Data Protection

A Practical Guide to UK and EU Law

Fourth Edition

Peter Carey

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

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. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

First Edition published in 2009
Fourth Edition published in 2015

Impression: 1

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2014958062

ISBN 978–0–19–968712–1

Printed and bound by
CPI Group (UK) Ltd, Croydon, CR0 4YY

Cover image: © Shutterstock

1

HISTORY OF DATA PROTECTION AND INTRODUCTION TO THE LEGISLATION

INTRODUCTION

Data protection law gives people rights in their personal information, and it restricts the ways in which organizations can use people's personal information.

The perceived need for data protection legislation arose out of the growing use of computers in the 1970s and the threat to personal privacy that rapid manipulation of data potentially posed. In the United Kingdom the existing law at that time (which consisted of not much more than a possible action in breach of confidence) was insufficient to deal with concerns about the amount of information relating to individuals that was held by organizations in electronic form.

In the early 1970s, the Younger Committee on Privacy (Cmnd 5012, 1972) recommended ten guiding principles for the use of computers that manipulated personal data:

(a) Information should be regarded as held for a specific purpose and should not be used, without appropriate authorization, for other purposes.
(b) Access to information should be confined to those authorized to have it for the purpose for which it was supplied.

(c) The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.
(d) In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
(e) There should be arrangements whereby a subject can be told about the information held concerning him.
(f) The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.
(g) A monitoring system should be provided to facilitate the detection of any violation of the security system.
(h) In the design of information systems, periods should be specified beyond which the information should not be retained.
(i) Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
(j) Care should be taken in coding value judgments.

The UK government's response to the report of the Younger Committee was to publish a White Paper (Cmnd 6353, 1975). In it the government stated that, 'the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy' (paragraph 30). The threat to privacy was identified by the White Paper as arising from five particular features or characteristics of computer operations:

(a) They facilitate the maintenance of extensive record systems and retention of data in those systems.
(b) They can make data easily and quickly accessible from many different points.
(c) They make it possible for data to be transferred quickly from one information system to another.
(d) They make it possible for data to be combined in ways that might not otherwise be practicable.
(e) The data are stored, processed, and often transmitted in a form which is not directly intelligible.

The remit of the Younger Committee had been to consider whether legislation was needed to 'give further protection to the individual citizen and to commercial and industrial interests against intrusion into privacy by private persons and organisations'. The Committee was therefore concerned more with privacy than with data protection as such.

Although the proposals of the Younger Committee were never enacted, the government subsequently set up the Lindop Committee to obtain detailed advice on the creation and composition of a Data Protection Authority. Paragraph 2.04 of the Lindop Committee's Report (Cmnd 7341, 1978) stated:

> The Younger Committee had to deal with the whole field of privacy. Our task has been to deal with that of data protection. In fact, the two fields overlap, and the area of overlap can be called 'information privacy' or, better, 'data privacy'. It is an important area, and we have a good deal to say about it in this report. But it is not by itself the whole field of data protection, and we have had to consider some matters that do not directly raise questions of privacy. However, we found it useful to examine the concept of data privacy, and its implications and consequences. For this purpose we have used the term data privacy to mean the individual's claim to control the circulation of data about himself.

The Lindop Report went on to recommend the establishment of a Data Protection Authority and Codes of Practice particular to different sectors of the business community. These proposals were not ultimately implemented.

It was the Council of Europe Convention of 1981 that provided the impetus for the passage of the Data Protection Act 1984, the provisions of which correspond more closely with the Convention than with the Lindop Report (in fact the Convention had, at least in part, been based on the Younger Committee's Report). The most compelling reason for this was the desire of Parliament to conform to an internationally agreed standard for data protection. Without such provision the UK was likely to be excluded from a new-style club of countries that provided a basic level of protection for individuals and prohibited transborder data flows to non-members.

The Council of Europe's 1981 Convention contained the following principles of personal data processing:

(a) Personal data should be obtained and processed fairly and lawfully.
(b) Personal data should be stored only for specified purposes.
(c) Personal data should not be used in ways incompatible with those specified purposes.
(d) Personal data should be adequate, relevant, and not excessive in relation to the purposes for which the data are stored.
(e) Personal data should be accurate and where necessary kept up-to-date.
(f) Personal data should be preserved in identifiable form for no longer than is necessary.
(g) There should be appropriate security for personal data.
(h) Personal data should be available to be accessed by individuals, who additionally have rights of rectification and erasure.

DATA PROTECTION ACT 1984

The UK's first Data Protection Bill was introduced into the House of Lords in December 1982 but its passage was halted by the 1983 General Election. A second Bill, introduced in July 1983, went on to become the Data Protection Act 1984, one of the world's first substantial data protection enactments. Although the Act has been repealed, it may be of interest to consider its provisions.

General provisions

The 1984 Act introduced in the UK a new regime for the holding and processing of 'information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose' (data). For the first time, data users—those persons who held data—were obliged to register with a supervisory authority: the Office of the Data Protection Registrar. The Act introduced criminal offences for failing to comply with its provisions and a system of compensation for individuals who suffered damage by non-compliance.

The requirement to register with the Data Protection Registrar arose when a data user automatically (which basically meant 'using computers') processed 'personal data' (information which related to a living individual who could be identified from the information, including any expression of opinion about the individual). The registration form requested the following details:

(a) the name and address of the data user;
(b) a description of the personal data held and a statement of the purposes for which the data are held;
(c) a description of the sources from which the data are obtained, and persons to whom they may be disclosed;
(d) a list of the countries to which any data may be transferred; and
(e) an address for the receipt of requests from data subjects for access.

Once the Registrar was satisfied with the application, it was entered on the Register, which was open to public inspection. A person carrying on a 'computer bureau' needed only to register his or her name and address. A data user who processed personal data without being registered committed a criminal offence.

A data subject had the right to request access to any personal data that a data user held on him or her (a small fee was chargeable), and the data user was obliged to supply the information within 40 days of the request. The request could be enforced by the Data Protection Registrar or in the courts.

A data subject who suffered damage that was directly attributable to the inaccuracy, loss, or unauthorized disclosure of data could claim compensation from the data user. This right was enforceable in the courts. A further enforceable right of the data subject was to have any erroneous information held by the data user rectified or erased.

Data protection principles

The regime under the 1984 Act was underpinned by certain fundamental principles, which formed a code for the proper processing of personal data. The legislation adopted the model used in certain other European countries by expressing the eight principles in very general terms. For this reason they were not enforceable through the courts but only by the Data Protection Registrar and the Data Protection Tribunal (as the Information Rights Tribunal was then called). The principles, with one exception, were not dissimilar to those now contained in the Directive and the 1998 Act, and were as follows:

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up-to-date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled—
   (a) at reasonable intervals and without undue delay or expense—
      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (ii) to access to any such data held by a data user; and
   (b) where appropriate, to have such data corrected or erased.
8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure, or destruction of, personal data and against accidental loss or destruction of personal data.

Although the principles formed the backbone of the 1984 data protection legislation, there was no requirement as such to comply with their provisions. There were, however, potential consequences for non-compliance, such as, for example, the service of an enforcement notice.

THE DATA PROTECTION DIRECTIVE

The European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (referred to in this book as 'the Data Protection Directive' or 'the Directive') was adopted as a legislative measure in October 1995. As with all EU Directives, Member States are obliged to pass national legislation that gives effect to the Directive by the implementation date prescribed. Notwithstanding that Member States therefore have their own local implementing legislative measures, the Directive remains important. This is due to the general principle of EU law that Member States' implementing legislation must be interpreted to give effect to the Directive—this principle is overseen by the Court of Justice of the European Union, as the final court of appeal on matters of interpretation of EU law.

The current Member States of the European Union are shown in Box 1.1. In addition, the three non-EU members of the European Economic Area (Iceland, Liechtenstein, and Norway) have ratified the Directive. The Channel Islands and the Isle of Man are outside the European Union and, therefore, the Data Protection Directive does not apply to those islands.

Box 1.1 Membership of the European Union

Austria	Germany	Poland
Belgium	Greece	Portugal
Bulgaria	Hungary	Romania
Croatia	Ireland	Slovakia
Cyprus	Italy	Slovenia
Czech Republic	Latvia	Spain
Denmark	Lithuania	Sweden
Estonia	Luxembourg	UK
Finland	Malta	
France	Netherlands	

The Data Protection Directive required implementation in Member States by 24 October 1998. Only Sweden met this deadline. The UK complied with its legislative obligations by passing the Data Protection Act 1998, which came into force on 1 March 2000 (but allowed most organizations until 24 October 2001 to achieve compliance).

The Data Protection Directive, the full text of which is reproduced in Appendix 1, can be seen as a general framework legislative provision, which has, as its principle aims:

(a) the protection of an individual's privacy in relation to the processing of personal data; and
(b) the harmonization of data protection laws of the Member States.

It sets out the conditions under which the processing of personal data is lawful, the rights of data subjects and the standards of data quality. The Data Protection Directive seeks to establish an equivalent level of protection for personal data in all Member States so as to facilitate the transfer of personal data across national boundaries within the European Union.

The Directive applies to personal data processed wholly or partly by automatic means, and to manual data held in filing systems structured by reference to individuals, but it does not apply to activities that fall outside the scope of EU law. It excludes areas within Titles V and VI of the Treaty on European Union, public safety, defence, State security (including the economic well-being of the State when the processing relates to State security matters), and the activities of the State in areas of criminal law. It also specifically excludes domestic or household activities.

Conditions for processing

Article 6 establishes fundamental principles that have to be respected when personal data are processed. These principles are superficially similar to those in the 1984 Act. Detailed study, however, will reveal that they are of significantly wider application. Article 7 sets out a number of conditions that must be satisfied before data can be processed. Data processing must be undertaken only with the data subject's consent except when processing is necessary:

(a) for the performance of a contract to which the data subject is party;
(b) for compliance with a legal obligation;
(c) to protect the vital interests of the data subject;
(d) to perform a task carried out in the public interest or in the exercise of official authority; or
(e) to meet the legitimate interests of the data controller, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Sensitive personal data

Certain special categories of data which reveal information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, and data concerning offences and criminal convictions, may be processed only under certain strict conditions.

Fair collection

Where data are collected either from the data subject or from a third party, the data subject should be informed of the identity of the data controller, the purposes for which the data are used, and of any further information which is necessary to ensure fair processing.

Rights of individuals

The rights of individuals include:

(a) the right of access to personal data without constraint, at reasonable intervals, and without excessive delay or expense;
(b) the right to have incomplete or inaccurate data rectified, erased, or blocked;
(c) the right to object to processing of personal data, and, where there is a justified objection, to have the processing stopped;
(d) the right to object to personal data being used for the purposes of direct marketing;
(e) the right not to be subject to a decision that has legal effects or which significantly affects the individual and which is based solely on automated processing of data (unless the decision is in connection with a contract where the results do not adversely affect the data subject, or is authorized by law and provided that the data subject's interests are safeguarded).

Security

Data security must be such as to ensure that personal data are protected against accidental or unlawful destruction or accidental loss. Data must also be protected against unauthorized alteration, disclosure, or access, and all other forms of unlawful processing. The level of security must be appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of technology and cost.

Foreign transfers

The Data Protection Directive sets out the conditions under which personal data that are being processed or which are intended for processing may be transferred to countries outside the European Economic Area. In general, a transfer may take place only if the third country ensures an adequate level of protection for the rights and freedoms of data subjects. There are certain exceptions, for example, where the data subject gives consent or where the transfer is necessary for contractual performance or legally required on public interest grounds.

Data Protection Authorities

Each Member State is required to set up a supervisory authority to oversee the application in its own country of the national provisions giving effect to the Data Protection Directive. Computerized processing (which is essentially what 'automated' processing amounts to) operations must be notified to, and registered by, the supervisory authority. It is for Member States to decide whether or not to apply these requirements to manual data. There is provision for exemption from, or simplification of, the notification requirements in certain cases.

Compensation

Member States are required to provide adequate legal redress (including compensation for damage) for breach of the provisions of the Data Protection Directive.

The Article 29 Working Party

Article 29 of the Directive set up a Working Party (referred to in this book as 'the Article 29 Working Party' or 'the Working Party') to act as an independent advisory body on questions relating to the protection of individuals with regard to the processing of personal data.

The Working Party is composed of a representative from each Member State's Data Protection Authority, a representative for the EU institutions, and a representative from the Commission. The Working Party gives opinions and makes recommendations on aspects of European data privacy law that it feels are important. Whilst not legally enforceable per se, statements from the Working Party are taken seriously due to the nature of its composition. Thus, when considering the meaning of the words in both the Directive and the 1998 Act, as well as their practical application, regard should be had to any relevant opinion that has been issued by the Working Party. All documents issued by the Working Party are available on the

European Commission's website at: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>.

UK DATA PROTECTION ACT 1998

The Data Protection Act 1998 (referred to variously in this book as 'the DPA' or 'the Act' or 'the 1998 Act') implemented Directive 95/46/EC in the UK. It received the Royal Assent on 16 July 1998 and came fully into force on 1 March 2000. At the time of writing, the Act represents the current law in force in the UK. However, as for all Member States' implementing legislation, it is likely to be replaced by a European Regulation (known as the General Data Protection Regulation) which, at the time of writing, is still being discussed. Although the final text is not yet agreed, a brief summary of the proposed changes, based on the Commission's text, is included at the end of relevant chapters.

Changes from the 1984 Act regime

The 1998 Act, in implementing the Data Protection Directive, took data protection legislation to a new level of complexity in the UK. It provides a new definition of 'processing' (which includes virtually anything that can be done with data) and incorporated the following features which represent significant changes to the 1984 Act regime:

(a) *Manual processing*—The 1998 Act applies to certain paper-based records in addition to electronically (automatically) processed personal data.
(b) *Legitimacy of processing*—New conditions for processing exist as minimum threshold requirements before processing may be lawfully undertaken.
(c) *Sensitive data*—A new category of personal data has been created. Sensitive personal data may not be processed unless one of a set of certain pre-conditions is satisfied.
(d) *Data exports*—Transfers of personal data to countries outside the European Economic Area are banned unless certain conditions are satisfied.
(e) *Data security*—The security requirements were extended and new requirements regarding data processors were established.
(f) *Individual rights*—Significantly more and stronger rights for individuals exist under the new legislation including the right to compensation for damage or distress caused by unlawful processing.

Further discussion of the 1998 Act is not merited here, as it is the subject of much of the remainder of this book.

RELATIONSHIP BETWEEN THE DIRECTIVE AND THE ACT

It may be helpful briefly to consider the nature of European law and the relationship between such law and the national laws of Member States. There are two main types of legislation that derive from the European Union: Regulations and Directives. Regulations are immediately applicable in each Member State and require no local implementing legislation. Directives, on the other hand, must be implemented in Member States individually. Implementation is carried out by the creation of national laws by the Parliaments of each Member State.

The significance of this for global or European-based organizations is that they potentially have a multitude of laws to consider when undertaking business across national boundaries. Although the UK Act, as for each implementing statute in the other Member States, must be interpreted by national courts so as to give effect to the provisions of the Directive, there remain differences in the various national laws, not least due to the fact that the Directive allows Member States the freedom to implement various aspects of the law in their own particular way.

UK SECONDARY LEGISLATION

At the time of writing, 40 separate sets of Regulations, Orders, and Rules under the Data Protection Act have been produced. They add greater depth to, and in many cases, clarify, the provisions of the 1998 Act. The following legislation (which appears in Appendix 3) is dealt with, where relevant, in the remaining chapters of this book:

1. The Data Protection Act 1998 (Commencement) Order 2000 (SI 2000/183)
2. The Data Protection (Corporate Finance Exemption) Order 2000 (SI 2000/184)
3. The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 (SI 2000/185)
4. The Data Protection (Functions of Designated Authority) Order 2000 (SI 2000/186)
5. The Data Protection (Fees under section 19(7)) Regulations 2000 (SI 2000/187)
6. The Data Protection (Notification and Notification Fees) Regulations 2000 (SI 2000/188)
7. The Data Protection Tribunal (Enforcement Appeals) Rules 2000 (SI 2000/189)
8. The Data Protection (International Co-operation) Order 2000 (SI 2000/190)
9. The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 (SI 2000/191)

10. The Data Protection Tribunal (National Security Appeals) Rules 2000 (SI 2000/206)
11. The Consumer Credit (Credit Reference Agency) Regulations 2000 (SI 2000/290)
12. The Data Protection (Subject Access Modifications) (Health) Order 2000 (SI 2000/413)
13. The Data Protection (Subject Access Modifications) (Education) Order 2000 (SI 2000/414)
14. The Data Protection (Subject Access Modifications) (Social Work) Order 2000 (SI 2000/415)
15. The Data Protection (Crown Appointments) Order 2000 (SI 2000/416)
16. The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417)
17. The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (SI 2000/419)
18. The Data Protection Tribunal (National Security Appeals) (Telecommunications) Rules 2000 (SI 2000/731)
19. The Data Protection (Designated Codes of Practice) (No. 2) Order 2000 (SI 2000/1864)
20. The Data Protection (Miscellaneous Subject Access Exemptions) (Amendment) Order 2000 (SI 2000/1865)
21. The Data Protection (Notification and Notification Fees) (Amendment) Regulations 2001 (SI 2001/3214)
22. The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations 2001 (SI 2001/3223)
23. The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2002 (SI 2002/2722)
24. The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002/2905)
25. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 (SI 2004/3244)
26. The Information Tribunal (National Security Appeals) Rules 2005 (SI 2005/13)
27. The Information Tribunal (Enforcement Appeals) Rules 2005 (SI 2005/14)
28. The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2005 (SI 2005/450)
29. The Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2005 (SI 2005/467)
30. The Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068)

31. The Data Protection Act 1998 (Commencement No. 2) Order 2008 (SI 2008/1592)
32. The Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 (SI 2009/1677)
33. The Data Protection (Processing of Sensitive Personal Data) Order 2009 (SI 2009/1811)
34. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31)
35. The Tribunal Procedure (Amendment) Rules 2010 (SI 2010/43)
36. The Data Protection (Monetary Penalties) Order 2010 (SI 2010/910)
37. The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) (Amendment) Order 2010 (SI 2010/2961)
38. The Data Protection Act 1998 (Commencement No. 3) Order 2011 (SI 2011/601)
39. The Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2011 (SI 1034/2011)
40. The Data Protection (Processing of Sensitive Personal Data) Order 2012 (SI 2012/1978)

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

In December 2000, all three bodies of the European Union (EU) that have legislative functions—the European Commission, the European Parliament, and the Council—agreed in Nice (hence the 'Nice Charter') the Charter of Fundamental Rights of the European Union. The Charter represented the first occasion when the EU institutions had agreed on a set of individuals' rights, separate and distinct from (although related to, in terms of content) the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'). The Charter sought to give more effective legal force to existing rights by enshrining them as a 'fundamental' aspect of the EU.

Article 8 of the Nice Charter, with the title of 'Protection of Personal Data', provides as follows:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

In 2009, the Lisbon Treaty granted legally binding force to the Nice Charter, consolidating the existence in EU law of the fundamental right to the protection of personal data.

DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS

EU Directive 2002/58/EC on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ('the E-Privacy Directive') applies 'to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community'. It replaced the 1997 Telecoms Data Protection Directive (implemented in the UK by the Telecommunications (Data Protection and Privacy) Regulations 1999). As mentioned in the explanatory memorandum of the European Commission's document, the E-Privacy Directive is primarily aimed at adapting and updating the existing provisions to reflect new and foreseeable developments in electronic communications services and technologies. In other words, it is designed to be technologically neutral and hence to apply to transactions over the Internet in the same way as to transactions using telephone or fax. The E-Privacy Directive does not change or amend the Data Protection Directive and thus may be seen as an extra set of regulations applicable only to electronic communications (and e-commerce).

The preamble to the E-Privacy Directive states that:

> [t]he Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

The E-Privacy Directive was amended in 2009 by EU Directive 2009/136/EC. The 2009 changes included the introduction of security breach notification requirements for electronic communications service providers, and the obligation to obtain user consent to the use of cookies and similar technologies.

Amongst other matters, the E-Privacy Directive (as amended):

- imposes obligations on providers of publicly available electronic communications services to ensure the confidentiality of communications and related traffic data (for example, prohibiting tapping, interception, and surveillance);

- imposes a requirement to inform users of, and obtain their consent to, the use of devices to store information, or gain access to information stored, in the terminal equipment of a user (for example, via cookies, web bugs, hidden identifiers, and similar devices);
- requires service providers to provide options for restricting calling line identification;
- imposes a requirement to inform users of, and obtain their consent to, the processing of location data (unless only processed anonymously). Such processing must be necessary for a 'value added service' and users may withdraw their consent at any time;
- contains some exceptions to the rights and obligations described earlier, for example, where necessary to safeguard national security, defence, public security, or the prevention, investigation, detection, and prosecution of criminal offences;
- contains provisions relating to the retention of traffic data (also by reference to Directive 2006/24/EC on the retention of communications data);
- imposes obligations on providers of publicly available electronic communications services to maintain the security of the service. Such providers must notify their national regulator and, in some cases, individual subscribers, of security breaches involving personal data;
- gives a right to subscribers to electronic communications services to receive non-itemized bills;
- gives individual subscribers to communications services a right to determine whether their personal data are included in publicly available directories. Member States may also require subscriber consent where public directories have a purpose wider than a search of contact details based on name and a minimum of other identifiers;
- requires that the use of automated calling systems, fax, email, or short message service (SMS) for purposes of direct marketing to individuals is only permitted with the consent of the individuals. This is subject to a limited exception in respect of emails or SMSs to existing customers. For other unsolicited communications to individuals for direct marketing purposes (for example, by telephone), it is up to Member States to decide whether to require consent or to prohibit such communications only where individuals have indicated that they do not wish to receive them;
- requires Member States to ensure that the interests of corporate bodies are protected in relation to unsolicited communications; and
- prohibits the practice of sending unsolicited commercial emails disguising or concealing the identity of the sender, or without a valid address to which the recipient may send a request that such emails cease.

PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS

In October 2003, the Department of Trade and Industry (now the Department for Business, Innovation and Skills) published the final wording for the Regulations produced to implement the E-Privacy Directive (described above). These were amended in June 2004 and again in May 2011, the latter to reflect the changes to the E-Privacy Directive in 2009. The provisions of the Regulations differ slightly from those of the E-Privacy Directive that they are designed to implement, and are discussed in detail in Chapter 14 and, where relevant, throughout this book.

OTHER LEGISLATION

Data protection legislation cannot, in practice, be considered in isolation. Each area of personal or business life in which the reader is engaged will have its own rules and regulations.

In addition, when dealing with personal data, appropriate consideration must be given to the Human Rights Act 1998, the Freedom of Information Act 2000 (readers who work for, or advise, public bodies in the UK are referred to *Blackstone's Guide to the Freedom of Information Act 2000* by John Wadham, Jonathan Griffiths, and Kelly Harris, *Freedom of Information Handbook*, published by Law Society Publishing, and *Freedom of Information Journal*, published by PDP Journals), the Regulation of Investigatory Powers Act 2000, and to employment law generally.

When looking at the law applicable to electronic commerce, both the Directive on Consumer Rights and the E-Commerce Directive must additionally be considered.

PROPOSED GENERAL DATA PROTECTION REGULATION

The changes to existing law that have been proposed by the European Commission in the draft General Data Protection Regulation are considered at the end of each relevant chapter.