

This handbook is a summary of some of the main clauses in the Data Protection Act 1998 and is not a complete, exhaustive review of the Act. No liability can be accepted by Experian for any loss or damage incurred as a result of any material contained in this publication. For full details of the Act, readers should obtain a copy of the Act itself.

For further reference, readers are also advised to be in touch with:

The Data Protection Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF

Information line: 01625 545 745

or visit the Commissioner's website  
on [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)

For further copies of this booklet  
or details of Experian's services, contact:

Experian Customer Services  
Telephone: 0115 992 2555



Published by:  
Experian  
Information Services Division  
Riverleen House  
Electric Avenue  
Nottingham  
NG2 1RP

Telephone: 0115 941 0888

Experian is an information solutions company. It uses the power of information to help its clients target prospective customers, manage existing customer relationships and identify opportunities for profitable growth. Experian is a subsidiary of The Great Universal Stores PLC and has headquarters in Nottingham, UK and Orange, California. Its 12,000 people support clients in over 50 countries. Annual sales are in excess of £900 million.

Experian's Business Information Division provides information on businesses and on the people who run them, with its own databases in the UK, US and the Republic of Ireland. Its databases hold detailed information on every commercially active organisation in the UK - over 1 million limited companies with up to ten years of full financial data and over six million company directorships. Its Non-limited Businesses Database contains information on over 2.4 million businesses, sole traders and partnerships.

This information and Experian's products for assessing commercial credit risk enable its clients to make informed lending and credit decisions by examining a company's financial performance, its credit and risk profiles and the records of its directors. On-line analysis is enhanced by instant performance comparisons between companies and their competitors and records of payments behaviour with other organisations.

For more information, visit the  
company's web site on  
[www.experian.com](http://www.experian.com)

# A simplified guide to the Data Protection Act 1998

To assist businesses holding personal information on  
customers, suppliers, directors, shareholders or others



## Foreword

*FOREWORD BY Elizabeth France, Data Protection Commissioner*

The Data Protection Act 1998 is based on a European Directive which requires member states 'to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data'. I am pleased that many organisations increasingly see the need to follow proper information handling procedures as a key requirement of their business activity and it is my view that where businesses and organisations build in compliance with the rules designed to ensure respect for that privacy, they will not be taking on an undue burden.

The new Act places a number of new responsibilities on businesses and organisations of all types and sizes in the way they collect, hold and process personal data. When processing becomes fully subject to the requirements of the new Act, Data Controllers will be faced with a number of new judgments to make, which I appreciate may raise some questions.

This simplified guide to the new Act by Experian provides a useful overview of many of the key issues that you will face when making these judgments. I suggest you read it carefully and seek advice where necessary. The new rules - and those carried over unchanged from the 1984 Act - must become integrated into the way you handle personal data.

*Elizabeth France*



## Contents

Introduction .....	4
What you should know about the Data Protection Act .....	5
What are the significant terms of the new Act ? .....	5
The Act refers to 'processing' data - what does this mean?.....	5
What conditions do I have to meet if I process personal data? ..	6
Do I have to obtain consent from individuals to process data on them? .....	6
How does this apply to credit references?.....	7
Are there changes in the regulations relating to directors? ....	7
Is it the same for shareholders? .....	8
How does the Act affect trade references? .....	8
Are there special regulations about 'sensitive data' ? .....	8
How much time do I have to comply with the Act?.....	9
Timetable for compliance .....	9

Who should take special note of the new Act? .....	9
What about trade names? .....	10
Is data obtained from overseas covered by the Act and can I transfer personal data overseas from the UK? .....	10
What happens if a partnership or a company is dissolved? .....	11
What is the difference between a Data Controller and a Data Processor? .....	11
What are the rights of individuals over the data held on them? .....	12
What if I want to use personal data for research or analysis? .....	14
Who regulates compliance with the Act? .....	14
What powers does the Data Protection Commissioner have? .....	14
What do I have to do now? .....	15
Are there penalties for offences against the new Act?.....	15
Essential Steps .....	15

## Introduction

This booklet is published by Experian as an aid to UK businesses of all sizes to appreciate the terms of the Data Protection Act 1998 and to understand how it affects them.

It is vital for all managers to be aware of the terms of the Act, no matter what size or type of business you are in, as it affects any personal data you may hold, whether on your workforce, customers, suppliers, directors, shareholders or whoever. The terms of the Act do not simply relate to trading on credit, but apply to virtually every aspect of business, including, for example, marketing, personnel and accounts.

A central principle of the 1998 Act is that data held on individuals must be fairly collected and used. This means you must be transparent and open about what you use data for.

Anyone is entitled to apply to your business to have access to any data you hold that relates to them. There are penalties, including possible fines, for non-compliance with regard to the content of personal files (manual or computer-held) and the way they are compiled and accessed.

Virtually any organisation, whether a multi-national company, sole trader, partnership, credit circle, small limited company, or members' club - any organisation that holds personal data - is affected.

### *Example:*

Builders' merchant with a customer base of small builders, sole traders and amateur DIY enthusiasts. This company will hold data, either manually or on computer, on:

- Sales records
- Credit payments/records
- Mailing/prospect list
- Orders
- Customer notes, such as, 'never knows the correct specification for parts'; 'keeps disputing invoices'; 'high proportion of suspect returns';
- Intentions, such as 'reduce credit limit'; 'impose larger minimum order quantity'; 'convert to newer model'
- Employees and job applicants

Every one of these types of data, if relating to individuals, sole traders, identifiable partnerships or directors, falls under the requirements of the Act.

This handbook is a summary of some of the main clauses in the Data Protection Act 1998 and is not a complete, exhaustive review of the Act.

For full details, readers should obtain a copy of the Act itself, or refer to guidance notes issued by the Data Protection Commissioner, which can be found on the Commissioner's website on [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)

## What you should know about the Data Protection Act 1998

The Data Protection Act 1998 affects every business in the UK. The Act is effective from 1 March 2000, so everyone should be aware of what it is and how it affects them personally and in business.

The Act has been framed as a result of the years of experience gained from the 1984 Act and is wider in scope, but has its emphasis on good practice and fairness to individuals and to those holding and using the data. It makes good practice in the handling of personal data legally enforceable, preventing the processing of personal information in an unfair, damaging or intrusive way.

### *Example:*

Destruction of personal data can be construed as unfair or damaging. If sales records needed for the calculation of agreed retrospective discounts are destroyed, the customer can claim that their destruction is detrimental to his business.

The Act introduces two new concepts to describe those involved in the handling of personal data: the Data Controller and the Data Processor.

The Data Controller is the person responsible for determining the purposes for, and the manner in which, any personal data is processed. The Data Processor is any person (other than an employee of the Data Controller) who processes the data. Both Data Controller and Data Processor can be an individual, a group of individuals or an organisation.

The definitions, roles and responsibilities of Data Controllers and Data Processors are explained more fully on page 11.

## What are the significant terms of the new Act ?

For the first time the Data Protection Act applies to manually kept paper records - and not only to those held on a computer.

The Act applies exclusively to records relating to people, not companies. However, data on sole proprietorships and small partnerships will be personal data subject to the Act; so will data held on directors and shareholders of companies.

All computer records come within the terms of the Act if they can be used to identify the individual the record refers to, no matter how they are filed. They do not need to be filed by name, but could, for example, be filed by amount of business transacted, geographical location or type of business. So long as the personal information within these files can be used to identify the individuals concerned, then they are covered by the Act as personal data. Manual records will be covered if specific information relating to particular individuals is readily accessible.

## The Act refers to 'processing' data - what does this mean?

'Processing' has a broader meaning within the Act than in normal usage. It covers: obtaining, recording or holding information and the organisation, alteration, retrieval, accessing, disclosure or even erasure or destruction of that data, whether in a manual or electronic form.



## What conditions do I have to meet if I process personal data?

It is a key principle under the 1998 Act that personal data can only be processed if certain conditions are met. These are where:

- The individual has given his or her consent to the processing
- The processing is necessary for the performance of a contract where the person concerned is one of the parties to the contract
- The Data Controller is legally obliged to process the data
- The processing is necessary to protect an individual's vital interests\*
- The processing is necessary for the administration of justice or other functions on behalf of the Crown or a Government department
- The processing is necessary for pursuit of the legitimate interests of the Data Controller or a third party to whom the data is disclosed, except where the processing is unwarranted because it may prejudice the rights or legitimate interests of the individual.

*\* The vital interests of a subject might, for instance, be where his or her medical history has to be disclosed to a casualty department in a medical emergency, such as an accident at work.*

It is important to distinguish between legal requirements and company rules. Examples of legal requirements are for Inland Revenue and VAT purposes. The fact that company rules require certain processing does not, in itself, mean the processing is permissible.

## Do I have to obtain consent from individuals to process data on them?

This is probably the most onerous duty of Data Controllers and the Data Protection Act 1998. It gives Data Controllers responsibility for obtaining consent from individuals to process their personal data and to ensure it is processed fairly.

People have to 'signify' their consent, which must be interpreted as a positive communication from the individual that the data can be processed.

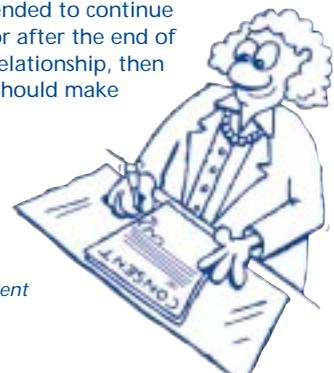
Failure to reply to a message from a Data Controller to the effect that personal data is being held and accessed does not mean that consent has been given.

**Individuals must be made aware of the purposes the data will be processed for; for example:**

- For analysis to market other products and services
- To use for telemarketing
- To determine credit limits

Consent, also, must be 'specific' and 'informed'. This means it has to be relevant to all the uses registered, including the type of information to be held, the purposes of the processing, the type of people who may be given access to it and the length of time that it might be on file (which can be 'indefinitely').

If the processing to which the consent relates is intended to continue indefinitely or after the end of the trading relationship, then the consent should make that clear.



*Giving consent*

## How does this apply to credit references?

The consent of individuals is a key element when obtaining consumer credit references and this principle is now extended to obtaining commercial credit references on sole traders, partnerships and directors of limited companies. Notification that credit references will be sought must be prominently displayed. This can be on the premises at the point of sale, within order acknowledgement documentation or within terms and conditions of sale paperwork. The individual must also be informed that a footprint (record) of that search will be kept.

### *Suggested wordings:*

"We will make a search with a credit reference agency, which will keep a record of that search and will share that information with other businesses. We may also make enquiries about the principal directors with a credit reference agency."

If supplying payment data to a credit reference agency:

"We will monitor and record information relating to your trade performance and such records will be made available to credit reference agencies, who will share that information with other businesses in assessing applications for credit and fraud prevention."

For Credit Circle members:

"We will monitor and record information relating to your trade credit performance and such records will be made available to other organisations to assess applications for credit."

If transacting business by telephone, the operator must make verbal notification and seek consent. It is advisable to establish an audit trail to prove notification and consent.

## Are there changes in the regulations relating to directors?



Yes. The new Act encompasses any personal information that allows an individual to be identified. Under the 1984 Act, if customer records relating to large limited companies listed the names of the directors of the company, that was not considered to be personal as the information was kept simply by virtue of their position. When they left or moved, their name was replaced by the new director's name. Under the new Act, simply noting the name of the Marketing Director makes it personal data subject to the 1998 Act.

Even if records refer to directors of the largest companies *by name*, any information held on those directors is covered by the Act.

### *Example:*

An organisation makes credit reference checks on its customers and their directors and keeps notes about the directors, such as their track record, family circumstances, outside interests and favourite sporting events, which it uses for planning corporate hospitality. The information about the directors falls within the scope of the new Act, even if it is destroyed immediately the director leaves his or her post.

## Is it the same for shareholders?

Basically, yes. If shareholdings are held by corporates, charities and so on, then there is no personal data involved, but when they are personal shareholdings held by named individuals, all the information about that individual, including their address, dealings or prices at which shares have been bought or sold, falls within the scope of the new Act.

## How does the Act affect trade references?

Once again, it depends to whom the trade reference refers but, in general, any trade reference relating to an individual, sole trader, partnership or even a small limited company when the individual is identifiable, will have to be handled and processed in the same way as all other personal information.

In these circumstances, under the new Act, data can only be processed for the purposes notified by the Data Controller. Trade references can be given, therefore, if the Data Controller has notified the Data Protection Commissioner that data will be used for that purpose, even if the information is held by a third party with no immediate relationship with the individual on whom the reference is being made.

Trade references can only be given with the consent of the individual. When the names of organisations to approach for trade references are provided to a supplier by the subject of the reference, this is deemed to be giving consent. The organisation supplying the reference must be aware that the individual has the usual rights over the information in the reference (see page 11 for rights of individuals) and can demand to see it.

### *Example:*

If a trade reference contains information which is not correct or contains damaging and subjective opinion about an individual's credit-worthiness or payment records, for example, it could be construed as causing distress or damage and the individual might have a right to compensation. In addition, if the trade reference is withheld when the individual asks to see the information held on him or her, the Data Controller will be liable under the new Act.

Trade references on limited companies where there is no reference to any individuals or when no individual could be identified from the information about the company (i.e. some small and all large and medium-sized companies) are not subject to the provisions of the Act. When giving trade references on these companies it is important not to include any comments about individuals at the company.

## Are there special regulations about 'sensitive data' ?

The Act lists 'sensitive data' that it assumes will not normally be required in a database on individuals and which can only be included if certain conditions are satisfied. The sensitive data is defined as racial or ethnic, political opinions, religious and similar beliefs, membership of trade unions, information on physical or mental health and condition, sex life, offences committed and any proceedings for any offence committed or alleged to have been committed.

Sensitive data may only be processed where one or more defined conditions is met:



*Sensitive Data*

- Where the individual has given their explicit consent
- Where the data is essential for the Data Controller to meet statutory or legal requirements
- Where they are essential to protect the interests of the individual and consent cannot reasonably be obtained
- Where a non-profit organisation is processing the data and exists legitimately for purposes relating to the sensitive data, such as a political party, a trade union or a church; and where the data relates to its membership.

Furthermore, the processing of such sensitive data must be protected by adequate safeguards and not be disclosed to a third party without the consent of the individual.

### How much time do I have to comply with the Act?



*How long have you got to comply?*

Although the Act received Royal Assent in July 1998, it came into effect in March 2000. From that time on the Act applies fully to all data systems, either electronically or manually held, which have been initiated since October 24 1998.

Anyone operating a system in which data processing has been under way since before October 1998 can benefit

from a transition period up to October 2001, after which all systems must comply with the terms of the new Act.

### Timetable for compliance

<p><b>March 2000</b> All systems initiated since 24 October 1998</p>
<p><b>March 2000</b> All systems where the purpose of the processing or the type of data has materially changed even if the system was set up before 24 October 1998</p>
<p><b>October 2001</b> All new paper entries on manual systems (i.e. a card index or a handwritten ledger) even if the system was set up before 24 October 1998</p>
<p><b>October 2001</b> All systems initiated before 24 October 1998</p>

### Who should take special note of the new Act?

The Act applies to all businesses processing personal data, even if they are exempt from notification. Exemption only applies to those required to make their data public e.g. Companies House.

Virtually all other sets of data used by businesses come within the Act, so it covers, for example, most personnel records in a company (it would be difficult to imagine a commercial personnel list that could be exempt), records of sales calls (made in person or by telephone), customer records, mailing lists. The only exceptions would be records that relate exclusively to companies or partnerships that are so large, that it would not be possible to connect the information with any individually identifiable people.

*Example:*

Data on partnerships are affected by the new Act, but not if there are so many partners that they could not be individually associated with what is on record. Therefore, data on the large accountancy and legal firms are not subject to the Act, but information held on a local accountancy firm with two or three partners is. Partnerships that are part of a network of independent businesses should be treated as individual partnerships.

### What about trade names?

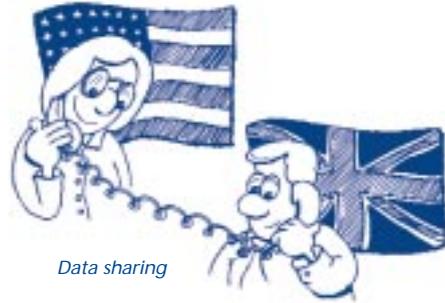
Even where a sole proprietor is operating under a trade name, any data recorded about the trade name is likely to be personal data subject to the 1998 Act, as it is immediately identifiable with the person running the business.

*Example:*

When a sole proprietorship such as a corner shop is sold, any payment records relating to that business name cannot be transferred. They have to be regarded as relevant only to the former sole proprietor and not to the new owner or owners. It would be illegal to continue to classify the business as, say, 'uncreditworthy', if a supplier had had bad payment experiences with the business under its previous ownership.

### Is data obtained from overseas covered by the Act and can I transfer personal data overseas from the UK?

Personal data cannot be transferred outside the European Economic Area (the 15 EU member states plus Iceland,



Data sharing

Liechtenstein and Norway) unless the destination country has an 'adequate' level of privacy and data protection. At present, virtually no country outside the EEA meets this condition so the Government and Data Protection Commissioner are considering the development of a 'model contract' to guarantee the protection of personal data transferred overseas.

There are some exceptions to this rule:

- Where the individual has given express consent
- Where the transfer of data is necessary for the performance of a contract between the individual and Data Controller
- Where the transfer of data is necessary to meet the needs of a legal process, for example, in drawing up a contract

*Example:*

A small partnership wants to purchase goods directly from a supplier in the Far East. The supplier approaches a credit reference agency for a credit check on its customer. In order to do so, the supplier has to obtain the consent of the partnership before the results of the credit check can be sent to him.

Personal data obtained from overseas, even if from outside the EEA, is covered by the requirements of the new Act.

The principle here is that data is protected by the rules that apply where the data is processed rather than the country of source.

## What happens if a partnership or a company is dissolved?

It is important at the outset to determine (in a formal contract or letter) what would happen in the event of a split amongst directors or partners; who would then be the owner of the database, who would then be responsible for its maintenance to comply with the terms of the Act.

## What is the difference between a Data Controller and a Data Processor?

The new Act makes an important distinction between the Controller and the Processor of data held on record and all businesses should also be sure to make the same distinction.

The Data Controller, put simply, is the company, organisation or person (or persons) who makes decisions about the data being recorded. In many cases, the company will be the Data Controller, but for sole traders and many small partnerships and small companies, it will be an individual. These decisions cover

- what data is held
- how it is held
- why it is held
- who has access to it



The Data Controller

**Any organisation keeping personal records must make it clear within their own organisation exactly who is making decisions on the data records and who is responsible for adhering to the terms of the Act. Ignorance of who was responsible will not be acceptable in the event of court proceedings because of a failure to obey the law.**

*If there are personal records, there has to be a Data Controller.*

In the previous 1984 Act, the term was the Data User, but the new Act has tightened this definition. If a person or persons process data on behalf of the Data Controller, the onus is now fair and square on the shoulders of the Data Controller to ensure that the terms of the new Act are followed to the letter. This includes the use to which the processing is put, the people who are allowed access to the data and the security for keeping the data protected.

**More than one person can be designated a Data Controller:**

Several Data Controllers can act 'jointly', where they make decisions relating to the data together, or they can act 'in common', when they make their own decisions about the same data which they share.

### *Example:*

In a credit circle, where groups of businesses agree to pool their credit experiences, each of the credit circles member companies have to have to be a Data Controller, who will be acting 'in common'.

## What are the rights of individuals over the data held on them?

The Data Protection Act 1998 applies to personal data that can be related to individually identifiable people. It gives powerful rights to the subjects of the data held. It allows them to make claims for substantial compensation if the responsible Data Controller has caused them damage or distress by breaking the terms of the Act.

The Rights of the individual can be listed under seven main headings. It is obviously very important for Data Controllers to be aware of these in detail, so that any data processing systems can be designed to comply fully with these rights at minimum expense. It could otherwise make the Controllers vulnerable to legal proceedings or involve them in great expense at a later date in order to comply.

### 1 Right of access

Individuals can make a request in writing or by electronic means and pay a fee (maximum £10) to discover if they are included on a database, to learn what data are held, why they are held and



*Right of access*

who can have access to the information. They are entitled to a copy of the data relating to them and Data Controllers are required to reveal any information they hold including details regarding the source of the data. (An exception might be the right to withhold the name of an individual who has provided information). If a computer system is used to produce an assessment or rating of an individual's status or performance, such as a credit rating or limit, then the individual has a right to ask for details of how the automated decision was reached.

### 2 Right to prevent processing likely to cause damage or distress

An individual can serve written notice prohibiting Data Controllers from processing data that can cause 'substantial damage or distress'. The Data Controller has 21 days in which to give evidence that they have complied or, instead, to give the reasons why they think that the individual's request is unjustified.

Examples of causing substantial damage or distress:

- Sending letters to dead people or to their family, relating to the deceased
- Passing adverse data relating to business premises rather than the occupants to debt collectors
- Revealing payment details to a third party without consent

### 3 Right to prevent processing for direct marketing

Individuals have the right to require Data Controllers to ensure that data will not be used for the purpose of sending them advertising or direct marketing material.

#### 4 Right in relation to automated decision-making

It is a growing practice to process computer-held data automatically in order to produce in-house league tables or to assess aspects of individuals. These automatic ratings can relate to customers payment performance, employees time-keeping and absenteeism, drivers vehicle accidents, reprimands and so on. Under the Data Protection Act 1998, an individual can give written notice preventing a Data Controller from taking such decisions based solely on scorecards or processing by other automatic means.

Furthermore, if no such written request has been made, it is still the responsibility of the Data Controller to notify an individual that a decision has been made by such means. Then the individual has 21 days in which to require the Data Controller to reconsider the decision or take a new decision on another basis.

##### *Exceptions:*

- Where automatic means of assessment are essential for considering whether or not to enter into a contract with the subject or in the course of performing such a contract.
- Where the decision based on automatic means is required to satisfy legal requirements.
- Where the decision is to satisfy a request from the subject of the assessment.
- Where all necessary steps have been taken to safeguard the legitimate interests of the individual (such as permitting them to make representations).

A builder's merchant has 2,000 customers. It automatically processes customer data by sales and profitability so that the top 20% of customers are offered special privileges such as additional discounts and preferred credit terms. Customers in the lowest category - who must pay on delivery according to the computerised system - can attempt to prevent their sales data being used in this way.

#### 5 Right to compensation

An individual suffering damage or distress as the result of a contravention of the requirements of the Act is entitled to compensation where the Data Controller is unable to prove that every reasonable care has been taken to comply with the terms of the Act.

#### 6 Rectification, blocking, erasure and destruction

Individuals can apply to a Court for an order requiring Data Controllers to rectify, block, erase or destroy any inaccurate data relating to them and any assessment or opinion based on such inaccurate data. Data Controllers can even be required to inform third parties, who have had access to the inaccurate data, that it has now been erased or amended.



*Rectification, blocking, erasure or destruction of data*

## 7 Requests for assessment

Any person, a Data Controller as well as an individual, can ask the Data Protection Commissioner to assess whether or not, in a particular instance, data is being processed in compliance with the Act.

## What if I want to use personal data for research or analysis?

Many organisations use personal data in order to analyse their markets, look for new business opportunities and so on. The new Act provides certain exemptions from seeking consent on the use or processing of data for research purposes, providing that the processing is exclusively for that purpose, and that:

- The analysis does not identify individuals
- The analysis is not in support of measures or decisions relating to particular individuals; and
- Substantial damage or distress is not, or is unlikely to be, caused to any individual

## Who regulates compliance with the Act?

The responsibility for overseeing compliance with the terms of the 1998 Act are similar to those for the 1984 legislation, but there have been some name changes. The Data Protection Registrar is now the Data Protection Commissioner. Anyone holding a relevant database now has to 'notify' the Data Protection Commissioner for inclusion in the registry, rather than 'register'.

## What powers does the Data Protection Commissioner have?

The Commissioner, who reports directly to Parliament, is responsible for promoting good practice by Data Controllers, for ensuring observance of the terms of the Act and for promoting awareness of the Act and how it works.

The Commissioner's powers are very similar to those afforded under the previous 1984 Act. The Commissioner has very wide discretion in coming to a decision on whether or not a Data Controller is complying with the terms of the new Act in the way data are collected and processed, the secure way in which they are held and the control of access by third parties.

The Commissioner can issue enforcement notices for Data Controllers to take steps to introduce methods in order to comply or to refrain from processes that contravene the Act. The Commissioner may initiate her own action or may take action as the result of an approach from an individual. There are, of course, procedures for Data Controllers to appeal against such notices.

If there are reasonable grounds to suspect that an offence against the Act is being committed, the Commissioner may apply for a warrant to enter and search the relevant premises. The Commissioner can also use powers of seizure of any documents which may constitute evidence of a contravention of the Act.



*The Data Protection Commissioner*

## What do I have to do now?

The Data Protection Commissioner will continue to maintain a register under the new Act.

There is a set of particulars that a Data Controller has to notify. The deadline for notification will depend on the factors described in an earlier section on the timetable of the terms of the Act.

### *Notifiable details:*

- Name and address of the Data Controller.
- Name and address of the representative of the Data Controller, if one has been nominated.
- Description of the data being processed.
- Purposes of the processing.
- Other parties who may have access to the data.
- Countries outside the European Economic Area (EEA) that may be given access to the data. (EEA members are the countries within the EU plus Norway, Iceland and Liechtenstein).

Data Controllers, when making notification to the register, must also include a description of the measures being taken to keep a database secure. This description will, naturally, not be included in the register itself.

## Are there penalties for offences against the new Act?

Offences against the requirements for notification under the 1998 Act can be taken to Magistrates Courts (where there is a maximum fine possible of £5,000); or to the Crown Courts, where unlimited fines are possible.

### *Essential Steps:*

- ✓ First look into all the records that are being used by your business, whether manually or computer held; whether at head office, branch office or even outside the business, such as at the homes of salesmen or on the premises of a computer bureau. Examine the extent to which they consist of personal data and come within the terms of the Act.
- ✓ Secondly, assuming the records can be defined as personal data, a Data Controller or Controllers should be appointed with the responsibilities described elsewhere in this booklet.
- ✓ You should then notify the Data Protection Commissioner of the data being held and the person or persons responsible for their control. The simplest way is to register your details by phone by calling 01625 545 740.
- ✓ Install the means by which consent is obtained from data subjects to hold and use information about them.
- ✓ Set up the systems whereby individuals can inspect the data you hold on them.
- ✓ Inform all relevant staff about the terms of the Act relating to how they collect, hold and access personal data.



Penalties