

# Data Security - Data Protection Act

Many businesses are totally reliant on the data stored on their PCs, laptops, networks, mobile devices and in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the key compliance issues surrounding data protection and the Data Protection Act (the Act).

Most businesses process personal data to a greater or lesser degree. If this is the case, compliance with the Act is required unless one of the exemptions applies (see below).

Complying with the Act includes a notification process, handling data according to the principles of data protection and dealing with subject access requests.

In the UK, the Information Commissioner (ICO) is responsible for the public Data Protection Register and for enforcing the Data Protection Act.

## Summary of the principles of the Data Protection Act

1. Personal data must be fairly and lawfully processed;
2. Personal data must be processed for limited purposes;
3. Personal data must be adequate and not excessive;
4. Personal data must be accurate and up to date;
5. Personal data must be kept no longer than necessary;
6. Personal data must be processed in line with the data subjects' rights;
7. Personal data must be secure;
8. Personal data must not be transferred to countries outside the European Economic Area (EEA) without adequate protection.

## Exemptions

There are 5 main categories of exemption –

- organisations that process personal data only for:
  - staff administration (including payroll)
  - advertising, marketing and public relations (in connection with their own business activity) and
  - accounts and records
- some not-for-profit organisations

- organisations that process personal data only for maintaining a public register
- organisations that do not process personal information on computer and
- individuals who process personal data only for domestic purposes.

There are a number of more specific exemptions. However, most companies find the exemptions are too narrow, and opt to notify (see below).

## Notification

Notification is the method by which a company's usage of personal data is added to the public Data Protection register maintained by the ICO. The process starts by completing the notification documentation (available from [www.ico.gov.uk](http://www.ico.gov.uk)) and sending this back with the annual notification fee (currently £35 for the small business).

Notification needs to be performed annually (even if there are no changes).

N.B. Be wary of organisations who say they represent the ICO and who charge more than the standard £35 fee.

## Subject access request (SAR)

Individuals have rights under the Act to find out whether you are processing their personal data, and to provide them with a copy of the data which is stored about them.

Most SARs must be responded to within 40 days.

An individual has the right to ask you to:

- correct or delete information about them, which is inaccurate;
- stop processing their personal data for direct marketing purposes; or
- stop processing their data completely or in a particular way (depending upon the circumstances)

A fee can be levied for dealing with an SAR - but only up to £10 (except for health or education records).

If a fee is levied, the access request does not have to be complied with until the fee has been received.

Secondly, the Act makes it clear that the SAR must contain enough information to validate that the person making the request is the individual to whom the personal data relates. So it may be necessary and legitimate to ask for further identification from the originator of the SAR.

## Data security

The Act says there should be security that is appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

The Act does not define "appropriate" - but it does say that "an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved".

So, there a number of key areas to concentrate on -

### Management and organisational measures

Someone in the organisation should be given overall responsibility for data security.

#### Staff

Staff need to understand the importance of protecting personal data; that they are familiar with the organisation's security policy; and that they put security procedures into practice.

### Physical security

Technical security measures to protect computerised information are of obvious importance. However, many security incidents relate to the theft or loss of equipment, or to the disposal of old equipment and old printouts.

## Computer security

As well as a comprehensive backup regime, appropriate access controls and mechanisms need to be in place. Websites, in particular, need sophisticated security measures in place.

As well as the Data Protection Act, there are various other Acts and regulations, which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations (PECR) 2003 - which cover 'Spam' and mass-marketing mail shots. Regulations under the PECR are also issued from time to time. For example, regulations on the use of cookies on websites were introduced as from 2012.
- Copyright Design and Patents Act – amended 2002 to cover software theft.

There may be other IT standards and regulations applicable to your business sector. For example, companies processing credit card transactions need to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

## How we can help

We can provide help in the following areas:

- performing a security/information audit
- training staff in security principles and procedures
- notification and/or compliance with regulations as applicable to the type of organisation.

Please do not hesitate to contact us if we can be of further assistance.

**For information of users:** This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.