Torfaen Voluntary Alliance

Your local county voluntary council

2. Running your organisation

2.12 Data protection

What is data protection all about?

The **Data Protection Act 1998** (the Act) came into force on 1 March 2000 and sets out the obligations of those who process data, the powers of the Information Commissioner to enforce those obligations, and the offences that may be committed when they are not complied with.

The Act imposes obligations on **data controllers**. A data controller is someone who directs how and why personal data is processed, and they may be an individual or an organisation.

Personal data is any data that serves to identify a specific living individual (who will be classed as the **data subject**), and examples might include an email address, postal address, National Insurance number, date of birth, photographs, employee number, and so on. Personal data does not include information about organisations as these are not living individuals. The Act says that to fall within the definition of 'personal data', the data must be recorded

- on a computer or automated system, or
- in a relevant manual filing system (this is a set of information that is not held on a computer but is structured in a way so that specific information about a particular individual is readily accessible), or
- with the intention of putting it in to one of these systems.

Processing is very widely defined, and in practical terms it is likely to cover anything your organisation does with personal data.

The data protection principles

Data processors must comply with the **data protection principles** that are set out under the Act. There are eight of them:

- Personal data must be processed fairly and lawfully
- Personal data must only be used for specified, limited purposes
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and up to date
- Personal data must not be kept longer than necessary
- Personal data must only be processed in accordance with the rights of the data subject
- Personal data must be held securely

- Personal data must not be transferred outside the European Economic Area (EEA) without adequate protection.

The first principle refers to data needing to be processed fairly. Whilst there is no statutory definition of what is 'fair', the Act gives specific guidance on what is likely to be regarded as fair. The key requirements are that:

- The data subject must not be deceived or misled
- The data subject must know the purpose for which the data is intended
- The data subject must be informed of the identity of the data controller
- The data subject must be informed whether the data is likely to be passed to a third party.

It is important to note that the above requirements are for guidance only and compliance with them will not automatically ensure fair processing.

The last principle states that personal data must not be transferred to a country or territory outside the EEA unless that country or territory ensures ‘an adequate level of protection’ for the rights and freedoms of data subjects.

If you are considering sending personal data outside the EEA you may find it helpful to work through a checklist that is set out on the Information Commissioner’s Office (ICO) website, to help you decide if the eighth principle applies and, if so, how to comply with it to make a transfer.

Sensitive Data

There is increased protection for what is termed **sensitive data**. This is personal data consisting of information about a data subject’s:

- racial or ethnic origin
- political opinions
- religious or other similar beliefs
- membership of a trade Union
- physical or mental health condition
- sexual life
- commission or (alleged commission) of any offence
- court proceedings

Sensitive data can be processed provided:

- The data subject has given his/her explicit consent
- It is a legal requirement of the data subject's employment
- It is necessary to protect the vital interests of the data subject
- Is carried out by certain non-profit bodies that are established for political, philosophical , religious or trade union purposes
- It is necessary for legal proceedings
- It is necessary for medical purposes
- It is necessary for monitoring equal opportunities
- The Secretary of State has given his consent
- It is necessary for the prevention or detection of any unlawful act
- It is necessary for the provision of services such as confidential counselling or advice
- It is necessary for insurance or occupational pension scheme contracts.

The list is not exhaustive and new categories can be added by way of Statutory Instrument.

Sensitive data cannot be used unless at least one of the above conditions has been met. The most important of these conditions is often that the subject has given explicit consent. This must have been freely given and, where possible, should relate to the exact data in question and method of processing. It need not be in writing and sometimes can be implied: for example, the completion of a booking form for a conference which states clearly that the information may be used for other specific purposes (although ideally the data subject should be given an option to ‘opt out’ of this happening because she objects to it).

Rights of a data subject

A data subject has the following rights:

- To access a copy of the information comprised in their personal data (access is gained by submitting a **subject access request**)
- To object to processing that is likely to cause damage or distress
- To opt out of direct marketing
- To object to decisions being made by automated means
- To, in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- To compensation for breaches caused by a breach of the Act.

If the data controller receives a written subject access request from the data subject, the data controller must respond to it. A data subject that makes a written request (by hard copy, email, fax or even via social media) is entitled to:

- Be told whether any personal data is being processed
- A description of the personal data being processed, why it is being processed, and whether it will be given to any other people or organisations
- A copy of the information comprising the personal data
- The source of the data (where this is available).

The data controller is entitled to charge a fee of up to £10 for dealing with a request if they wish to, but there is no requirement to do so. Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but the data controller is not obliged to do this.

The data controller is, however, required to respond to the subject access request within 40 calendar days of receiving it, and they must supply everything that is held by them about the data subject at the time the application was made (in line with the above list of what the data subject is entitled to). Embarrassing information cannot be withheld. However, information may be withheld either if the data subject agrees, or if the supply of information would involve disproportionate effort. Some types of personal data may also be exempt from the right of subject access, and further details of what that might include can be found in the ICO's subject access code of practice.
The Act also states that you do not have to comply with a subject access request if doing so would mean that you would provide information about another individual who could be identified from that information, except where:

- The other individual has given consent for the disclosure to be made, or
- It is reasonable in all the circumstances to comply with the request without that individual's consent.

As mentioned above, a data subject has the right to opt out of direct marketing, and this can be particularly relevant in relation to charity fundraising. A named individual who receives, for example, a flyer inviting a donation can request that the data controller no longer uses their personal data for this purpose. A general flyer is that is sent out to unnamed recipients will not come under the remit of processing data, although it is good practice to include a tick box to allow recipients to opt out of receiving further marketing materials from you. Marketing covers telemarketing as well as written material.

Notification

The ICO maintains a public register of data controllers, which individuals can check to see what type of processing of personal information is being done by a specific data controller. Notification is the process by which a data controller's details are added to this register. Notification is mandatory unless a data controller is exempt, although those who are exempt can still make a voluntary notification to the ICO if they wish. It

should be noted that some not-for-profit organisations can be exempt from notification, and you can find out more about this from the ICO's website.

Offences

The following are criminal offences which are punishable by a fine of up to £5,000:

- Failure to notify the ICO (unless exempt, as above)
- Unlawfully obtaining personal data
- Unlawfully selling personal data.

The ICO can also issue fines of up to £500,000 for serious breaches of the Data Protection Act and Privacy and Electronic Communications Regulations. The ICO have had the power to issue such fines since 2010, and a number of charities have been fined significant sums for breaches in recent years, so it is vital for organisations to ensure they are complying with the data protection regulations as required.

Exemptions

The rights of data subjects can be restricted on the following grounds:

- National security
- Crime and taxation
- Health, education and social work
- Regulatory activities
- Journalism, literature and art
- Research, history and statistics
- Legal privilege
- Confidential references given by the data controller
- Further categories introduced by the Secretary of State.

Action points

Organisations should:

- Appoint an individual to oversee compliance with data protection regulations, including registration with the ICO if that is required (i.e. notification)
- Identify employees and volunteers who process data, ensuring they are aware of and complying with the provisions set out under the Act, and those set out in your organisation's data protection policy (see below)
- Review standard contracts of employment to ensure they include provisions regarding consent to data processing issues
- Introduce a formal procedure with regard to references
- Review procedures to ensure that personal data is only collected when necessary, and to ensure that the data kept is up to date, accurate and only kept for as long as is necessary

- Ensure data is kept securely. This may include having lockable filing cabinets, password protected or encrypted computers, files and memory sticks, procedures for staff and volunteers taking personal data off site, and so on
- Introduce a data protection policy which includes provisions on:
    - The processing and transmission of data, particularly to third parties and abroad
    - Dealing with requests for access to information (subject access requests)
    - Dealing with both manual and automated records systems
    - The recognition of sensitive data

- Have a standard data protection notice on documentation (both electronic and paper) that states
    - why personal data is being collected
    - how it might be used by the organisation
    - whether the data may be passed to third parties, and
    - how data subjects can opt out of the organisation storing and processing their personal data.

Further information

Information Commissioner's Office
Tel: 01625 545745 or 0303 123 1113
www.ico.org.uk

Disclaimer

The information provided in this sheet is intended for guidance only. It is not a substitute for professional advice and we cannot accept any responsibility for loss occasioned as a result of any person acting or refraining from acting upon it.

For further information contact

Torfaen Voluntary Alliance
Portland Buildings, Commercial Street, Pontypool, Torfaen, NP4 6JS
Registered Charity: *1097079*

Tel: 01495 742420 info@TVAWales.org.uk
Fax: 01495 742419 www.torfaenvoluntaryalliance.org.uk

Produced by WCVA, County Voluntary Councils and Volunteer Centres.
Last Updated:26/01/2017

Tel: 0800 2888 329
www.wcva.org.uk