Data processing is a broad term, covering every conceivable thing that can be done to data: from initial collection to its final deletion, including its organization, alteration, use and disclosure. Data protection laws cover the processing of information relating to individuals. Every business and every person with a PC comes under data protection legislation.

Contents include:
- The Data Protection Act 1998
- Enforcing data protection laws
- Compliance
- Transparency
- The right of access to personal data
- The eight data protection principles
- Privacy and electronic communications
- Preventing processing
- Transborder data flows

Data Protection and Compliance in Context provides comprehensive and practical guidance on protecting data privacy. Ideal for those without qualifications or specialist knowledge of law, Data Protection and Compliance in Context is a trustworthy and accessible guide for small businesses, IT professionals and data protection officers.

About the author
Stewart Room, is the chair of the National Association of Data Protection and Freedom of Information Officers (NADPO). A barrister and solicitor, he is a partner at Rowe Cohen Solicitors and a visiting lecturer at Queen Mary, University of London.

This pragmatic guide: explains data protection laws; provides practical advice on protecting data privacy under the Data Protection Act, human rights laws and freedom of information legislation; gives data controllers a platform for building compliance strategies.
Data Protection and Compliance in Context
The British Computer Society

BCS is the leading professional body for the IT industry. With members in over 100 countries, BCS is the professional and learned society in the field of computers and information systems.

BCS is responsible for setting standards for the IT profession. It is also leading the change in public perception and appreciation of the economic and social importance of professionally managed IT projects and programmes. In this capacity, the society advises, informs and persuades industry and government on successful IT implementation.

IT is affecting every part of our lives and that is why BCS is determined to promote IT as the profession of the 21st century.

Joining BCS

BCS qualifications, products and services are designed with your career plans in mind. We not only provide essential recognition through professional qualifications but also offer many other useful benefits to our members at every level.

BCS membership demonstrates your commitment to professional development. It helps to set you apart from other IT practitioners and provides industry recognition of your skills and experience. Employers and customers increasingly require proof of professional qualifications and competence. Professional membership confirms your competence and integrity and sets an independent standard that people can trust. Professional Membership (MBCS) is the pathway to Chartered IT Professional (CITP) Status.

www.bcs.org/membership

Further Information

Further information about BCS can be obtained from: BCS, First Floor, Block D, North Star House, North Star Avenue, Swindon SN2 1FA, UK.
Telephone: 0845 300 4417 (UK only) or + 44 (0)1793 417 424 (overseas)
Contact: www.bcs.org/contact
Data Protection and Compliance in Context

Stewart Room, LLM
Barrister & Solicitor
Chairman, National Association of Data Protection and Freedom of Information Officers
Proprietor, DPA Law
Partner, Rowe Cohen Solicitors & Head of Information Law Unit
For Samantha and Annabel,
with all my love
## Contents

Figures and tables  
x
About the author  

xiii
Acknowledgements  

xv
Abbreviations  

xvii
Glossary  

xix
Useful Websites  

xxiii
Preface  

xxv

1 Introduction to Data Protection  

1
   Data Protection in the UK – The Data Protection Act 1998  

1
   Overview and history of data protection laws  

3
   Key aspects within data protection laws  

21
   Key words and phrases – data, personal data and processing  

29
   The DPA – important miscellany  

45

2 Transparency  

51
   Introduction  

51
   Consensual processing (including the first data protection principle)  

51
   Fair processing (the first data protection principle)  

54
   Processing for specified purposes (the second data protection principle)  

69
   Notification  

70
   The right of access to personal data  

79
   Information notices  

89
   Part IV exemptions  

92

3 General Rules on Lawfulness  

101
   Introduction  

101
   The first data protection principle  

102
   The second data protection principle  

104
   The third data protection principle  

105
   The fourth data protection principle  

108
   The fifth data protection principle  

109
   The sixth data protection principle  

111
   The seventh data protection principle  

112
Contents

Schedule 2 conditions (for personal data and sensitive personal data) 122
Schedule 3 conditions (for sensitive personal data) 126
The Data Protection (Processing of Sensitive Personal Data) Order 2000 133
The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 140
The Data Protection (Processing of Sensitive Personal Data) Order 2006 140
Part IV exemptions 140

4 The Right to Object
   Introduction 143
   Substantial and unwarranted damage or distress 143
   Direct marketing 146
   Automated decision taking 148
   Exempt manual data 150
   The right to object and the sixth data protection principle 151

5 Transborder Data Flows
   Introduction 152
   Third countries and adequate protection 153
   Derogations and binding corporate rules 161
   Derogations and contractual clauses 168
   Transborder data flows and the DPA 178

6 Privacy and Electronic Communications
   Introduction 183
   The Directive on Privacy and Electronic Communications 184
   UK implementation of DPEC 193
   Regulation of Investigatory Powers Act 2000 194
   Anti-terrorism, Crime and Security Act 2001 204
   Reconciling RIPA and ATCSA 204

7 Enforcing Data Protection Laws
   Introduction 206
   Enforcement by the data subject 206
   Enforcement by the data controller 210
   Enforcement by the European Commission 211
   Enforcement by the Information Commissioner 211
   Criminal proceedings 220

8 Compliance
   Introduction 231
   Prioritization of action 232
   Stage 1 – gathering information about data 234
Contents

Stage 2 – lawfulness and the criterion for legitimacy 240
Stage 3 – implementing compliance mechanisms 241

References 261

Index 271
Figures and tables

Figure 1.1 Does the DPA apply? 47  
Figure 8.1 Flow of data captured through a website 239

Table 1.1 Data quality 24  
Table 1.2 Criteria for making processing legitimate 25  
Table 1.3 Criteria for the processing of the special categories of personal data (sensitive personal data) 26  
Table 1.4 Structured data and relevant filing systems 35  
Table 1.5 Data in the public and private sectors 36  
Table 1.6 The meaning of personal data 36  
Table 1.7 The meaning of processing 41  
Table 3.1 The subject information provisions and the non-disclosure provisions 141  
Table 4.1 Direct marketing 147  
Table 6.1 The meaning of traffic data 198  
Table 8.1 Transparency and the supply of information 235  
Table 8.2 Categories of data subjects from the Information Commissioner’s templates 238  
Table 8.3 Processing within a financial services organization 240  
Table 8.4 Processing within a financial services organization, with criterion for legitimacy 241
About the author

Barrister and solicitor Stewart Room is a partner at Rowe Cohen Solicitors, where he heads the Information Law Unit and the firm’s London office. He has previously been in private practice at the Bar. His clients include EMC², Computer Associates, Dell, Novell, Hitachi, Fujitsu, the Chartered Institute of Public Finance and Accountancy, the Direct Marketing Association, the Federation of Small Businesses, Veredus, UNICEF, the National Theatre and the International Cricket Council. Stewart Room is the National Chair of the National Association of Data Protection and Freedom of Information Officers (NADPO) and a member of the BCS Information Privacy Expert Panel. He is also a visiting lecturer on Computer and Communications Law, Queen Mary, the University of London, and the proprietor of DPA Law, a leading online resource on data protection and privacy.
Acknowledgements

I do have some very important acknowledgements to make. First and foremost I wish to thank my wife, Samantha, for all of her encouragement and support throughout the writing of this book and in the six years leading up to it. If it was not for Samantha I would not have been confident enough, or sufficiently informed, to tackle this project. Thank you Samantha, I owe you everything.

My partners at Rowe Cohen Solicitors are also very deserving of mention, for giving me the space, time and encouragement I needed to grow our position in the data protection legal market place. Particular thanks are due to Ian Lewis, Graham Small and Simon Cohen.

I also wish to acknowledge my peers in data protection, from whom I have learned so much. They have all contributed to this book in some way. First, my colleagues at the National Association of Data Protection and Freedom of Information Officers (NADPO), who have accorded me the very great privilege of electing me to the Chair of this most impressive organization. I do encourage others to join NADPO and to take a role in its new National Council. Dr Ian Walden, at the Centre for Commercial Law Studies, Queen Mary, is also owed a debt of gratitude. He has been a great inspiration.

I would like to thank two other great supporters. First, my pupil master, Charles Joseph of Tanfield Chambers, who nurtured me as a young barrister and has been a great help to me ever since. Second, my assistant, Emily Chantzi, an excellent data protection lawyer in her own right and a good friend whose value cannot be overstated.

I would also like to thank Hugh Small, for giving me a comfortable and quiet place to work.

Finally, thanks to Matthew Flynn, Florence Leroy and Suzanna Marsh at the BCS, my colleagues on the BCS Information Privacy Expert Panel, the BCS itself and my copy editor Sarah Price, of Sprite Documentation Services, and my proofreader Barbara Eastman, who have helped to make sense of my ramblings.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATCSA</td>
<td>Anti-terrorism, Crime and Security Act 2001</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>DPEC</td>
<td>Directive on Privacy and Electronic Communications</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EEC</td>
<td>European Economic Community</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently asked question</td>
</tr>
<tr>
<td>FSA</td>
<td>Financial Services Authority</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Government Communications Headquarters</td>
</tr>
<tr>
<td>HR</td>
<td>Human resources</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>IFA</td>
<td>Independent financial advisor</td>
</tr>
<tr>
<td>NSA</td>
<td>National Supervisory Authority</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>Ofcom</td>
<td>Office of Communications</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal digital assistant</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger name record</td>
</tr>
</tbody>
</table>
Glossary

Anonymization  The removal of personal identifiers so that information no longer identifies a living individual.

Article 29 Working Party  An independent body with advisory status that is constituted under Article 29 of the Data Protection Directive. It is composed of representatives of the national supervisory authorities for data protection and European Community (EC) officials. Its duties require it to examine the operation of the Data Protection Directive and to provide opinions and advice to the European Commission.

Binding Corporate Rules  A scheme approved by a Decision of the European Commission for making lawful the transfer of personal information within a group of companies, covering the situation where information is transferred from a company situated within the European Economic Area (EEA) to a company situated in a country outside of the EEA.

Blagging  A colloquialism for the unlawful obtaining of personal information by a person who conceals their true identity by pretending to be a person with a lawful entitlement to the information sought.

Bluetooth technologies  Bluetooth is a an industrial specification for wireless personal area networks, used to connect Bluetooth enabled devices such as personal digital assistants (PDAs), mobile telephones and laptop computers.

Convergence  The term given to the harmonization in 2002 of EC laws regulating communications by telecommunications, internet and broadcasting media.

Council of Europe  An intergovernmental human rights organization that was founded after the Second World War, now with 46 Member States.

Council of Europe Data Protection Convention 1981  The first and only European treaty on data protection.

Data  For the purposes of the Data Protection Act 1998, (i) information that is being processed by automated equipment; (ii) information that is recorded with the intention that it will be processed by automated equipment; (iii) information that is recorded as part of a relevant filing system or with
the intention that it should form part of a relevant filing system; (iv) information that forms part of an accessible record; and (v) recorded information held by a public authority.

**Data controller**  A person or organization with the power to control the purpose or manner of processing of personal data.

**Data processor**  A person or organization that processes personal data on behalf of a data controller.

**Data protection principles**  For the purposes of the Data Protection Act 1998 a series of eight rules for the fair, lawful, legitimate and safe processing of personal data. It is the data controller’s duty to comply with the data protection principles.

**Data subject**  A person who is the subject of personal data.

**Digital safe**  A colloquialism for a storage device for digital information that provides highly robust security.

**EC Data Protection Directive 1995**  A legal instrument of the EC implemented in the UK by the Data Protection Act 1998. The Data Protection Directive protects the fundamental rights and freedoms of natural persons, particularly their right to privacy with respect to the processing of personal data. The Directive also outlaws prohibitions and restrictions on the flow of personal data between EC Member States for reasons connected with the protection of fundamental rights and freedoms.

**Electronic shredding**  A colloquialism for the process by which digital information is permanently deleted from a storage device by repeated overwriting with new binary code.

**European Community (EC)**  Part of the European Union established in 1957 as the European Economic Community by the Treaty Establishing the European Community.

**Fair processing**  A key requirement within the data protection principles. Personal data must be processed fairly, meaning, among other things, that personal data must be collected by a fair method and that the data subject should be provided in most cases with the data controller’s identity, a description of the purposes for which the data are intended to be processed and information about any unusual or non-obvious circumstances.

**Firewall**  A logical barrier that is designed to prevent unauthorized or unwanted communications between parts of a computer network.

**Information Commissioner**  The national supervisory authority for the UK, established for the purposes of ensuring compliance with the requirements of Article 28 of the Data Protection Directive.
Information Tribunal (Data Protection Tribunal)  The tribunal established under the Data Protection Act 1998 for hearing appeals from information and enforcement notices served by the Information Commissioner.

Informational privacy  A key element within a state of privacy describing the right that individuals enjoy to control the flow of information about themselves.

Lifecycle  As in information lifecycle, the period between the initial collection of data and its final deletion or destruction.

Necessity test  A precondition of many of the conditions for making the processing of personal data and sensitive personal data legitimate is that the processing should be necessary for the particular purpose.

Non-adequate country  A country situated outside the EEA that does not ensure an adequate level of protection for personal data undergoing processing.

Organisation for Economic Co-operation and Development (OECD)  An intergovernmental organization that provides a forum for the governments of 30 leading market democracies to discuss and develop policies to meet the challenges of globalization.

Personal data  Information relating to an identified or identifiable living individual.

Recipient  Any person to whom personal data are disclosed in the course of processing done by, or on behalf of, the data controller, apart from persons who receive personal data as a result of a particular inquiry made in exercise of legal powers, such as the Information Commissioner or the police.

Relevant filing system  A highly structured manual file containing personal data. Such a file must be structured by reference to criteria relating to living individuals so as to give easy access to the personal data within.

Safe harbor  A scheme approved by a decision of the European Commission for making lawful the transfer of personal information from within the EEA to commercial undertakings in the US that have declared their compliance with the safe harbor principles.

Subscriber  A person or organization that subscribes to a publicly available electronic communications service.

Substantive privacy  A key element within a state of privacy describing the right that individuals enjoy to take substantive decisions about how they live their lives.
**Glossary**

**Technological measures**  In order to protect personal data, it is a requirement of the Data Protection Directive and the Data Protection Act that data controllers should take technological measures to guard against accidental loss and damage to personal data and unauthorized use. Technological measures include firewalls, anti-virus software and other privacy enhancing technologies.

**Technological threats**  Technological threats to personal data include malicious software, spyware, adware, ransomware and cookies.

**Teleworking**  A working arrangement in which employees enjoy flexibility in their place of work, hours of work and means of work. Rather than attending the workplace they connect to the workplace through electronic communications networks.

**Third party**  Anyone other than the data controller, the data subject or the data processor. A third party can be a natural person or legal persons, such as companies.

**Transborder data flows**  The movement of personal data across national boundaries.

**User (in the context of user and subscriber)**  A person who uses an electronic communications service.

**Value added service**  Any electronic communications service that requires the processing of traffic data or location data beyond what is necessary for the transmission of an electronic communication or its billing.

**White list**  A colloquialism for the group of countries situated outside the EEA whose laws, according to decisions made by the European Commission, ensure an adequate level of protection for personal data that are undergoing processing.
Useful Websites

Council of Europe  www.coe.int
DPA Law  www.dpalaw.co.uk
European Court of Human Rights  www.echr.coe.int/echr
European Union  www.europa.eu
European Commission data protection website  www.ec.europa.eu/justice_home/fsj/privacy
Council of the European Union  http://ue.eu.int/cms3_fo/index.htm
European Court of Justice  http://curia.europa.eu
European Parliament  www.europarl.europa.eu
European Data Protection Supervisor  www.edps.eu.int
UK Information Commissioner  www.ico.gov.uk/eventual.aspx
Information Tribunal  www.informationtribunal.gov.uk
Office of Public Sector Information  www.opsi.gov.uk
Organisation for Economic Co-operation and Development  www.oecd.org
US Department of Commerce safe harbor pages  www.export.gov/safeharbor/index.html
US Federal Trade Commission  www.ftc.gov/privacy
Preface

My publisher, Matthew Flynn at the British Computer Society, set a very challenging brief for this book. Taking account of the intended price, a modest 100,000 word allowance and a nine-month time limit, the idea was to write a book on data protection that will be of the greatest use to our target readers who are data protection officers and other professionals working in data protection, including consultants, training course providers and lawyers.

We hope that this book will also be of some assistance to people studying on data protection courses, but I should clarify at the outset that we did not set out to write a course book for the ISEB certificate in data protection, although I would estimate that we have covered about three quarters of the ISEB syllabus. I readily accept that the complete novice to data protection might struggle with the style and contents, but I will be publishing more penetrable summaries of the chapters on my website www.dpalaw.co.uk to act as companion guides for these readers.

The core of this book consists of a walk through and analysis of the Data Protection Act 1998 and related legislation supported by references to case law, European law and official guidance issued by the Information Commissioner and the Article 29 Working Party (an official body established by the Data Protection Directive) as appropriate. Of course, due to the constraints of space I have not been able to include everything, so I would encourage readers to regularly check my website for updates and more detailed references.

Chapter 1, ‘Introduction to Data Protection’, endeavours to put the Data Protection Act into context. I have tried to explain the history of data protection and how the law has developed, showing the wider international and European aspects of the law and the relationship with the right to privacy. I have also tried to identify the key aspects of data protection laws, including their aims and objectives, which involved tackling the main words, phrases and definitions, such as ‘data controller’, ‘data subject’, ‘data processor’, ‘data’, ‘personal data’ and ‘processing’. If all of this can be distilled down to one sentence, I would suggest that data protection laws have been formulated at intergovernmental level to achieve a balance between the right to privacy and the wider economic, political and social interest in ensuring that flows of personal information between countries are maintained.

Chapter 2, ‘Transparency’, is more thematic, drawing together a series of issues that are connected by one common thread. I have called this common thread ‘transparency’, because the law contains a multifaceted framework
that requires the data controller to give the data subject and the Information Commissioner adequate information about its processing operations, that is, the data controller must be transparent about these operations. Thus, Chapter 2 discusses consensual processing, fair processing, processing purposes, notification, the right of access and information notices. There are exceptions to the transparency provisions, however, which are identified. Subject to these exceptions, it might be fair to say that data protection laws require data controllers to adopt a ‘cards-up’ approach.

Chapter 3, ‘General Rules on Lawfulness’, identifies and analyses the basic processing standards required of data controllers, another key aspect of data protection laws, and contains the main discussion of the ‘data protection principles’. There are eight data protection principles in the Data Protection Act and in combination with the transparency provisions they provide the foundations upon which data protection laws are built. At this junction I should highlight the fact that the first and second data protection principles are also discussed within Chapter 2. Thus it can be said that transparency is part of lawfulness as well as being a standalone topic in its own right. Again, there are exceptions.

Chapter 4, ‘The Right to Object’, discusses the circumstances in which the data subject can prevent the data controller from processing their personal data. The right to object empowers the data subject to take control over their personal data and is a vital compliance mechanism in its own right.

Chapter 5, ‘Transborder Data Flows’, discusses the law concerning the movement of personal data between countries. In summary, European Community data protection laws prevent the flow of personal data to countries outside of the European Economic Area that do not offer adequate protection for privacy, although this rule can be overcome by use of certain approved devices, such as model contractual clauses endorsed by the European Commission, and in special circumstances, such as when the data subject consents to the transfer. Within the Data Protection Act it is the eighth data protection principle that contains the key provisions.

Chapter 6, ‘Privacy and Electronic Communications’, is concerned with the modified data protection rules that regulate the processing of personal data over electronic communications networks, such as the internet or by telephone.

Chapter 7, ‘Enforcing Data Protection Laws’, looks at the powers vested in the data subject, the Information Commissioner and the courts that can be used to enforce the requirements of the laws. The role of the criminal law is discussed, as is the right of the data subject to seek compensation for damage and distress. The regulatory tools at the disposal of the Information Commissioner are all identified.

Chapter 8, ‘Compliance’, aims to provide data controllers with some practical guidance on how they can start to make their processing operations legally compliant. Of course, the topic of compliance could fill a book of this size all by itself, so compromises in the coverage are inevitable I am afraid.
However, I hope that this chapter provides data protection officers with some inspiration. This chapter will be expanded upon on my website.

Data protection is a topic of global importance. Data protection laws can be found in all the major industrialized nations, they are being developed for developing nations and they are the focus of significant intergovernmental cooperation. International organizations, such as the United Nations, the Organisation for Economic Co-operation and Development, the Council of Europe and the European Community (EC), have invested heavily in data protection, issuing guidance and laws that are remarkably consistent in terms of their aims, objectives and requirements.

**DATA PROTECTION IN THE UK – THE DATA PROTECTION ACT 1998**

In the UK the framework piece of legislation is the Data Protection Act 1998, or ‘DPA’ for short. The DPA repealed and replaced its predecessor, the Data Protection Act 1984, in order to give effect to the requirements of the EC Data Protection Directive 1995. The DPA also gives effect to the requirements of the Council of Europe’s Data Protection Convention 1981. The DPA is supplemented and supported by many other pieces of legislation, which will be introduced at appropriate places.

The DPA describes itself as being an Act that makes ‘new provision for the regulation of the processing of information relating to individuals’. This statement is worth thinking about, for it has massive ramifications. Putting it simply, the processing of information relating to individuals is something that we all do. Every government body processes information relating to individuals, as does every public authority, every business and every person with a PC.

**Processing personal data – information relating to data subjects**

However, it is only the processing of information relating to identifiable living individuals that is regulated by the DPA. The DPA does not regulate the processing of information relating to unidentified or unidentifiable living individuals, or the processing of information relating to the deceased or the processing of information relating to companies, non-incorporated organizations (such as clubs and societies), public authorities, charities or similar bodies. Information relating to identifiable living individuals is known as ‘personal data’ and the people whose personal data are processed are known as ‘data subjects’.
Automated and manual processing by data controllers and data processors

The Act regulates both automated processing of personal data, that is, processing done by computers, and limited kinds of manual processing of personal data, but only where the processing is performed by ‘data controllers’ and ‘data processors’. The data controller, who is characterized by having the power to determine the purpose of the processing or the manner of the processing, carries most of the obligations under the DPA. A data processor processes personal data on behalf of a data controller, but is not an employee (for the purposes of the DPA employees of data controllers form part of the data controller). The data controller is ultimately responsible for ensuring that the data processor’s activities are compliant with the DPA.

The concept of processing

The concept of processing is extremely wide, covering every conceivable act that can be done on or towards personal data, from its initial collection right through to its final deletion or destruction. Acts of processing include organization, adaptation or alteration of data, retrieval, consultation or use of data, disclosure of data by transmission and dissemination and the alignment, combination, blocking, erasure or destruction of data.

Summary – the key things to remember

A person who is interested in data protection should remember the following things:

- Data protection laws regulate the processing of personal data by data controllers and data processors. The DPA also concerns ‘third parties’ and ‘recipients’. A third party is anyone other than the data controller, the data subject or the data processor and can include legal persons, such as companies, as well as individuals. A recipient is any person to whom personal data are disclosed in the course of processing done by or on behalf of the data controller, apart from persons who receive personal data as a result of a particular inquiry made in exercise of legal powers, such as the Information Commissioner or the police.

- The fairness, lawfulness and legitimacy of data processing are benchmarked against the ‘data protection principles’. There are eight data protection principles in the DPA.

- The Information Commissioner is the UK’s supervisory authority, responsible for promoting the following of good practice by data controllers and for enforcing compliance with the DPA.

- Personal data is information relating to living individuals and includes opinions about living individuals and indications of the data controller’s intentions towards living individuals.

- Within Europe, the most important laws are the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Data Protection Convention and the Data Protection Directive.
• Within Europe, the main law-making bodies are the Council of Europe, the EC, the Article 29 Working Party, the national governments, the national supervisory authorities and the courts.

• The aims of data protection laws are twofold: they protect privacy and they support the free flow of personal data between data controllers and between countries.

• The DPA replaced and repealed the Data Protection Act 1984, in order to give effect to the requirements of the Data Protection Directive 1995. The DPA also gives effect to the requirements of the Data Protection Convention 1981.

OVERVIEW AND HISTORY OF DATA PROTECTION LAWS

The DPA forms part of a comprehensive and harmonized European legal framework for the regulation of the processing of personal data. This framework is a consequence of work done by the Council of Europe and the EC. Of course, data protection laws can be found outside of Europe too.

The two principal aims of data protection laws

Wherever they are found, data protection laws have two principal aims. These are:

• The protection of privacy during the processing of personal data.
• The maintenance of free flows of personal data between countries. This requires the elimination of obstacles to the free flow of personal data between countries that are based solely on the protection of privacy.

These dual aims certainly appear to be in conflict (privacy of personal information v. the free flow of it), but data protection laws have to deal with the realities of modern life, which include the fact that free flows of personal information are vital to the economy and to the effective performance of public functions, hence they must be maintained. Maintaining free flows of personal data obviously interferes with personal privacy, so the law compensates for the interference by requiring a high level of protection for the privacy of personal data undergoing processing. The high level of protection is that prescribed by data protection laws themselves, which put in place strong mechanisms to prevent unfair or unlawful processing. Ensuring a high level of protection for the privacy of personal data that is undergoing processing is a prerequisite to the continuance of free flows of personal data.

Putting the same point differently, the law will allow a person to transfer data to another person or to another country provided that the transferor meets the minimum standards prescribed by the law.
Laws in Europe should be in harmony – the reason for Council of Europe and EC activity

The Council of Europe and the EC are the two organizations responsible for the development of data protection laws in Europe. These organizations are separate and distinct. The Council of Europe, founded in 1949, is essentially a human rights organization consisting of 46 European Member States. The other organization, the EC, started life as the European Economic Community in 1957 and it currently has 25 Member States. The UK, like all other EC Member States, is a member of both organizations and the DPA gives effect to the requirements of the data protection laws of both organizations, namely the Data Protection Convention and the Data Protection Directive.

The Council of Europe and the EC have taken the lead in the development of data protection laws within Europe due to the fact that European governments recognize that there need to be harmonized data protection laws across Europe in order to achieve the two principal aims of data protection, namely the protection of privacy and the maintenance of free flows of personal data.

The need for harmonization of laws is explained by the fact that a key theory within data protection laws is that differences in the levels of protection offered by national laws can cause obstacles to the free flow of personal data between countries, that is, a country with a high level of protection for privacy could impede the flow of personal data to a country with weaker protection. The harmonization of laws addresses this problem, because where laws are harmonized the scope for differences between countries on fundamental issues is removed.

It would be a mistake to fall into the trap of thinking that the harmonization process requires the national laws of the countries within the area of harmonization to be exactly the same. Harmonization is not meant to achieve exactness in the laws of each participating country. In fact, despite harmonization, participating countries have a wide margin for manoeuvre, with the result that differences in national laws are still being detected. For instance, penalties for breach of data protection laws differ from country to country.

The protection of privacy

Privacy is a very wide concept. It includes the private space (such as the home), private items (such as letters and photographs), private relationships (such as sexual relationships) and private information (such as information about people).

The right to respect for personal privacy is a recognized human right. Within Europe the principal human rights law is the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (or the ‘ECHR’ for short). The ECHR has been incorporated into UK law by the Human Rights Act 1998.
Article 8 of the ECHR protects the right to privacy and provides the founding principles upon which European data protection laws are built. It says:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It often comes as a surprise to learn that neither the DPA, nor the Data Protection Convention or the Data Protection Directive have tried to define the meaning of the word privacy. Thus, we need to look elsewhere for a definition.

**Concepts within privacy – informational and substantive privacy**

One early definition of privacy that still holds well is that it is a ‘right to be let alone’.\(^5\) This definition is supported by two newer concepts, ‘substantive privacy’ and ‘informational privacy’. The theory behind substantive privacy is that people should be free to make substantive decisions about how they lead their lives, free from interference by the State or by others. The theory behind informational privacy is that people should be able to control the flow of information about them. These two concepts are interconnected and a state of informational privacy is often a prerequisite to enjoyment of substantive privacy.

To illustrate, imagine a country passing a law to ban the practice of a particular religion. Such a ban interferes with substantive privacy, that is, the freedom of individuals to choose to practice the religion. The State’s interference with substantive privacy will not be enough to completely eradicate the religion, however, as devotees will practice in private, out of view of the State. If the State really wants to eradicate the religion, it will also need to identify who is practising the religion, which means interfering with informational privacy.

**Privacy versus other rights and interests**

The right to privacy is not an absolute right in the sense that it does not transcend all other rights and interests. Instead, the right to privacy is one of many competing interests and it is the law’s job to find an appropriate balance between them. This is why Article 8.2. of the ECHR allows interference with the right to privacy by public authorities where the interference ‘is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the
country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

Another competing interest is freedom of expression, which is also a human right. Freedom of expression is a powerful friend of journalists and publishers who rely upon its terms to justify the publication of personal information, with the justification being that a free press is in the public interest. Article 10 of the ECHR says the following about freedom of expression:

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

Recent cases on the meaning of privacy

Although there is no universally agreed definition of privacy, in most cases the difficulty does not lie in deciding whether information is private, but, rather, whether the interference with privacy was lawful. Indeed, in a very important case, A v. B & C, Lord Woolf said:

the question of whether there is an interest capable of being the subject of a claim for privacy should not be allowed to be the subject of detailed argument . . . In those cases in which the answer is not obvious, an answer will often be unnecessary.

The difficult issue, whether the interference with privacy is lawful, is the issue to which data protection laws are addressed; that is, they seek to strike a balance between the privacy rights of the individual and the rights and interests of data controllers as far as the processing of personal data is concerned.

The following series of recent cases stand to illustrate the fact that a wide variety of information can be said to be private:

- In 2003 the European Court of Human Rights decided in the case of Peck v. United Kingdom that CCTV footage showing Mr Peck attempting to commit suicide in the street contained private information. This was despite the fact that his suicide attempt was in a public place.
- In 2004 the UK House of Lords decided in the case of Campbell v. Mirror Group Newspapers that covertly taken photographs showing the claimant outside premises where a Narcotics Anonymous meeting was held contained private information. This was despite the fact that the defendant enjoyed a legitimate press right to publish a story about the claimant’s attendance at Narcotics Anonymous in light of her previous denials of drug abuse.
- In 2004 the European Court of Human Rights decided in the case of Von Hannover v. Germany that covertly taken photographs of the
claimant in a French restaurant with a companion contained private information.

- In 2005 the UK Court of Appeal held in the case of *Douglas v. Hello! Ltd (No 2)*¹⁰ that covertly taken photographs at the claimants' wedding contained private information, despite the fact that the claimants were under contract with a magazine for publication of wedding photographs.

In the case of *Douglas v. Hello! Ltd (No 2)* Lord Phillips addressed the question ‘what is the nature of private information’. His answer was:

What is the nature of 'private information'? It seems to us that it must include information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public. The nature of the information, or the form in which it is kept, may suffice to make it plain that the information satisfies these criteria.

**The relationship between the ECHR and the DPA, including protections for manual data**

It is important to recognize that the connection between the ECHR and European data protection laws is inviolable. Data protection laws are best regarded as modified privacy laws, in the sense that they build upon the right to respect for privacy contained in Article 8 of the ECHR, in order to provide clearer protections for the privacy of personal data undergoing processing. In the UK because of the Human Rights Act 1998, the courts and the Information Commissioner are obliged when interpreting the DPA to ensure that their interpretations are compatible with the ECHR. Every court case commenced under the DPA can also be brought under the Human Rights Act.

If data protection laws are viewed in their wider context it will be seen that despite the limitation they place on the protections for the manual processing of personal data, privacy in manual data is generally protected due to the right to privacy within Article 8 of the ECHR. In the UK a breach of confidence action can be used to protect the right to privacy if in the circumstances of the case the data subject has a reasonable expectation of privacy. UK law has moved on significantly since the introduction of the Human Rights Act and clarification of the fact that the protections in Article 8 of the ECHR extend to threats from the private sector.

**The emergence of European data protection laws – law making to protect privacy**

The first European data protection law was a regional law passed by the German State of Hesse in 1970 (the first national data protection law was introduced by Sweden in 1973), but the movement towards European data protection laws actually began in the late 1960s after it had become appreciated that scientific and technological advances, particularly the invention of
the semi-conductor chip and increasing computerization within the private sector, posed new threats to personal privacy; it was foreseen that computers would be able to automatically process personal data in unprecedented ways, in unprecedented volumes and at unprecedented speeds. The passage below, taken from a Council of Europe Recommendation from 1968 provides a fascinating insight into the nature of the concerns at the beginning of the development of data protection laws:

newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy . . .

These new threats led to calls for new laws to protect privacy within the context of the automated processing of personal data stemming from worries about the adequacy of the protection for privacy afforded by Article 8 of the ECHR. To explain, while it is clear that Article 8 guarantees respect for private and family life, the home and correspondence, in the late 1960s, governments were not sure that the wording of Article 8 extended to computer processing or to threats to privacy emerging from the private sector. A Resolution issued by the Council of Europe in 1974 reported that:

A survey, conducted in 1968–70 by the Committee of Experts on Human Rights of the Council of Europe, on the legislation of the Member States with regard to human rights and modern scientific and technological developments has shown that the existing law does not provide sufficient protection for the citizen against intrusions on privacy by technical devices. Generally, the existing laws touch upon the protection of privacy only from a limited point of view, such as secrecy of correspondence and telecommunications, inviolability of the domicile, and so on. Moreover, the ramifications of the concept of privacy have never been established. It is also doubtful whether the European Convention on Human Rights, of which Article 8 (1) guarantees to everyone ‘the right to respect for his private and family life, his home and his correspondence’, offers satisfactory safeguards against technological intrusions into privacy. The Committee of Experts on Human Rights has noted, for example, that the Convention takes into account only interferences with private life by public authorities, not by private parties.

Privacy and the private sector
It is now settled that the right to privacy contained in the ECHR does apply to the private sector as well as to activities of the State and the public sector. This is despite the fears expressed in the early years of development of data protection laws. For example, in the case of Douglas v. Hello! Ltd (No 2) Lord Phillips explained that:
the European court has recognised an obligation on Member States to protect one individual from an unjustified invasion of private life by another individual and an obligation on the courts of a Member State to interpret legislation in a way which will achieve that result.

Thus, the State will protect an individual’s right to privacy from invasion by another individual, which includes private sector and voluntary sector companies and organizations. This is the effect of the decisions in *Campbell v. Mirror Group Newspapers* and *Von Hannover v. Germany*.

The late 1960s and early 1970s – the initial work undertaken by the Council of Europe: Data protection rules to protect privacy

The Council of Europe is an intergovernmental human rights organization that was established after the end of the Second World War. Its most famous legal instrument is the ECHR. The Council of Europe commenced its work in the field of data protection in 1968, at a time when a small number of its Member States were considering the introduction of national laws on data protection. In this year a Council of Europe Parliamentary Assembly issued Recommendation 509, which required the Council’s Committee of Experts on Human Rights to examine whether ‘having regard to Article 8 of the Convention on Human Rights, the national legislation in the Member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods’ and, if not, ‘to make recommendations for the better protection of the right of privacy.’

The efforts of the Committee of Experts on Human Rights resulted in the Council’s Committee of Ministers addressing two Resolutions to the Member States on the protection of privacy. The first Resolution, in 1973, \(^{13}\) concerned the protection of privacy in the context of private sector ‘electronic data banks’. The second Resolution, \(^{14}\) in 1974, concerned public sector electronic data banks.

Both of these Resolutions are based around a series of ‘principles’ that address the key privacy concerns within data protection, such as the accuracy of electronic personal data, the security of electronic personal data, the purposes for which electronic personal data are processed and the right of access. These principles have remained remarkably stable and consistent over the years and they can now be found, almost unchanged, within Schedule 1 of the DPA.

The Resolutions required the Council of Europe Member States to take all necessary steps to give effect to the principles. These Resolutions therefore represent the true beginnings of European data protection laws.

The UK’s first tentative steps towards data protection – the 1970s

The UK was one of the Council of Europe Member States that considered data protection at this initial stage of development of the law. In 1972 the
‘Report of the Committee on Privacy’ (sometime called the ‘Younger Report’, after its Chair, Kenneth Younger), published 10 principles for the handling of personal information by computers. In 1975 this Report was followed by two government white papers, which indicated plans for legislation on private sector and public sector computer use. These white papers were followed by the establishment of the Data Protection Committee in 1976, chaired by Sir Norman Lindop. The ‘Report of the Committee on Data Protection’ was published in 1978, recommending rules that mirror modern data protection laws.

Data protection between 1980 and 1990 – from privacy to maintaining free flows of personal data (transborder data flows)

The 10 years between 1980 and 1990 saw thinking on data protection laws develop and mature. While the primary focus of concerns in the late 1960s and early 1970s was the protection of privacy within the context of automated processing of personal data, the 1980s saw the emergence of the second aim of data protection laws, the removal of obstacles to the free flow of personal data between countries (sometimes called ‘transborder data flows’).

The transborder flow of personal data is of fundamental economic and societal importance. The global economy cannot survive without the movement of personal data between countries and across continents and the effective performance of vital public functions, such as law enforcement and the prevention and detection of crime, is often totally reliant upon data sharing between different countries.

Although the transborder flow of personal data is of fundamental economic and societal importance, it involves very obvious privacy implications arising from the fact that the person’s personal data leaves the borders of their country of residence, making it much harder to protect.

One foreseeable consequence of the drive to protect the privacy of personal data undergoing processing is that transborder data flows could be hindered, or prevented altogether, because of understandable fears that personal data will not be adequately protected when processed abroad. This consequence was addressed during the second phase of data protection laws, with the accepted solution being that once data protection laws were harmonized between countries it would be unlawful for one country to hinder or prevent data flows to another country within the harmonized area on the sole ground of protection of privacy; within the area of harmonization the right to privacy is adequately protected.

1980 – the OECD deals with transborder data flows

The first organization to address this issue was the Organisation for Economic Co-operation and Development (OECD). The OECD, which was originally established in 1947 as the Organisation for European Economic Co-operation, provides a forum for the governments of 30 leading market democracies to discuss and develop policies to meet the challenges of globaliz-
One of these challenges is the maintenance of transborder flows of personal data. In 1980 the OECD published its own data protection guidelines. The preface to these guidelines is highly illuminating of the issues:

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data.

The Guidelines contain a series of principles that echo those found in the Council of Europe’s initial 1973 and 1974 Resolutions, addressing issues such as the lawfulness of processing, the accuracy and security of personal data and transparency in processing. In respect of transborder flows of personal data, the Guidelines prefer a test of ‘equivalent protection’ saying that:

- a Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

1981 – the Council of Europe’s Data Protection Convention (Europe gets serious)

In 1981 the Council of Europe opened for signature the Data Protection Convention, the first and only European Treaty on data protection. The
principal reason for the Data Protection Convention was the Member States’ failure to respond to the 1973 and 1974 Resolutions in a consistent manner.

The Data Protection Convention represents a watershed for European data protection laws, being the moment when data protection moved from an aspiration to a fundamental goal. Like the OECD Guidelines, the Data Protection Convention echoed the principles contained in the 1973 and 1974 Resolutions and preserved the importance of free flows of personal data, saying that the Member States ‘shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party’. Thus, the Data Protection Convention cemented the second principal aim of data protection laws within Europe, namely the removal of obstacles to the free flow of personal data between countries.

1984 – the UK's first Data Protection Act

In 1984 the UK Parliament passed the Data Protection Act 1984, to give effect to the UK’s obligations under the Data Protection Convention. The 1984 Act regulated the ‘processing’ and the ‘disclosure’ of ‘personal data’ ‘recorded in a form in which it can be processed by equipment operating automatically’, that is, the processing of personal data by computers. Manual files were not regulated, a substantial omission rectified by the DPA.

From 1990 – the rise to prominence of the EC

In 1957 a small group of European countries created the European Economic Community (EEC) through the signing of the Treaty Establishing the European Economic Community, otherwise known as the Treaty of Rome. In 1997 the EEC was renamed the EC. The EC forms part of the European Union (EU) and it currently consists of 25 Member States. As stated earlier, the EC and the Council of Europe are separate entities.

During the first phase in the development of European data protection laws, from the late 1960s to the mid 1970s, the EEC played only a peripheral role. This was because the thinking behind the law in the first stage was focused upon the protection of privacy, which, as a human right, fell more naturally within the sphere of competence of the Council of Europe. However, the EEC was supportive of the developments in the field and in 1981 the European Commission issued a Recommendation addressed to the EEC Member States saying:

The Commission recommends those Member States of the Community which have not already done so to sign, during the course of 1981, the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data, and to ratify it before the end of 1982.

While the EEC was content to let the Council of Europe take the lead, its 1981 Recommendation also contained a statement of future intent, warning
the EEC member states that if they did not act promptly in signing and ratifying the Data Protection Convention, an EEC instrument could follow. This is what the Recommendation said:

The Commission of the European Communities accordingly welcomes the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data. It is of the opinion that this convention is appropriate for the purpose of creating a uniform level of data-protection in Europe. If, however, all the Member States do not within a reasonable time sign and ratify the convention, the Commission reserves the right to propose that the Council adopt an instrument on the basis of the EEC Treaty.

Unfortunately, by the end of the 1980s only a few of the EEC Member States had ratified the Data Protection Convention. Therefore, in 1990 the European Commission formally proposed the introduction of the Data Protection Directive. 18 This proposal marked the starting point of the EC’s leadership in European data protection and the relative downgrading of the importance of the Data Protection Convention. The Data Protection Directive was formally approved in 1995. 19

The EC, the Data Protection Directive and free movement

The Data Protection Directive is a very important harmonization measure that was introduced under the Internal Market provisions of the Treaty of Rome, to protect human rights and to maintain transborder flows of personal data. A recent report by the European Commission 20 has said:

[The Data Protection] Directive . . . enshrines two of the oldest ambitions of the European integration project: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important.

By way of background, the Treaty of Rome sets out the legal powers of the EC and at this moment in time the EC is unable to make standalone human rights laws, unlike the Council of Europe. Instead, it must base its laws on a specific power within the Treaty, hence the reason for the introduction of the Data Protection Directive as a harmonization measure under the Treaty’s Internal Market provisions, as is now explained.

The Treaty of Rome describes the Internal Market as ‘an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured’. In order to create the Internal Market, the Treaty requires ‘the abolition, as between Member States, of obstacles to the free movement of goods, persons, services and capital’. If it is not already clear, free movement is one of the principal goals of the EC, highly cherished
by politicians, businesses and EU citizens. Free movement entails many powerful rights and entitlements allowing, for example, workers to take up offers of employment from other EC Member States and enabling companies to set up offices abroad. Free movement improves the competitiveness of the European economy and benefits the consumer.

EXAMPLE

A London-based company wants to open an office in Paris. The ability to do this is based upon the free movement of services, capital and workers. It is highly likely that in this scenario there will be movement of persons, as the London-based company will no doubt want to send key management personnel to Paris to oversee the opening, which requires movement of information about these persons. Indeed, in the present scenario the movement of personal information between the London and Paris offices is inevitable. Typical incidents of transfer of personal information between the two offices will occur in the transfer of personnel records. However, if privacy laws could prevent the transfer of personal data from one country to the other, the business would soon grind to a halt and the rights of free movement would fail.

By 1990, when the creation of the Data Protection Directive was formally proposed, the EC (like the Council of Europe and the OECD) had long realized that differences (actual and potential) in the Member States’ national laws for the protection of privacy with respect to the processing of personal data could act as obstacles to free movement; a Member State with a high level of protection for privacy could ban the flow of personal data from within its borders to a Member State that provided a low level of protection for privacy, which would have obvious implications for free movement in the example.

Therefore, the EC decided that it was necessary to take action to bring the Member States’ national laws into line, based upon the provisions contained in the Data Protection Directive, a process known as harmonization. As mentioned earlier, the Directive’s provisions were designed to ensure a high level of protection for the fundamental rights and freedoms of natural persons, particularly the right to privacy. In addition, the Directive outlawed all national measures that restricted or prohibited the free flow of personal data between EC Member States for reasons connected with the protection of fundamental rights and freedoms. Based on this reasoning, the EC has been able to introduce the Data Protection Directive, which is clearly a human rights law, under the guise of protecting the Internal Market. Article 1 of the Directive, which describes its objectives, says:
In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

(2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

The EC has been able to overcome the prohibition against standalone human rights law making due to a number of factors. In addition to the factual connection between the protection of human rights and the proper functioning of the Internal Market, respect for human rights forms part of the general principles of EC law as well as part of the national laws of the EC Member States (the UK has the Human Rights Act 1998). It is also noteworthy that the EC is a signatory to the ECHR.

In conclusion, the thinking at the very heart of the Data Protection Directive connects the protection of privacy with free movement. The essence of the thinking is:

- Free movement of goods, persons, services and capital is impossible without free movement of personal data.
- Differences in national laws for the protection of privacy in personal data undergoing processing can act as obstacles to free movement.
- Differences in national laws can be overcome through a process of harmonization.
- Once national laws are harmonized, obstacles to free movement disappear.

**The structure of the Data Protection Directive**

The Data Protection Directive consists of 72 recitals and 34 articles. The recitals explain the theories behind the law and the motivations of the law makers, providing a vital aid to interpretation. The articles are arranged in seven chapters. The chapters are titled:

1. general provisions;
2. general rules on the lawfulness of the processing personal data;
3. judicial remedies, liability and sanctions;
4. transfer of personal data to third countries;
5. codes of conduct;
6. supervisory authority and working party on the protection of individuals with regard to the processing of personal data; and
7. community implementing measures.

As it is a harmonization measure the Data Protection Directive’s provisions leave EC Member States with much room for manoeuvre. Instead of prescribing in detail the obligations of the Member States, the Directive sets general principles and leaves the Member States to implement national measures in
the form and manner of their choosing. Due to this wide margin of discretion vested in the Member States there are still many differences in national laws and between national views and the EC’s view of how data protection laws should be.

Because it sticks to the general principles it is not surprising to see that certain concepts and phrases keep reappearing throughout the Directive. These will be encountered time and time again during an analysis of data protection laws and data protection in practice.

A very prominent concept within the Directive is ‘necessity’. This is because many of the grounds for making processing lawful are prefaced by the requirement that the processing should be necessary. Another prominent concept is ‘adequacy’, as the Directive prevents the flow of personal data from the EC Member States to other countries that do not offer adequate protection for personal data. A third prominent concept is ‘suitability’, as the Directive requires EC Member States to adopt ‘suitable measures’ to ensure the full implementation of its provisions. Collectively, these concepts provide the Member States with considerable discretion over the detail of their national laws.

The Data Protection Directive and the processing of manual data

A major advance made by the Data Protection Directive when compared to the Data Protection Convention was the extension of the law to cover manual data. While the Data Protection Convention gave Council of Europe Member States the option to regulate the manual processing of personal data, this was not compulsory. The Data Protection Directive changed this for EC Member States, making the regulation of manual processing compulsory where personal data are held in a ‘personal filing system’ (the DPA calls these ‘relevant filing systems’).

The Data Protection Directive and the European Economic Area

The Data Protection Directive is a legal instrument of the EC, but its protections extend to an area known as the ‘European Economic Area’ (EEA). The EEA is the combined area of the EC Member States and Iceland, Liechtenstein and Norway. The EEA was created by the Agreement on the European Economic Area in 1992.

The right to privacy in the UK

It has already been explained that the right to respect for privacy contained in Article 8 of the ECHR has been incorporated into UK law by the Human Rights Act 1998 (HRA). Due to the obligations placed on Member States by the ECHR it can now be said with certainty that the right to privacy will be protected by the UK courts, both from interferences by the State and by other individuals.

The HRA contains two key provisions that are central to the development of the law in this area. First, section 2 of the HRA requires courts and tribunals
to take into account decisions of the ECHR when determining a question that has arisen in connection with an ECHR right. Second, because of section 6 it is unlawful for courts and tribunals in their capacity as public bodies to act in a way that is incompatible with an ECHR right.

In the case of Campbell v. Mirror Group Newspapers\(^{21}\) Baroness Hale explained the court’s position. She said:

The 1998 Act does not create any new cause of action between private persons. But if there is a relevant cause of action applicable, the court as a public authority must act compatibly with both parties’ Convention rights.

The court’s obligation is to do justice between the parties and as a public authority it must perform this duty in a manner that is compatible with the Convention rights. The logical effect of these obligations is that the court should consider always whether a Convention right, like the right to privacy, is engaged in the case before it and this may often require a more detailed enquiry than merely asking the parties for their views. If the right to privacy is engaged the court will have to protect it and, if necessary, balance it against other interests, such as freedom of expression.

If an individual wishes to start a court action to protect their privacy, their claim is determined in accordance with the law of confidence, with private information being treated as confidential information. The individual will be successful if they can show that the person threatening their privacy knows or ought to know that the individual has a reasonable expectation that their information will remain private. In the case of Douglas v. Hello! Ltd (No 2)\(^{22}\) Lord Philips explained the law following a decision of Lord Woolf in A v. B & C.\(^{23}\)

Lord Woolf then laid down guidelines which a court should follow when considering a similar application. These include the proposition that in the great majority of, if not all, situations where the protection of privacy is justified in relation to events after the 1998 Act came into force, an action for breach of confidence will provide the necessary protection. As to interests capable of being subject to a claim for privacy, these will usually be obvious. A duty of confidence will arise whenever a party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected. If there is an intrusion in a situation where a person can reasonably expect his privacy to be respected then that intrusion will be capable of giving rise to an action for breach of confidence unless the intrusion can be justified.

The state of the UK law concerning the right to privacy is that this will be protected by the courts in a claim for breach of confidence. A data subject claiming a breach of the DPA may also rely upon the law of confidence in a court action to enforce their rights.
The future of data protection laws

The Data Protection Directive is now 10 years old, which represents nearly one-third of the total lifespan of data protection laws. The key thinking upon which the Directive itself is built will soon reach its 40th anniversary.

The nature of the threats to privacy has changed substantially since the Council of Europe took its first steps, which presents new challenges. Furthermore, experience of the laws in action, plus some unusual court decisions, have led to calls for revision of the Data Protection Directive. Two important areas of concern are:

- the omnibus approach to regulation favoured by the Data Protection Directive;
- the failure to eradicate divergences in national laws.

**Problems with the omnibus approach and alternative solutions, including the Lindqvist case**

Subject to some exemptions the Data Protection Directive requires regulation of every act of data processing irrespective of the extent of the threat to privacy or the threat to the Internal Market. The fact that this can lead to harsh results was revealed in a recent case heard by the European Court of Justice, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*. The case in question concerned the activities of a Swedish lady, Bodil Lindqvist, who built a website to help her fellow parishioners who were preparing for their confirmation. Mrs Lindqvist’s website contained information about parishioners living in her village, Alseda, including names and other personal data, such as the fact that one person was off work with an injured foot. Mrs Lindqvist published this information without consent and without having notified under the Swedish law. She was prosecuted and convicted, receiving a criminal record and a fine. The Swedish appeal court referred the case to the European Court of Justice for a determination as to whether the Data Protection Directive applied to Mrs Lindqvist’s activities. The European Court of Justice held that the Directive did apply, despite making a finding that Mrs Lindqvist’s activities were ‘not economic but charitable and religious’.

Regarding the nature of the information published by Mrs Lindqvist, while it fell within the categories of private information identified earlier, there was no evidence that the publication of this information caused any negative effect for the persons concerned. As regards the link with the Internal Market, the best that can be said is that the link was indirect.

*Lindqvist* is the type of case that could bring the law into disrepute; it might be thought that it trivializes the subject matter, causes a drain on the scarce resources of the regulators and the courts and places an unjustifiable burden on ordinary persons. However, potentially harsh results are the natural consequences of the omnibus approach, where nearly everything is regulated.
An alternative to the omnibus approach is the sectoral approach favoured in the US. Rather than regulating everything, the sectoral approach identifies the areas of utmost concern and prioritizes regulatory action by reference to seriousness. For these reasons the US has introduced data protection and privacy legislation in the medical field (see the Health Insurance Portability and Accountability Act 1996), in the financial services field (see the Financial Services Modernization Act 1999), to prevent spam (see the Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003) and to protect the privacy of children using the internet (see the Children’s Online Privacy Protection Act 1998) as well as in other key areas. However, there is no general privacy law in the US.

There is evidence that the EC is becoming more favourably disposed to the sectoral approach and it remains possible that the law will develop more along the lines of the US model rather than continue along the current path. For instance, in 1997 the EC approved a separate Directive on data protection in the telecommunications sector, which was replaced in 2002 by the Directive on Privacy and Electronic Communications. The EC has also periodically considered a possible Directive on worker’s data protection and in December 2005 the European Parliament approved a Directive on the Retention of Communications Data, which was endorsed by the Ministers of Justice and Home Affairs in February 2006. In addition, the Working Party constituted under Article 29 of the Data Protection Directive regularly issues opinions and working documents on sectoral issues within data protection, which have addressed many diverse issues, such as data protection and genetic research, data protection and direct marketing, data protection and use of the internet and data protection and the use of airline passenger information by law enforcement agencies.

Another alternative might be to require evidence of a substantial negative privacy effect or evidence of a substantial negative Internal Market effect before serious sanctions can be imposed, an approach that may weed out trivial cases from the full scope of the regulatory regime.

The beginnings of this approach have already been detected within domestic law. In a landmark case in 2002, Durant v. Financial Services Authority, the Court of Appeal delivered a judgment that is widely considered to have significantly curtailed the DPA. By way of background, the Court of Appeal was asked to rule on the meaning of personal data. It has effectively introduced a privacy filter into domestic law, saying that for information to be personal data it has to be information that ‘affects (the data subject’s) privacy’, with the implication being that there is a threshold level of negative effect that is required before the DPA applies. Of course, the problem with this approach is that the data subject might be unable to learn the extent of the privacy effect without having a guaranteed legal right of access to information about processing, the use of which is not conditional upon prior proof
of a negative effect. *Durant* almost creates a chicken and egg circular argument about which comes first, the right of access in section 7 or the need to satisfy the *Durant* definition of personal data?

**Continuing divergences – the failure of harmonization?**

The EU introduced the Data Protection Directive in order to harmonize the national laws of the EU Member States. Although all of the Member States have introduced national data protection laws, worrying differences still exist, as a recent report by the EC has identified. The continuance of differences stems from the fact that the Directive gives the Member States a very wide margin for manoeuvre. It does not specify the precise detail required of national laws.

This very wide margin for manoeuvre enables the UK to take a rather lax attitude to sanctions, penalties and enforcement with the result that a prosecution in the circumstances described in the *Lindqvist* case is inconceivable in this country. Even now, 10 years after the introduction of the Data Protection Directive, there is very little legal action commenced against data controllers in this country. This is not because domestic data controllers are particularly fastidious about legal compliance. Rather, it is a result of a weak legal regime and, perhaps, a cultural resistance to privacy issues.

The potential for continuing divergences was fully revealed by *Durant v. FSA*. The Court of Appeal’s ‘privacy filter’, discussed above, surprised commentators and is considered to have put the UK out of kilter with mainland Europe. Indeed, the decision is so problematic that the European Commission is reported to have asked the UK government to justify certain aspects of the DPA, particularly whether, in light of *Durant*, the right of access is guaranteed within the UK as the Data Protection Directive requires.

**Future direction, including the Charter of Fundamental Rights of the European Union**

An important distinction has already been made between the human rights law-making powers of the Council of Europe and those of the EC, with the core point being that the EC does not currently have standalone human rights law-making powers. For this reason the Data Protection Directive is constructed as an Internal Market measure. Of course, the reality of the situation is that the EC embraces human rights law making and it wishes to see its competence grow in this field.

Thus, in 2000 the EU ‘proclaimed’ the Charter of Fundamental Rights of the European Union. At the moment the legal status of the Charter is ambiguous, but if the proposal for an EU Constitution is adopted, the Charter will be directly incorporated into the Constitution, making it part of EU law. Articles 7 and 8 of the Charter provide as follows:
Article 7
Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

Article 8
Protection of personal data

(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.

It is moot whether the Charter will make much difference to the law in the UK, but it does send out a very important message about the relative importance of privacy laws and data protection laws.

**KEY ASPECTS WITHIN DATA PROTECTION LAWS**

When data protection laws are properly analysed the following key aspects become apparent:

(1) The processing of personal data must be transparent.
(2) The processing must comply with the general rules on lawfulness.
(3) The data subject must be given a right to object.
(4) Transborder flows of personal data are allowed, subject to a test of adequacy.
(5) There must be appropriate remedies, sanctions and penalties.

However, there are some powerful exceptions. For example, the transparency provisions will not apply if they would defeat the purpose of the processing.

**The data protection principles**

European data protection laws are structured around key principles, which the DPA calls the ‘data protection principles’. The DPA contains eight data protection principles and these are found in the first schedule to the Act.
Data Protection and Compliance in Context

The principles and the data controller
The DPA places the obligation to comply with the data protection principles on the data controller, who is the person or entity with the power to determine the manner of processing and its purpose. Section 4(4) of the DPA says that ‘it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller’. This obligation also extends to ensuring that data processors (persons or organizations processing personal data on behalf of data controllers) comply with the seventh data protection principle. Data controllers who take advantage of model contractual clauses to render lawful transfers of personal data to non-adequate countries outside the EEA also carry an obligation tantamount to ensuring that the data importer complies with the principles.

The principles and the interpretation
The data protection principles are supported by interpretation contained in Schedule 1, Part II of the DPA. Section 4(2) says ‘those principles are to be interpreted in accordance with Part II of Schedule 1’.

Key aspect – transparency (including the first and second data protection principles)
The need for transparency in processing, while not quite sacrosanct, is one of the most important aspects of data protection laws. Putting the matter bluntly, a real respect for privacy means being open about one’s processing activities. Of course, there are times when transparency will be counterproductive or harmful to other interests (for example, in the fight against serious crime), but these instances are limited in number and are subject to strict rules.

The DPA’s approach to the issue of transparency is complex and multifaceted, but the essential elements can be categorized as follows:

- **The promotion of consensual processing**: The DPA encourages processing operations that are conducted with the data subject’s consent, wherever this is possible. For example, the first criterion for making the processing of personal data legitimate is that the data subject has given consent.

- **Fair processing**: The first data protection principle requires processing to be fair and lawful. This is a complicated requirement because the first data protection principle merges a series of separate requirements within the Data Protection Directive, namely those contained in Articles 6, 7, 8, 10 and 11. As far as fairness is concerned, processing must be generally fair (the equivalent provision is contained in Article 6 of the Data Protection Directive) and must be specifically fair in the sense that the data subject should be supplied with information about the data controller and the processing prior to the commencement of processing (see Articles 10 and 11 of the Data Protection Directive for
the equivalent provisions). Furthermore, the data subject should not be deceived or misled about the processing purpose, requirements that are not actually contained in the Data Protection Directive.

- **Obtaining for specified purposes**: The second data protection principle requires personal data to be obtained for specified, lawful purposes. This requires the data controller to notify the data subject of the purpose prior to collection of the personal data. The notice can be given direct to the data subject or it can be included within the data controller’s notification.

- **Notification**: Most data controllers are obliged to register with the Information Commissioner prior to the commencement of processing, a process known as notification. In summary, this process involves the data controller supplying the Information Commissioner with information about itself and its data processing activities, which the Information Commissioner then enters on a publicly accessible register. Where the obligation to notify exists (there are some exemptions from the obligation), it is a criminal offence to process personal data without having notified. It is also a criminal offence to fail to keep notifications accurate and up to date. Additionally, in certain cases where the obligation to notify is exempted the data subject may serve a written request on the data controller for ‘the relevant particulars’, which form the bulk of the information that would be provided if the obligation to notify existed.

- **The right of access to personal data**: Data subjects are generally allowed access to their information and access to information about the data controller’s activities. Where the right of access applies the information usually has to be supplied within 40 days. The right of access is one of the DPA’s ‘subject information provisions’.

- **Information notices**: The Information Commissioner is empowered to serve information notices on data controllers requiring them to furnish him with key information about their processing activities.

**Key aspect – general rules on lawfulness (the first to fifth data protection principles)**

Chapter II of the Data Protection Directive is titled ‘general rules on the lawfulness of the processing of personal data’. These general rules consist of nine sections including:

1. principles relating to data quality;
2. criteria for making data processing legitimate; and
3. special categories of processing.

The general rules on the lawfulness of the processing of personal data also include the transparency provisions, identified above, and the right to object, discussed later.
The Data Protection Directive’s principles relating to data quality are incorporated in the DPA’s data protection principles, which are contained in the first schedule of the Act. The criteria for making data processing legitimate are contained in the second and third schedules. For comparative purposes Table 1.1 shows the critical parts of the data quality principles as they appear in the Data Protection Directive and the DPA.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>See Article 6.1.</td>
<td>See Schedule 1, Part I</td>
</tr>
<tr>
<td><strong>Personal data must be:</strong></td>
<td><strong>Personal data shall be:</strong></td>
</tr>
<tr>
<td>(a) Processed fairly and lawfully.</td>
<td>1. Processed fairly and lawfully and, in particular, shall not be processed unless –</td>
</tr>
<tr>
<td></td>
<td>(a) at least one of the conditions in Schedule 2 is met, and</td>
</tr>
<tr>
<td></td>
<td>(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.</td>
</tr>
<tr>
<td>(b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.</td>
<td>2. Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.</td>
</tr>
<tr>
<td>(c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.</td>
<td>3. Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.</td>
</tr>
</tbody>
</table>
| (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. | 4. Accurate and, where necessary, kept up to date.  
**Note:** The DPA gives the data subject the right to have inaccurate data rectified, blocked, erased or destroyed, but this right is contained in section 14 of the Act and not in the principles. |
| (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. | 5. Not be kept for longer than is necessary. |

Within the Data Protection Directive the criteria for making processing legitimate apply only to personal data that does not fall within one of the 'special categories'. The special categories are the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life. Following the approach of Table 1.1, the critical parts of the criteria for making the processing of personal data legitimate are shown in Table 1.2.
Table 1.2  Criteria for making processing legitimate

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>See Article 7</strong></td>
<td><strong>See Schedule 2</strong></td>
</tr>
<tr>
<td>Member States shall provide that personal data may be processed only if:</td>
<td>Conditions for the processing of personal data referred to in the first data protection principle:</td>
</tr>
<tr>
<td>(a) The data subject has unambiguously given his consent.</td>
<td>1. The data subject has given his consent to the processing.</td>
</tr>
<tr>
<td>(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.</td>
<td>2. The processing is necessary – (a) for the performance of a contract to which the data subject is a party, or (b) for the taking of steps at the request of the data subject with a view to entering into a contract.</td>
</tr>
<tr>
<td>(c) Processing is necessary for compliance with a legal obligation to which the controller is subject.</td>
<td>3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.</td>
</tr>
<tr>
<td>(d) Processing is necessary in order to protect the vital interests of the data subject.</td>
<td>4. The processing is necessary in order to protect the vital interests of the data subject.</td>
</tr>
<tr>
<td>(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.</td>
<td>5. The processing is necessary – (a) for the administration of justice, (b) for the exercise of any functions conferred on any person by or under any enactment, (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.</td>
</tr>
<tr>
<td>(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.</td>
<td>6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.</td>
</tr>
</tbody>
</table>

The Data Protection Directive and the DPA both prohibit the processing of the special categories of personal data, or ‘sensitive personal data’ as the DPA prefers, unless the processing satisfies one of the specified conditions. For completeness, Table 1.3 shows the grounds upon which the special categories of personal data may be processed.

It is important to note that if sensitive personal data are processed, the data controller will need to satisfy a criterion for legitimacy from Schedule 2 and a criterion from Schedule 3.
<table>
<thead>
<tr>
<th><strong>Data Protection Directive 1995</strong></th>
<th><strong>Data Protection Act 1998</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>See Article 8.2.</strong></td>
<td><strong>See Schedule 3</strong></td>
</tr>
<tr>
<td><strong>The prohibition against the processing of the special categories of personal data shall not apply where –</strong></td>
<td><strong>The data subject has given his explicit consent to the processing of the personal data.</strong></td>
</tr>
</tbody>
</table>

(a) The data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition may not be lifted by the data subject's giving his consent.

(b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards.

(c) Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

(d) Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.

(e) Processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
   (2) The Secretary of State may by order –
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary –
   (a) in order to protect the vital interests of the data subject or another person, in a case where –
   (i) consent cannot be given by or on behalf of the data subject, or
   (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing –
   (a) is carried out in the course of its legitimate activities by any body or association which –
   (i) is not established or conducted for profit, and
   (ii) exists for political, philosophical, religious or trade-union purposes,
   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects
   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing –
   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   (b) is necessary for the purpose of obtaining legal advice, or
   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary –
   (a) for the administration of justice, (aa) for the exercise of any functions of either House of Parliament,
   (b) for the exercise of any functions conferred on any person by or under an enactment, or
   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
   (2) The Secretary of State may by order –
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by –
   (a) a health professional, or
   (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
   (2) In this paragraph ‘medical purposes’ includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing –
   (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
   (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
   (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
   (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.
Key aspect – the right to object (preventing processing)

The right to object enables the data subject to exert control over their personal data. The DPA provides the data subject with a right to prevent processing likely to cause damage or distress, a right to prevent processing for direct marketing purposes and, in certain circumstances, a right to prevent automated decision taking.

Key aspect – transborder data flows (including the eighth data protection principle)

As mentioned earlier, the removal of obstacles to the free flow of personal data is one of the two principal aims of data protection laws. This aim provides the legal basis for the Data Protection Directive itself. To recap, the Directive considers free flows of personal data to be integral components of the rights of free movement that are central to the Internal Market’s proper functioning.

The Directive’s starting point is that transborder flows of personal data between the EC Member States may not be restricted or prohibited on the sole ground of protection of privacy (see Article 1.2.). However, transfers to countries outside the EU may only take place if the third country offers an ‘adequate’ level of protection for personal data.

The DPA adopts a similar approach, saying at the eighth data protection principle that ‘personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data’.

Both the Directive and the DPA explain how the adequacy of third countries is measured. They both also contain derogations from the general rule so that in certain circumstances transfers to non-adequate third countries are allowed.

Key aspect – enforcement (remedies, sanctions and penalties)

The Data Protection Directive requires the EC Member States to provide every person with a right to ‘a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question’ (Article 22) and an entitlement to ‘receive compensation from the controller for [any] damage suffered’ as a result of ‘an unlawful processing operation or of any act incompatible with the national provisions adopted’ (Article 23). In addition, it is stated that ‘Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted’ (Article 24). Finally, the Member States are required to establish completely independent supervisory authorities endowed with sufficient investigative powers, effective powers of intervention, the power to engage in legal proceedings and the power to hear complaints from data subjects (Article 28).
Taking these obligations in reverse order, the independent supervisory authority under the DPA is the Information Commissioner. Using their powers under the DPA, the Information Commissioner can commence criminal proceedings against data controllers, they can serve ‘enforcement notices’, ‘information notices’ and ‘special information notices’, they can conduct proceedings in the Information Tribunal, they can assess processing for legal compliance upon the request of the data subject and, with a warrant, they can enter upon premises to inspect, examine, operate or test processing equipment and to seize documents or materials containing evidence.

The DPA also creates a small series of primary criminal offences, by which it is meant that a criminal prosecution can be commenced directly by the Information Commissioner or the Director of Public Prosecutions upon the obtaining of evidence of a breach of the rule concerned. However, it is important to note that all breaches of the DPA can ultimately lead to criminal prosecutions, although the notice procedures have to be followed first in the majority of cases.

The data subject may commence civil proceedings for compensation where damage is suffered as a result of a breach of the DPA. If distress is suffered as well, a claim for compensation can be maintained for that harm, but there is no standalone right to sue for compensation for distress where no damage is caused, except where the processing is done for journalistic, artistic or literary purposes.

The data subject may also commence civil proceedings to enforce the right or access or the right to object.

The sixth, seventh and eighth data protection principles

As mentioned earlier, the DPA contains eight data protection principles. For completeness, the sixth, seventh and eighth data protection principles say the following:

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

KEY WORDS AND PHRASES – DATA, PERSONAL DATA AND PROCESSING

It is the processing of personal data by data controllers and data processors that is regulated by the DPA. To recap, the person whose personal data are
processed is known as the data subject, the data controller is the person with the power of control over the purpose or manner of the processing and the data processor is the person who processes personal data on behalf of a data controller. While the status of data subject is reserved for living individuals only, data controllers and data processors can be living individuals or organizations, such as companies, public bodies, clubs, associations and charities.

What are data?
The DPA is concerned with two kinds of data, electronic data and manual data. During the first phase in the development of European data protection laws, from the late 1960s to the mid-1970s, the focus was electronic data. However, by the start of the 1980s it was recognized that manual processing of data caused problems too. Thus, the definition of ‘personal data’ within the OECD Guidelines of 1980\(^{36}\) is ‘any information relating to an identified or identifiable individual’, although the Guidelines left the regulation of manual processing optional. The Data Protection Convention also gave its signatory countries the option of regulating manual processing (the UK declined this option, restricting the Data Protection Act 1984 to electronic data).

The Data Protection Directive takes a different line, making compulsory the regulation of certain kinds of manual files known as ‘personal data filing systems’ as well as manual processing that is connected to automated processing. The DPA has given effect to the Directive’s requirements in respect of personal data filing systems through its rules on ‘relevant filing systems’. The DPA has also extended coverage to other kinds of manual data thereby going further than the Directive’s mandatory requirements.

For the purposes of the DPA, ‘data’ are special kinds of information, namely information that falls within one of the five categories described in section 1(1) of the DPA. It can be said that all data are information, but not all information is data. The five categories of data are:

1. Information that is being processed by means of equipment operating automatically in response to instructions given for that purpose. It is important to note the tense preferred by the DPA, which is the present tense. The DPA does not talk about information that was processed by means of equipment operating automatically. The present tense is repeated in all of the categories.

2. Information that is recorded with the intention that it should be processed by means of equipment operating automatically in response to instructions given for that purpose.

3. Information that is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

4. Information that does not fall into any of the first three categories but forms part of an ‘accessible record’.

5. Information that is recorded information held by a public authority that does not fall into any of the first four categories.
These definitions are complex, but in a nutshell they are describing two kinds of information, electronic information and manual information. The first category is electronic information processed by computers and computerized equipment. Categories 3, 4 and 5 are manual information. The second category can be either electronic or manual information.

The relationship between information and data

It was stated earlier that all data are information but not all information is data. This statement needs further explanation because an understanding of the relationship and distinction between information and data is an imperative within a proper understanding of the DPA.

Information will become data when it is processed in the manner described in one of the five categories above. Thus, when information enters a computer, or a relevant filing system or an accessible record, it becomes data for the purposes of the DPA. Information will also become data prior to its entry into a computer or one of the regulated manual files, if it is recorded with the intention that it should enter them.

Perhaps the more complicated issue is the status of information that is extracted from data, as occurs when an electronic file is printed, or a page from a regulated manual file is removed and photocopied. Such information will still be treated as data due to the fact that the definition of processing includes the use of data and the disclosure of data. According to section 1(2) of the DPA, using or disclosing data includes using or disclosing the information contained in the data. This means that information extracted from data will be regulated by the DPA provided, of course, that the data are personal data. The effect of this is as follows:

- If information is recorded with the intention that it will enter a computer, or one of the regulated manual files, it is treated as data for the purposes of the DPA and for the definition of processing.
- Once information enters a computer, or one of the regulated manual files, it is also treated as data.
- Information that leaves a computer or one of the regulated manual files is also treated as data.

The first category of data – electronic information

Equipment that operates automatically in response to instructions given for that purpose is computerized equipment and includes PCs, mobile telephones, PDAs, voice dictation machines and telephone answering machines. For this reason the first category of data is usually referred to as electronic data.

In order for information to fall within this category it must be being processed by automated equipment, because of DPA’s use of the present tense. If information is no longer being processed by automated equipment it cannot fall within this category, which is the effect of the decision of Mr Justice Laddie in Smith v. Lloyds TSB Bank Plc. Conversely, information that is
extracted from electronic data, such as printed copy, will be treated as data as confirmed by the Court of Appeal in *Campbell v. Mirror Group Newspapers*\(^{38}\) and in *Johnson v. Medical Defence Union*\(^{39}\) provided that the electronic form continues to exist.

**The second category of data – electronic or manual information**

The second category of data can be either electronic information or manual information, depending upon the circumstances. Two common examples of the second category of data can help with understanding of this point.

**EXAMPLES**

(1) A customer telephones a call centre to complain about a product. The telephonist who answers the call is required to type details of complaints received into a computer database, for record-keeping purposes. Because of a temporary technical fault, the telephonist cannot access the database, so they jot down details on a pad of paper, so that they can enter them later, when the fault is corrected. In this example information is recorded, a requirement of the second category of data, albeit manually. As the telephonist’s intention is to enter the information into a computer database it can be said that the manual information is recorded with the intention that it will be processed by equipment operating automatically, making the manual information fall into the second category of data.

(2) A person copies an electronic file from a PC to a CD, for backup purposes. The PC is later destroyed in a fire, but the CD is kept safe. The information in the CD is clearly electronic information but it cannot fall within the first category of data, because it is not being processed by equipment operating automatically (it is merely being held in electronic form, in a carrier for electronic information). Therefore, it must be information falling within the second category of data, because it is recorded with the intention that it will be processed by equipment operating automatically at a later date.

**The third category of data – highly structured manual information**

The third category of data covers highly structured information, namely information that forms part of a relevant filing system and information that is recorded with the intention that it will form part of a relevant filing system. The definition of relevant filing system is also contained in section 1(1) of the DPA and means:

> any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either
by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

The meaning of relevant filing system expressly excludes information that is processed by equipment operating automatically and, logically, any information that may be processed by such equipment (if manual information is recorded with the intention that it will be processed by equipment operating automatically, it will fall within the second category, as explained above). Thus, there can be no doubt that a relevant filing system can consist only of manual information.

The Durant case – manual files
That a relevant filing system is highly structured arises from the fact that the structure makes specific information relating to a particular individual ‘readily accessible’. According to the Court of Appeal in the case of Durant v. Financial Services Authority, this means that the structure of the file should ‘enable easy location’ of the personal data within it, which is only possible within highly structured files. Indeed, and as the Court of Appeal rightly observed, the Data Protection Directive says that relevant filing systems enable ‘easy access’ to the personal information within them. In fact, the Court of Appeal said that ‘the required "easy" access to such data must be on a par with that provided by a computerised system’.

So, what type of manual file will meet the definition of relevant filing system? The starting point is to consider the Court’s description of the manual files held by the Financial Services Authority (FSA), as these provide the best example of files that fail to meet the definition. The following description is taken from the judgment of Lord Justice Auld:

The first [category of manual file] was the Major Financial Groups Division systems file (‘the MFGD Systems file’). It was a file, in two volumes, relating to the systems and controls that Barclays Bank was required to maintain and which was subject to control by the FSA. The file, which was arranged in date order, also contained a few documents relating to part of Mr Durant’s complaint against the Bank, which concerned such systems and controls.

The second category of file was ‘the MFGD Complaints file’ – relating to complaints by customers of Barclays Bank about it to the FSA – the subdividers being ordered alphabetically by reference to the complainant’s name, containing behind a divider marked ‘Mr Durant’ a number of documents relating to his complaint, filed in date order.

The third category of file was the Bank Investigations Group file (‘the B.I.G file’), maintained by the FSA’s Regulatory Enforcement Department, relating and organised by reference to issues or cases concerning Barclays Bank, but not necessarily identified by reference to an individual complainant. It contained a sub-file marked ‘Mr Durant’, containing documents relating to his
complaint. Neither the file nor the sub-file was indexed in any way save by reference to the name of Mr Durant on the sub-file itself.

The fourth category of file was the Company Secretariat papers, a sheaf of papers in an unmarked transparent plastic folder held by the FSA's Company Secretariat, relating to Mr Durant's complaint about the FSA's refusal to disclose to him details and the outcome of its investigation of his complaints against Barclays Bank, not organised by date or any other criterion.

While it is clear that the definition of relevant filing system applies to only highly structured manual information, the question remains whether only highly structured manual information can fall within the third category of data.

Taking the third category literally, it would seem that it can consist of both highly structured manual information (relevant filing systems) and manual information that is not highly structured (or not structured at all). This is because the third category refers to two types of information: (i) information that forms part of a relevant filing system; and (ii) information that is recorded with the intention that it will form part of a relevant filing system, that is, information that will form part of a relevant filing system at some point in time after its recording.

**EXAMPLE**

A Human Resources (HR) Director conducts an annual appraisal of one of the work force. In advance of the appraisal the HR Director explains to the worker that they may submit a short manuscript statement describing their achievements in the period under review, which will be inserted into the worker's personnel file at the end of the appraisal process. When this happens an entry will be made in the index at the front of the file identifying the document, its location and page number. In this example the statement itself is not part of a relevant filing system but when it is written, the intention exists that it will form part of a relevant filing system at a later date.

The fourth category of data – manual data of specific character

The fourth category of data can only be manual, because the fourth category excludes the first and second categories, but it cannot be a relevant filing system or recorded with the intention that it will form part of a relevant filing system, because the fourth category excludes the third category. Information falling within the fourth category is known as an ‘accessible record', which is defined in section 68 of the DPA. According to section 68 there are three kinds of accessible records: (i) ‘health records'; (ii) ‘educational records'; and (iii) ‘accessible public records'.

Health records are defined in section 68(2) of the DPA and they have two essential characteristics. The first characteristic is that they consist of
‘information relating to the physical or mental health or condition of an individual’. The second characteristic is that they are made by or on behalf of a ‘health professional’ in connection with the care of the individual concerned. The meaning of health professional is contained in section 69 of the DPA and includes health professionals working in the public and private sectors, such as registered medical practitioners, registered dentists, registered opticians and registered pharmaceutical chemists (see section 69 of the DPA for the full list).

Educational records are defined in Schedule 11 of the DPA. The meaning of educational record is different for each part of the UK, although there is one element that is common to all areas, namely that records prepared by teachers solely for their own use are not educational records.

Accessible public records are defined in Schedule 12 of the DPA. The public bodies covered by Schedule 12 differ within the UK, but the nature of the records is the same; they are records about public sector residential tenancies and records held for social work purposes.

The fifth category of data – public sector manual information

This category of data, recorded information held by a public authority that does not fall within any of the other categories, was introduced into the DPA as a result of an amendment made by the Freedom of Information Act 2000. The fifth category can only be manual data.

Recorded information falls into two categories, structured and unstructured. The definition of structured data is very similar to the definition of relevant filing system but, of course, structured data and relevant filing systems are not the same thing. The definitions are shown in Table 1.4.

<table>
<thead>
<tr>
<th>Structured data</th>
<th>Relevant filing system</th>
</tr>
</thead>
<tbody>
<tr>
<td>See DPA section 9(A)(1)</td>
<td>See DPA section 1(1)</td>
</tr>
<tr>
<td>. . . information which is recorded as part of, or with the intention that it should form part of, any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals.</td>
<td>. . . any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.</td>
</tr>
</tbody>
</table>

Both definitions refer to sets of information, sets of information relating to individuals and structuring by reference to individuals or criteria relating to individuals. The key difference is that in relevant filing systems the structure makes specific information relating to a particular individual readily accessible. Structured public sector manual data falling within the fifth category lacks the necessary ingredient of ready accessibility found within relevant filing systems.
Consequences of the definitions of data

The cumulative effect of the five categories of data has some very important consequences depending upon whether the data controller is part of the private sector or part of the public sector. The key point is that the DPA applies to a wider variety of information in the public sector than in the private sector, as Table 1.5 shows.

<table>
<thead>
<tr>
<th>Category of data</th>
<th>Public sector</th>
<th>Private sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>First – electronic information processed by automated equipment</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Second – electronic information to be processed by automated equipment</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Second – manual information to be processed by automated equipment</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Third – relevant filing system</td>
<td>Applies</td>
<td>Applies</td>
</tr>
<tr>
<td>Fourth – accessible records</td>
<td>Applies</td>
<td>Applies, but to a lesser extent</td>
</tr>
<tr>
<td>Fifth – public sector recorded information</td>
<td>Applies</td>
<td>Does not apply</td>
</tr>
</tbody>
</table>

The main point to be drawn from Table 1.5 is that manual data undergoing processing are subject to greater protection in the public sector than in the private sector. However, due to the ECHR, incorporated into UK law by the Human Rights Act, privacy in manual data is generally protected in both the private and public sectors.

Personal data

Understanding the meaning of personal data is vital to a proper understanding of the DPA and the implementation of compliance strategies. Table 1.6 shows how the definition has evolved from the Data Protection Convention through to the Data Protection Directive and to the DPA.

<table>
<thead>
<tr>
<th>Convention</th>
<th>‘personal data’ means any information relating to an identified or identifiable individual (‘data subject’);</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directive</td>
<td>‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;</td>
</tr>
<tr>
<td>DPA</td>
<td>‘personal data’ means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;</td>
</tr>
</tbody>
</table>
Personal data under the DPA

Information falling within one of the five categories of data can only be personal data in two circumstances:

- if the data relate to a living individual and that individual can be identified from those data;
- if the data relate to a living individual and that individual can be identified from those data and any other information that is in the possession of the data controller or is likely to come into the possession of the data controller.

The meaning of personal data also includes expressions of opinion about the data subject and any indication of the data controller’s intention in respect of the data subject, or any indication of another person’s intention in respect of the data subject.

Thus, there are two key issues within the meaning of personal data. First, does the data identify a living individual? Second, does the data relate to the identified living individual?

Identification of the living individual

The requirement of identification stems from the fact that data protection laws are intended to protect the privacy of personal data undergoing processing. Information that cannot and does not identify a person cannot be said to affect someone’s privacy. This means that information about anonymous people that is undergoing processing will not be regulated.

The second definition of personal data covers the situation where an anonymous person can be identified when the anonymous information is combined with other information in the data controller’s possession or other information that is likely to come into the data controller’s possession.

EXAMPLE

A supermarket introduces a loyalty card scheme. Each loyalty card has a unique number. The current series of numbers in circulation are recorded in an electronic master file. A second electronic file contains the names and contact details of the persons to whom the loyalty cards have been allocated. In this example the electronic master file of the current series of loyalty card numbers does not identify any individuals when it is read in isolation. However, if the reader of the electronic master file can gain access to the second electronic file, the ability to identify people from their loyalty card numbers becomes immediately achievable. Thus, the electronic master file contains personal data and is regulated by the DPA.

On a practical level, this has important implications for persons and organizations that wish to avoid the DPA by anonymizing files. This technique will only work if there is complete and effective anonymization. Merely applying
codes and ciphers will not work if they can be broken or deciphered with the use of other information in the data controller’s possession.

**The Durant case – does the information ‘relate to’ a living individual?**

A thorny question is can a document refer to an identified living individual without relating to that person for the purpose of the definition of personal data? This question was examined by the Court of Appeal in *Durant v. Financial Services Authority*.41

*Durant v. Financial Services Authority* is a controversial case but, for the time being at least, it should be regarded as being the definitive case on the meaning of personal data. As it is a decision of the Court of Appeal it binds all courts below, including the High Court, the County Court and the Information Tribunal. The case is controversial due to the fact that it is considered to put English and Welsh law into conflict with the laws of other European countries. In a nutshell, *Durant* is considered to unduly restrict the operation of the DPA.

Of course, not everyone will agree that *Durant* is a bad decision. In fact, many data controllers, particularly commercial operators in the private sector, had good cause to celebrate when the decision was announced, because it relieves them of many burdens of regulation.

The background to *Durant* is long and complicated, but it is clear that Mr Durant was once a customer of Barclays Bank. Unfortunately, a dispute arose between him and Barclays that could not be resolved. Thus, Mr Durant commenced litigation against Barclays, which ended in failure in 1993. Following this Mr Durant embarked upon a long battle to reopen his case, which included making complaints to the FSA. In 2001 he sought disclosure of his personal data held by the FSA, using his right of access contained in section 7 of the DPA. The FSA gave disclosure of some electronic records, but it refused to disclose a series of manual files. Therefore, Mr Durant commenced a court action under section 7(9) of the DPA, to obtain an order enforcing his right of access. One of the questions identified by the court was ‘what makes "data", whether held in computerized or manual files, "personal" within the meaning of the term "personal data" in section 1(1) of the 1998 Act so as to entitle a person identified by it to its disclosure under section 7(1) of the Act?’

The Court of Appeal identified the key issue to be the ‘meaning of the words "relate to" in the opening words of the definition [of personal data], in particular to what extent, if any, the information should have the data subject as its focus, or main focus’.

Mr Durant argued that the words ‘relate to’ have a very broad meaning covering ‘any information retrieved as a result of a search under his name, anything on file which had his name on it or from which he could be identified or from which it was possible to discern a connection with him’. The FSA argued the opposite, saying that the words ‘relate to’ have a narrow meaning, that they imply a ‘more or less direct connection with an individual’.
The Court of Appeal preferred the FSA’s argument. The leading judgment in the case was given by Lord Justice Auld, who said:

not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree.

In amplification of this Lord Justice Auld identified two concepts, biographical significance and focus, which, in simple terms, means that information will only be personal data if it affects the privacy of the individual. He said:

The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person’s or body’s conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.

In light of this case, it is now clear that a document can refer to a living individual without ‘relating to’ that person for the purposes of the DPA. The mere mention of a person in a document does not make that document personal data.

Of course, from time to time data controllers will find it difficult to apply the concepts of biographical significance and focus. In an attempt to provide assistance on the proper application of the concepts, in October 2004 the Information Commissioner published a guidance paper on the impact of Durant. In this paper the Information Commissioner suggests in ‘cases where it is not clear whether information relates to an individual’ the data controller ‘should take into account whether or not the information in question is capable of having an adverse impact on the individual’. This seems to be a fair restatement of the Court of Appeal’s decision that personal data is information that affects the person’s privacy, but it also draws attention to the significant problem within the Durant formulation, which is how much adverse effect is required for information to be personal data? Helpfully the Information Commissioner uses the guidance paper to give some examples of what is and what is not personal data. Examples of personal data are:

- marketing lists containing a name and contact details (e.g. address, telephone number, email);
- information about an individual’s medical history;
- information about an individual’s salary;
• information about an individual’s tax liabilities;
• information within an individual’s bank statements;
• information about individuals’ spending habits.
Examples of what are not personal data are:
• the mere reference to a person’s name where the name is not associated with any other personal information;
• incidental mention in the minutes of a business meeting of an individual’s attendance in an official capacity;
• where an individual’s name appears on a document or email indicating only that it has been sent or copied to that particular individual.

For the purposes of legal compliance by data controllers the real importance of the Information Commissioner’s guidance paper lies in the fact that it shows his thinking and hints at a regulatory approach that is based on some kind of proof of an adverse privacy effect. In borderline cases this might discourage the Information Commissioner from taking regulatory action against a data controller. This approach to regulation was confirmed by the Information Commissioner on 22 November 2005, at the Annual Conference of the National Association of Data Protection Officers, when a new enforcement strategy was announced.43

Legitimate criteria for the processing of personal data
In order to render the processing of personal data legitimate, the first data protection principle says that the data controller must satisfy one of the conditions in Schedule 2. These are shown in Table 1.2.

Sensitive personal data
Reference has already been made to the ‘special categories’ of personal data. The DPA calls the special categories ‘sensitive personal data’ (section 2 of the DPA). Sensitive personal data are personal data consisting of information as to the data subject’s:
• racial or ethnic origin;
• political opinions;
• religious beliefs or other beliefs of a similar nature;
• membership of a trade union;
• physical or mental health or condition;
• sexual life;
• commission or alleged commission of any offence, including any proceedings commenced and the disposal of such proceedings or the sentence of the court.

In addition to satisfying one of the conditions in Schedule 2 the first data protection principle requires the data controller to satisfy one of the conditions contained Schedule 3 of the DPA in order to make the processing of sensitive personal data legitimate. The conditions within Schedule 3 are shown in Table 1.3.
Other criteria for making the processing of sensitive personal data legitimate are contained in an important order made under the DPA. This order provides a framework for the processing of sensitive personal data in the absence of explicit consent, for example where the processing is in the substantial public interest and is necessary for the purposes of the prevention or detection of any unlawful act.

### Processing

The concept of processing is very wide, covering every single act that can be done on or towards data, from its initial capture right through to its final deletion or destruction. Table 1.7 shows how the definition has evolved since the Data Protection Convention.

<table>
<thead>
<tr>
<th>Table 1.7  The meaning of processing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention</strong></td>
</tr>
<tr>
<td><strong>Directive</strong></td>
</tr>
<tr>
<td><strong>DPA</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**The Johnson case, other cases and the meaning of processing**

Although the definition of processing is extremely wide, this does not mean that everyone agrees its scope. In the case of *Johnson v. Medical Defence Union*, the defendant unsuccessfully argued for a narrowing definition, saying that where computer data are concerned there will only be processing
if every operation is automated. Mr Justice Rimer, the judge in the case, summarized the defendant’s argument as follows:

Here, he says, Dr Roberts was not engaging in any ‘automatic’ processing of Mr Johnson’s data. In relation to the four electronic files, she was not making her selection by any automatic process. She made it by applying her own, non-automatic judgment to a computer database. In relation to the manual files, they do not come into the picture at all because they are not part of a ‘relevant filing system’. There was, therefore, no relevant processing at all of Mr Johnson’s personal data.

This was a difficult argument for the defendant, for two reasons. First, most computers are not fully automated; the existence of the keyboard and the mouse proves this. This point was made by the Data Protection Tribunal in CNN Credit Systems Ltd v. The Data Protection Registrar, a 1991 decision concerning the first data protection principle in the Data Protection Act 1984. The Tribunal said:

We do not see the function of the Act as being the regulation of computers in the sense of fully automatic machines behaving automatically. Rather it is designed to regulate the use of such machines by human beings who feed information into them, extract information from them, and instruct machines what do to by computer programs or keyboard or other instructions.

Second, the law on the meaning of processing was clarified by the Court of Appeal in the case of Campbell v. MGN Ltd. In Campbell Lord Phillips said:

The Directive and the Act define processing as ‘any operation or set of operations’. At one end of the process ‘obtaining the information’ is included, and at the other end ‘using the information’. While neither activity in itself may sensibly amount to processing, if that activity is carried on by, or at the instigation of, a ‘data controller’, as defined, and is linked to automated processing of the data, we can see no reason why the entire set of operations should not fall within the scope of the legislation. On the contrary, we consider that there are good reasons why it should.

In this part of his judgment Lord Phillips was saying that manual processing by a data controller that is linked to automated processing will be processing for the purposes of the Data Protection Directive and the DPA.

Mr Justice Rimer followed Lord Phillips’ judgment, dismissing the defendant’s argument. In order to understand the full effect of this case, it is necessary to understand a little about the processing operations performed by the Medical Defence Union (MDU). By way of background, the MDU provides
members of the medical profession with a discounted professional indemnity insurance policy, as well as associated advisory services. Mr Johnson was a member of the MDU for over 10 years during which time he had 17 contacts with the organization, including about complaints. These contacts resulted in the creation of 17 files, some electronic and some manual. Although he was never the subject of a clinical negligence claim, the MDU decided to terminate his membership as he presented an unacceptable risk. A significant factor in the MDU’s decision was the number of contacts that Mr Johnson had with the organization.

When assessing whether or not to terminate his membership a member of the MDU’s staff, Dr Roberts, completed a series of documents on her computer, one of which summarized the information in the 17 files relating to Mr Johnson. Twelve of these files were manual files, three were computer files, one was on CD and one was on microfiche. The computer summary was then printed and circulated to the persons involved in the decision-making process.

The MDU’s legal team objected to this being treated as processing, because the selection of the information from the 17 files was not done automatically, but by a human being. Therefore, they said, this could not be processing and nor could the resulting hard copies of the computer summary. Mr Justice Rimer rejected the MDU’s argument, holding that there was automated processing by reason of the inputting of data into the computer on which the summary was created. He said:

I accept, therefore, that Dr Roberts’s selection of material from the various manual and microfiche files and their inputting into a computer amounted to ‘processing’ within the meaning of the definition of ‘processing’ in section 1(1) [DPA] as expanded in section 1(2)(a) [DPA]; and that it makes no difference that none of such files was or formed part of a ‘relevant filing system’. I accept also that her selection of information from the computerised files for inputting into the computer similarly amounted to ‘processing’ within the meaning of that definition as elaborated in section 1(2)(a) and/or (b) [DPA].

The Smith case and the meaning of processing

There are limits to the meaning of processing, however, as clarified in the case of Smith v. Lloyds TSB Bank Plc. In this case the claimant’s barrister unsuccessfully tried to develop an argument that he called the ‘once processed always processed’ point. In fact, a variant of this argument was first presented by the same barrister in the first hearing in Johnson v. MDU, in 2004 again unsuccessfully. The ‘once processed always processed’ argument says that if information was processed by the data controller on automatic equipment it will become data and will remain data even if the automatic equipment ceases to exist. The judge in Smith v. Lloyds TSB Bank Plc, Mr Justice Laddie, summarized the argument as follows:
Thus, for example, if a series of letters about the data subject were typed on word processors and thereafter retained on computer hard discs, they would have been processed, i.e. held, on relevant automatic equipment. Even if the data controller has wiped all the hard discs clean some years ago and only retains hard copies of the documents in unstructured files, they still contain data within the meaning of the 1998 Act because, once processed always processed.

Mr Justice Laddie, who also tried the first hearing in *Johnson v. MDU*, did not like this argument. He said:

I do not accept this argument. Even if s 1 of the 1998 Act is treated as including the words from Article 3, it does not help Mr Smith. As I said in Johnson, the question of whether information is data has to be answered at the time of the data request. [The] argument involves a subtle sleight of hand. What he is saying is that because the information was held on automatic equipment but now is not, this means that it is partly so held. However this runs together two situations which are separated by time. What is relevant for the 1998 Act is whether, at the time of the data request, the information is wholly or partly held by means of equipment operating automatically. That is not the position here. As of 2001 Lloyds did not hold information relating to Mr Smith either wholly or partly on automatic equipment. Rewriting the section makes no difference.

Mr Justice Laddie’s rejection of the ‘once processed always processed’ argument is entirely consistent with Lord Phillips’ judgment in *Campbell v. MGN*, but this does not mean that the argument is totally devoid of merit. Indeed, when Article 3.1. of the Data Protection Directive is considered, which sets the Directive’s scope, it is possible to interpret it to mean that the Directive does not require synchronous automatic and manual processing for the manual by-products of automatic processing to be regulated. If this observation is correct, then the ‘once processed always processed argument’ may also be regarded as being consistent with Lord Phillips’ judgment in *Campbell v. Mirror Group Newspapers*. For completeness, Article 3.1. of the Data Protection Directive says:

This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

There is another variant of the ‘once processed always processed’ argument that has not yet been presented in argument before the court. This
variant concerns deleted electronic data, in the sense that deletion as understood by most computer users does not actually delete the data, but merely removes references to it in the file allocation tables against which a computer searches when data are sought to be retrieved. True deletion can only be accomplished by a process colloquially known as electronic shredding, which consists of the repeated overwriting of the data to be deleted with new binary code. If electronic data are not shredded in this fashion, they may be retrievable despite deletion. Consequently, in many cases where the data controller claims that only manual records exist it could be possible to disprove this assertion provided that the original processing equipment exists. In *Harper v. The Information Commissioner*, a recent Information Tribunal case brought under the Freedom of Information Act 2000, it was confirmed that a public authority’s duty to disclose information under an access request made under section 8 of the Freedom of Information Act can extend to deleted data.50

The special purposes – journalism, art and literature

Section 3 of the DPA refers to the ‘special purposes’, which means processing for the purposes of journalism, for artistic purposes and for literary purposes. The special purposes are acknowledged in the DPA due to their long-standing importance within the freedom of expression. Processing for the special purposes benefit from significant exemptions contained in section 32 of the DPA.

THE DPA – IMPORTANT MISCELLANY

The DPA achieved Royal Assent on 16 July 1998 and the majority of its provisions came into force on 1 March 2000. This repealed and replaced the Data Protection Act 1984, but it is subject to some important transitional provisions that are designed to ensure a smooth transition from the 1984 Act to the DPA. Most of the transitional provisions expired on 24 October 2001, but a few still remain:

- Until 24 October 2007 ‘eligible manual data’, which are manual data that were first held by a data controller before 24 October 1998, and ‘accessible records’, which are certain kinds of health records, educational records and public records, are exempt from most of the data protection principles as well as from the data subject’s right to seek a court order for the rectification, blocking, erasure or destruction of inaccurate personal data.
- Until 24 October 2007 ‘recorded information held by a public authority’ are exempt from the DPA’s rules about accuracy.
- There is a limited, permanent exemption for processing of personal data for historical research purposes.
The jurisdiction of the DPA

The Data Protection Directive required EC Member States to apply its national laws where 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State' (Article 4).

In order to work out whether they are regulated by the DPA, data controllers need to consider the provisions contained in section 5 of the Act, which can be distilled down to three primary questions:

- Are they processing personal data?
- Are they established in the UK?
- Are they processing personal data in the context of the UK establishment?

If the answer to all of these questions is yes, the DPA will apply, subject to some important exemptions described in Part IV of the Act.

However, if the data controller is not established in the UK nor in any other country within the EEA, the DPA will still apply if the data controller ‘uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom’ (section 5(1)(b) of the DPA). In these cases the data controller must nominate a representative established in the UK (section 5(2) of the DPA).

Figure 1.1 shows the issues in sequence.

The meaning of establishment

A data controller who is an individual will be established in the UK for the purposes of the DPA if he is ordinarily resident in the UK. In the recent case of Skjevesland v. Geveran Trading Co Ltd it was decided that whether a businessman with residences in several countries including the UK was ordinarily resident for the purposes of the Insolvency Act 1986 was a question of fact and degree and it was necessary to look at the cumulative effect of the evidence.

A data controller that is a company will be established in the UK if the company is incorporated under the law of any part of the UK. A data controller that is a partnership or an unincorporated body will be established in the UK if it is formed under the law of any part of the UK.

Further assistance with the meaning of establishment is provided by an Article 29 Working Party working document, which explains:

The notion of establishment is relevant in Article 4(1)c of the directive in the sense that the controller is not established on Community territory. The place, at which a controller is established, implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. According to the Court, the concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period. This requirement is also fulfilled where a company is constituted for a given period.
Establishment in more than one EC Member State

Data controllers established in more than one EC Member State will be subject to the data protection laws of each country of establishment. This point is dealt with in Article 4.1.(a) of the Data Protection Directive, which says:

When the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable . . .

The Article 29 Working Party’s working document says:

When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down
by the respective law of each of the Member States for the processing carried out by them in course of their activities . . . where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments.

**Data controller not established in the EC**

If the data controller is not established anywhere in the UK, this is not the end of the matter. In these situations the data controller needs to ask whether they are using equipment situated within the UK other than for the purposes of transiting data through the UK. This issue arises often in internet transactions.

Before addressing the substantive issues it needs to be asked when is equipment used only for transit? Again, the Article 29 Working Party’s working document provides assistance, saying:

> A typical case where equipment is used for transit only are the telecommunications networks (back bones, cables etc.), which form part of the Internet and over which Internet communications are traveling from the expedition point to the destination point.

For the purposes of the Data Protection Directive a website based outside the EC may make use of equipment situated in the UK to process personal data, although it is important to recognize, as the Article 29 Working Party says, that ‘not any interaction between an Internet user in the EU and a web site based outside the EC leads necessarily to the application of EU data protection law’. In order for the law to apply, it seems necessary for the foreign website to make use of the internet user’s computer in such a fashion that it can be said that the computer is under the control of the foreign website. Of course, this taking of control element needs to involve the processing of personal data for the Data Protection Directive to apply. The Article 29 Working Party says:

> The Working Party considers that the concept of ‘making use’ presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process personal data.

The Article 29 Working Party’s working document also gives some examples of the kind of activities that can result in the application of the Data Protection Directive. These are:

- the use of cookies;
- the use of JavaScript;
- the use of spyware.
The location and nationality of the data subject

An important question is does the data subject need to be located in the EC, or be a national of an EC Member State for the Data Protection Directive to apply? The answer to this question is no. Again, the Article 29 Working Party’s working document is of help:

It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States laws on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen. It is the location of the processing equipment used that counts.

Exemptions to the DPA

The DPA contains a complex framework of exemptions and restrictions. The main ones are contained Part IV of the DPA, the full list of which is as follows:

- national security (section 28);
- crime and taxation (section 29);
- health, education and social work (section 30);
- regulatory activity (section 31);
- journalism, literature and art (section 32);
- research, history and statistics (section 33);
- manual records held by public authorities (section 33a);
- information available to the public by or under an enactment (section 34);
- disclosures required by law or made in connection with legal proceedings (section 35);
- parliamentary privilege (section 35a);
- domestic purposes (section 36).

Only the domestic purposes exemption is a full exemption, so that where personal data are processed by an individual only for the purposes of that individual’s personal, family or household affairs (including recreational purposes) the DPA will not apply. The national security exemption can act as a complete exemption, but first a government minister needs to sign a certificate to that effect. All the other exemptions are partial exemptions. Some of them are fleshed out in subordinate legislation made under the DPA.

There are other exemptions within Schedule 7 of the Act. These exemptions concern the right of access and the supply of prior information, which both form part of the DPA’s transparency safeguards. The obligation to supply prior information forms part of the first data protection principle. The DPA
refers to the right of access and the obligation to supply prior information as the ‘subject information provisions’ (section 27(2)).

Staying with transparency, the right of access and the obligation to notify are themselves both subject to exemptions.

Finally, section 38 of the DPA allows the Secretary of State to make further exemptions.
Index

data protection principles 22
eighth 250
fifth 109–111, 259
first 102–104
fourth 108–109, 259
generally xx, 21–23
interpretation and 22
second 69, 104–105
seventh 72, 112–121, 249–250, 259
sixth 80, 111–112, 151
third 105–108, 259
Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 140
Data Protection (Processing of Sensitive Personal Data) Order 140
Data Protection (Processing of Sensitive Personal Data) Order 2000 133–140
Data Protection (Subject Access Modification) (Education) Order 2000 94–95
Data Protection (Subject Access Modification) (Health) Order 2000 93
Data Protection (Subject Access Modification) (Social Work) Order 2000 95
data subject action by 233–234
categories of 237
data controller and 235
enforcement by 206–210
identification of 237
information to, supplying 242–245
location of 49
meaning of xx
nationality of 49
data subject notice court action 145
data controller’s reaction to 145
form and content of 144
data subject rights compliance strategies 253–260
enquiries as to 257
exercise of, identifying 253–254
information technology and 253
investigations, handling 258–259
notices, service of 257
data transfers 250
derogations
Binding Corporate Rules and 161–167
contractual clauses and 168–178
digital safe xx
Directive on Privacy and Electronic Communications (DPEC) generally 146, 184–193
interception 187
publicly available electronic communications services 185
subscribers 184–185
surveillance 187
traffic data 188–190
UK implementation of 193–194
users 184–185
direct marketing cases on 148
electronic communications services 146–148
generally 146
Information Commissioner’s
guidance on 148
rules on 146
directories 193
disclosures
communications data, of 202–205
law, required by 142
special purposes 135
unlawful 223–227
disproportionate effort exemption 61–62
domestic purposes exemption 78
Durant case 33–34, 38–40–236, 244
education exemption 93–95
electronic communications confidentiality of 186–188
Directive on 184–193
privacy and 183–260
publicly available 185
security of 186
services for 146–148
electronic information 31–32
electronic shredding xx
employees monitoring of 116
organizational measures and 115–117
relationships with 249
training 250
vetting of 116
enforcement
assessment, requesting 210
compensation, claims for 208–210
data controller, by 210–211
data subject, by 206–210
European Commission, by 211
generally 28–29, 206–230
Information Commissioner, by 211–220, 233
equal opportunities processing 138
establishment
meaning of 46
more than one EC Member State, in 47–48
European Commission, enforcement by 211
European Community (EC)
free movement and 13–15
generally xx
rise to prominence of 12–13
European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)
DPA and 2, 7
privacy and 5
examination marks 99
examination scripts 99
exemptions from non-disclosure provisions art 142
crime 141
disclosure required by law 142
journalism 142
literature 142
manual data 142
parliamentary privilege 142
Pt IV 140–142
public, information available to 142
exemptions from notification provisions
domestic purposes 78
manual data 75–76
national security 75
no prejudice to data subjects 76–78
public record 75
exemptions from subject access provisions
art 96
class-based 92
crime 93
education 93–95
health 93
history 96
journalism 96
literature 96
manual data 97
order, made by 100
parliamentary privilege 97
prejudice-based 92
Pt IV 89, 92–100
regulatory activity 95
research 96
social work 93, 95
statistics 96
taxation 93
Fair Credit Reporting Act 1970 (US) 156
fairness
cases on 55–56, 57–59, 62–69
generally 55–56
fair obtaining 56
fair processing xx, 22, 54–69, 103
Financial Services Modernization Act 1999 (US) 156
firewall xx
free movement 13–15
health exemption 93
Health Insurance Portability and Accountability Act 1996 (HIPPA) (US) 156
history exemption 96
information
data and 31
electronic 31–32
gathering of 234–240
lifecycle of xx
informational privacy xx, 5
Information Commissioner data controller and 235
dealing with 256–259
direct marketing, guidance on 148
enforcement by 211–220, 233
‘Legal Guidance’ of 120–121
notification, guidance on 74
offences 229–230
role of xx
system of 72–74
transborder data flows and 182
Index

information notices generally 23, 89–90
prerogative, legal professional 92
requests for assessments 90
special 90–91
time for compliance 91
information technology
data proliferation and 251–252
data subject rights and 253
security and 252
Information Tribunal xxi
insurance company processing 136–138
interception of communications business, for 199–201
foreign 199–201
generally 117, 187
intentional 198
lawful 201–202
meaning of 195
RIPA 2000 195–202
traffic data, of 197
UK, within 197
warrant, without 199
interpretation, and supply of prescribed information 59–60
investigations, handling 258–259
itemized billing 190–192
Johnson case 41–45, 55–56, 57–59, 62–69
journalism exemption
non-disclosure provisions, from 142
not-for-profit organizations, legitimate 96
judicial appointments 98
lawfulness
general rules on 23, 101–142
legitimacy and 240
lawful processing 103–104
legal advice necessity 131
‘Legal Guidance’ of Information Commissioner 120–121
legal proceedings necessity 131
legal professional privilege
information notices and 92
subject information provisions and 99
legal rights necessity 131
legislation
aims of 3
enforcing 206–230
European 7
future of 18–20
generally 3, 18–20, 20–21
history of 3–20
key aspects in 21–29
legitimacy, lawfulness and 240
cycle of information xxi
Lindqvist case 18–20
literature exemption
non-disclosure provisions, from 142
subject information provisions, from 96
litigation disclosure and 89
location data 192, 192
management forecasts 98
manual data
Data Protection Directive and 16
exempt 75–76–97, 142, 150
manual data exemption
data controller and 150
notification 75–76
public authorities 142
subject access provisions 97
manual information
generally 32
highly structured 32–34
public sector 35
specific character, of 34
medical data, processing of 137
monitoring
cover 116
employees, of 116
national security exemption 75
necessity
contractual 123
employment 127–128
legal rights 131
legitimate interests 125–126
medical purposes 132
non-contractual legal 123
public functions 124–125, 131–132
rational or ethnic monitoring 132–133
test for xxi, 122, 127
vital interests 124, 128–130
negotiations 99
networks, services distinguished 185
non-adequate country xxi
non-disclosure provisions 141
not-for-profit organizations, legitimate interests of 130
notices
CCTV 244–245
service of 257
notification
domestic purposes, for 78
exemptions to requirement 75–79
generally 23, 70
guidance on 74
offences 71, 221
partnerships, by 79
procedure for 71–72
schools, by 79
up to date, keeping 75
voluntary 79
object, right to 28
exempt decisions 150
exercising 148–149
generally 143–151
sixth data protection principle and 151
obstruction offences 222–223
obtaining
fair 56
statutory 57
unlawful 223–225, 226–227
offences
data controllers 232
Information Commissioner 229–230
notification 71, 221
obstruction 222–223
omnibus approach 18
opt-ins 246
opt-outs 246
Organisation for Economic Co-operation and Development (OECD)
generally xxi, 1
transborder data flows 10–11
organizational measures
data processors and 117–119
employees and 115–117
generally 115
parliamentary privilege exemption 97, 142
Part IV exemptions 89, 92–100, 140–142
partnerships, notification by 79
passenger name record (PNR) 160–161
pension schemes established processing by 136–138
medical data, processing by 137
personal data
access to 23, 79–89
accuracy of 246–249
cost of 2, 36, 41
Data Protection Directive and 36–40
DPA, under 37–40
identification of 236–237
information on data subjects 1–2
meaning of xvi, 36, 41–45
methods of processing 239–240
processing 1, 25, 40
reasons for processing of 237–239
Schedule 2 conditions 122–126
technological threats to 113–114
police constables, processing by 139–140
political parties, processing by 138
prejudice-based exemptions 92
prejudice, processing unlikely to 76–78
prescribed information, supply of interpretation and 59–60
third party, from 60
timing of 60
transparency and 57
preventing processing 28
privacy
data protection and 8–10
Directive on 146, 184–193
ECHR and 5
electronic communications and 183–260
informational xxi, 5
meaning of 6–7
other rights and interests and 5–6
private sector and 8
protection of 4–10
right to 16–17
substantive xxi, 5
UK, in 16–17
Privacy and Electronic Communications (EC Directive) Regulations 146, 193
privacy statements 242–243
private sector, data in 36
processing
concept of 41
consensual 22, 51–54
<table>
<thead>
<tr>
<th><strong>Index</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>data controller, by 2</td>
</tr>
<tr>
<td>data processor, by 2</td>
</tr>
<tr>
<td>domestic purposes, for 78</td>
</tr>
<tr>
<td>equal opportunities 138</td>
</tr>
<tr>
<td>exempt 78–79</td>
</tr>
<tr>
<td>fair 22, 54–69, 103</td>
</tr>
<tr>
<td>insurance companies, by 136–138</td>
</tr>
<tr>
<td>lawful 103–104</td>
</tr>
<tr>
<td>legitimacy criteria 24</td>
</tr>
<tr>
<td>meaning of 41–45</td>
</tr>
<tr>
<td>medical data 137</td>
</tr>
<tr>
<td>methods of 239–240</td>
</tr>
<tr>
<td>personal data 25, 40</td>
</tr>
<tr>
<td>police constables, by 139–140</td>
</tr>
<tr>
<td>political parties, by 138</td>
</tr>
<tr>
<td>preventing 28</td>
</tr>
<tr>
<td>reasons for 237–239</td>
</tr>
<tr>
<td>research, for 139</td>
</tr>
<tr>
<td>Secretary of State, order of 126, 133</td>
</tr>
<tr>
<td>specified purposes, for 69</td>
</tr>
<tr>
<td>prosecution of data controller 232</td>
</tr>
<tr>
<td>public</td>
</tr>
<tr>
<td>authorities 97</td>
</tr>
<tr>
<td>information made 130–131, 142</td>
</tr>
<tr>
<td>protecting the 135</td>
</tr>
<tr>
<td>publicly available electronic communications services 185</td>
</tr>
<tr>
<td>public record exemption 76</td>
</tr>
<tr>
<td>public sector data in 36</td>
</tr>
<tr>
<td>manual information in 35</td>
</tr>
<tr>
<td>quality of data 24</td>
</tr>
<tr>
<td>recipient of data xxi</td>
</tr>
<tr>
<td>register entries additional information in 72</td>
</tr>
<tr>
<td>copies of, obtaining 75</td>
</tr>
<tr>
<td>fee for 71</td>
</tr>
<tr>
<td>Regulation of Investigatory Powers Act 2000 (RIPA 2000) ATCSA 204–205 generally 194–204 regulatory activity 95, 135 relevant filing system xxi research exemption for 96 processing for 139</td>
</tr>
<tr>
<td>Schedule 2 conditions contractual necessity 123 data subject consent 122–123 generally 122–126 legitimate interests necessity 125–126 necessity test 122 non-contractual legal necessity 123 public functions necessity 124–125 vital interests necessity 124 Schedule 3 conditions employment necessity 127–128 explicit consent 127</td>
</tr>
<tr>
<td>generally 126–133 legal rights necessity 131 medical purposes necessity 132 necessity test 127 not-for-profit organizations 130 public functions necessity 131–132 public information 130–131 racial or ethnic monitoring necessity 132–133 vital interests necessity 128–130 schools, notification by 79 scripts 244 self-incrimination 100 sensitive personal data DPA and 40 processing criteria 25–27 Schedule 2 conditions 122–126 Schedule 3 conditions 126–133 services electronic communications 146–148 networks distinguished 185 security of 186 Smith case 43–45 social work exemption 93, 95 special purposes disclosures 135 statistics exemption 96 statutory obtaining 57 structured data 35 subject access, enforced 227–229 subscriber DPEC, under 184–185 meaning of xxi substantial and unwarranted damage or distress generally 143–145 likelihood of 144 substantive privacy xxi, 5 surveillance 187</td>
</tr>
</tbody>
</table>
BCS Products and Services

Other products and services from the British Computer Society, which might be of interest to you include:

**Publishing**

BCS publications, including books, magazine and peer-review journals, provide readers with informed content on business, management, legal, and emerging technological issues, supporting the professional, academic and practical needs of the IT community. Subjects covered include Business Process Management, IT law for managers and transition management.

[www.bcs.org/publications](http://www.bcs.org/publications)

**BCS Professional Products and Services**

**BCS Group Membership Scheme**. BCS offers a group membership scheme to organizations who wish to sign up their IT workforce as professional members (MBCS). By encouraging their IT professionals to join BCS through our group scheme organizations are ensuring that they create a path to Chartered Status with the post nominals CITP (Chartered IT Professional).

[www.bcs.org.uk/forms/group](http://www.bcs.org.uk/forms/group)

BCS promotes the use of the **SFIaplus™** IT skills, training & development standard in a range of professional development products and services for employers leading to accreditation. These include BCS IT Job Describer, BCS Skills Manager and BCS Career Developer. [www.bcs.org/products](http://www.bcs.org/products)

**Qualifications**

**Information Systems Examination Board** (ISEB) qualifications are the industry standard both here and abroad, and with over 100,000 practitioners now qualified, it is proof of their popularity. They ensure that IT professionals develop the skills, knowledge and confidence to perform to their full potential. There is a huge range on offer covering all major areas of IT. In essence, ISEB qualifications are for forward looking individuals and companies who want to stay ahead – who are serious about driving business forward. [www.iseb.org.uk](http://www.iseb.org.uk)

**BCS Professional Examinations** are internationally recognised and essential qualifications for a career in computing and information technology (IT). At their highest level, the examinations are examined to the academic level of a UK university honours degree and acknowledge practical experience and academic ability. [www.bcs.org/exams](http://www.bcs.org/exams)

**European Computer Driving Licence**™ (ECDL) is the internationally recognised computer skills qualification which enables people to demonstrate their competence on computer skills. ECDL is managed in the UK by the BCS.
ECDL Advanced has been introduced to take computer skills certification to the next level and teaches extensive knowledge of particular computing tools. 

www.ecdl.co.uk

**Networking and Events**

BCS’s Specialist Groups and Branches provide excellent professional networking opportunities by keeping members abreast of latest developments, discussing topical issues and making useful contacts. 

www.bcs.org/bcs/groups

The Society’s programme of social events, lectures, awards schemes, and competitions provides more opportunities to network. **www.bcs.org/events**

**Further Information**

This information was correct at the time of publication, but could change in the future. For the latest information, please contact:

The British Computer Society  
First Floor, Block D  
North Star House  
North Star Avenue  
Swindon  
SN2 1FA, UK

Telephone: 0845 300 4417 (UK only) or + 44 1793 417 424 (overseas)  
E-mail: customerservice@hq.bcs.org.uk  
Web: www.bcs.org
Data processing is a broad term, covering every conceivable thing that can be done to data: from initial collection to its final deletion, including its organization, alteration, use and disclosure. Data protection laws cover the processing of information relating to individuals. Every business and every person with a PC comes under data protection legislation.

Contents include:
- The Data Protection Act 1998
- Enforcing data protection laws
- Compliance
- Transparency
- The right of access to personal data
- The eight data protection principles
- Privacy and electronic communications
- Preventing processing
- Transborder data flows

Data Protection and Compliance in Context provides comprehensive and practical guidance on protecting data privacy. Ideal for those without qualifications or specialist knowledge of law, Data Protection and Compliance in Context is a trustworthy and accessible guide for small businesses, IT professionals and data protection officers.

About the author
Stewart Room, is the chair of the National Association of Data Protection and Freedom of Information Officers (NADPO). A barrister and solicitor, he is a partner at Rowe Cohen Solicitors and a visiting lecturer at Queen Mary, University of London.