<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email, SMS text and MMS multimedia messages</td>
<td>80</td>
</tr>
<tr>
<td>Taking payments over the web</td>
<td>81</td>
</tr>
<tr>
<td><strong>NEW</strong> Chapter 12 – Operating a CCTV system</td>
<td>82</td>
</tr>
<tr>
<td>Basic rules for operating a CCTV system</td>
<td>82</td>
</tr>
<tr>
<td>CCTV Code of Practice</td>
<td>85</td>
</tr>
<tr>
<td><strong>NEW</strong> Chapter 13 – Security and disposal of personal information</td>
<td>86</td>
</tr>
<tr>
<td>Security</td>
<td>86</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>99</td>
</tr>
<tr>
<td>Disposal and destruction of personal information</td>
<td>101</td>
</tr>
<tr>
<td><strong>NEW</strong> Chapter 14 – Sector-specific guidance for using personal information</td>
<td>103</td>
</tr>
<tr>
<td>Accountants, solicitors and other professionals</td>
<td>103</td>
</tr>
<tr>
<td>Consultants</td>
<td>103</td>
</tr>
<tr>
<td>Independent financial advisers</td>
<td>104</td>
</tr>
<tr>
<td>Credit brokers</td>
<td>105</td>
</tr>
<tr>
<td>Private investigators and tracing agents</td>
<td>106</td>
</tr>
<tr>
<td>Health professionals</td>
<td>108</td>
</tr>
<tr>
<td>Schools</td>
<td>109</td>
</tr>
<tr>
<td>Charities, churches and unincorporated not-for-profit organizations</td>
<td>110</td>
</tr>
<tr>
<td><strong>NEW</strong> Chapter 15 – Maintaining compliance</td>
<td>112</td>
</tr>
<tr>
<td>Accountability and responsibility</td>
<td>112</td>
</tr>
<tr>
<td>Policies and procedures</td>
<td>112</td>
</tr>
<tr>
<td><strong>NEW</strong> Chapter 16 – Contact with the Information Commissioner</td>
<td>115</td>
</tr>
<tr>
<td>Dealing with problems</td>
<td>115</td>
</tr>
<tr>
<td>Contact from the Information Commissioner</td>
<td>115</td>
</tr>
<tr>
<td>What is the difference between enforcement and prosecution?</td>
<td>118</td>
</tr>
<tr>
<td>Who is liable?</td>
<td>118</td>
</tr>
<tr>
<td>Warrant to search premises</td>
<td>119</td>
</tr>
<tr>
<td>What happens if I am prosecuted?</td>
<td>119</td>
</tr>
<tr>
<td>Dealing with informal complaints from individuals</td>
<td>119</td>
</tr>
<tr>
<td>Changes to the Information Commissioner’s powers</td>
<td>120</td>
</tr>
<tr>
<td><strong>NEW</strong> Bibliography</td>
<td>121</td>
</tr>
<tr>
<td>Sources of information</td>
<td>123</td>
</tr>
</tbody>
</table>
Foreword

BSI would like to thank the Data Protection Editorial Board and the representatives of the following authoritative bodies for their assistance in reviewing this book.

- Barclays Bank plc
- Batchelor Associates
- Centrica plc
- Deloitte and Touche
- Department of Health
- Egg plc
- Essex Police
- Financial Services Authority (FSA)
- General Medical Council
- Information Commissioner’s Office
- The London Boroughs Data Protection Group
- European Privacy Partnership
About the authors

Nicola McKilligan is a privacy and information law consultant with over 13 years experience of advising businesses on compliance with UK, European and global data privacy laws. She has worked as a Strategic Policy and International Officer for the UK Data Protection Commissioner (now Information Commissioner) and has been an in-house Data Privacy Officer for British Gas and Accenture. She is editor of the *World Data Protection Report* and is an experienced technical writer.

Naomi Powell is a risk adviser who holds professional qualifications in data protection, financial crime prevention and training practice. She began her data protection career at the Information Commissioner’s Office, working in the Registration, Policy and Compliance teams. Her practical and common sense approach to compliance was developed as a data protection officer and privacy consultant in the financial services and energy sectors.
Preface to the Second Edition

This book is a guide to complying with the Data Protection Act 1998. It provides an overview of data protection law and practical advice and guidance for small organizations looking to comply with the spirit of the new British Standard for Data Protection: BS 10012. This second edition also contains new chapters on using CCTV systems in a way that complies with the law, maintaining ongoing compliance, updates on keeping data secure. The case studies are taken from the Information Commissioner’s Annual Reports or press releases.

The Data Protection Act sets out rules that must be followed wherever personal information is processed for anything other than a domestic purpose. The Data Protection Act is the primary piece of legislation which governs compliance in this area but organizations can also choose to comply on a voluntary basis with the British Standard BS 10012: Data protection — Specification for a personal information management system, which provides additional requirements for data protection compliance.

How this book relates to BS 10012

This book complements BS 10012 but if you want to comply with the standard you will also need to refer to its requirements by referencing the full text of BS 10012 itself. This book does not recreate all the requirements of the standard in full but merely provides some guidance on its practical implementation.

If you are not intending to implement BS 10012 in full but would still like to adopt some of its practical requirements you can follow the advice in this book. This may be particularly useful if you are a very small business that would otherwise find it difficult to implement the whole of BS 10012.

Who should read this book?

This book is intended to be used by anyone who needs to understand their obligations under the law. In particular, it provides practical, simple and easy to follow advice for small businesses, charities, unincorporated members’ clubs and anyone else who does not have the benefit of a large in-house compliance department. It is also a useful quick reference for managers and executives who are responsible for data protection compliance but who do not need an in-depth technical knowledge of the subject.
The Data Protection Act has a wide scope. Most organizations in the UK as well as individuals running their own businesses need to comply to some extent with its provisions.

If you or your organization operate in breach of the law when processing personal information you may incur civil, and sometimes criminal, liability. The adverse publicity may also cost you your business or ruin your organization’s reputation.

You do not need to be doing very much with personal information to find yourself having to comply with the Data Protection Act.

Have a quick look at the list below. Do you:

• hold contact details for customers on computer?
• keep copies of invoices from suppliers?
• have an overflowing filing cabinet in the corner that contains personal information?
• telephone customers or other individuals to enlist support or business?
• publish images on the internet?
• have staff working alongside you?
• use third-party outsourcers to do work for you?
• have a CCTV system?
• use portable devices such as laptops, palmtops and mobile phones in your organization or business?

If any of the above applies to you, you will probably need to comply with the Data Protection Act.

Why you?

Information on individuals is a valuable asset and like your other assets needs to be properly protected. Apart from making good business sense, the reputation and success of your organization can be under threat if you do not make looking after personal information your priority. Without it, you would not be able to function as an organization. With it, you can create, maintain and build relationships of mutual benefit with your customers, clients, suppliers, supporters, investors and staff, who in turn will recommend you to their customers, clients, suppliers, supporters, investors and staff. A review of the Information Commissioner’s Annual Reports shows that, so far, the majority of prosecutions under the law have been directed at small businesses that were either unaware of the law or failed to ensure compliance with it while running their business.
Preface to the Second Edition

**Why this book?**

There are a number of detailed law books and guides available that will take you through the requirements of the Data Protection Act but most organizations or individuals need to understand the practical application of the law and how it applies to them. This book provides you with this basic practical advice to help make compliance with the Data Protection Act easier.

This book is also helpful because it includes additional information about compliance, drawn from BS 10012, which can help you make sure that your approach to data protection compliance is fully effective.

This book relates the requirements of the law directly to the way you process your customer, client or contact information. It also explains what you have to do and provides examples of how to do it. In addition, it provides specific guidance for businesses or other organizations operating in high risk areas.

**What does this book cover?**

This book covers all the requirements of the Data Protection Act, and by the end of it you will be able to:

- identify what personal information you can legally collect and use;
- know what you can and cannot do with the personal information you have collected;
- understand the law as it applies to your particular business or activity;
- deal with data protection ‘emergencies’ such as requests for access to information from individuals, bad publicity and investigation by the Information Commissioner;
- keep on the right side of the law and avoid compensation, hefty fines or imprisonment;
- benefit from improved data management and a better relationship with customers, clients and other contacts;
- monitor and review your processes and procedures for compliance in line with the requirements of BS 10012.

Because this book is a basic guide to the Data Protection Act, we do not cover related legal topics such as compliance with the Human Rights Act, freedom of information legislation or laws that cover the interception or regulation of communications in any detail. Other guidance is available from BSI that addresses these issues in more detail.
Structure of this book

The law applies to personal information from the moment of collection of that information to its destruction, and to all things that happen to that information in between – this is the way in which this book has been set out. It is structured to reflect the life cycle of the personal information used by your organization and to take you step-by-step through what you need to do.

This book provides guidance on:

• notifying the Information Commissioner of your processing (a legal requirement);
• collection of personal information;
• use of personal information, including some specific advice for specialist areas;
• security and disposal of personal information.

Troubleshooting tips are also included to help with common queries.

Terminology

This book avoids the use of legal terminology and the complicated definitions set out in the law. We have, however, tried to ensure that all the definitions we use are consistent with BS 10012. The main differences are that where the law refers to ‘personal data’, both this book and the British Standard refer to ‘personal information’, and rather than referring to organizations that comply with the law as ‘data controllers’ (as the statute does), this book refers to ‘you’ and ‘your organization’.
Chapter 1 – Introduction

Who must comply with the Data Protection Act?

All individuals and organizations who ‘process’ personal information for their own business purposes must comply with the Data Protection Act 1998.

Types of organization that process personal information and therefore must comply with the Data Protection Act include:

- small, medium and large commercial organizations including limited companies, partnerships, limited partnerships and sole traders;
- charities, churches, political parties, and public and state schools;
- self-employed health professionals such as GPs, opticians and dentists;
- hospitals and NHS trusts;
- local authorities and other public sector organizations;
- unincorporated members’ clubs and associations;
- anyone who employs staff.

What are the rules?

The Data Protection Act contains eight principles for good information handling. These are that personal information must be:

1. processed fairly and lawfully;
2. processed only for specified and compatible purposes;
3. kept accurate and up to date;
4. relevant and not excessive;
5. retained for no longer than necessary;
6. processed in accordance with the rights of the individual whose personal information is being processed;

7. kept secure;

8. adequately protected if it is to be transferred outside the European Economic Area (EEA).¹

Guidance on how to comply with these principles is the main focus of this book. Further information about the EEA is given in Chapter 8, Transferring personal information overseas.

In addition to complying with these rules, organizations and individuals who must comply with the Data Protection Act may also have to notify the Information Commissioner of the details of how they process personal information. Chapter 2, Notification deals with this requirement.

The law also contains a number of criminal offences that relate to the misuse of personal information. These are covered in the relevant chapters.

**What personal information is protected by the law?**

Any information from which a living individual can be identified is protected under the Data Protection Act as long as that individual is the focus of the information in question.

A few examples of data that might be considered personal information, providing that it is possible to identify a living individual from the information in question and make them the focus of the information, include:

- name and address details;
- health information;
- information in emails;
- email addresses;
- CCTV footage featuring the individual’s image;
- call recordings featuring the individual’s voice;
- photos, either digital or on paper;
- NHS numbers;
- National Insurance numbers;

¹ The European Economic Area or EEA consists of the member states of the European Union plus Norway, Iceland and Liechtenstein.
• full postcodes;
• information in a personnel file.

Information processed by automated means, such as on computer, is always protected.

Information held in ‘manual’ or paper-based files will be covered by the law to a different extent depending on whether it is processed in the public or the private sector.

If the paper-based information is processed by a public sector organization, it is covered by the Data Protection Act.

If the same information is processed in the private sector, it will only be covered by the law when it is held in a very organized way (for example information that is held in a paper-based filing system, where it can easily be retrieved because it is organized so that someone who does not have any previous knowledge of the system could locate the information they require).

**When is an organization ‘processing’ personal information?**

You will only have to comply with the law if you are ‘processing’ personal information. The Data Protection Act defines what is meant by ‘processing’, and the definition is very wide.

‘Processing’ personal information means doing anything at all with the information, including collecting, using, storing and destroying it. Even just reading or accessing information can be ‘processing’ it.

Examples of processing:
• collecting information via an application form, over the telephone or via a website;
• publishing information;
• selling information;
• using information for administration;
• using information for marketing;
• intercepting information;
• recording information;
• data matching, data mining or profiling;
• archiving information;
• reading information from a screen;
• disclosing or passing information to another organization or individual;
• shredding information in a personal file or erasing information from electronic media;
• making information available on a website.

As the definition of processing is so wide, most organizations that use personal information will find it difficult to argue that they are not processing personal information.

**Data processors**

The only organizations that might escape being covered by the Data Protection Act are those that only process personal information on behalf of other individuals or organizations under their instructions. Such organizations or individuals are referred to as ‘data processors’ under the Data Protection Act.

These relationships must be governed by a contract that specifically sets out what can and cannot be done with the information being processed by the data processor. If you process personal information under an outsourcing contract like this, the organization that is instructing you will be responsible for complying with the law, not you.

Examples of types of organization that will often be data processors include:
• mailing houses;
• IT consultants that have access to clients’ personal information when servicing IT systems;
• waste disposal companies that dispose of personal information on behalf of another organization;
• printers that print material, such as business cards, that contain personal information.

If you are processing your own personal information, for example in relation to your employees, you will have to comply with the requirements of the Data Protection Act with respect to this information. (See Chapter 10, *Employers and employee information.*)

However, in practical terms, whether or not you are processing information on your own behalf or on someone else’s, it is unlikely to make much difference to the safeguards that you are required to put in place. The main difference is likely to be that when you process on behalf of another, you will have to comply with the restrictions in any contract rather than the obligations set out in the Data Protection Act. However, these requirements are likely to mirror each other, especially in relation to the security of the information.
**Remember**

*Even if you are not directly affected by the requirements of the Data Protection Act 1998, you will probably be obliged to comply with its requirements under contractual arrangements.*

---

**Who enforces the law?**

The Data Protection Act is enforced by an independent regulator – the UK Information Commissioner. The Information Commissioner also provides advice and guidance to those trying to comply with the law and has a helpful enquiry service that will provide advice on a ‘no names’ basis. There is also a Scottish Information Commissioner who has responsibility for freedom of information regulation in Scotland. However, only the UK Information Commissioner enforces the Data Protection Act in the UK.

For contact details for the UK Information Commissioner’s Office, see *Sources of information* at the back of this book.

The courts can also enforce the law. Criminal prosecutions are usually brought by the Crown Prosecution Service on behalf of the Information Commissioner.