technical factsheet 176

Data Protection

CONTENTS

1. INTRODUCTION

The Data Protection Act 1998 came into force on 1 March 2000 and replaced the Data Protection Act 1984. The Act sets out rules for processing personal information, places obligations on those who process information and gives rights to those who are the subject of that data.

2. REGISTER WITH THE INFORMATION COMMISSIONER'S OFFICE

Every organisation that processes personal information in an automated form must notify the Information Commissioner's Office (ICO) unless they are exempt. Failure to notify is a criminal offence. Register entries should be renewed annually, failure to renew when required to do so is also a criminal offence.

The Act provides an exemption from notification for some organisations. The exemption is available for:

1. organisations that process personal data only for:
   (a) staff administration (including payroll)
   (b) advertising, marketing and public relations (in connection with their own business activity)
   (c) accounts and records
2. some not-for-profit organisations
3. organisations that process personal data only for maintaining a public register
4. organisations that do not process personal information on computer
5. individuals who process personal data only for domestic purposes.

Data controllers who are exempt from notification must comply with the other provisions of the Act, and may choose to notify voluntarily.

The following is a link to the ICO website which explains whether or not there is a need to notify and how to do so, which includes specific guidance on notification for data controllers for "not-for-profit" organisations, barristers' chambers and pension trust schemes: http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

The Data Protection Act protects the rights of individuals whom the data is about, mainly by placing duties on those who decide how and why such data is processed ('data controllers').

A data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
A data controller must be a 'person' recognised in law, that is to say:

(i) individuals
(ii) organisations
(iii) other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

A data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor. Where roles and responsibilities are unclear, they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles. For these reasons organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing. The ICO have published a good-practice note on 'Outsourcing: a guide for small and medium-sized businesses' which gives more advice about using data processors, which can be found at:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/outsourcing_gpn_version_2.1_080409.pdf

3. PERIOD PROTECTION RIGHTS AND DUTIES REMAIN EFFECTIVE

The duties under the Act apply throughout the period when personal data is being processed, as do the rights of individuals in respect of that personal data. The Act must be complied with from the moment the data is obtained until the time when the data has been returned, deleted or destroyed. The duties extend to the way the personal data is destroyed when it no longer needs to be kept. The data must be disposed of securely and in a way which does not prejudice the interests of the individuals concerned.

Changes in an organisation's circumstances do not reduce an individual's rights under the Act, however responsibility for ensuring this happens may shift, depending on the circumstances. For example if a company goes into administration, control of the company's assets (including the customer database) passes from the board of directors to the administrators, who decide to sell some of the assets. As the administrators now control the purpose and manner in which the database is used, they become data controllers in respect of the personal data it contains. The administrators must comply with the Data Protection Act in connection with any possible sale of the customer database.

4. THE DATA PROTECTION PRINCIPLES

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical 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 or territory outside the European Economic Area 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.

5. THE RIGHTS OF INDIVIDUALS

The Act gives rights to individuals in respect of the personal data that organisations hold about them. The rights of individuals that it refers to are:

1. A right of access to a copy of the information comprised in their personal data
2. A right to object to processing that is likely to cause or is causing damage or distress
3. A right to prevent processing for direct marketing
4. A right to object to decisions being taken by automated means
5. A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
6. A right to claim compensation for damages caused by a breach of the Act.

6. INFORMATION SECURITY

There must be appropriate security to prevent the personal data which is held from being accidentally or deliberately compromised in particular the following should occur:

1. Design and organise security to fit the nature of the personal data being held and the harm that may result from a security breach
2. Be clear about who in the organisation is responsible for ensuring information security
3. Ensure the organisation has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
4. Be ready to respond to any breach of security swiftly and effectively.

If, despite the security measures taken to protect the personal data being held, a breach of security occurs, it is important to deal with the security breach effectively. Having a policy on dealing with information security breaches is another example of an organisational security measure to be taken. There are four important elements to any breach-management plan:

(a) Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.
(b) Assessing the risks – risks associated with the breach should be assessed, as these are likely to affect what action is taken once the breach has been contained. In particular assessment should be made of the potential adverse consequences for individuals, how serious or substantial these are, and how likely they are to happen.
(c) Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. It should be clear who needs to be notified and why. It may be appropriate to notify the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
(d) Evaluation and response – the causes of the breach should be investigated and the effectiveness of the response to it. If appropriate the policies and procedures should be updated accordingly.

7. SENDING PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

The first principle (relating to fair and lawful processing) will in most cases require disclosure to the individuals that their personal data has been transferred to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using subcontractors abroad.

In addition to the countries in the EEA the European Commission has decided that certain countries have an adequate level of protection for personal data. Currently, the following countries are considered as having adequate protection:

Andorra
Argentina
Canada
Faroe Islands
Guernsey
Isle of Man
Israel
Jersey
Switzerland

Further information can be found on the ICO website at the following address:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx

Although the United States of America (US) is not included in the European commission list, the Commission considers that personal data sent to the US under the 'Safe Harbor' scheme is adequately protected. There is a list of the organisations signed up to the Safe Harbour arrangement on the US Department of Commerce website at:
http://safeharbor.export.gov/list.aspx

If the data protection law in a country has not been approved as adequate, it may still be possible to send personal data to that country. The sender should be satisfied that in the particular circumstances there is an adequate level of protection, such as:

1. Assess adequacy oneself
2. Use contracts, including the European Commission approved model contractual clauses
3. Use Binding Corporate Rules approved by the Information Commissioner (only applies to multinational organisations transferring information outside the EEA but within their group of companies)
4. Rely on the exceptions from the rule.

The ICO have produced guidance on the points above which can be found at the following address:
http://www.ico.gov.uk/for_organisations/data_protection/overseas.aspx

Model contractual clauses can be found at the following address:
http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm

8. THE CONDITIONS FOR PROCESSING

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies at least one of the following conditions must be met whenever you process personal data:

1. The individual who the personal data is about has consented to the processing.
2. The processing is necessary:
    (a) in relation to a contract which the individual has entered into; or
    (b) because the individual has asked for something to be done so they can enter into a contract.
3. The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
4. The processing is necessary to protect the individual's 'vital interests'. This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
5. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
6. The processing is in accordance with the "legitimate interests" condition. Three requirements need to be met to qualify as a 'legitimate interest':

(a) The first requirement is that the information needs to be processed for the purposes of legitimate interests or for those of a third party to whom the information will be disclosed.
(b) The second requirement is that these interests must be balanced against the interests of the individual(s) concerned. Where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.
(c) The third requirement is that the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

There are additional conditions which must be satisfied if processing sensitive personal data, these conditions are listed in the Data Protection Act.

9. THE RIGHTS OF INDIVIDUALS

Commonly referred to as 'subject access' is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this and an individual who makes a written request and pays a fee is entitled to be:

1. Told whether any personal data is being processed
2. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
3. Given a copy of the information comprising the data
4. Given details of the source of the data (where this is available).

On individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it.

On organisation receiving a subject access request may charge a fee for dealing with it. If you choose to do this, you need not comply with the request until you have received the fee. The maximum fee you can charge is £10. There are different fee structures for organisations that hold health or education records (where the maximum fee is £50, depending on the circumstances).

The Act allows you to confirm two things before you are obliged to respond to a request. First, you can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. Second, you are entitled to ask for information that you reasonably need to find the personal data covered by the request.

If you use a data processor, then you need to make sure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the data processor. Responsibility for complying with a subject access request lies with the data controller. The Act does not allow any extension to the 40-day time limit in cases where you have to rely on a data processor to provide the information that you need to respond.

10. THE RIGHT TO OBJECT TO PROCESSING

An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question. An individual who wants to exercise this right has to put their objection in writing to the organisation concerned and state what they require that organisation to do to avoid causing damage or distress. This notice is referred to as an 'objection to processing' or a 'section 10 notice'.

The organisation concerned must respond within 21 days of receiving the objection to processing. The response must state what the organisation intends to do and, if it intends to comply with the objection in some way, give reasons for the decision.

If the organisation decides that an objection to processing is not justified and it does not comply with it, the individual can apply to the court. The court can decide whether the objection is justified and, if necessary, order the organisation to take steps to comply.

11. THE RIGHT TO PREVENT DIRECT MARKETING

Individuals have the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not to begin) using their personal data for direct marketing. Any individual can exercise this right, and the organisation must comply within a reasonable period of receiving the notice.

12. RIGHTS RELATING TO AUTOMATED DECISION TAKING

The right of subject access allows an individual access to information about the reasoning behind any decisions taken by automated means. The Act complements this provision by including rights that relate to automated decision taking. Consequently:

1. An individual can give written notice requiring an organisation not to take any automated decisions using their personal data
2. Even if they have not given notice, an individual should be informed when such a decision has been taken
3. An individual can ask an organisation to reconsider a decision taken by automated means.

Some decisions are called ‘exempt decisions’ because the rights do not apply, even though they are taken using solely automated means and do significantly affect the individual concerned.
Exempt decisions are:

1(a) authorised or required by legislation; or
(b) taken in preparation for, or in relation to, a contract with the individual concerned; and
2(a) are to give the individual something they have asked for; or
(b) where steps have been taken to safeguard the legitimate interests of the individual, such as allowing them to appeal the decision.

13. RIGHTS RELATING TO INACCURATE PERSONAL DATA

Where personal data is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. In addition, where an individual has suffered damage in circumstances that would result in compensation being awarded and there is a substantial risk of another breach, then the court may make a similar order in respect of the personal data in question.

14. THE RIGHT TO COMPENSATION

If an individual suffers damage because an organisation has breached the Act, they are entitled to claim compensation from that organisation. This right can only be enforced through the courts. The Act allows the organisation to defend a claim for compensation on the basis that it took all reasonable care in the circumstances to avoid the breach.

15. EXEMPTIONS

There are some exemptions from the Act to accommodate special circumstances. If an exemption applies, then (depending on the circumstances) the organisation will be exempt from the requirement:

1. To notify the Information Commissioner; and/or
2. To grant subject access to personal data; and/or
3. To give privacy notices; and/or
4. Not to disclose personal data to third parties.

Most organisations that process personal data must notify the ICO of certain details about that processing. However, the Act provides exemptions from notification for:

1. Organisations that process personal data only for:
   (a) Staff administration (including payroll);
   (b) Advertising, marketing and public relations (in connection with their own business activity); and
   (c) Accounts and records;
2. Some not for profit organisations;
3. Organisations that process personal data only for maintaining a public register;
4. Organisations that do not process personal information on computer.

There are also exemptions from 'subject access' from 'disclosure' and 'non-disclosure' and in relation to other areas. Further details and other aspects of data protection can be found on the ICO website: http://www.ico.gov.uk/

16. RULES ON USE OF COOKIES AND SIMILAR TECHNOLOGIES

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (the Regulations) cover the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as their computer or mobile.

A cookie is a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites. Cookies are then sent back to the originating website on each subsequent visit. Cookies are useful because they allow a website to recognise a user's device. The Regulations apply to cookies and also to similar technologies for storing information. Using such technologies is not prohibited by the Regulations but they do require that people are told about cookies and given the choice as to which of their online activities are monitored in this way. This guidance uses the term "cookies" to refer to cookies and similar technologies covered by the Regulations.

Regulation 6 of the Privacy and Electronic Communications Regulations 2003 (PECR) says:
A person shall not store or gain access to information stored in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met. Paragraph 2 says the requirements are that the subscriber or user of that terminal equipment:

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
(b) has given his or her consent.

Those setting cookies must:

1. Tell people that the cookies are there,
2. Explain what the cookies are doing, and
3. Obtain their consent to store a cookie on their device.

There is an exception to the requirement to provide information about cookies and obtain consent where the use of the cookie is:

(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

First steps to consider to comply with these regulations would be:

1. Check what type of cookies and similar technologies you use and how you use them.
2. Assess how intrusive your use of cookies is.
3. Where you need consent – decide what solution to obtain consent will be best in your circumstances.

The ICO website and the following guide from the ICO gives further details on various aspects of these regulations:
http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx