# Data Protection
## Your Rights

### Overview

The Data Protection Act 1998 ("the DPA") protects you by ensuring that organisations holding personal data about you, use it in a fair and proper way. It covers a wide variety of organisations, including government, employers, supermarkets, banks and those sending out junk mail. This factsheet gives an overview of the DPA and highlights some of the issues which might arise in an employment situation.

### What is covered by the DPA

The DPA applies when any personal information is held either digitally by computer/electronic equipment or on paper. The person the information is about is called the 'data subject'. The person or organisation holding and processing the information is called the 'data controller'.

The DPA protects your personal data, which means information relating to you. This could include opinions as well as facts about you. There are more strict rules for dealing with sensitive personal data, which relate to your racial or ethnic origin, political opinion, religious beliefs, health, sexual orientation, criminal convictions and trade union membership.

Any personal information that is processed or filed is covered by the DPA. Processing includes obtaining, recording, amending, holding or deleting information. A relevant filing system under the DPA is one where personal information is held in a structured way and accessible in a similar way to information on a computer.

> "The DPA protects your personal data, which means information relating to you."

### The principles of data protection

The DPA imposes eight obligations on organisations processing personal data. These are that data must be:-

- Processed fairly and lawfully
- Obtained and processed for specific purposes
- Adequate, relevant, not excessive
- Accurate, up to date
- Held for no longer than is necessary
- Processed in accordance with the rights of individuals
- Kept secure
- Only transferred outside the European Economic Area if there are adequate safeguards.

### Lawful processing

The key principle is the first, that data must be fairly and lawfully processed. For this to be the case, at least one of the following conditions must met for processing personal information:

- You have consented
- It is necessary for carrying out a contract with you
- It is required to comply with a legal obligation
- It is necessary to protect your vital interests
- It is necessary to carry out public functions such as the administration of justice
- It is necessary for the organisation's legitimate interests and does not prejudice your rights.

At least one of these additional conditions must be met when processing sensitive personal data:

- You have given explicit consent
- It is necessary for a legal duty in connection with employment
- It is carried out as part of the legitimate activities of a non-profit organisation
- It is necessary in connection with legal proceedings or the administration of justice
- It is undertaken by a health professional for necessary medical purposes.

Any processing of personal data or sensitive personal data which is carried out without meeting these conditions will be unlawful.

Continue overleaf ›

## Your rights

As well as imposing obligations on organisations processing information, you have rights under the DPA in relation to that information. This is known as "subject access rights". This gives you the right to see the information held about you, for example, employment records, provided that the DPA applies to that information. There are a number of exemptions, for example, information held for the purposes of preventing/detecting crime.

You can make a subject access request to any organisation processing personal data. They must respond within 40 days. They can charge you an administrative fee of up to £10 (£50 for medical records).

The information they must provide includes:

- A description of all personal information held on the individual and its sources
- A copy of all the information including an explanation of any codes used
- The purposes for which the information is being held or processed
- The likely recipients of any data.

## Making a complaint under the DPA

If you have been affected by the way your personal information has been processed, you can ask the Information Commissioner to assess whether there has been a breach of the DPA. The Commissioner is appointed by the government to oversee the operation of the DPA and the Freedom of Information Act (which relates to information held by public authorities not covered by the DPA). Although it is not legally binding, the Commissioner has also issued a code of practice for dealing with data in employment.

You can get a copy of the code and an assessment application form on the Commissioner's website at www.ico.gov.uk

In the first instance, if the Commissioner decides the DPA has been breached, there may be informal steps to find a resolution. If this is not possible, the commissioner may serve an enforcement notice on the organisation.

You have the right to seek compensation from the court if you have suffered damage and distress because of a breach of the DPA. Compensation is not normally awarded for distress alone. You can also ask the court to make an order for correction or destruction of inaccurate data.


## Some implications of the DPA in the workplace

**Record keeping** - Part 1 of the code deals with recruitment and selection and Part 2 deals with record keeping in employment. These should be read alongside other relevant provisions such as the Police Regulations and internal policies on record keeping.

**Monitoring individuals' communications** - Part 3 of the code covers monitoring at work and guidance on the use of CCTV. Monitoring telephone calls, email messages and internet access must be lawful and fair to individuals and comply with the Regulation of Investigatory Powers Act 2000. The DPA may also apply depending on how the monitoring is carried out and the records kept. Monitoring should not intrude unnecessarily on your privacy or autonomy at work. Your force should be able to show that the benefits of getting this information outweigh any negative impact on you.

Any monitoring should be done openly – secret monitoring is only allowed in very limited circumstances. The Information Commissioner recommends there should be a policy explaining how and why your calls, emails and internet access are being monitored.

**Medical testing** - Part 4 of the code covers information about workers' health. Where medical tests are carried out, there should be a clear operational need for them. The results of any medical tests are also covered by the DPA.



**If you need further assistance, in the first instance please contact your local Joint Branch Board.**

**W:** www.slatergordon.co.uk/policelaw

Slater & Gordon is one of the UK's leading and largest legal practices with offices throughout England, Wales and Scotland.



Slater Gordon Lawyers