



data protection a complete legal service

your guide to complying with the Data Protection Act 1998

There are many myths and misconceptions about the Data Protection Act, and it can be difficult to navigate your way through the conflicting advice. The Data Protection Act is built on a set of principles, which in many cases means that an organisation controlling personal data will have to make decisions based on the exercise of judgement, rather than being able to refer to a set of absolute requirements. To complicate matters, we currently have a situation where some of the provisions of the legislation have been supplemented and clarified by case law.

Although data protection is not always a simple matter, we aim to make compliance as straightforward for you as possible. This guide is designed to give you simple guidance on the basics, and to give you some pointers as to when you might require our expert advice. An explanation of the terminology we use is at the end of this document.

essential compliance

notification

Most data controllers need to notify their processing to the Information Commissioner on an annual basis. There is a useful web-based software tool that is designed to help you assess whether you should notify. It can be found at: <http://forms.informationcommissioner.gov.uk/notify/self/question1.html>.

Alternatively, telephone one of our experts, and we will make the assessment for you.

Notification costs £35 per year, and can be done on-line, although the notification does not become effective until the Information Commissioner's Office receives payment. We recommend that you pay by annual direct debit, as this avoids the notification lapsing as a result of an oversight, but we also recommend that you review your processing each time you renew. Please note that it is a criminal offence to fail to notify, or to fail to keep a notification up to date.

the data protection principles

There are eight principles that govern how personal data should be processed:

1. personal data shall be fairly and lawfully processed
2. personal data shall only be processed for one or more specified and lawful purposes and shall not be further processed in a manner incompatible with those purposes.
3. personal data shall be adequate, relevant and not excessive for the purposes for which it is processed.
4. personal data shall be accurate and where necessary up-to-date

the natural choice in law

5. personal data shall not be kept for longer than is necessary for the purposes for which it is processed
6. personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act
7. appropriate technological 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 outside the European Economic Area unless that country provides an adequate level of protection for the rights and freedoms of data subjects

what they mean in practice - in brief

when you collect personal data, you should tell people what you will do with it, and must not use it for any other purpose or allow any other data controller to process it for their own purposes unless you obtain further consent. Usually this information is given by means of a written statement, known as a data protection notice, but it can be given verbally.

You should be careful to ensure that you do not collect more personal data than is necessary for the purposes for which you are processing it. The personal data has to be relevant, but note that it should be adequate – you should avoid situations where the data that you have provides an inaccurate picture about the individual concerned, simply because not enough information has been collected.

You should take steps to ensure that the personal data you collect is accurate, and up-to-date, and you should not keep it for longer than is necessary. Often personal data can be held for the period during which it remains current, and then for six years after, on the basis that the information might be needed as evidence to take or defend legal action. However, this should always be considered on a case by case basis.

Data subjects have several rights under the Data Protection Act. The main rights are to have incorrect information corrected, to prevent or stop their details from being used for direct marketing purposes, to see information held about them, and to stop processing that causes them substantial

and unwarranted distress. As a data controller you need to be aware of these rights and act in accordance with them.

You need to ensure that personal data is held securely. You therefore have to ensure that employees that have access to personal data are reliable and that you have appropriate policies and train your staff so that they comply with the Data Protection Act. You should also take technical measures where necessary to prevent unauthorised and unlawful access and processing (such as controlling access to computer systems holding personal data) and ensure you have disaster recovery and back up systems in place to prevent loss of personal data. When you appoint data processors, you must have a written agreement with them that requires them to process personal data only in accordance with your instructions and requires them to comply with terms equivalent to data protection principle seven. You also must obtain sufficient guarantees that they will comply and take reasonable steps to assure yourself that they are complying.

When transferring personal data outside the European Economic Area (the EU countries plus Iceland, Liechtenstein, Norway and Switzerland) you need to assure yourself that rights and freedoms of data subjects are adequately protected. There is a list of countries that the European Commission has confirmed provide adequate protection, there is a list of exceptions to principle eight in Schedule four of the Data Protection Act, and there are contractual terms approved by the European Commission that are deemed to provide adequate protection.

some situations where you may need our help:

- when you need to notify
- when you are processing sensitive personal data. This is personal data which relates to: racial and ethnic origin, political opinions, religious beliefs, or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, commission of or alleged commission of offences, and any proceedings in relation to them. The rules for processing sensitive personal data are stricter than for processing ordinary personal data

- when a data subject wants to exercise their rights. There are strict time limits and rules about the fulfilment of such requests. Requests to see information held are the most frequent
- when you are asked to disclose personal data to a third party. There are exemptions that allow disclosure where it might otherwise be unlawful, but you need also to comply with the principles when making the disclosure
- when you are required to send personal data outside the European Economic Area – as there is more than one way of dealing with the issues arising
- when you appoint a data processor – to ensure that the requirements of the Act are fulfilled
- when you are procuring a database that holds personal data – as not all databases comply with the requirements of the Act, no matter what the salesman says
- when you have a complaint from someone
- when you need someone to use as a sounding board, or some idea of what other people in your situation might have done before
- when you need practical, commonsense advice

terminology

Here are some key terms from the Act:

data controller – is the person or organisation that controls the purposes for and the manner in which personal data is processed. Employees of controlling organisations will not be data controllers. Sometimes there are two data controllers of the same information, operating for the same purposes, or for completely different purposes, for example where two companies share a common database. When there is a breach of the Data Protection Act, it will be the data controller that is primarily liable, even if the breach was committed by someone else acting on the data controller's behalf.

data processor – is a person or organisation that carries out processing of personal data for and on behalf of a data controller. Some data processors are less obvious than others – for example, many data controllers fail to realise that when they outsource functions of their

business to service providers, those service providers will be data processors.

personal data – is information relating to a living individual from which that information can be recognised. Note that even if the information itself has been stripped of identifying details, such as by allocating a code number, the information must still be treated as personal data if it is possible for the data controller to use other information within its possession or control to identify who the individual is. This definition changed as a result of a case called *Durant v FSA*. Following that case, the information must also be focussed on the individual, significantly biographical, and capable of affecting that person's privacy, whether at home or at work. Note that information about sole traders and partnerships can also be personal data.

data subject – means the person who can be identified from the personal data in question.

CONTACT

Jo Dawtrey (OXFORD)
jo.dawtrey@bllaw.co.uk
Jimmy Desai (LONDON)
jimmy.desai@bllaw.co.uk
Lynda Smedley (PORTSMOUTH)
lynda.smedley@bllaw.co.uk

SOUTHAMPTON

T: 023 8090 8090
F: 023 8090 8092

WINCHESTER

T: 01962 844440
F: 01962 842300

OXFORD

T: 01865 248607
F: 01865 728445

PORTSMOUTH

T: 023 9222 1122
F: 023 9222 1123

LONDON

T: 020 7405 2000
F: 020 7814 9421

E: info@bllaw.co.uk

www.bllaw.co.uk