



Data protection

Data protection practice note - 18 February 2009

Contents

1. Introduction
 - 1.1 Who should read this practice note
 - 1.2 What is the issue?

2. What does the Data Protection Act cover?

3. Good practice for compliance
 - 3.1 Appointing someone to be responsible for compliance
 - 3.2 Notifying the Information Commissioner
 - 3.3 Audit your use of personal data
 - 3.4 Check compliance against the data protection principles
 - 3.5 A written data protection policy

4. The data protection principles
 - 4.1 First principle: fair and lawful processing
 - 4.2 Second principle: purpose of data
 - 4.3 Third principle: relevance of data
 - 4.4 Fourth principle: accuracy of data
 - 4.5 Fifth principle: retention of data
 - 4.6 Sixth principle: rights of subject
 - 4.7 Seventh principle: unauthorised or unlawful processing, and loss or damage
 - 4.8 Eighth principle: non-transfer of data outside the EEA

5. Exceptions: Manual data
6. Rules of professional conduct
7. Statutory provisions
8. More information

8.1 Status of this practice note8.2 Terminology in this practice note8.3 Other products**1. Introduction****1.1 Who should read this practice note?**

Managing partners, practice managers and all staff concerned with the management and day to day operations of practices.

1.2 What is the issue?

Processing personal data is fundamental to the work of a solicitor. The Data Protection Act 1998 (DPA) regulates the processing of information relating to individuals. Solicitors must comply with the DPA. Failure to do so may constitute a criminal offence.

This Practice Note sets out how solicitors can comply with the Act.

2. What does the Data Protection Act cover?

You must comply with the Act if you or your staff process personal data.

'Personal data' means data which relate to a living individual who can be identified either:

- from those data, or
- from those data and other information which is in your possession, or is likely to come into your possession, and includes any expression of opinion about the individual and any indication of your intentions or those of any other person in respect of the individual

If in doubt you should consult the Information Commissioner's Technical Guidance on determining personal data.

3. Good practice for compliance

Practices should undertake the following activities to ensure data are adequately protected.

3.1 Appointing someone to be responsible for compliance

Firms should appoint someone with appropriate authority to take the lead on data protection. This person should:

- familiarise themselves with the Act, guidance and relevant case law and keep abreast of changes
- notify the Information Commissioner, keep the notification up to date and renew it annually
- regularly 'audit' the firm's use of personal data and check compliance

draw up a written data protection policy and ensure that other members of staff are aware of, understand and comply with it
take the lead to ensure that data subject access and other legitimate DPA requests are handled in a timely manner

Larger firms are likely to appoint a specialist data protection officer who may report to a senior partner.

3.2 Notifying the Information Commissioner (IC)

The Information Commissioner oversees the DPA. You must not process personal data until you have provided the IC with both:

1. your 'registrable details'
2. a general description of the security measures you will take to protect personal data

Registrable details include:

your name and address,
a description of personal data
the purposes for which the data is being processed

This information is then entered into on the Public Register of Data Controllers. The register is available via the [ICO website](#).

3.2.1 Notification process

You must complete a form to provide notification. You may do this in one of three ways:

1. Complete the [online form](#). You must print off and sign a copy.
2. Telephone the notification helpline: 01625 545740. An advisor will assist you and the completed form will be sent to you.
3. Postal submission. You may request a form by writing to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

A fee of £35 is charged for notification. Annual renewal costs an additional £35.

Further information, form templates and a step-by-step guide are available at the [Commissioner's website](#).

The Information Commissioner has issued warnings about fake data protection agencies offering to complete the notification process. Firms should be aware of the [Commissioner's advice](#)

3.2.2 Failure to notify

Processing personal data without notifying the IC is an offence. Failure to notify may result in a fine. In 2008 there were at least three prosecutions of solicitors who did not comply.

You should note that the Information Commissioner does not have to inform you, or remind you, of this obligation.

3.3 Audit your use of personal data

You should understand the ways in which you are managing personal data. You may achieve this by creating a basic model of the personal data you are processing. The notification process will provide you with a starting point, but you should also understand and identify:

1. The different categories of individual about whom you process personal information, for example: clients, business partners etc.
2. Whether you receive that information directly from the individual themselves or indirectly through other people.
3. Where the information is kept, for example: on a central data store, on local machines, in e-mail accounts etc.
4. What is done with the data, for example: who has access to it, who it is shared with etc.

Constructing a formal model is not a requirement of the Act. However, keeping rough notes and/or diagrams that help you understand the way you use personal data may help when checking compliance with the DPA. It should also help to ensure that you haven't missed any categories of data processing from your compliance check.

3.4 Check compliance against the data protection principles

The Act sets out eight data protection principles with which you must comply. Check your data processing against each principle. (See [section 4: Principles](#)).

You should read carefully the principles and their interpretation which can be found in the [DPA Schedule 1](#), Part I (principles) and Part II (interpretation).

3.5 A written data protection policy

A written data protection policy is not a requirement of the DPA. Drawing one up will however ensure a systematic approach to compliance. Additionally, if you have staff, it will help to inform them about their own duties under the Act.

A typical data protection policy should cover the following:

The general principles of the Act and the obligation of all members of the firm to help ensure full compliance

Contact details of the person/s responsible for taking the lead on compliance and the circumstances in which they should be contacted or consulted

Procedures for dealing with both internal and external access requests. Usually it should only be necessary for staff to recognise an access request, before passing it on to whoever is responsible for compliance.

Staff responsibility for personal data

Information security procedures - this may involve cross-referencing to an information security policy document

4. The data protection principles

There are eight principles with which you must comply under the DPA.

4.1 First principle: fair and lawful processing

The first data protection principle states that personal data shall be processed 'fairly and lawfully', and shall not be processed unless:

- at least one of the conditions in Schedule 2 is met
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

You should therefore list all the data you process and check that conditions for schedule 2 have been met in each case, and in schedule 3 where appropriate.

4.1.1 Sensitive personal data

'Sensitive personal data' is defined as information consisting of a person's:

- (a) racial or ethnic origin
- (b) political opinions
- (c) religious beliefs or other beliefs of a similar nature
- (d) membership of any trade union
- (e) physical or mental health or condition
- (f) sexual life
- (g) commission or alleged commission of any offence, including details of:
 - any proceedings for any offence committed or alleged to have been committed by him
 - the disposal of such proceedings
 - the sentence of any court in such proceeding

4.1.2 Other considerations

You should also consider the following in order to comply with the first principle:

1. Have you misled anyone?

You should look at:

- how the data has been obtained
- whether the person from which the information was obtained has been deceived or misled as to the purpose or purposes for which the data will be processed

2. How you have satisfied basic information requirements?

Consider whether you have informed the data subjects of:

- your identity
- the purpose or purposes for which the data are intended to be processed
- anything else which you think is necessary in order to make the processing fair

3. **Have you complied with any additional, special, rules?**

Special rules apply to the collection and processing of personal information by e-mail etc and, in particular, unsolicited electronic marketing communications. These are covered by the Privacy and Electronic Communications (EC Directive) Regulations 2003

4.2 Second principle: processing for limited purposes

The second data protection principle states that personal data:

1. shall be obtained only for one or more specified and lawful purposes
2. shall not be further processed in any manner incompatible with that purpose or those purposes

The importance of 'purpose' is stated throughout the Act and reinforced most clearly in this principle. You should do the following to comply:

1. check whether or not a purpose for obtaining the data has been specified - generally, the person concerned should have been informed of this purpose in order to comply with the first principle
2. ensure the specified purpose is lawful

If 'further processing' does not fall within the specified purpose, you must identify whether it is compatible with the original processing of the data. If so, you may continue with further processing.

4.3. Third principle: adequate, relevant and not excessive

The third data protection principle states that, in relation to the purpose or purposes for which they are processed, personal data shall be:

adequate
relevant
not excessive

You should therefore check that any personal data you are holding meets these criteria.

4.4 Fourth principle: accurate and up to date

The fourth data protection principle states that personal data must be accurate and, where necessary, kept up to date.

The Act defines inaccurate data as 'incorrect or misleading as to any matter of fact.'

Inaccurate data that accurately record the information you have been given do not contravene the fourth principle if:

you have taken reasonable steps to ensure their accuracy - 'reasonable' depends on the purpose of the processing and
you include in the data any notification of inaccuracy made by the data subject

4.5 Fifth principle: not kept for longer than is necessary

The fifth data protection principle states that personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

You should set up data retention and review schedules for categories of personal data to help you to comply with this principle. After a set period of time the data should be reviewed, and destroyed when they no longer need to be retained.

4.6 Sixth principle: processed in line with subjects' rights

The sixth data protection principle requires that personal data be processed in accordance with the rights of data subjects under the Act.

The DPA gives data subjects a number of rights, the foremost of which is the right to have access to their personal data where permitted under the Act.

Data subject rights also include:

- prevention of processing for direct marketing purposes
- rights related to automated decision-taking
- prevention of processing which is likely to cause damage or distress

4.7 Seventh principle: security

The seventh data protection principle requires data controllers to take appropriate technical and organisational measures against:

1. unauthorised or unlawful processing of personal data,
2. accidental loss or destruction of, or damage to, personal data

This principle is complemented by the obligation to inform the Information Commissioner about security measures to protect personal data ([see section 3.1](#)).

You should consider all of the following to determine the appropriateness of your security measures:

- implementation cost
- technological developments
- nature of the data: note that sensitive personal data will merit particular attention
- harm that might result from unauthorised or unlawful processing, or from accidental loss destruction and damage to the data

These factors must be balanced and a risk-based approach to compliance is appropriate.

You must also take reasonable steps to ensure the reliability of any employees who have access to personal data.

4.7.1 Data processors

Special rules apply to contractors and others who are not employees but who are processing personal data on your behalf. The Act refers to them as "data processors".

In order to comply with the seventh principle you must only use a data processor who can:

- provide sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out
- take 'reasonable steps' to ensure compliance with those measures

You will not be regarded as compliant with the seventh principle unless this work is carried under a contract which:

1. is made or evidenced in writing
2. states that the data processor is to act only on instruction from you
3. requires the data processor to comply with obligations equivalent to those imposed on you by the seventh principle

4.8 Eighth principle: not transferred to other countries without adequate protection

The eighth data protection principle states that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) 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.

The EEA encompasses the European Union (EU) along with Iceland, Liechtenstein and Norway. EU findings of adequacy have been made in respect of Switzerland, Hungary and (partially) Canada. 'Safe Harbor' arrangements with individual companies in the United States (US) have been in operation since 2000. The scheme is enforced by the US Federal Trade Commission.

You should consult more detailed guidance if you are considering transferring personal data overseas.

5. Exceptions: manual data

If you do not use computers to process personal data you should consult the information commissioner's [guidance on manual data](#).

See also the Information Commissioner's guidance on [what constitutes personal data](#).

6. Rules of professional conduct

Rule 5: Business management in England and Wales

Rule 5 deals with:

- the supervision and management of a firm or in-house practice
- the maintenance of competence, and
- the internal business arrangements essential to the proper delivery of services to clients.

5.01(1)(k) requires provision for 'the continuation of the practice of the firm in the

event of temporary absences and emergencies, with the minimum of disruption to clients' business.'

5.01(1)(l) requires provision for 'the management of risk'.

7. Statutory provisions

Data Protection Act 1998

8. More information

8.1 Status of this practice note

Practice Notes are issued by the Law Society as a professional body for the benefit of its members. They represent the Law Society's view of good practice in a particular area. They are not intended to be the only standard, nor do they necessarily provide a defence to complaints of misconduct or of inadequate professional service. Solicitors are not required to follow them.

They do not constitute legal advice and, while care has been taken to ensure that they are accurate, up-to-date and useful, the Law Society will not accept any legal liability in relation to them.

For queries or comments on this practice note contact the Law Society's Practice Advice Service. www.lawsociety.org.uk/practiceadvice.

8.2 Terminology in this practice note

Must - a specific requirement in the Solicitors' Code of Conduct or legislation. You must comply, unless there are specific exemptions or defences provided for in the code of conduct or relevant legislation.

Should - good practice for most situations. If you deviate from this, you must be able to justify why this is appropriate, either for your firm, or in the particular retainer.

May - a non-exhaustive list of options for meeting your obligations. Which option you choose is determined by the risk profile of the individual firm, client or retainer. You must be able to justify why this was an appropriate option to oversight bodies.

8.3 Other products

The Law Society's [information security practice note](#)

[Data Protection Handbook 2nd Edition](#)

[Freedom of Information Handbook 2nd Edition](#)

[Intellectual Property Law Handbook](#)

Copyright 2010 Law Society All Rights Reserved
