

FACTSHEET 26

Data Protection - An Introduction

2001 saw the Data Protection Act come in to force. The Act covers "personal information" about identifiable living individuals.

The Act covers information that is:

- Held on any relevant filing system (this includes paper systems about clients and files on service users)
- Stored on any form of computer or automated filing system
- Any information that is intended to be placed on either of the above systems.

Much of the Act applies to the **Data Controller** - this is the person or people that are identified as being responsible for deciding how personal information is used within an organisation.

The **Data Controller** is usually not a person in isolation, in most circumstances organisations themselves are classed as the **Data Controller**. Individuals within that organisation (paid and unpaid staff) are agents of the **Data Controller**.

The main focus of the Data Protection Act is the **eight Data Protection Principles** covering:

- How information is processed
- Ensuring information accuracy
- Security of information
- Lawfulness of the data collection process
- Rights of the subject of the data

The Act does try to strike a balance between the needs of the **Data Subject** and **Data Controller**. For example advice-giving organisations may hold information about other organisations or individuals for the sole purpose of passing on to clients.

There are a number of key questions that any organisation should ask itself when looking to ensure that Data compliance is in order:

1. Is personal data fair?

The information you hold should be used in the right way, the Act is not there to prevent use of information but to ensure that it is used in _ right way. Does your organisation make use of the information it has or are there any elements of information that are not needed.

2. Do people and organisation know you hold information about them?

If you are holding information on an organisation or individual it is good practice that they are aware of this and agree to this information being held

3. When do we need people's consent?

Often consent is not needed for "standard" information such as contact and organisation details. Consent though should be sort for personal information such as:

- Racial or ethnic origin
- Religious beliefs
- Political beliefs

- Trade Union or Professional Body membership . Sexual orientation
- Criminal Record

There are exceptions to this but the best way to approach this is with common sense and think about what information you as an individual would be happy for an organisation to hold about you.

4. **Is information protected?**

Information should be protected from unauthorised access. Access to information should only be by people with a good reason. Special care needs to be taken when information is being given to individuals outside the Data Controller's organisation.

5. **Are information collection processes up to date?**

The process by which information is collected may have been in place for a significant period of time and information that is collected could be because "that is how it has always been done". The process in which you collect information and the information you collect should be reviewed should be periodically reviewed. Some information you may only need in a small amount of cases and this information may be better collected as and when needed.

6. **How long do you keep information for?**

As the Data Protection Act covers paper and electronic files how long you keep information needs to be thought out very carefully. The question that needs to be answered is whether there will ever be a situation that it really matters that we no longer have this information. If the answer is no then it is possible that the information can be discarded or processed into an anonymous or statistical format. There are a different set of rules that cover accounting information and they should be adhered to.

7. **Are there procedures for people who want to stop information being used for certain purposes?**

Some groups or individuals may wish for their information not to be used in certain ways. In commercial organisations this is often in relation to marketing purposes. Within the voluntary sector there may be organisations and individuals that are willing for their information to be passed on to your organisation clients but are unwilling for the information to be passed on to

the general public, this can be especially relevant when thinking about information you put on a website that anyone can view. It is important that procedures are in place to accommodate this requirement.

8. **What information can be placed online?**

When putting information on your website it must be remembered the information can be accessed by anyone, anywhere in the world. The very least your organisation should be doing if you are publishing a list of contacts is to get prior agreement from those whose information is going to be published that this is acceptable.

It is especially important to consider issues of privacy if photograph's of identifiable individuals are going to be used. This information is considered as an overseas transfer and should be treated as such.

A final area that should be considered is the Criminal Records Bureau - using this organisation is the way in which all criminal record checks should be carried out - for more information please visit - www.crb.gov.uk

For further information on the Data Protection Act please visit: www.dataprotection.gov.uk

"Data Protection for the Voluntary Sector" is available from the Directory of Social Change (www.dsc.org.uk) for £14.95 (ISBN1 903991 196)

DATA PROTECTION - KEY ACTION POINTS

- As far as possible get consent for the information you hold, it is suggested that if you hold sensitive information then written consent is the best way to protect your organisation.
- Make sure that everyone you hold information about knows it and what you use the information for. Also if this information is going to be passed on to a third party make sure people are aware of that. A statement on publications such as leaflets and any forms that you require to be completed can cover this.
- Give people or organisations that option to opt out of any direct marketing and modify systems to reflect this.
- Make adequate security arrangements for both paper and computer records. This will include making sure paper filing is kept in a secure office. Electronic records should be


in a secure location and require some form of password verification to access.

- Implement an organisation policy (linked to organisations Confidentiality Policy) that outlines what staff (paid and unpaid) are able to do with people's information. Importantly this should also highlight what they are not able to do and where to get guidance if they are not sure.

These Action Points are meant as a guide to help your organisation think about the requirements of the Data Protection Act - for more information visit the Data Protection website - www.dataprotection.gov.uk

FURTHER HELP

Core Services
Dudley Council for Voluntary Service
7 Albion Street
Brierley Hill
West Midlands
DY5 3EE

 01384 78166

www.dudleycvs.org.uk