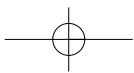
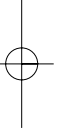
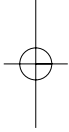
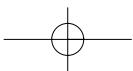
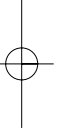
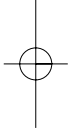




EUROPEAN DATA PROTECTION LAW

Corporate Compliance and Regulation





EUROPEAN DATA PROTECTION LAW

Corporate Compliance and Regulation

SECOND EDITION

CHRISTOPHER KUNER

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford OX2 6DP

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide in

Oxford New York

Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in

Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press
in the UK and in certain other countries

Published in the United States
by Oxford University Press Inc., New York

© Christopher Kuner, 2007

The moral rights of the author have been asserted
Database right Oxford University Press (maker)

Crown copyright material is reproduced under Class Licence
Number C01P0000148 with the permission of OPSI and the
Queen's Printer for Scotland

First published 2003

Second edition published 2007

All rights reserved. No part of this publication may be reproduced,
stored in a retrieval system, or transmitted, in any form or by any means,
without the prior permission in writing of Oxford University Press,
or as expressly permitted by law, or under terms agreed with the appropriate
reprographics rights organization. Enquiries concerning reproduction
outside the scope of the above should be sent to the Rights Department,
Oxford University Press, at the address above

You must not circulate this book in any other binding or cover
and you must impose the same condition on any acquirer

British Library Cataloguing in Publication Data
Data available

Library of Congress Cataloging in Publication Data

Kuner, Christopher.

European data protection law : corporate compliance and regulation / Christopher
Kuner.—2nd ed.

p. cm.

Rev. ed. of: European data privacy law and online business / Christopher Kuner,
2003.

Includes bibliographical references and index.

ISBN 978-0-19-928385-9 (hardback : alk. paper) 1. Data protection—Law and
legislation—European Union countries. 2. Electronic commerce—Law and legislation—
European Union countries. I. Kuner, Christopher. European data privacy law and online
business. II. Title.

KJE6071.K86 2007

342.2408'58—dc22

2007001434

Typeset by Cepha Imaging Private Ltd., Bangalore, India
Printed in Great Britain
on acid-free paper by
Biddles Ltd, King's Lynn

ISBN 978-0-19-928385-9

1 3 5 7 9 10 8 6 4 2

FOREWORD TO THE SECOND EDITION

I very much welcome this second edition of Christopher Kuner's book on European data protection law, as well as its wider scope and changed emphasis, as reflected in the new title. This book no longer deals with '*European Data Privacy Law and Online Business*', but with 'European Data Protection Law' and 'Corporate Compliance and Regulation'. This is a deliberate choice of the author—explained in his preface—but also a clear recognition of developments since the first edition was published in 2003 and an encouraging perspective for the years ahead.

The original emphasis on online business has lost most of its relevance, since online and offline environments have become increasingly interlinked and even integrated. This is certainly true for all organizations—business and non-business alike—that aim to benefit from the opportunities which the new internet-based world of e-services seems to have in store for better efficiency, quality and effectiveness. The treatment of personal data in all stages of activity is essential for this development.

These organizations discover that the way in which they handle the treatment of personal data may have great consequences for their relations with customers, employees and other stakeholders. Issues like how to ensure trust and confidence from those involved have been among the first to arise in a market perspective, and they have led to increased attention to 'data privacy'. In a principle-based approach, however, it is even more important that the new electronic world that is developing around us remains in line with the basic values of our societies, as we continue to cherish them today, inclusive of strong protection of fundamental rights, like the right to privacy and protection of personal data. The rights and obligations arising from this approach are a typical feature of European data protection law.

Whatever the source of inspiration may be, it is clear that 'data protection' in this perspective is not only a legal obligation that responsible organizations have to respect and comply with, but also a critical success factor for their ambitions in the electronic age. As more and more activities depend on the lawful processing of personal data, effective protection of these data should be seen and acted upon as a critical condition for their success. It is for this reason that a stronger emphasis

Foreword to the Second Edition

on compliance and mechanisms to ensure compliance is most welcome and even of crucial importance.

It is not surprising that data protection law itself is also in constant development. The main legal instruments are subject to regular evaluation or revision. Some of these developments may seem contradictory, as in the case of the Data Retention Directive, which was clearly driven by law enforcement considerations. It is unavoidable that some of these developments and their repercussions will go beyond this new edition.

Peter Hustinx
European Data Protection Supervisor

FOREWORD TO THE FIRST EDITION

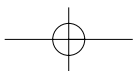
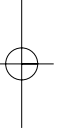
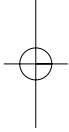
Christopher Kuner says in his Preface that data protection is a fluid and ever-moving subject. We should all be grateful that this realization has not led him to abandon this project. Many others would have been discouraged, or have been tempted to wait (probably in vain) for a moment when things were more stable. Fortunately, he has been neither discouraged nor tempted and we have as a result this entirely useful and relevant book.

The year 2002 (I am writing this in November) has been a busy one for those of us in the European Commission involved in data protection. The revision of one of the two main legal instruments which this book describes—now the Electronic Communications Data Protection Directive—has been completed; and the other, the general framework Directive, is under review.

We have made the review process as open and participative as possible. Interested readers can find the results and follow progress on our website <<http://europa.eu.int/comm/privacy>>. I mention this review, not in order to rub in the ‘moving target’ point, but because it has confirmed a very welcome shift in attitudes in the business community. There is a growing acceptance of data protection law as a fact of life, a permanent presence in the market place and there is a growing readiness to work constructively with the regulators to make it work better. Christopher Kuner—perhaps unknowingly but I suspect quite deliberately—has been one of the instruments of that shift. It is interesting to note that a lot of the people who have contributed to the shift are Americans or belong to US-based companies. Maybe we just notice the difference more, because US businesses have been amongst the loudest critics of the Directive

Be that as it may, it is clear that neither data protection regulators, nor the businesses on which their rules impact, can ignore the growing irrelevance of geographical borders in today’s economy. How to regulate the internet is a question which goes far beyond data protection and we all need to do a lot more thinking about that, but until somebody comes up with an answer, the least we can do is promote transparency and a broad-based dialogue on regulatory matters. Christopher Kuner’s book will, I trust, be on the desks of all serious participants in the dialogue on data protection.

Susan Binns
Director, DG Internal Market, European Commission



PREFACE TO THE SECOND EDITION

In the four years since the first edition of this book was published under the title *European Data Privacy Law and Online Business*, data protection law has developed so rapidly, and changed in so many ways, that a new edition had become a necessity, if the book was not to become completely outdated.

These changes have come in many ways. Some of them have been legal developments, including the first cases of the European Court of Justice interpreting the Data Protection Directive 95/46; a number of important new papers by the Article 29 Working Party; and a new directive dealing with data retention. Other changes have been political, including the accession of ten new Member States to the EU, and the seeming collapse of the EU Constitution. Just as importantly, data protection law has ceased being an exotic niche area and has become a topic with important ramifications for any company's bottom line.

The approach for the second edition has remained the same. The book remains firmly focused on European data protection law as it relates to legal compliance issues for companies, and thus does not attempt to cover a wide range of other topics of limited relevance to business, such as law enforcement, human rights issues, and other similar topics. The book has been completely revised and rewritten, and has also been thoroughly updated to cover developments through August 2006 such as new case law of the European Court of Justice, the Data Retention Directive, the EU Constitution, and developments in the Member States.

The author remains convinced that the reader navigating the shoals of European data protection law requires first a high-level understanding of the main instruments of the law, as well as of the institutions which underpin it. At the same time, enforcement and day-to-day compliance are determined by national and local law, so that companies must apply the law of the Member States in which they operate. As it would be impossible to give a detailed discussion of the law of all, or even of a few, Member States in such a book, the approach has remained that of selecting examples from Member State law, and contrasting and comparing them with the higher-level legal infrastructure of European data protection law. Armed with this knowledge, readers will be well-equipped to cope with detailed issues of local data protection law.

At the same time, a number of important changes have been made to the book. The most obvious of these is the title: whereas four years ago, the internet and

Preface to the Second Edition

electronic commerce could still be dealt with as discrete topics, in the intervening years they have become ubiquitous, so that it no longer makes any sense to focus the book solely on online issues.

The appendices have also been substantially expanded to include charts giving information about a number of important issues across all Member States, as well as additional legal texts (such as the recitals to the standard contractual clauses and the safe harbor FAQs).

The reader will also notice a change in the footnotes, where almost all URLs have been deleted. Experience over the past few years has shown that URLs change so frequently that giving them in the footnotes is of little utility, and takes up valuable space. However, a few exceptions have been made, where it is believed that the material will be particularly difficult to locate without giving the URL. The companion website to this book (located at <http://www.oup.co.uk/law/practitioner/cws/>) includes a list of all Internet addresses contained in the book, as well as regular updates to the text.

The author hopes that this book can make a contribution, however small, to the development of a *European* view of data protection law, which is a subject that is still viewed too often in purely national terms. National tradition is important in data protection law, as in so many other areas of European life; but, as a great European modernizer (Gustav Mahler) once said, ‘Tradition ist Bewahrung des Feuers und nicht Anbetung der Asche’ (‘tradition means maintaining the fire, not worshipping the ashes’). At a time when countries such as China and India are evaluating and comparing regulatory models for data protection in order to develop their own legal frameworks, data protection law in Europe must move away from national approaches and develop a more pan-European perspective if it is to retain its global influence.

The author remains deeply indebted to a number of colleagues whose accumulated wisdom has educated him over the years and without whom this book would not be possible. Besides those persons mentioned in the preface to the first edition, thanks are also due to Kirsty Asher and Chris Rycroft at Oxford University Press; Bojana Bellamy; the members of the European Privacy Officers Forum (EPOF); Peter Fleischer; Matteo Gofriller; Peter Hustinx; Dr Waltraut Kotschy; Dr Ewa Kulesza; Dr Jose Luis Piñar Mañas; Nuala O’Connor Kelly; and Philippe Renaudière. Special thanks go to my colleagues at Hunton & Williams, in particular Isabelle Chatelier; Dr Jörg Hladjk; Susana Rodríguez Ballano; Anne Ruwet; and Lisa Sotto.

Christopher Kuner
ckuner@hunton.com
Brussels, September 2006

PREFACE TO THE FIRST EDITION

Information has become the new raw material of the world economy. Just as, in past centuries, iron, wood, and coal were the foundation upon which the economy was based, so nowadays it is data and information.

At the same time, there is increasing concern about the societal consequences of processing the personal data of individuals, and confusion about where the line should be drawn between the economic benefits of data processing and the dangers to personal privacy and liberty which this may bring. Headlines such as ‘The end of privacy’¹ or ‘The death of privacy?’² have unsettled consumers and given rise to fears that we have entered a ‘brave new world’ in which personal liberty is a thing of the past.

This is a book about how the regulatory system in one region of the world, namely Europe, has attempted to draw a line between the benefits and dangers of processing personal data in the context of online business. It has been written in the conviction that the regulation of data processing and data flows is destined to remain one of the most important regulatory and policy issues of the 21st century, and that electronic commerce is no longer limited to the ‘new economy’, but has become ubiquitous. It is hoped that the book will help companies, and their legal advisors, involved in electronic commerce navigate the shoals of European data protection law. The title ‘data privacy’ rather than ‘data protection’ was chosen to make it clear that this book does not deal with the copyright protection of databases under the EU Database Directive, with which topic data protection law is often confused.

Europe was the first region to develop a specific regulatory structure for the processing of personal data. As other regions (such as the Americas and Asia) have gradually discovered the subject of ‘data protection’, more and more of them have been adopting elements of the European regulatory structure into their own law. Thus, knowledge of how data processing is regulated in Europe is useful in predicting how other regions may deal with the subject as well.

¹ The Economist, 17 May 1999.

² A M Froomkin, ‘The Death of Privacy?’ (2000) 52 Stanford Law Review 1461.

Preface to the First Edition

The reader should keep in mind several things when using this book:

First, data protection is an extraordinarily broad topic, and a book dealing with all aspects of the subject would be much lengthier than the present one. Thus, this book does not purport to deal with all aspects of European data protection law, but only with those that are particularly relevant to online business (meaning, in essence, both business-to-business and business-to-consumer electronic commerce).

Second, data protection law is also a very fact-specific and fluid subject. Thus, the reader should never take the discussion herein as legal advice, and should always check the current status of the law in a particular jurisdiction when dealing with a legal issue, as the law may well have changed since this book was published. The revisions to the Directive on Privacy and Electronic Communications (formerly the Telecommunications Data Protection Directive) passed in the summer of 2002 have been taken into account.

Third, this book provides information on the law of selected EU Member States, without any attempt to be comprehensive. This is a much more difficult undertaking than just analysing EU law, since Member State law is more difficult to access, is available in a myriad of different languages, and is subject to different national legal regimes. Nevertheless, the author felt it imperative to give at least a basic overview of how some of the key legal questions are treated under national law, since it is Member State law which largely determines how important questions of data protection law are dealt with in practice. As data protection law also depends largely on the practices of data protection authorities, most of which are not written down anywhere, the author has included numerous examples of how data protection issues are dealt with in practice in Europe; such examples are based on the author's experience in practising law, and are included as points of orientation for the reader, rather than as definitive statements of how the data protection authorities might rule in any particular case.

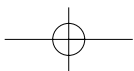
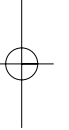
Fourth, the author has come neither to bury European data protection law, nor to praise it. This book attempts to analyse European data protection law objectively as it relates to electronic commerce without a particular ideological slant; at the same time, the author has not hesitated to indicate where, in his view, the law is in danger of losing touch with the realities of globally networked commerce.

Finally, in writing this book the author has become acutely aware of the truth of the adage that a work of scholarship can only be achieved by standing on the shoulders of others. And indeed, European data protection law is so complex, and the issues involved are so many, that it would have been impossible to even contemplate this book without a number of people who have had a hand (even if

Preface to the First Edition

unknowingly) in educating the author on this subject. Thanks are due in particular to Sakari Aalto; Diana Alonso-Blas; Rosa Barcelo; Prof Lucas Bergkamp; Dr Johann Bizer; Susan Binns; Leonardo Cervera-Navas; Amanda Chandler; Dr Ulrich Dammann; Dr Markus Deutsch; Jan Dhont; Harald Eul; Pascale Gelly; Ann-Charlotte Högberg; Rosemary Jay; Waltraut Kotschy; Karin Retzer; Heather Rowe; Armgard von Reden; the law firm of Hunton & Williams and my secretary Anne Ruwet; and last but not least Oxford University Press, particularly Chris Rycroft and Meg Zawadzki.

Christopher Kuner
ckuner@hunton.com
Brussels, July 2002



CONTENTS—SUMMARY

<i>Table of Cases</i>	xxv
<i>Table of Primary and Secondary Legislation</i>	xxvi
<i>Table of International Instruments</i>	xxxv
<i>List of Abbreviations</i>	xxxvii
1. European Data Protection Law and Institutions	1
2. Fundamental Legal Concepts	63
3. Applicable Law and Jurisdiction	109
4. International Data Transfers	151
5. Compliance Challenges and Strategies	233
Appendix 1. Useful Internet Links	325
Appendix 2. European Data Protection Authorities	327
Appendix 3. EU Data Protection Directive (“General Directive”) 95/46/EC	335
Appendix 4. EU Directive on Privacy and Electronic Communications 2002/58/EC	361
Appendix 5. EU Data Retention Directive 2006/24/EC	379
Appendix 6. United States Safe Harbor Principles and FAQs	391
Appendix 7. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Controller Transfers)	409
Appendix 8. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Processor Transfers)	439
Appendix 9. Forms and Precedents	453

Contents—Summary

Appendix 10. Mail, Fax, Telephone and e-mail Marketing Requirements in EU Member States	465
Appendix 11. Summary of Notification Requirements for Commercial and Human Resources Data in EU Member States	471
Appendix 12. Standard Contractual Clauses Filing Requirements	483
Appendix 13. Selected Enforcement Measures in EU Member States and Article 29 Working Party from September 2002 through May 2006	487
Appendix 14. Documents adopted by Article 29 Working Party through August 2006	503
Appendix 15. Binding Corporate Rules Materials	513
<i>Glossary</i>	533
<i>Selected Bibliography</i>	537
<i>Index</i>	543

Companion Website

This book will be updated by means of a companion website, freely accessible to all purchasers of the book. Key developments will be reported and analysed on the website on an occasional basis.

While the site will not attempt to provide comprehensive updates, references will be included from time to time to particularly significant developments of which the author feels the readers should be made aware. The author will provide updating commentary where appropriate. The companion website will also carry links to a large number of useful websites referred to in the book.

To register for free access, please visit:

<http://www.oup.co.uk/law/practitioner/cws>

and click on the link for *European Data Protection Law: Corporate Compliance and Regulation*.

CONTENTS

<i>Table of Cases</i>	xxv
<i>Table of Primary and Secondary Legislation</i>	xxvi
<i>Table of International Instruments</i>	xxxv
<i>List of Abbreviations</i>	xxxvii

1. European Data Protection Law and Institutions

A. Introduction	1.01
B. EU Institutions	1.04
(1) European Commission	1.08
(2) Council of the European Union	1.11
(3) European Parliament	1.13
(4) European Court of Justice	1.14
(5) European Data Protection Supervisor (EDPS)	1.16
(6) Article 29 Working Party	1.18
(7) Article 31 Committee	1.21
(8) Other institutions	1.25
C. EU Member States' Authorities	1.26
(1) Data protection authorities	1.26
(2) Other authorities and entities	1.34
D. Regulatory Instruments	1.35
(1) EU law	1.35
Treaties	1.35
General Directive	1.39
Directive on Privacy and Electronic Communications	1.49
Interaction of the General Directive and the Directive on Privacy and Electronic Communications	1.51
Data Retention Directive	1.54
Further instruments	1.57
(2) Member State law	1.58
(3) Supremacy of EU law and implementation of directives	1.61
(4) Standardization	1.70
E. Legislative Process	1.76

Contents

F. Non-EU International Institutions	1.77
(1) Council of Europe	1.77
(2) OECD	1.78
(3) United Nations	1.79
(4) Berlin Group	1.80
G. Enforcement of the Law	1.81
H. Future Directions	1.92
2. Fundamental Legal Concepts	
A. Introduction	2.01
B. Access and Related Rights	2.02
C. Anonymous and Pseudonymous Data	2.08
D. Consent	2.13
E. Data Controllers and Data Processors	2.19
F. Data Minimization	2.30
G. Data Processing: Definition and Grounds	2.33
H. Data Subject	2.36
I. Data Transfer	2.42
J. Establishment	2.51
K. Freedom of Expression	2.54
L. Freedom of Information	2.62
M. Free Flow of Data within the EU	2.68
N. Legitimacy	2.70
O. Personal Data	2.73
P. Processing	2.87
Q. Purpose Limitation	2.89
R. Sensitive Data	2.92
S. Third Party	2.99
3. Applicable Law and Jurisdiction	
A. Introduction	3.01
B. Distinguishing Choice of Law and Jurisdiction	3.06
(1) Conflict of laws and the General Directive	3.06
(2) Jurisdictional rules	3.09

Contents

C. The General Directive	3.12
(1) Overview	3.12
(2) Member State implementations	3.13
(3) Outline of legal bases	3.20
Establishment of data controller in the EU	3.21
Use of equipment in a Member State by a non-EU data controller	3.23
Application of EU law based on public international law	3.37
(4) Application to data processors	3.38
(5) Corporate structure	3.40
(6) Intra-EU conflict of laws	3.44
(7) Appointment of a representative in the EU	3.48
(8) Outlook	3.51
D. The Directive on Privacy and Electronic Communications	3.52
(1) Overview	3.52
(2) Material scope	3.53
(3) Personal scope	3.57
(4) Geographic scope	3.58
(5) Applicable law and jurisdiction	3.59
(6) National implementations	3.62
E. The Directive on Data Retention	3.65
F. Case Studies	3.68
(1) Introduction	3.68
(2) Websites based outside Europe	3.69
(3) Global companies	3.74
(4) Data transfers routed through a single Member State	3.78
4. International Data Transfers	
A. Introduction	4.01
B. Selecting a Data Transfer Mechanism	4.05
C. Basic Principles	4.07
(1) Data transfers	4.07
(2) Legal bases for data export	4.10
(3) Legal basis for data processing	4.14
(4) Member State law	4.23
(5) Data transfer and applicable law	4.31
(6) Enforcement	4.35
(7) Onward transfers and processor-to-processor transfers	4.38
(8) Data imports into the EU	4.47
D. Adequacy Decisions	4.48
(1) Introduction	4.48
(2) Determining adequacy	4.53

Contents

E. Safe Harbor	4.59
(1) Introduction	4.59
(2) Membership	4.61
(3) Substantive principles	4.63
(4) Issues	4.66
(5) Outlook	4.67
F. Contractual Clauses	4.68
(1) Introduction	4.68
(2) Evolution of the standard contractual clauses	4.70
Controller-to-controller clauses	4.75
Controller-to-processor clauses	4.78
(3) Using the standard contractual clauses in practice	4.81
Practical issues	4.81
Strategies for signing the clauses	4.92
(4) Ad hoc and national contracts	4.99
G. Exceptions	4.103
(1) Introduction	4.103
(2) Consent	4.105
(3) Transfers necessary for performance of a contract	4.107
(4) Transfers in the public interest or in defence of legal claims	4.112
H. Binding Corporate Rules (BCRs)	4.120
(1) Introduction	4.120
(2) Application and approval of BCRs	4.124
(3) Legal issues	4.128
(4) Drafting BCRs	4.135
(5) Substance of BCRs	4.138
Processing and flows of information	4.139
Data protection safeguards	4.140
Mechanism for reporting and notifying changes	4.141
Internal measures for ensuring compliance within the organization	4.143
Verification of compliance	4.144
Complaint handling	4.145
Cooperation with the DPAs	4.146
Jurisdiction	4.148
Redress for individuals	4.149
Liability	4.150
Promoting awareness of BCRs	4.151
Binding nature of BCRs	4.152
(6) Implementation of BCRs	4.153

Contents

5. Compliance Challenges and Strategies	
A. Introduction	5.01
B. Developing a Data Protection Compliance Strategy	5.05
(1) Introduction	5.05
(2) Steps of a compliance project	5.09
C. Legal Grounds for Processing Personal Data	5.26
(1) Introduction	5.26
(2) Legal grounds	5.28
(3) Application to compliance issues	5.29
D. Notification of Data Processing to the DPAs	5.30
(1) Introduction	5.30
(2) Member State law	5.36
(3) Compliance strategies	5.41
Is notification necessary?	5.46
What data processing should be notified?	5.48
Who should perform notification and how should it be done?	5.53
When should notification be made?	5.57
E. Processing of Employee Data	5.61
(1) Introduction	5.61
(2) Legal basis for data processing	5.62
(3) Monitoring employee computer usage	5.63
An incremental approach to monitoring	5.68
Ensuring technical functionality of the network	5.72
Detecting significant deviations in system use	5.74
Dealing with significant misuse	5.78
Recommendations	5.81
(4) Whistleblower hotlines	5.86
Introduction	5.86
Conflict between EU and US law	5.90
Article 29 Working Party guidance	5.96
Remaining issues	5.98
(5) Works councils	5.101
Introduction	5.101
Member State examples	5.104
(6) Placing employee information on the internet	5.116
F. Website Compliance	5.119
(1) Introduction	5.119
(2) Requirements for websites	5.122
(3) Privacy policies	5.126
(4) Highlights notices	5.132

Contents

G. Security and Security Breaches	5.135
(1) Introduction	5.135
(2) Legal status of security breaches	5.140
The US experience	5.141
EU law	5.145
(3) Responding to security breaches	5.151
H. Corporate Acquisitions and Due Diligence	5.156
(1) Introduction	5.156
(2) ‘Due diligence’	5.157
Evaluating the data to be processed	5.161
Finding a legal basis for processing	5.163
Providing notice	5.167
Ensuring security	5.168
Providing a legal basis for transfers outside the EEA	5.170
(3) Corporate acquisitions	5.171
I. Outsourcing	5.173
(1) Introduction	5.173
(2) Legal issues	5.176
Types of outsourcing transactions	5.176
Contractual provisions	5.181
Security	5.184
International data transfers	5.185
DPA guidance	5.187
J. Marketing	5.189
(1) Introduction	5.189
(2) Specific issues	5.196
Member State implementations	5.196
Definition of e-mail	5.201
Consent	5.203
Legal persons	5.206
Acquisition of addresses	5.208
Similar products and services to existing customers	5.209
Opt-out lists	5.212
K. Records Management	5.213
(1) Introduction	5.213
(2) Legal requirements	5.216
(3) Implementing a records management programme	5.222

Contents

Appendix 1. Useful Internet Links	325
Appendix 2. European Data Protection Authorities	327
Appendix 3. EU Data Protection Directive ('General Directive') 95/46/EC	335
1. Implementation	335
2. Text	337
Appendix 4. EU Directive on Privacy and Electronic Communications 2002/58/EC	361
1. Implementation	361
2. Text	362
Appendix 5. EU Data Retention Directive 2006/24/EC	379
Appendix 6. United States Safe Harbor Principles and FAQs	391
1. Safe harbor privacy principles issued by the U.S. Department of Commerce on 21 July 2000	391
2. Frequently Asked Questions issued by the U.S. Department of Commerce on 21 July 2000	394
Appendix 7. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Controller Transfers)	409
1. SET I (2001)	409
2. SET II (2004, Industry Alternative Clauses)	424
Appendix 8. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Processor Transfers)	439
Appendix 9. Forms and Precedents	453
1. CEN (European Committee for Standardization) Article 17 Model Contract	453
2. Sample safe harbor onward transfer agreement (for transfers to 'agents' or data processors)	460
3. Sample website privacy policy (full version)	461
4. Sample website privacy policy (highlights notice version)	463

Contents

Appendix 10. Mail, Fax, Telephone and E-mail Marketing Requirements in EU Member States	465
Appendix 11. Summary of Notification Requirements for Commercial and Human Resources Data in EU Member States	471
Appendix 12. Standard Contractual Clauses Filing Requirements	483
Appendix 13. Selected Enforcement Measures in EU Member States and Article 29 Working Party from September 2002 through May 2006	487
Appendix 14. Documents Adopted by Article 29 Working Party through August 2006	503
Appendix 15. Binding Corporate Rules Materials	513
1. ICC standard application form for approval of BCRs	513
2. Decision of Austrian DPA approving BCRs of an Austrian bank	528
<i>Glossary</i>	533
<i>Selected Bibliography</i>	537
<i>Index</i>	543

TABLE OF CASES

Amann v Switzerland (2000) 30 EHRR 843, ECHR	2.83
Ayuntamiento de Madrid v Hispanomocion, SA, Taibesa, Consesionario Peugeot, 13 January 2005 R/00734/2004 [2004] AEPD 13/01/2005	2.42
Bodil Lindqvist (C101/01) [2003] ECR I-12971	1.15, 1.47, 1.62, 1.63, 2.47, 2.48, 2.49, 2.50, 2.57, 2.60, 2.87, 3.27, 3.30, 4.07, 4.08
Campbell v Mirror Group Newspapers Ltd; Sub Nom: Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] 2 All ER 995; [2004] EMLR 15; [2004] HRLR 24; [2004] UKHRR 648; 16 BHRC 500; (2004) 101(21) LSG 36; (2004) 154 NLJ 733; (2004) 148 SJLB 572; Times, 7 May 2004; Independent, 11 May 2004, HL; reversing [2002] EWCA Civ 1373; [2003] QB 633; [2003] 2 WLR 80; [2003] 1 All ER 224; [2003] EMLR 2; [2003] HRLR 2; (2002) 99(42) LSG 38; (2002) 146 SJLB 234; Times, 16 October 2002; Independent, 18 October 2002, CA (Civ Div); reversing [2002] EWHC 499; [2002] EMLR 30; [2002] HRLR 28; (2002) 99(19) LSG 28; (2002) 146 SJLB 107; Times, 29 March 2002; Daily Telegraph, 11 April 2002, QBD	1.19
Commission v Belgium see Motor Vehicle and Tractor Directives, Re (C102/79)	
Commission v Grand Duchy of Luxembourg (C450/00) [2001] ECR I-07069	1.66
Costa v Ente Nazionale per l'Energia Elettrica (ENEL) (C6/64) [1964] ECR 1141; [1964] CMLR 425, ECJ	1.61
Durant v Financial Services Authority (Disclosure of Information) [2003] EWCA Civ 1746; [2004] FSR 28; Times, 2 January 2004, CA (Civ Div)	2.06, 2.84, 2.86, 2.88
Ireland v Council and Parliament (C301/06) [2006]	1.56
Johnson v Medical Defence Union Ltd; Sub Nom: Johnson v Medical Defence Union Ltd (No 2) [2006] EWHC 321; (2006) 89 BMLR 43; Times, 4 April 2006, Ch D	2.06
Motor Vehicle and Tractor Directives, Re (C102/79); Sub Nom: Commission of the European Communities v Belgium (C102/79); Type Approval Directives, Re (C102/79) [1980] ECR 1473; [1982] 2 CMLR 622; [1981] 1 CMLR 282, ECJ	1.65
Niemietz v Germany (A/251-B) (1993) 16 EHRR 97, ECHR	2.83
Nikon v Onof, Decision No 4164 (2 October 2001)	4.105, 5.83
Pal (Dr Rita) v General Medical Council [2004] EWHC 1485, QBD	5.216
Parliament v Council (C317/04 and C318/04) [2006]	1.15, 1.17, 1.45, 1.56, 2.35, 4.49, 4.117
Public Prosecutor v Ramsbro, 12 June 2001, Case No B 293-00	2.57
Rechnungshof v Osterreichischer Rundfunk (C465/00) [2003] ECR I-4989; [2003] 3 CMLR 10, ECJ	1.15, 1.68, 2.86
Rotaru v Romania 8 BHRC 449, ECHR	2.83

TABLE OF PRIMARY AND SECONDARY LEGISLATION

EC Legislation	xxvi
National Legislation	xxx

Paragraph references in bold indicate where legislation has been set out in part or in full in the text.

EC LEGISLATION	Treaty of Rome
Treaties	Art 100a 1.07, 1.62
Accession Treaty [2005] OJ L157/11	Charters
Art 4(2) 1.05	Charter of Fundamental Rights
Amsterdam Treaty 2.62	of the European Union [2000]
Art 14 1.64	OJ C364/1
Art 30 1.76	Art 8 1.35 , 1.38
Art 31 1.76	Art 42 2.63
Art 95 1.07, 1.62, 1.64, 1.76	Decisions
Art 251 1.76	Commission Decision (EC) 2000/518
Art 286 1.16	[2000] OJ L215/1 of 26 July 2000
EC Treaty 1.62	pursuant to Directive (EC) 95/46 on
Art 205(2) (ex art 148) 1.21, 1.26	the adequate protection of personal
Art 230 4.28	data provided in Switzerland 4.48
Art 251 1.23, 2.62	Commission Decision (EC) 2000/519
Art 255 2.62	[2000] OJ L215/4 of 26 July 2000
Art 286 1.16	pursuant to Directive (EC) 95/46 on
Protocol on the Enlargement of the	the adequate protection of personal
European Union	data provided in Hungary 4.48
Art 3 1.21	Commission Decision (EC) 2000/520
Art 5 1.26	[2000] OJ L215/7 of 26 July 2000
Nice Treaty (Consolidated Version	pursuant to Directive (EC) 95/46
of the Treaty Establishing the	on the adequacy of the protection
European Community) [2002]	provided by the safe harbor privacy
OJ C325/33 1.15, 1.16, 1.21,	principles and related frequently asked
1.22, 1.76	questions issued by the US Department
Treaty establishing a Constitution for	of Commerce 4.48, 4.59, 4.61,
Europe [2004] OJ C310/1 1.37	4.63, 4.67
Treaty on European Union [2002]	Art 2 4.66
OJ C325/5	Art 5 4.60
Art 34(2)(b) 1.76	Recital 6 4.61
Art 36 1.76	
Art 39 1.76	

Table of Primary and Secondary Legislation

Commission Decision (EC) 2001/16 [2002] OJ L6/52 of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46 4.71, 4.78, 4.90, 4.94 Recital 14 4.40	Record of air passengers transferred to the United States' Bureau of Customs and Border Protection 4.49
Commission Decision (EC) 2001/497 [2001] OJ L181/19 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive (EC) 95/46 4.71, 4.73, 4.90, 4.94, App 7 Recital 6 4.28 Recital 7 4.28 Recital 8 4.77	Commission Decision (EC) 2004/915 [2004] OJ L385/74 of 27 December 2004 amending Decision (EC) 2001/497 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries 4.73 Art 1(2) 4.28
Commission Decision C(2001)1539 of 15 June 2001 Recital 6 4.85 Recital 7 4.85	Commission Decision C(2004)5271 4.73
Commission Decision (EC) 2002/2 [2002] OJ L2/13 of 20 December 2001 pursuant to Directive (EC) 95/46 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act 4.48 Art 4 4.58	Council Decision (EEC) 87/95 of 22 December 1986 on standardization in the field of information technology and telecommunications [1987] OJ L36/31 1.73
Commission Decision (EC) 2002/16 of 27 December 2001 on standard contractual clauses for the transfers of personal data to processors established on third countries, under Directive 95/46/EC App 8	Council Decision (EC) 1999/468 of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission [1999] OJ L184/23 1.23, 1.76
Commission Decision (EC) 2003/821 [2003] OJ L308 of 21 November 2003 on the adequate protection of personal data in Guernsey 4.48	Council Decision (EC) 2004/496 of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [2004] OJ L183/83 1.44
Commission Decision C (2003)1731 [2003] OJ L168 of 30 June 2003 pursuant to Directive (EC) 95/46 on the adequate protection of personal data provided in Argentina 4.48	Council Decision (EC) 2004/535 of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection [2004] OJ L235/11 1.44
Commission Decision (EC) 2004/411 [2004] OJ L151/1 of 28 April 2004 on the adequate protection of personal data in the Isle of Man 4.48	Decision (EC) No 1247/2002 of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties [2002] OJ L183/1 1.16
Commission Decision (EC) 2004/535 [2004] OJ L235/11 of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name	Decision (EC) 2004/55 of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty [2004] OJ L12/47 1.16

Table of Primary and Secondary Legislation

Directives	Arts 6–8	1.50
Directive (EEC) 90/619	Art 6	4.15
Directive (EC) 94/45 [1994]	Art 6(1)(a)	2.70
OJ L254/64 European Works	Art 6(1)(b)	2.30, 2.70, 2.89, 5.145, 5.216
Council Directive	Art 6(1)(c)	1.68, 2.30, 5.216
Directive 95/46/EC, [1995]	Art 6(1)(d)	5.216
OJ L281/31 General Data	Art 6(b)	1.40
Protection Directive	Art 6(d)	1.40
1.06, 1.07,	Art 7	1.40, 1.95, 2.34, 4.15, 4.19, 4.20, 5.28, 5.29
1.12, 1.15, 1.36, 1.39, 1.40, 1.41,	Art 7(1)	2.33
1.42, 1.45, 1.47, 1.48, 1.50, 1.51,	Art 7(a)	4.20, 5.28, 5.29, 5.163
1.58, 1.62, 1.63, 1.64, 1.66, 1.68,	Art 7(b)	5.28, 5.29, 5.72
1.69, 1.76, 1.82, 1.94, 1.95, 1.97,	Art 7(c)	1.68, 2.35, 5.28
2.05, 2.17, 2.20, 2.33, 2.34, 2.41,	Art 7(d)	5.28
2.43, 2.44, 2.52, 2.54, 2.56, 2.57,	Art 7(e)	1.40, 1.68, 4.116, 5.28, 5.29
2.60, 2.75, 2.79, 2.81, 2.83, 2.87,	Art 7(f)	1.40, 2.35, 5.28, 5.29, 5.163, 5.179
2.88, 2.101, 3.04, 3.13, 3.22, 3.23,	Art 7(r)	4.20
3.27, 3.47, 3.49, 3.50, 3.51, 3.56,	Art 8	1.40, 1.64, 1.95, 2.79, 2.92, 2.93, 4.15, 5.28
3.57, 3.66, 3.70, 4.03, 4.09, 4.25,	Art 8(1)	1.95, 2.92
4.28, 4.30, 4.32, 4.33, 4.56, 4.63,	Art 8(2)(a)	2.17, 2.92
4.118, 5.35, 5.39, 5.42, 5.62, 5.65,	Art 8(2)(b)	2.95, 5.62
5.120, 5.123, 5.147,	Art 8(2)(c)	4.11
App 3 337–360, App 15–519	Art 8(2)(e)	2.79
Art 1(1)	Art 8(4)	2.93
Art 1(2)	Art 8(5)	2.93, 2.96
Art 1(4)	Art 8(6)	1.69
Art 2	Art 9	1.50, 1.95, 2.55 , 2.56, 2.58, 4.15
Art 2(a)	Arts 10–11	1.40
Art 2(b)	Art 10	1.95, 1.96, 2.94, 2.99, 3.49, 5.120, 5.145
Art 2(c)	Art 11	1.96, 3.49, 5.120
Art 2(d)	Art 12	1.40, 1.50, 1.95, 2.02, 5.217
Art 2(e)	Art 13	1.95, 4.72
Art 2(f)	Art 13(1)	1.50
Art 2(h)	Art 13(2)	1.50
Art 3(1)	Art 14	1.50, 2.07, 5.217
Art 3(2)	Art 14(a)	1.40, 5.28, 5.165
Art 4	Art 14(b)	2.17, 2.99, 5.190
1.50, 1.76, 1.95, 3.04, 3.06 ,	Art 14(1)(b)	1.25, 2.07
3.07, 3.08, 3.12, 3.13, 3.14,	Art 15	2.07
3.15, 3.17, 3.18, 3.19, 3.20, 3.21,	Art 15(1)	1.50, 2.07
3.23, 3.27, 3.30, 3.31, 3.38, 3.39,	Art 15(2)	2.07
3.44, 3.45, 3.46, 3.51, 3.52, 3.61,	Art 17	1.40, 1.72, 2.28, 2.29, 4.63, 4.78, 4.99, 5.31, 5.137, 5.176, 5.177, 5.216, App 9
3.66, 3.80, 4.31, 4.32, 4.33,	Art 17(1)	1.69, 5.135
4.66, 5.34, 5.34	Art 17(2)–(4)	2.28
Art 4(1)		
Art 4(1)(a)		
Art 4(1)(b)		
Art 4(1)(c)		
Art 4(2)		
Art 5		
Art 5(3)		

Table of Primary and Secondary Legislation

Directive 95/46/EC, [1995]	Art 28(3)	1.30
OJ L281/31 General Data	Art 28(6)	3.10
Protection Directive (<i>cont.</i>)	Art 28(7)	1.28
Art 17(2)	Art 29	1.18 , 1.19, 1.20, 1.24, 1.28, 1.50, 1.51, 1.52, 1.57, 1.69, 1.71, 1.76, 1.81, 1.82, 1.96, 2.13, 2.16, 2.32, 2.41, 2.56, 2.66, 2.72, 2.76 , 2.79, 2.81, 3.24, 3.27, 3.28, 3.30, 3.31, 3.33, 3.34, 3.36, 3.49, 3.58, 4.12, 4.31, 4.37, 4.39, 4.51, 4.53, 4.57, 4.58, 4.73, 4.83, 4.103, 4.105, 4.106, 4.109, 4.110, 4.115, 4.116, 4.118, 4.119, 4.120, 4.125, 4.127, 4.130, 4.132, 4.135, 4.136, 4.138, 5.36, 5.37, 5.41, 5.62, 5.64, 5.66, 5.72, 5.81, 5.83, 5.84, 5.96, 5.98, 5.99, 5.117, 5.122, 5.134, 5.196, 5.202, 5.203, 5.207, 5.209, App 11–471, App 13 App 14 , App 15–519
Art 17(3)	Art 29(1)	1.19
Arts 18–21	Art 30(b)	4.51
Art 18	Art 31	1.12, 1.21, 1.23, 1.24, 1.76, 4.29, 4.51, 4.73
Art 18(1)	Art 31(2)	1.76, 4.68
Art 18(2)	Art 32(1)	1.95
Art 19(1)	Art 33	1.69, 1.95
Art 19(2)	Recital 7	4.78
Art 20	Recitals 8–9	1.63
Art 20(1)	Recital 9	1.62
Art 21(2)	Recital 12	4.79
Art 23	Recital 14	4.79
Art 23(1)	Recital 15	4.72
Arts 25–26	Recital 19	2.51, 3.40
Art 25	Recital 24	2.37
2.47, 3.27, 3.30, 4.07, 4.10, 4.12, 4.13, 4.23, 4.24, 4.32, 4.33, 4.37, 4.39, 4.65, 4.103, 4.126	Recital 26	2.75
Art 25(1)	Recital 47	3.27
4.14 , 4.51, 4.66	Recital 58	4.11, 4.116
Art 25(2)	Recital 60	4.15
4.51, 4.56, 4.58, 4.68	Directive (EC) 1997/7 [1997]	
Art 25(3)	OJ L144/19 Distance Selling	
1.09, 4.51	Directive	1.57, 3.30, 3.58
Art 25(4)	Art 9	1.57
1.21, 1.76	Art 10	5.191
Art 25(6)	Directive (EC) 97/66 [1998]	
1.21, 1.76, 4.27, 4.58, 4.72	OJ L24/1 Telecommunications	
Art 26	Data Protection Directive	1.49, 1.52, 1.69, 5.213, 5.218, 5.219
1.95, 4.10, 4.12, 4.23, 4.24, 4.32, 4.33, 4.37, 4.39, 4.40, 4.58, 4.103	Directive (EC) 98/27	5.191
Art 26(1)	Directive 98/34/EC	
1.96, 2.13, 2.16, 4.12, 4.13, 4.28, 4.39, 4.103, 4.105, 4.106, 4.109, 4.110, 4.116, 4.119	Art 1	1.55, 5.194
Art 26(1)(a)		
4.10, 4.105		
Art 26(1)(b)		
4.10, 4.107, 4.109, 4.110		
Art 26(1)(c)		
4.107, 4.110		
Art 26(1)(d)		
1.48, 4.10, 4.112		
Art 26(1)(e)		
4.11		
Art 26(1)(f)		
2.79, 4.11		
Art 26(2)		
1.96, 4.10, 4.12, 4.13, 4.28, 4.29, 4.39, 4.68, 4.85, 4.99, 4.103, 4.120, 4.126, 4.127, App 15–525		
Art 26(3)		
1.69, 1.95, 4.28, 4.29, 4.101		
Art 26(4)		
1.21, 1.76, 4.25, 4.28, 4.58, 4.68, 4.71, 4.85, 4.99, 4.125		
Art 27		
1.76, 1.96		
Art 27(1)		
1.76		
Art 27(2)		
1.76		
Art 27(3)		
1.76		
Art 28		
1.28, 1.30, 1.40, 3.11, 4.28, 5.30		
Art 28(1)		
1.33		

Table of Primary and Secondary Legislation

Directive (EC) 1999/5 [1999]	Recital 8	1.64
OJ L91/10 Radio and	Recital 10	1.50, 1.54, 3.66
Telecommunications Terminal	Recital 17	5.203
Equipment Directive	Directive (EC) 2002/65	5.191
1.73	Directive (EC) 2003/98 [2003]	
Directive (EC) 1999/93 [2000]	OJ L345/90 Re-use of Public	
OJ L13/12 Electronic Signatures	Sector Information Directive	1.57
Directive	Directive (EC) 2006/24 Data Retention	
Art 8	Directive	1.54, 1.64, 1.76, 3.65,
1.57	3.66, 3.67, App 5 379–390	
Directive (EC) 2000/31 [2000]	Art 1	3.66
OJ L178/1 E-Commerce &	Art 1(1)	1.55
Internal Market Directive	Art 1(2)	1.55
1.57,	Art 4	1.55
5.119, 5.212	Art 5	1.55
Art 6	Art 6	1.55
1.57	Art 7(d)	1.55
Art 7	Art 8	1.55
1.57, 5.190	Art 9	1.55
Directive (EC) 2002/21 [2002]	Art 15(1)	1.64
OJ L108/33 Regulatory Framework	Art 15(3)	1.55, 1.64
Directive	Recital 6	1.64
1.69, 3.54, 5.194	Recital 15	3.66
Art 2(a)		
1.55		
Art 2(c)		
1.55, 3.54		
Art 2(d)		
3.54		
Directive (EC) 2002/58 [2002]		
OJ L201/37 of 12 July 2002 Privacy		
and Electronic Communications		
Directive		
1.17, 1.49, 1.52, 1.54,		
1.55, 1.64, 1.69, 1.73, 1.76, 1.80,		
2.37, 2.74, 3.52, 3.54, 3.55, 3.56,		
3.57, 3.58, 3.59, 3.60, 3.62, 3.63,		
3.64, 3.66, 3.67, 5.65, 5.123,		
5.139, 5.149, 5.191, 5.194, 5.195,		
5.196, 5.205, 5.212,		
App 4 362–378, App 10–465		
Art 1(1)		
3.53		
Art 1(3)		
2.37		
Art 2(h)		
5.202		
Art 3		
3.53, 3.55, 3.57, 5.194		
Art 3(1)		
1.50, 3.58		
Art 4		
3.57, 5.72, 5.136,		
5.139, 5.147		
Art 4(2)		
5.136, 5.146		
Art 5(3)		
1.64, 3.55		
Art 6		
1.64, 3.57		
Art 13		
3.55, 5.190,		
5.194, 5.196		
Art 13(2)		
5.196, 5.209		
Art 13(3)		
5.190		
Art 13(4)		
5.204		
Art 13(5)		
5.206		
Art 14		
5.194		
Art 14(3)		
1.73		
Art 50(1)(2)		
2.37		
Recital 5		
3.55		
Recital 7		
2.37		

Regulations

Regulation (EC) 44/2001 [2001] OJ L12/1	
(Brussels Regulation)	3.09, 3.60
Art 5(3)	3.09
Recital 21	3.09
Regulation (EC) No 45/2001 [2001]	
OJ L8/1	1.16, 1.76, 5.38
Art 47(1)(i)	1.17
Regulation 1049/2001 [2001]	
OJ L145/43	2.64
Regulation (EC) No 1882/2003	1.23

NATIONAL LEGISLATION

Argentina

Habeas Data Act (2000)	4.04
Art 12	4.04
Personal Data Protection Act	
(4 October 2000)	1.01

Australia

Privacy Amendment (Private Sector)	
Act 2000 (WP40)	4.57

Austria

Data Protection Act 2000	2.40,
5.137, App 3–335	

Table of Primary and Secondary Legislation

Data Protection Act 2000 (<i>cont.</i>)	Protection of Personal
§ 3 3.13, 3.14	Data Act App 3–335
§ 3(1) 3.38	Denmark
§ 3(3) 3.36	Electronic Communications Act
§ 4(1) 2.12	(No 450 2003) App 4–361
§ 4(15) 2.52	Personal Data Protection Act
§ 6(3) 3.49	§ 3(1) 2.37
§ 9 2.95	§ 4(3) 3.17
§ 12 App 11–472	§ 41 5.137
§ 12(3) 4.24	§ 43(2)(8) 5.39
§ 12(3)(2) 2.12	§ 43(2)(9) 5.39
§ 12(3)(5) 4.105	§ 50(1) 2.94
§ 18(2) 5.35	Processing of Personal Data
§ 30(6)(2) 1.82	Act 2000 App 3–335
§ 46 2.31	Estonia
§ 53 5.40	Personal Data Protection
Telecommunications Act 2003	Act 2003 App 3–335
s 107 App 4–361	Society Service Act 2004 App 4–361
Belgium	Finland
Act of 11 December 1998	Personal Data Act 1999 App 3–336
Art 3bis 1 3.18	§ 7 2.97
Data Protection Act 2.97	§ 11 2.93
Art 6 2.97	Protection of Privacy in Electronic
Art 6(2) 2.95	Communications 2004 App 4–361
Art 17(3)(4) 5.39	Protection of Privacy in Working
Art 17(3)(9) 5.39	Life Act 2004 5.61
Art 17(3)(10) 5.39	France
Law on the Protection of Personal	Communications Act 1.55
Data 2006 App 3–335	Confidence in the Digital Economy
Legal aspects of Information Society	Law 2004–575 5.194,
Services Law 2003	App 4–361
Art 13 App 4–361	Data Protection Act (Loi 78–17)
Art 14 App 4–361	1978 5.90, App 3–336
Canada	Art 2 2.82
Personal Information Protection and	Art 7(5) 5.28
Electronic Documents Act	Art 8 2.97
(PIPEDA) 4.51	Art 22(3) 5.38
Cyprus	Art 25 5.35
Processing of Personal data (Protection	Art 30.I(5) 5.39
of Individuals) Law 2001 (amended	Art 30.I(6) 5.39
2003) App 3–335	Art 30.I(8) 5.39
Regulation of Electronic	Art 35 4.44
Communications and Postal Services	Art 39 5.39
Law (Num.112(I)2004) App 4–361	Art 69(8) 4.130
Czech Republic	Labour Code
Certain Information Society Services	Art L 431-5 5.107
Act (480/2004) 5.196, App 4–361	Art L 432-2-1 5.106
§ 7 5.205	Art L 483-1 5.108

Table of Primary and Secondary Legislation

Germany	
Federal Data Protection Act (BDSG)	2.32, 2.44, 3.17, 4.28, 5.112, App 3–336
§ 1(5)	3.16 , 3.22, 3.38
§ 3a	2.09, 2.31
§ 3(1)	2.82
§ 3(4)3	2.44
§ 3(6)	2.08
§ 3(6a)	2.08
§ 3(8)	2.45
§ 3(9)	2.97
§ 4(1)	5.110
§ 4(3)	5.126
§ 4(3)(2)	2.30
§ 4a(3)	2.18
§ 4b(6)	2.91
§ 4c(2)	4.130
§ 4d(5)–(6)	5.35
§ 4d(4)	5.38
§ 4d(5)	2.97
§ 4f	5.38
§ 9	5.137
§ 9a	1.74
§ 11	5.177
§ 28	2.35
§ 28(1)–(3)	5.28
§ 28(6)	2.97
§ 35(2)(3)	5.219
§ 38	1.86
§ 44	1.82
Telecommunications Act	
(TKG)	App 4–361
§ 3(10)	1.50, 5.65
§ 6	1.50
§ 88	1.50, 5.65
§ 88(2)	5.65
§ 109	1.50
Teleservices Data Protection Act	
(TDDSG)	1.27, 2.11
§ 4(1)	5.126
§ 4(2)–(3)	2.18
§ 6(3)	2.09
Unfair Competition Act	
2004	App 4–361
§ 8(3)(3)	1.34
Works Council Act (BetrVG)	5.111
§ 75(2)	5.109
§ 80(1)(1)	5.109
§ 87	5.67, 5.110
Greece	
Data Protection Act (Law 2472/1997)	
.	3.15, App 3–336, App 10–467
Art 3(3)(a)	3.38
Art 3(3)(b)	3.15
Art 6(1)(b)	5.39
Art 6(1)(e)	5.39
Art 7(1)(a)	5.46
Protection of Personal Data and Private	
Life in the Electronic Communications	
Sector	App 10–467
Protection of Personal Data in the	
Telecommunications Sector Act	
(2774/99)	App 4–361
Hong Kong	
Personal Data Ordinance	1.01
Hungary	
Data Protection Act	
§ 9	4.30
Electronic Commerce Services and	
Information Society Services Act	
(No CVIII 2001)	App 4–361
Electronic Communications Act	
(No C 2003)	5.194, 5.196, App 4–361
Protection of Personal Data and	
Disclosure of Data of Public Interest	
Act No LXIII 1992	App 3–336
Ireland	
Data Protection (Amendment)	
Act 2003	App 3–336
s 3(b)	2.95
Electronic Communications Networks	
and Services Act 2003	5.194, App 4–361
Italy	
Data Protection Act 1996	
Art 15(2)	5.137
Art 24	2.93
Data Protection Code 2004	5.41, App 3–336, App 4–361
Art 113	5.114
Penal Code	
Art 650	5.115
Personal Data Protection Code 2003	
s 31	5.137
Arts 32–36	5.137
Workers' Statute (law 300 of 1970)	
Art 4	5.114
Art 4(1)	5.114
Art 4(2)	5.114, 5.115

Table of Primary and Secondary Legislation

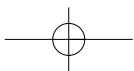
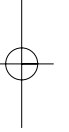
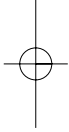
Workers' Statute (law 300 of 1970) (<i>cont.</i>)	Decree on Standardized exemptions, para 2	5.113 5.46
Art 19		5.113
Art 28		5.115
Art 38		5.115
Latvia		
Electronic Communications		
Law 2004	App 4–361	
Personal Data Protection		
Law 2002	App 3–336	
Lithuania		
Electronic Communications Law 2004		
Art 68	App 4–362	
Legal Protection of Personal data		
Law 2003	App 3–336	
Governmental Resolution No 262	5.38	
Luxembourg		
Data Protection Act		
Art 12(3)(a)	5.38	
Art 13(1)(b)	5.39	
Art 13(1)(h)	5.39	
Art 14	5.35	
Protection of Persons with regard to the Processing of Personal Data		
Law 2002	App 3–336	
Specific Matters of Personal Protection		
Law 2005	App 4–362	
Criminal Instruction Code 2005		
Art 88(2)	App 4–362	
Art 88(4)	App 4–362	
Malta		
Data Protection Act (CAP 440)		
2001	App 3–337	
Data Protection Act 2002	App 3–337	
§§ 30–31	5.38	
Processing of Personal Data		
Regulations (Telecommunications Sector) 2003	App 4–362	
Netherlands		
Personal Data Protection Act (WBP)	2.49, 4.11, 4.77, 4.86, App 3–337	
Art 1a	2.82	
Art 1(b)	2.42	
Art 8f	5.28	
Art 62	5.38	
Art 76	2.49	
Telecommunications		
Act 2004	App 4–362	
Poland		
Protection of Personal Data		
Act 1997	App 3–337	
Art 6	2.82	
Art 23(5)	5.28	
Art 36	5.137	
Civil Code, Act of 23 April 1964	3.49	
Provision of Services by Electronic Means Act 2002	5.194, 5.196, App 4–362	
Portugal		
Data Protection Act 1998	App 3–337	
Art 3(a)	2.82	
Art 6(e)	5.28	
Art 29(e)	5.39	
Art 29(f)	5.39	
Art 29(g)	5.39	
Art 29(h)	5.39	
Decree Law No 7/2004	App 4–362	
Russia		
Federal Personal Data Act (2007)		
Art 11	4.04	
Slovakia		
Data Protection Act	App 3–337	
Electronic Communications Act (No 610/2003)	App 4–362	
Slovenia		
Consumer Protection		
Act 2003	App 4–362	
Personal Data Protection		
Act 2004	App 3–337	
§ 19(2)	5.38	
Spain		
Data Protection Act	App 3–337	
Art 6	4.19	
Art 12(2)	4.44	
Art 12(4)	2.27	
General Communications Law (32/2003)	App 4–362	
Information Society Services and Electronic Commerce Act (Law 34/2002)	3.63, 5.194, App 4–362	

Table of Primary and Secondary Legislation

<p>Organic Law 15/1999 of 13 December 1999 Art 3(a) 2.82 Art 12 4.21, 4.40</p> <p>Sweden</p> <p>Marketing Act 2004 App 4–362 Personal Data Protection Act 2.58, 2.59 § 13 2.97 § 16 2.95, 5.62 §§ 38–40 5.38</p> <p>United Kingdom</p> <p>Companies Act 1985 s 722 5.138 Data Protection Act 1998 1.19, 1.94, 2.06, 2.46, 3.49, 5.137, 5.216, App 3–337 Pt I 2.82 Pt V 1.86 s 27(1)–(2) 3.18 s 27(2) 3.49 s 27(3) 2.53 Sch 3 5.62 Financial Services Act 1986 5.138 Data Protection (Notification and Notification Fees) Regulations SI 2000/188 reg 3.2 5.46</p>	<p>Privacy and Electronic Communications Regulations 2003 App 4–362</p> <p>United States</p> <p>Constitution, 1st Amendment 4.72 False Statements Act 18 USC 1001 4.61 Federal Reserve Act 4.61 Federal Trade Commission Act 15 USC s 5 4.61 Patriot Act 2004 5.174 Sarbanes-Oxley Act 2002 (SOX) 5.87, 5.88, 5.90, 5.92, 5.96, 5.214, 5.215 s 301 5.88, 5.89 Securities Exchange Act 1934 s 10-A(m)(4) 5.88</p> <p>US Dept. of Commerce Document</p> <p>Safe Harbor Privacy Principles 2000 App 6</p> <p>State Legislation—California</p> <p>Computer Security Breach Notification Act (SB 1386) 5.140, 5.141, 5.142</p>
--	--

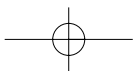
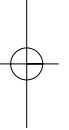
TABLE OF INTERNATIONAL INSTRUMENTS

<p>Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) 1.77, 4.51</p> <p>Convention Abolishing the Requirements of Legalisation for Foreign Public Documents (The Hague Convention) (5 October 1961) 4.87</p> <p>Convention for the Protection of Human Rights and Fundamental Freedoms (European Human Rights Convention) (Rome, 4 November 1950; TS 71 (1955)) 2.60</p> <p>Art 8 1.03, 2.83</p> <p>Art 10 2.54, 2.60</p>	<p>United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention) (10 June 1958) 330 UNTS 38</p> <p>Art II(3) 4.79</p>
--	---



LIST OF ABBREVIATIONS

B2B	business-to-business
B2C	business-to-consumer
BCRs	binding corporate rules
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CNIL	Commission Nationale de l'Informatique et des Libertés (French data protection authority)
DG	Directorate General
DG InfoSo	DG Information Society
DG Markt	DG Internal Market
DPA	data protection authority
EDPS	European Data Protection Supervisor
EEA	European Economic Area, ie EU Member States plus Iceland, Liechtenstein and Norway
EFTA	European Free Trade Association, ie Iceland, Liechtenstein, Norway and Switzerland
EICTA	European Information and Communications Technology Association
ENISA	European Network and Information Security Agency
EPOF	European Privacy Officers Forum
ETSI	European Telecommunications Standards Institute
EU	European Union
FEDMA	Federation of European Direct and Indirect Marketing
FTC	Federal Trade Commission
General Directive	Data Protection Directive (EC) 95/46
http	hypertext transfer protocol
ICRT	International Communication Round Table
IP	internet protocol
ISP	internet service provider
OECD	Organization for Economic Co-operation and Development
PNR	passenger name record
RFID	radio frequency identification
SMS	short message service, also known as text messages
SWIFT	Society for Worldwide Interbank Financial Telecommunication
WP	publications of the Article 29 Working Party



2

FUNDAMENTAL LEGAL CONCEPTS

A. Introduction	2.01	I. Data Transfer	2.42
B. Access and Related Rights	2.02	J. Establishment	2.51
C. Anonymous and Pseudonymous Data	2.08	K. Freedom of Expression	2.54
D. Consent	2.13	L. Freedom of Information	2.62
E. Data Controllers and Data Processors	2.19	M. Free Flow of Data within the EU	2.68
F. Data Minimization	2.30	N. Legitimacy	2.70
G. Data Processing: Definition and Grounds	2.33	O. Personal Data	2.73
H. Data Subject	2.36	P. Processing	2.87
		Q. Purpose Limitation	2.89
		R. Sensitive Data	2.92
		S. Third Party	2.99

A. Introduction

Clarification of legal issues under European data protection law often depends on evaluating fundamental legal concepts and determining how they fit into the appropriate business framework. Basic legal concepts are also important for data protection compliance. Many compliance issues are dependent on the application of basic concepts such as legitimacy and proportionality, which makes it imperative to have an understanding of them. **2.01**

B. Access and Related Rights

Article 12 of the General Directive grants data subjects the right to obtain certain basic information from the data controller about the processing of their personal data. While Article 12 explicitly requires only that exercise of the rights contained in section (a) (those of confirmation, communication, and knowledge) be 'without constraint at reasonable intervals and without excessive delay or expense', it is generally accepted in practice and under Member State laws that these conditions **2.02**

Chapter 2: Fundamental Legal Concepts

apply to the exercise of the rights contained in sections (b) and (c) (those of rectification, erasure, blocking, and notification to third parties) as well.¹

- 2.03** Complying with subject access requests gives rise to many difficult practical issues, such as how much information to provide; whether a reasonable fee may be charged; whether some of the information may be redacted (for example, if the information provided also contains personal data of third parties); and others. These points are all governed by the applicable Member State data protection law, which should be consulted when such issues arise.²
- 2.04** Given the distributed nature of computing nowadays, personal data might be contained in a variety of databases located in different geographic regions, so that it can be difficult to locate all the data necessary to respond to a data subject's request. Indeed, locating all the data pertaining to a particular data subject in order to allow him to know what data are being held about him, or to allow him to assert his rights of erasure, blockage, etc, might require the data controller to comb through masses of data contained in various databases, which in itself could lead to data protection risks.
- 2.05** The European Commission has found that the level of harmonization regarding the right of access is 'satisfactory',³ but substantial differences still exist among the Member States. For instance, in Finland the data controller may charge its costs in accessing the data and requests by data subjects are limited to one per year, while in the UK the controller may charge a fee of up to £10 for access to each entry and 'reasonable time' must elapse between requests. This disharmony of the law creates problems for data controllers that process data of data subjects from different Member States.
- 2.06** The UK Court of Appeal substantially limited the access right in *Durant v Financial Services Authority*.⁴ The Court refused the appellant Durant's request for disclosure of his unredacted computerized documents and manual records held by Barclay's Bank, first on the basis that the records did not all qualify as 'personal data', and second, that the manual records concerned may not constitute

¹ U Dammann and S Simitis, *EG-Datenschutzrichtlinie* (Baden-Baden: Nomos Verlagsgesellschaft, 1997) 199.

² Regarding practical issues under UK law see R Morgan and R Boardman, *Data Protection Strategy* (London: Sweet & Maxwell, 2003) 125–147.

³ European Commission, *First report on the implementation of the Data Protection Directive* (95/46/EC), COM(2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States 20.

⁴ *Durant v Financial Services Authority* [2003] EWCA Civ 1746, Court of Appeal (Civil Division). See paras 2.84–2.85 below. See also *Johnson v Medical Defence Union* [2006] EWHC 321 (Ch), in which the UK High Court further clarified the duties of data controllers in complying with subject access requests.

C. Anonymous and Pseudonymous Data

a 'relevant filing system' under UK data protection law.⁵ As this book was finalized, the *Durant* case was the subject of discussions between the UK government and the European Commission as to whether the judgment is in compliance with EU data protection law.

The General Directive grants individuals other rights as well, such as the right to object to data processing in certain situations (Article 14), and the right not to be subjected to 'automated individual decisions' (Article 15). The right to object to data processing is to be broadly interpreted.⁶ An 'automated decision' is defined as one 'which produces legal effects concerning a data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc'.⁷ Individuals are granted certain rights with regard to automated decisions, which are based on implementation in national law.⁸ An automated decision would be one, for example, in which based on certain numerical criteria a customer is denied a loan automatically, such as by computer, without any human intervention to make the final decision. Companies can reduce the risks by avoiding the use of automated decision-making as much as possible; the way to do this is to ensure that the final decision to grant or take away benefits or privileges to employees or customers is always made by a human being, rather than by a machine. **2.07**

C. Anonymous and Pseudonymous Data

European data protection law recognizes the concepts of *anonymous* and *pseudonymous* data. For example, the German Federal Data Protection Act defines the terms as follows: **2.08**

§3(6) Anonymising means altering personal data so that the individual information about personal or factual relations cannot be attributed to an identified or identifiable natural person, or this can only be done with an unreasonably large expenditure of time, cost, and effort.

⁵ In February 2004, the UK Information Commissioner released a commentary on the impact of the judgment on the interpretation of the Data Protection Act 1998, which was updated on 12 May 2004, and again on 8 September 2004.

⁶ See Decision of the European Ombudsman on complaint 2467/2004/PB against the European Commission, 9 June 2006, para 1.6, in which the Ombudsman upheld the case of a citizen whose complaint against the German federal state of Hamburg had initially been rejected by the European Commission. The citizen had alleged that Hamburg had transferred personal data to third parties who used it for marketing purposes, and that he had not been informed of this nor had the right to object. The Ombudsman found that 'a wider interpretation of Article 14(1)(b) of the Data Protection Directive might be required' than that which the Commission had recognized.

⁷ General Directive 95/46, [1995] OJ L281/31, Art 15(1).

⁸ Art 15(2).

Chapter 2: Fundamental Legal Concepts

§3(6)(a) Pseudonymising means replacing the name and other identifiable characteristics by a symbol, for the purpose of making identification of the person impossible or considerably more difficult.

- 2.09** These are fairly liberal definitions in comparison with what is contained, for example, in certain local German data protection laws, which contain an absolute requirement that it must be impossible for anonymized data to be traced back to an identifiable person.⁹ German law encourages anonymizing or pseudonymizing of data, for example, by requiring that they be used for processing whenever possible,¹⁰ and by stating that online profiling can be done only by pseudonym and that any user profile covered by a pseudonym may not be combined with data concerning the holder of the pseudonym.¹¹
- 2.10** One important difference between anonymous and pseudonymous data should be noted: while data which are truly anonymous cannot be tied to an identifiable individual and are not considered ‘personal data’, pseudonymous data *are* still subject to data protection law, since they could be tied to an individual. For instance, in Germany the holder of a pseudonym can exercise rights of access relating to information held by an online service relating to his pseudonym.¹² It should also be remembered that the terms ‘anonymous’ and ‘pseudonymous’ are relative, and that DPAs will look behind nomenclature to determine whether data truly does conform to the requirements for such data. As a rule of thumb, it is quite difficult to satisfy DPAs that data truly are anonymous, and companies should not assume that data will be found to be anonymous unless there are very strong reasons for arguing that they cannot be matched, by *anyone* and at any reasonable cost, with the identity of identifiable persons.
- 2.11** The question may arise as to whether an online alias, an IP address, or some other symbol which serves to hide the true identity of a user can be considered a ‘pseudonym’. A user browsing the internet might be identified to a website only by the IP address assigned to him by his ISP; does this mean that, if the website follows the user’s online activity and compiles a profile of it, the IP address can be considered a ‘pseudonym’ and such profile is permissible under the provision of the German Teleservices Data Protection Act cited above? There is no definitive answer to this question, but a number of DPAs would answer ‘no’, since the IP address was not personally selected by the user, and it is not clear how easily

⁹ See Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder, *Datenschutzfreundliche Technologien* (1998) 14.

¹⁰ German Federal Data Protection Act §3a.

¹¹ German Teleservices Data Protection Act §6(3). See C Golembiewski, ‘Das Recht auf Anonymität im Internet’ (2003) *Datenschutz und Datensicherheit* 129.

¹² L Gundermann, ‘E-Commerce trotz oder durch Datenschutz?’ (2000) *Kommunikation und Recht* 225, 233.

D. Consent

the ISP could go behind the IP address and find out the true identity of the user. On the other hand, some DPAs have stated in informal conversations that they are willing to deem an online alias selected by a user to be a pseudonym. So, there is still a great deal of uncertainty in this area.

Austrian law contains the concept of ‘indirectly personal data’, which is the case when a data controller, processor, or recipient of a data transfer cannot determine the identity of a data subject with legally permissible means;¹³ indirectly personal data are thus a kind of pseudonymous data. The processing of indirectly personal data is legally privileged; for example, their transfer outside the EU does not require approval of the Austrian DPA.¹⁴ They are often used in situations such as the processing of encrypted data in a pharmaceutical trial, when the data are encrypted and the encryption key is known only to the leader of the study.¹⁵ **2.12**

D. Consent

The General Directive defines consent of the data subject as ‘any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed’.¹⁶ The Article 29 Working Party has indicated that consent must satisfy four criteria in order to be legally valid: **2.13**

- ‘Consent must be a clear and unambiguous indication of wishes;
- Consent must be freely given;
- Consent must be specific;
- Consent must be informed’.¹⁷

This is quite a restrictive definition, which requires that the data subject be clearly informed in advance of what he is consenting to, and that any further processing of the data will be deemed not to have been consented to. This interpretation is in line with Member State laws, which define consent with similar restrictiveness.¹⁸ **2.14**

¹³ Austrian Data Protection Act 2000 §4(1).

¹⁴ Ibid, §12(3)(2).

¹⁵ See R Knyrim, *Datenschutzrecht* (Vienna: Manz, 2003) 15.

¹⁶ Art 2(h).

¹⁷ Article 29 Working Party, ‘Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995’ (WP 114, 25 November 2005) 10–12.

¹⁸ See, eg, P Blume, ‘Denmark’, in P Blume (ed), *Nordic Data Protection* (Copenhagen: DJØF Publishing, 2001) 20 (regarding Danish law); Swedish Personal Data Protection Act 1998 §3, which defines consent as ‘[e]very kind of voluntary, specific, and unambiguous expression of will by which the registered person, after having received information, accepts processing of personal data concerning him or her’ (translation from Blume, *Nordic Data Protection* (above) 231).

Chapter 2: Fundamental Legal Concepts

Also, Member States, courts have not hesitated to invalidate consent when it does not meet the conditions listed above.¹⁹

- 2.15** DPAs believe that there are special risks associated with obtaining consent in the context of electronic commerce, since there is increased danger that the data subject might not have been fully informed or might not really understand what he is consenting to.²⁰ Thus, if the data subject clicks ‘I accept’ on a form on a commercial website, his consent may be invalid if it is shown that the standard terms and conditions he was supposed to accept were very long and untransparent, and were buried somewhere on the site under several levels of hyperlinks, so that in effect he had not been given a reasonable opportunity to review and understand them before accepting. Also, language is obviously relevant, as a person cannot consent based on a document written in a language he does not fully understand.
- 2.16** Restrictions on consent exist in many other areas as well. DPAs believe that, in many instances, employees may not freely consent to the processing of their personal data, since their dependent relationship to their employer means that consent is not freely given.²¹ DPAs are also reluctant to allow consent as a legal basis for the transfer of personal data to countries outside the EU which do not provide an ‘adequate level of data protection’.²² Further, many DPAs will not recognize as valid consent given by a minor or child. These restrictions mean that companies are well advised to reduce their reliance on consent as a legal basis for data processing to situations where it is absolutely necessary.
- 2.17** The general definition of consent contained in Article 2 of the General Directive is not phrased in terms of whether consent must be ‘opt-in’ (ie, on the basis of an affirmative act, such as clicking a box on an online form) or ‘opt-out’ (ie, by failing to take action, such as not unclicking a box on such a form). Rather, it concerns whether the absence of the term ‘explicit’ (which is used, for example, in Article 8(2)(a) of the General Directive to refer to the level of consent that must be granted for the processing of sensitive data) indicates that opt-in consent is not required as a general matter. Article 2 seems to set a standard between opt-out and opt-in,

¹⁹ See, eg, Landgericht München, Judgment of 9 March 2006, no 12 O 12679/05 (2005) *Datenschutz und Datensicherheit* 309, in which a German court invalidated consent given to a rebate and discount system. The court found that the consent clause was not sufficiently transparent or highlighted, and that consent should be given on an opt-in rather than an opt-out basis.

²⁰ See P. Schaar, ‘Datenschutzrechtliche Einwilligung im Internet’ (2001) *Multimedia und Recht* 644.

²¹ See, eg, Article 29 Working Party, ‘Working document on the surveillance of electronic communications in the workplace’ (WP 55, 29 May 2002) 21, stating with regard to the monitoring of employee e-mails that ‘consent of workers must be freely given and fully informed and employers should not rely on consent as a general means of legitimising such processing’.

²² See Article 29 Working Party, ‘Working document, Article 26(1)’ (above n17) 10–12.

E. Data Controllers and Data Processors

since it does not require opt-in consent generally, but the requirement that the data subject ‘signify’ his consent seems to imply that simple inaction is insufficient, and that some sort of action is required to constitute ‘consent’.²³ Thus, for example, a data subject remaining totally silent would not in itself constitute ‘consent’, but this might be sufficient if combined with some other action (for example, silence combined with the fact that earlier on the data subject had given some positive indication of his consent). The General Directive also provides data subjects with a right to opt out of certain types of processing.²⁴

Some Member State laws also restrict the possibility to give consent electronically. **2.18** For instance, under the German Federal Data Protection Act, consent to the processing of personal data must be given ‘in writing’, meaning pen on paper,²⁵ unless consent is to be given in the course of using ‘teleservices’ under the Teleservices Data Protection Act,²⁶ in which case consent may be given electronically under certain conditions.

E. Data Controllers and Data Processors

The General Directive divides the universe of actors who process personal data into ‘data controllers’ and ‘data processors’, which are defined as follows in Article 2: **2.19**

- (d) ‘controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- (e) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller . . .

The classification of an actor as a ‘controller’ or a ‘processor’ has important consequences in a number of areas, including the following: **2.20**

- most data protection obligations under the General Directive must be met by the controller;

²³ W Kotschy, ‘Directive 95/46/EC’, in *Concise European IT Law* (The Hague: Kluwer Law International, 2006) 35.

²⁴ See Art 14(b), which provides data subjects with the right to object to the use of their personal data for direct marketing purposes.

²⁵ §4a(3).

²⁶ §4(2)–(3) specify that electronic consent when using teleservices must (1) be given by an unambiguous and deliberate act of the user; (2) be recorded; and (3) be accessible at any time by the user. This allows consent by internet and e-mail, and removes the uncertainty caused by the previous formulation of the law which seemed to require the use of digital signatures using asymmetric cryptography for electronic consent. See P Schaar, *Datenschutz im Internet* (Munich: CH Beck, 2002) 181.

Chapter 2: Fundamental Legal Concepts

- in most cases, data controllers (rather than data processors) are liable for data protection violations,²⁷ and
- data processors have a severely reduced role, and, in effect, are supposed only to process personal data as directed by the controller.

2.21 Unfortunately, guidance issued by national DPAs is generally too vague to be of much value in determining when a company can be considered a data controller.²⁸ It is possible to have multiple controllers for the same data set, and the General Directive explicitly recognizes the possibility of there being such ‘co-controllers’,²⁹ though some Member States do not explicitly recognize the concept of ‘co-controller’.³⁰

2.22 Data processing in a business environment is often performed by corporate entities with highly complex structures, many of which may have access to or control, wholly or in part, over personal data. For example, in a multinational corporation the personnel department might enter employee data directly into a database, which might be accessible by other corporate entities established in different countries around the world, and be backed up on a computer system at the corporation’s home office on another continent. Indeed, such multiple access to data is becoming more common, as companies make use of the advantages of the internet to allow company-wide access to databases that were formerly managed only by a single department, and as they globalize their data processing structures.

2.23 In such cases, it can be extremely difficult to establish whether or not a particular entity ‘determines the purposes and means of the processing of personal data’ in the sense of Article 2(d) of the General Directive. Among the issues that can arise in this context are two in particular.

- (1) **Whether an entity is sufficiently involved in the determination of the purposes and means of processing to be considered a controller.** Substantial inquiry into a company’s practices and procedures may be necessary to determine the extent to which a specific department, employee, or entity really has ultimate control over specific data. As an example, assume that parent

²⁷ See General Directive Art 23, which provides that ‘any person who has suffered damage as a result of an unlawful processing operation . . . is entitled to receive compensation from the controller for the damage suffered’ (though ‘the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage’).

²⁸ Eg, the UK Information Commissioner has issued the following definition of a data controller: ‘[a] person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed’. See press release dated 12 January 2001.

²⁹ Art 2(d): ‘“controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. . .’ (emphasis added).

³⁰ This is the case, for example, in France and Poland. However, the concept of ‘co-controller’ may be recognized by the DPAs in practice; this is the case, for example, in Poland.

E. Data Controllers and Data Processors

Company X is established in Germany, but has a subsidiary in Austria which gathers data on customers and employees. The controller for the data gathered by the subsidiary could be the subsidiary, or Company X, or both; the answer to this question will require an inquiry into the practices of both Company X and the subsidiary, as to which entity actually determines what is done to the data, whether they are transferred from the subsidiary to the home office, whether any written procedures exist as to which entity is entitled to use the data, etc. For example, if the entity is merely performing technical maintenance on a database, then it is probably a mere data processor, whereas if it is empowered to go beyond this and make decisions about the purposes for which the data are to be processed, then it is probably a data controller.³¹ DPAs generally hold that whether or not the company is independent is not the decisive factor in establishing whether there is a person in a particular place who is competent to determine the purposes of the processing of certain data, ie, a data controller. Rather, the question is whether or not there is a person who determines the purposes of the processing and where the actual control over the data occurs. 'Control' for data protection purposes is a very different concept than control under corporate law.

- (2) **Whether multiple controllers exist.** In the above example, assume that Company X is established both in Germany and in other Member States, and has a main database in Germany. However, the subsidiaries also have their own databases, which they maintain in their countries of establishment and which are merged into the main database stored at the home office via the internet. In this example, it would seem that both the parent German entity and the various subsidiaries would be data controllers, since the subsidiaries each have control over their national databases, and the parent would also have control over the national data when they are merged into the main database. Thus, German law would apply to the processing in the main database, and the Member State law of the country in which each of the subsidiaries is established would apply to the processing of the database over which that subsidiary has control. Each of these data controllers would thus be deemed to be a 'co-controller' with the controller established at the headquarters of the company, with the result that such co-controllers are jointly responsible for meeting data protection obligations towards the data subject.

The distinction between 'data controller' and 'data processor' is becoming increasingly difficult to apply in practice. When the General Directive was enacted, there **2.24**

³¹ See, eg, Report of the Hessen (Germany) DPA for 2001, Hessischer Landtag Drucksache 15/4659, 26 November 2002, §7.2, commenting that the mere technical maintenance of a database would most likely indicate that a party was only a data processor, but that powers in excess of this could indicate that it was a data controller.

Chapter 2: Fundamental Legal Concepts

was a much clearer distinction between parties who control the processing of data, and other parties who only process personal data on behalf of others. However, advances in computer technology and the scope of the internet have largely caused this distinction to break down. It is quite common nowadays for parties to process data jointly and to allocate their responsibilities with regard to processing in a way which does not allow for a clear distinction between the data controller and the data processor. For example, in complex outsourcing transactions, one party might be charged with processing personal data on behalf of another party, but may itself also be able to determine the purposes and means of processing to some limited extent. Moreover, the relationship of the parties might change quite rapidly as business models evolve and technology changes, so that one party might in effect be a data controller one week, and a data processor the next week.

- 2.25** The lack of clarity between the roles of data controller and data processor has substantial implications for legal compliance. National data protection law makes the necessary steps for legal compliance largely contingent on the characterization of a party as either a controller or a processor. Thus, for example, a data controller must typically take steps such as giving notice of data processing to affected data subjects, registering data processing with the national DPA, assuming liability for any data protection violations, etc. By contrast, the data processor must mainly comply with the instructions of the data controller and adopt adequate security measures. If it is not possible to clearly determine whether a party is a data controller or a data processor, then it becomes nearly impossible for parties to know exactly what their compliance obligations are.
- 2.26** Parties to data processing transactions often engage in a legal ‘tug of war’ as to whether they are data controllers or data processors, with each one attempting to structure the transaction so that it is a data processor and its counterpart is a data controller with all the attendant compliance obligations that controllers have. Companies should structure their data processing operations in order to ensure that, whenever possible, ambiguities with regard to the designation of data controllers are avoided, and that the data controllers are associated with establishments in Member States with data protection laws that are favourable to the company’s operations. However, in practice this is easier said than done, and companies must be ready to live with a certain amount of ambiguity as to whether they are acting as a data controller, a data processor, or both. The best strategy is to determine early on in the transaction whether the balance of facts argues for the company being defined as a data controller or data processor, structure the transaction to fit this characterization, and then stick to it as compliance questions arise.