

For European data protection professionals, the Certified Information Privacy Professional/Europe (CIPP/E®) is the preeminent professional credential and is part of a comprehensive, principles-based framework and knowledge base in data protection. The CIPP/E encompasses pan-European and national data protection laws, the European model for data protection, key data protection terminology, and practical concepts concerning the protection of personal data and cross-border data transfers.

European Data Protection: Law and Practice examines the territorial and material scope of the GDPR, legitimate processing criteria, information provision obligations, data subject rights, security of processing, accountability requirements, and supervision and enforcement. This second edition also includes updated information about GDPR enforcement actions, along with guidance – relative to GDPR regulations – from authorities and regulators, including the European Data Protection Board (EDPB).

Developed by the International Association of Privacy Professionals (IAPP), in association with data protection professionals, the CIPP/E is and continues to be the benchmark credential for European data protection and privacy. *European Data Protection: Law and Practice, Second Edition* is the principal reference for those working in this field, including data protection officers (DPOs) and CIPP/E candidates.



Global co-head of the Hogan Lovells Privacy and Cybersecurity practice, **Eduardo Ustaran** is widely recognised as one of the world's leading privacy and data protection lawyers and thought leaders. With over two decades of experience, Ustaran advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies. Ustaran has been involved in the development of the EU data protection framework and was listed by *Politico* as the most prepared individual in its 'GDPR power matrix'. Ustaran is co-founder and editor of *Data Protection Leader*, a member of the panel of experts of DataGuidance, and a former member of the Board of Directors of the IAPP. He is the author of *The Future of Privacy* (DataGuidance, 2013) and co-author of *Data Protection: A Practical Guide to UK and EU Law* (OUP, 2018), *Beyond Data Protection* (Springer, 2013), *E-Privacy and Online Data Protection* (Tottel Publishing, 2007) and the *Law Society's Data Protection Handbook* (2004). Ustaran has lectured at the University of Cambridge on data protection as part of its Master of Bioscience Enterprise programme and regularly speaks at international conferences.

Contributing Authors:

Ruth Boardman
James Fenelon, CIPP/E
Mariel Filippidis, CIPP/E, CIPM, FIP
Victoria Hordern, CIPP/E, CIPT
Hannah Jackson, CIPP/E
Mac Macmillan
Katie McMullan
Mary Pothos
Stewart Room, CIPP/E
Sian Rudgard, CIPP/E
Jyn Schultze-Melling
Wouter Seinen, CIPP/E
Robert Streeter, CIPP/E, CIPP/US
Lilly Taranto, CIPP/E
Nicholas Westbrook

An **iapp** publication

iapp.org



iapp

Second Edition

EUROPEAN DATA PROTECTION

EUROPEAN Data Protection Law and Practice

Second Edition

Executive Editor
Eduardo Ustaran, CIPP/E
Partner, Hogan Lovells



An **iapp** publication

Contents

About the IAPP	<i>ix</i>
Acknowledgments	<i>xi</i>
<i>Marla Berry, CIPT</i>	
Introduction	<i>xv</i>
<i>Paul Jordan</i>	
<u>SECTION I INTRODUCTION TO EUROPEAN DATA PROTECTION</u>	
Chapter 1: Origins and Development of European Data Protection Law	
<i>Sian Rudgard, CIPP/E</i>	
1.1 Rationale for data protection	3
1.2 Human rights law	4
1.3 Early laws and regulations	7
1.4 The need for a harmonised European approach	13
1.5 The Treaty of Lisbon	16
1.6 The General Data Protection Regulation	17
1.7 Convention 108+	18
1.8 Related Legislation	19
1.9 Brexit	20
Chapter 2: European Union Institutions	
<i>Lilly Taranto, CIPP/E</i>	
2.1 Background	27
2.2 European Parliament	29
2.3 European Council	32
2.4 Council of the European Union	33
2.5 European Commission	34

2.6 Court of Justice of the European Union.....	36
2.7 European Court of Human Rights.....	39
Chapter 3: Legislative Framework	
<i>Katie McMullan</i>	
3.1 Background.....	45
3.2 The Council of Europe Convention.....	45
3.3 The Data Protection Directive.....	47
3.4 The General Data Protection Regulation.....	52
3.5 The Law Enforcement Data Protection Directive.....	57
3.6 The Privacy and Electronic Communications Directive.....	58
3.7 The directive on security of network and information systems.....	64
3.8 The Data Retention Directive.....	65
3.9 Impact on member states.....	65
<u>SECTION II EUROPEAN DATA PROTECTION LAW AND REGULATION</u>	
Chapter 4: Data Protection Concepts	
<i>Mac Macmillan</i>	
4.1 Introduction.....	73
4.2 Personal data.....	73
4.3 Sensitive personal data.....	79
4.4 Controller and processor.....	80
4.5 Processing.....	88
4.6 Data subject.....	88
4.7 Conclusion.....	89
Chapter 5: Territorial and Material Scope of the General Data Protection Regulation	
<i>Ruth Boardman and James Fenelon, CIPP/E</i>	
5.1 Introduction.....	91
5.2 Territorial scope.....	91
5.3 Material scope of regulation.....	97
5.4 Conclusion.....	101
Chapter 6: Data Processing Principles	
<i>Mariel Filippidis, CIPP/E, CIPM, FIP</i>	
6.1 Introduction.....	103
6.2 Lawfulness, fairness and transparency.....	103

Contents

6.3 Purpose limitation	107
6.4 Data minimisation.....	109
6.5 Accuracy	111
6.6 Storage limitation	112
6.7 Integrity and confidentiality.....	113
6.8 Conclusion	113
Chapter 7: Lawful Processing Criteria	
<i>Victoria Hordern, CIPP/E, CIPT</i>	
7.1 Background	117
7.2 Processing personal data	117
7.3 Processing sensitive data	129
7.4 Data on criminal convictions and offences, and security measures.....	137
7.5 Processing which does not require identification.....	138
7.6 Conclusion	138
Chapter 8: Information Provision Obligations	
<i>Hannah Jackson, CIPP/E</i>	
8.1 The transparency principle.....	141
8.2 Exemptions to the obligation to provide information to data subjects	151
8.3 The requirements of the ePrivacy Directive.....	155
8.4 Fair processing notices	156
8.5 Conclusion	162
Chapter 9: Data Subject Rights	
<i>Jyn Schultze-Melling</i>	
9.1 Background	167
9.2 The modalities – to whom, how and when	168
9.3 The general necessity of transparent communication	168
9.4 Right to information (about personal data collection and processing).....	169
9.5 Right of access	169
9.6 Right to rectification.....	171
9.7 Right to erasure ('right to be forgotten')	172
9.8 Right to restriction of processing	174
9.9 Right to data portability	176
9.10 Right to object	177

9.11 Right to not be subject to automated decision-making	179
9.12 Restrictions of data subject rights	179
9.13 Conclusion	180
Chapter 10: Security of Personal Data	
<i>Stewart Room, CIPP/E</i>	
10.1 Background	181
10.2 The security principle and the risk-based approach	184
10.3 Notification and communication of personal data breaches	189
10.4 Delivering on security	194
10.5 Incident response	206
10.6 Directive on security of network and information systems	208
10.7 Conclusion	210
Chapter 11: Accountability Requirements	
<i>Mary Pothos</i>	
11.1 Introduction and background	213
11.2 Responsibility of the controller	214
11.3 Data protection by design and by default	219
11.4 Documentation and cooperation with regulators	222
11.5 Data protection impact assessment	225
11.6 Data protection officer	227
11.7 Other accountability measures – binding corporate rules	230
11.8 Conclusion	231
Chapter 12: International Data Transfers	
<i>Eduardo Ustaran, CIPP/E</i>	
12.1 Introduction: limitations affecting international data transfers	233
12.2 Scope of data transfers	234
12.3 Meaning of an ‘adequate level of protection’	235
12.4 Procedure to designate countries with adequate protection	236
12.5 The situation in the United States	237
12.6 Providing adequate safeguards	241
12.7 Data transfers within a multinational corporate group – binding corporate rules	244
12.8 Relying on derogations	246
12.9 The future of the restrictions on international data transfers	248

Chapter 13: Supervision and Enforcement

Stewart Room, CIPP/E

13.1 Introduction 251

13.2 Self-regulation 251

13.3 Regulation by the citizen 255

13.4 Administrative supervision and enforcement 258

13.5 Competence and international cooperation 263

13.6 Sanctions and penalties 270

13.7 The Law Enforcement Data Protection Directive 276

13.8 Regulation supervision and enforcement – key provisions 276

13.9 Conclusion 281

SECTION III COMPLIANCE WITH EUROPEAN DATA PROTECTION LAW AND REGULATION

Chapter 14: Employment Relationships

Victoria Hordern, CIPP/E, CIPT

14.1 Employee data 285

14.2 Legal basis for processing employee personal data 286

14.3 Processing sensitive employee data 288

14.4 Providing notice 289

14.5 Storage of personnel records 289

14.6 Workplace monitoring and data loss prevention 290

14.7 Works councils 298

14.8 Whistle-blowing schemes 299

14.9 Bring your own device 302

Chapter 15: Surveillance Activities

Robert Streeter, CIPP/E, CIPP/US

15.1 Introduction 305

15.2 Technology 306

15.3 Regulating surveillance 307

15.4 Communications data 308

15.5 Video surveillance 310

15.6 Biometric data 314

15.7 Location data 315

15.8 Conclusion 317

Chapter 16: Direct Marketing

Wouter Seinen, CIPP/E

16.1 Data protection and direct marketing	319
16.2 Postal marketing	324
16.3 Telephone marketing	325
16.4 Marketing by electronic mail, including email, SMS and MMS	327
16.5 Fax marketing	330
16.6 Location-based marketing	331
16.7 Online behavioural advertising	333
16.8 Enforcement	337
16.9 Conclusion	338

Chapter 17: Internet Technology and Communications

Nicholas Westbrook

17.1 Introduction	341
17.2 Cloud computing	341
17.3 Cookies, similar technologies and IP addresses	348
17.4 Search engines	354
17.5 Social networking services	357
17.6 Online behavioural advertising	361
17.7 Applications on mobile devices	368
17.8 Internet of things	371
17.9 Conclusion	372

Chapter 18: Outsourcing

Eduardo Ustaran, CIPP/E

18.1 Introduction	377
18.2 The roles of the parties	378
18.3 Data protection obligations in an outsourcing contract	382
18.4 The German case	385
18.5 Offshoring and international data transfers	387
18.6 Conclusion	390

About the Contributors	393
---	------------

Index	401
------------------------	------------

Introduction

The global privacy and data protection community continues to look to Europe as its privacy regulation evolves and matures. Following the passage of the General Data Protection Regulation (GDPR, or ‘Regulation’) over a year ago, the European Union underwent a comprehensive transformation resulting in the most robust privacy and data protection regime in the world – increasingly serving as a reference worldwide. The GDPR came into being with the promise of unifying the regulatory patchwork landscape of the EU’s 28 member states. It is, however, still in its infancy, and it is therefore premature to estimate its overall impact. Nevertheless, we are witnessing a number of significant developments such as the beginnings of cross-border enforcement.

As the largest data protection and privacy organisation in the world, the International Association of Privacy Professionals (IAPP), with more than 55,000 members as of this writing, remains one of the more eminent and trusted market leaders in the provision of robust tools and information products to help privacy professionals navigate what may seem at times like stormy seas. With this new edition of the established textbook, I am confident we have, once again, provided an unimpeachable resource, that will allow professionals – be they directly active in the data protection profession or not – at every level to adequately prepare and continually adjust for what the future of the privacy field may hold.

With Eduardo Ustaran, CIPP/E, at the helm, this team of data protection experts has compiled a tome that puts the GDPR in context, brings data protection law and regulation down to the practical level, and goes beyond a simple explanation of the law. While each organisation will find its own way to operationalise compliance, this textbook is a foundation upon which everyone can build.

As with any new law, it takes time for the respective authorities and regulators to provide adequate guidance to organisations with regard to their obligations. This second edition incorporates some of the guidance that has been forthcoming with the advent of GDPR, both from the EDPB – the European Data Protection Board – as well as from the member state authorities.

We hope, too, that this textbook is just the beginning of your journey through what the IAPP has to offer. From the publications on IAPP.org to the education available at our many conferences to the valuable networking and peer-to-peer intelligence-gathering that can be done at our hundreds of KnowledgeNet meetings around the globe, there is so much available to you as you build your data protection career. We hope you take advantage.

Ultimately, each reader of this textbook will take away something different. Each organisation has its own data protection challenges that are unique to its business plan or mission. I'm happy to say that we've created something here that is both accessible and truly useful.

Good luck as you embark upon your data protection work.

Paul Jordan

Managing Director, Europe

International Association of Privacy Professionals