection	108
Transfers to the United States—Privacy Shield	110
Providing Adequacy Safeguards	114
The Contractual Route	115
Codes of Conduct and Certification Mechanisms	116
Binding Corporate Rules	117
The Derogations	119
Non-repetitive Transfers	121
Advice for Organizations	121
7. The Rights of Individuals	122
<i>Heledd Lloyd-Jones and Peter Carey</i>	
Introduction	122
Responding to Individuals	123
Exemptions	125
The Right of Access	126
Data Portability	137
Rectification	139
Rights to Object	140
The Right to Object to Direct Marketing	140
Right to Erasure	143
Right to Restriction of Processing	147
Automated Decision-taking	149
Compensation	151
Right to a Judicial Remedy	153
Complaints to the Commissioner	154
8. Enforcement and the Role of the Regulator	155
<i>Alison Deighton and Peter Carey</i>	
Introduction	155
Supervisory Authority Enforcement Role	156
Other Remedies	162
Consistency Mechanism	162
Cross-border Processing and Appointing a Lead Authority	163
UK Enforcement Action	166
UK Enforcement Procedures	166
Information Notice	167
Assessment Notice	169
Enforcement Notice	170
Monetary Penalty Notices	171

Appeals	173
Powers of Entry and Inspection	173
9. Outsourcing Personal Data Processing	175
<i>Suzanne Rodway and Peter Carey</i>	
Introduction	175
The Nature of a Processor	177
Obligations on Processors	178
Choice of Processor	179
Ongoing Assurance	179
The Written Contract	180
Pre-GDPR Arrangements	181
Sub-processors	181
Processor Versus Controller	182
Cloud Services	183
Foreign Processors	183
10. Electronic Communications	184
<i>Peter Given and Peter Carey</i>	
Introduction and Historical Background	184
Definitions	186
Email Marketing	189
Text Message Marketing	194
Telephone Marketing	195
Fax Marketing	196
Location Data	197
Cookies and Similar Devices	198
Limitations on Processing of Traffic Data	200
Calling and Connected Line Identification	200
Telephone Directories	202
Non-itemized Bills	202
Termination of Unwanted Call Forwarding	202
Security	202
Breach Notification	203
Enforcement	203
11. Data Protection Impact Assessments	205
<i>Olivia Whitcroft</i>	
Introduction	205
What Is a DPIA?	206
When to Carry Out a DPIA	207
Identifying Whether a DPIA Is Required	210
Who Should Carry Out a DPIA	211
How to Conduct a DPIA	212
Reporting and Publication of the DPIA	221

12. Accountability and the Role of the Data Protection Officer	223
<i>Jenai Nissim</i>	
Introduction	223
The Accountability Requirement	224
The Role of the DPO	226
When Is a DPO Mandatory?	226
Accessibility	231
Expertise and Skill of the DPO	233
Involvement of the DPO	234
Necessary Resources	235
Independence	236
Security of Tenure	236
Conflict of Interest	237
Data Protection Impact Assessments	238
Record Keeping	238
Policies and Procedures	239
13. Creating a Data Protection Compliance Programme	240
<i>Jenai Nissim</i>	
Introduction	240
Stage 1—Assessing Data Processing Activities	241
Stage 2—Creating Data Protection Policies	242
Stage 3—Data Protection Training and Raising Awareness	244
Stage 4—Implementing Controls to Reduce and Monitor Risk	246
Stage 5—Monitoring Compliance	248
Stage 6—Reporting	249
Stage 7—Annual Review Process	249
<i>Appendix 1: Regulation (EU) 2016/679 of the European Parliament and of the Council</i>	251
<i>Appendix 2: Addresses and Websites</i>	351
<i>Index</i>	355