EUROPEAN PRIVACY

Law and Practice for Data Protection Professionals

Executive Editor
Eduardo Ustaran
Partner, Field Fisher Waterhouse

An IAPP Publication
CONTENTS

About the IAPP ................................................................. viii
Acknowledgments ............................................................ ix
  Richard Soule
Introduction ................................................................. xi
  Bojana Bellamy

SECTION ONE: Introduction to European Data Protection

Chapter 1: Origins and Historical Context of Data Protection Law
  Sian Rudgard
    Rationale for data protection ........................................ 3
    Human rights law ....................................................... 4
    Early laws and regulations ......................................... 6
    The need for a harmonised European approach .................. 11
    The Treaty of Lisbon ................................................. 14

Chapter 2: European Union Institutions
  Michelle Levin and Lilly Taranto
    Background ............................................................. 19
    European Parliament ................................................ 21
    European Council ................................................... 24
    Council of the European Union (Council of Ministers) ....... 24
    European Commission .............................................. 27
    European Court of Human Rights .................................. 29
    Court of Justice of the European Union .......................... 31
    Article 29 Working Party ........................................... 33
### Chapter 3: Legislative Framework

*Brian Davidson*

- Background ........................................................................................................... 35
- The Council of Europe Convention .................................................................... 35
- The Data Protection Directive .............................................................................. 37
- The Privacy and Electronic Communications Directive ............................................. 40
- The Data Retention Directive .............................................................................. 43
- Impact on member states ..................................................................................... 46

### SECTION TWO: European Data Protection Law and Regulation

### Chapter 4: Data Protection Concepts

*Nuria Pastor*

- Introduction ......................................................................................................... 51
- Personal data ......................................................................................................... 51
- Sensitive personal data ......................................................................................... 56
- Controller and processor ...................................................................................... 57
- Processing ............................................................................................................. 62
- Data subject .......................................................................................................... 63

### Chapter 5: Application of the Law

*Antonis Patrikios*

- Applicability criteria under the Directive ............................................................... 65
- Establishment in the EU ......................................................................................... 67
- No establishment in the EU .................................................................................. 71
- The e-Privacy Directive ......................................................................................... 76
- The Data Retention Directive .............................................................................. 76

### Chapter 6: Data Protection Principles

*Lilly Taranto*

- Introduction ......................................................................................................... 81
- Fairness and lawfulness ......................................................................................... 82
- Purpose limitation .................................................................................................. 85
- Proportionality ....................................................................................................... 87
- Data quality ............................................................................................................ 89

### Chapter 7: Legitimate Processing Criteria

*Victoria Hordern*

- Background ......................................................................................................... 93
- Processing personal data ...................................................................................... 93
- Processing sensitive data ..................................................................................... 100
# CONTENTS

## Chapter 8: Information Provision Obligations

*Hannah Jackson*

- The Transparency Principle .............................................. 107
- Exemptions to the obligation to provide information to data subjects .......... 112
- Privacy Notices ............................................................ 115

## Chapter 9: Data Subjects’ Rights

*Michelle Levin*

- Background ................................................................. 125
- The right of access under Article 12 .................................. 126
- The right to obtain rectification, erasure or blocking of the data processing .. 132
- The right to object .......................................................... 133
- The right not to be subject to fully automated decisions ......................... 137

## Chapter 10: Confidentiality and Security

*Stewart Room*

- Background ................................................................. 141
- The approach taken by the Data Protection Directive and national legislations . 142
- Appropriate technical and organisational measures ............................. 146
- Dealing with data processors ............................................. 155
- The regime in the e-Privacy Directive .................................... 157
- The regime in the Data Retention Directive .................................. 158
- Breach disclosure .................

## Chapter 11: Notification Requirements

*Brian Davidson*

- Introduction ................................................................. 163
- Notification obligation and exemptions ..................................... 164
- Content and format of notification ....................................... 165
- Prior authorisation ......................................................... 167
- Lack of harmonisation ...................................................... 167
- Timescales ................................................................. 169
- The future of notification in the EU ...................................... 169
- Conclusion and practicalities ................................................ 170

## Chapter 12: International Data Transfers

*Eduardo Ustaran*

- Introduction: Limitations affecting international data transfers ............... 173
- Scope of data transfers ..................................................... 174
- Meaning of an ‘adequate level of protection’ ................................ 175
- Procedure to designate countries with adequate protection .................... 177
- The situation in the United States ........................................ 178
CONTENTS

Legitimising data transfers by adducing adequacy—model contracts ............ 180
Data transfers within a multinational corporate group—
  Binding Corporate Rules ........................................ 184
Data transfers to service providers .................................. 186
Relying on derogations .................................................. 187
The future of the prohibition on international data transfers ................. 189

Chapter 13: Supervision and Enforcement
Stewart Room
  Introduction ..................................................... 191
  Administrative supervision ..................................... 193
  Regulation by the citizen and access to justice ................... 197
  Sanctions ....................................................... 198
  The Article 29 Working Party ................................. 198
  The European Data Protection Supervisor ......................... 200
  Supervision and enforcement within the e-Privacy Directive .......... 205
  Strategies for coping with supervision and enforcement ............ 206

SECTION THREE:
Compliance with European Data Protection Law and Regulation

Chapter 14: Employment Relationships
Victoria Hordern
  Employee data ................................................ 211
  Legal basis for processing employee personal data ................ 211
  Processing sensitive employee data ................................ 213
  Providing notice ................................................. 214
  Storage of personnel records ................................... 214
  Workplace monitoring ........................................... 215
  Works councils .................................................. 221
  Whistle-blowing schemes ....................................... 222

Chapter 15: Surveillance Activities
Antonis Patrikios
  Introduction ................................................ 227
  Communications ............................................... 229
  CCTV ............................................................... 233
  Biometrics ..................................................... 238
  Location-based services ....................................... 242

Chapter 16: Direct Marketing
Phil Lee
  Data protection and direct marketing ............................ 249
  Postal marketing ................................................ 253
CONTENTS

Telephone marketing .................................................. 254
Marketing by electronic mail (including e-mail, SMS and MMS) .......... 255
Fax marketing .......................................................... 258
Location-based marketing ........................................... 259
Online behavioural advertising ....................................... 261
Enforcement ............................................................ 265

Chapter 17: Internet Technology and Communications

Hannah Jackson
Cloud computing ....................................................... 269
Cookies and IP addresses ............................................. 274
Search engines ........................................................ 279
Social Networking Services (SNS) .................................. 282

Chapter 18: Outsourcing

Eduardo Ustaran
Introduction ............................................................. 287
The roles of the parties ............................................... 288
Data protection obligations in an outsourcing contract .................... 290
The German case ....................................................... 292
Offshoring and international data transfers ............................ 294

Appendices
Appendix 1: EU Legislative References ................................ 301
Appendix 2: EU Institutions ........................................... 303

About the Contributors .............................................. 305
Index ........................................................................ 311
The International Association of Privacy Professionals (IAPP) is the world’s largest association of privacy professionals, representing more than 8,000 members from businesses, governments and academic institutions across 70 countries.

The IAPP was founded in 2000 with a mission to define, support and improve the privacy profession globally through networking, education and certification. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for professionals who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations. The program has since grown to include the CIPP/G, CIPP/C, CIPP/IT and CIPP/E. Today, many thousands of professionals worldwide hold an IAPP privacy certification.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice. Learn more about the IAPP at www.privacyassociation.org.

About IAPP Europe

IAPP Europe is a unique community for European data protection and privacy professionals. IAPP Europe was created to provide education, networking, conferences and professional development resources tailored to the unique needs of the European data protection community and has been guided by an esteemed group of European privacy and data protection experts. Learn more at www.privacyassociation.org/europe.
The IAPP is pleased to present this textbook, which underpins the first professional credential program created specifically for European data protection professionals—the Certified Information Privacy Professional/Europe (CIPP/E).

The development of the CIPP/E program—and this book—would not have been possible without the leadership of IAPP Europe Managing Director Rita Di Antonio and the guidance and support of our European Advisory Board members. This esteemed group includes privacy and data protection experts from many areas of both the public and private sectors.

Our sincere thanks go out to Rita and these dedicated individuals. Past and present members of the IAPP’s European Advisory Board include:

Bojana Bellamy, LLM, Director of Data Privacy, Accenture
Ruth Boardman, Partner, Bird & Bird
Gary Davis, Deputy Commissioner, Office of the Data Protection Commissioner, Ireland
Pascale E. Gelly, CIPP/E, Cabinet Gelly
Sue Gold, Executive Counsel, The Walt Disney Company Limited
Rafael Garcia Gozalo, Head of the International Department, Spanish Data Protection Authority
Hazel Grant, Partner, Bristows
Christoph Klug, Managing Director, German Association for Data Protection and Data Security (GDD)
Gabriela Krader, Corporate Data Protection Officer, Deutsche Post
Christopher Kuner, Partner, Hunton & Williams LLP
Denise Lebeau-Marianna, Partner, Baker & McKenzie
ACKNOWLEDGMENTS

Xavier Leclerc, Responsable Service Correspondant Protection des Données, Axil-Consultants
Neil Matthews, CSMB EMEA Data Protection Coordinator, Dell Corporation Limited
Fabrice Naftalski, Partner, Attorney at Law, Ernst & Young, société d’avocats
Mikko Niva, CIPP/E, Global Privacy Counsel, Nokia
Rocco Panetta, Partner, Panetta & Associati
Christian Pardieu, Counsel—Europe Privacy Leader and Government Affairs & Policy, General Electric
Florence Raynal, Head of International and European Services, Commission Nationale de l’Informatique et des Libertés
David Smith, Deputy Commissioner, UK Information Commissioner’s Office
Toby Stevens, Director, Enterprise Privacy Group Ltd
Omer Tene, Associate Professor, College of Management School of Law, Israel
Florian Thoma, Chief Data Protection Officer, Siemens AG
Richard Thomas, Global Strategy Advisor, Hunton & Williams LLP
Henriette Tielemans, Partner, Covington & Burling LLP
Bridget C. Treacy, Partner, Hunton & Williams LLP
Eduardo Ustaran, Partner and Head of the Privacy and Information Law Group, Field Fisher Waterhouse LLP

On behalf of the IAPP, I would like to thank Eduardo Ustaran and the members of his team at the Field Fisher Waterhouse Privacy and Information Law Group, who researched, drafted and revised this text for the CIPP/E program. It has been a pleasure working with this talented group of data protection professionals on the development of this important book.

This project was fortunate to have input from Sue Gold of Disney, Neil Matthews of Dell and Matthias Pollmann of the Bundesministerium des Innern, who reviewed the manuscript and offered suggestions on content and delivery. I am grateful for their perspectives and expertise on European data protection and privacy matters, and for their constructive comments, which helped shape this text.

I thank Elissa Myers, CAE, editor, who brilliantly managed the editorial dialogue among the book’s many contributors. Elissa’s attention to detail and tenacity were critical to its successful production. Thanks, too, to Sarah Weaver, copy editor, who applied her outstanding skills to ensure consistency and accuracy in language and organization.

It has been an honor to work with so many fine European data protection and privacy professionals in the development of the CIPP/E program. To all who contributed to this effort, please accept my sincere gratitude.

Richard Soule
Certification Director, International Association of Privacy Professionals
I am honoured to present this book to the European data protection community.

*European Privacy* is the remarkable result of collaboration among European data protection experts. From their efforts emerges this body of knowledge—the foundational facts and concepts that all data protection professionals must understand to be effective in their roles and excel in the field.

This text has been created for many—from those new to the profession to the highly experienced data protection practitioner. But mostly, it will serve as an invaluable resource for those seeking a data protection credential. The IAPP’s Certified Information Privacy Professional/Europe (CIPP/E) credential brings an integrity measure to the field. For the first time, European and global professionals have a means of measuring and demonstrating their understanding of European data protection laws, concepts, criteria and obligations. The new CIPP/E certification will prove a useful credential for those looking for new data protection roles on the job market, but also for all organisations seeking to provide further education for their people—from data protection and privacy officers, lawyers, HR and marketing managers to engineers developing new products and services.

This book—and the credential—could not come at a better time.

The need for more data protection professionals is being recognised beyond Europe. On a global scale, organisations and regulators are realising the need for depth in this area. In the coming months and years, the number of professionals who spend day-in and day-out handling data protection matters will grow, as will their need for expanded and global knowledge.

The CIPP/E and this textbook mark a milestone in the evolution of our data protection field. The issues in our field are complex, and progress on them is often slow. A well-informed professional body will help us find harmony and resolution in an increasingly turbulent landscape of data protection practice and law.

Bojana Bellamy, LLM
*Chairman*, International Association of Privacy Professionals
*Director of Data Privacy*, Accenture