My Data - Your Business?
Complying with The Data Protection Acts

Facilitators guide
Data protection concerns the safeguarding of an individual’s privacy rights in relation to their personal information. In general terms, data protection legislation provides a framework for the management and protection of personal information. It has two functions:

- it places obligations on those who hold information about people, and
- it confers rights on an individual in relation to how their personal information is processed.

The purpose of this training video is to increase understanding and awareness of the Data Protection Acts 1988 and 2003, and promote good practice in an organisation when dealing with personal information.

The drama centres around a management meeting at a fictitious finance company. The various scenarios show, in a practical way, how things can go wrong if people don’t know about data protection, and how you can benefit from good information handling practices.

The video is intended for use as part of a staff training and awareness programme which will assist organisations in meeting their compliance requirements. Facilitators should make the viewers aware that not only are they in control of other people’s personal data, but that they too are the providers of personal information in their private lives. The individual needs to put himself/herself in the place of the data subject and ask ‘How would I feel if this were my data?’

In the video, a range of scenarios is presented, exploring each of the eight rules, and the intention is to encourage staff to think about how data protection applies to their own area of work.

To get the best out of the video, ideally, you should set aside at least an hour to view it and facilitate discussion on best practice in your organisation. It can also be used as a stand alone educational tool.
Trainers using the video in a training setting should, having first watched the video:

- Be familiar with the eight rules of data protection. More detailed information and guidance is available in the information booklet 'A Guide for Data Controllers' and on our website, [www.dataprotection.ie](http://www.dataprotection.ie).

- Present information specific to your organisation during the training session. This would include discussing the organisation’s privacy policy and information management procedures.

- Provide relevant supporting materials to participants


Feedback

Feedback on the usefulness of this video and suggestions for further training material or support are welcome. Please email us at info@dataprotection.ie or use the feedback form on our website,[www.dataprotection.ie](http://www.dataprotection.ie).

The material included in this training video and booklet is designed to give general guidance only. It is not a definitive interpretation of the law and should not be relied on for the purpose of legal advice.

Setting the scene

Discreet Industries is a finance company and they are holding their fortnightly management meeting. Those present are:

- **Cormac** General Manager
- **Fiona** Financial Controller
- **Derek** Head of Sales
- **Helen** HR Manager
- **Joanne** IT Manager

At the last meeting Cormac asked Joanne, a recent recruit to the company, to prepare a report on data protection compliance within the company. In her presentation she goes through the data protection rules and applies them to problems which she has uncovered.

The following are brief synopses of the various scenes as they illustrate the relevant data protection rule, along with suggested discussion points for your group.
<table>
<thead>
<tr>
<th>1. Obtain and process information fairly</th>
<th>2. Keep information only for one or more specified, explicit and lawful purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the first scenario, Joanne discovers that Derek has taken a copy of a customer contact database from his previous employment to his current job, without the permission of the individuals on that database.</td>
<td>Helen is seen discussing some images from the premises security CCTV footage with Frank, the security guard. She is considering doing random checks of CCTV footage against flexi-time records on a regular basis.</td>
</tr>
</tbody>
</table>

**Relate this to your own organisation**

1. What types of personal information do you hold?
2. How did you collect that information – was it directly from the individual or through a third party?
3. Are people made aware of how their information will be used and was their consent obtained, including consent for any secondary purposes such as marketing?
4. Do you have a good electronic and manual records management system?
5. Is there someone in your organisation who is responsible for data protection compliance?

**Relate this to your own organisation**

1. Your organisation may collect several categories of personal information, depending on functions. What is the primary purpose for collecting each category?
2. Are the relevant people in your organisation aware of the use made of personal information for which they are responsible?
3. Are you aware that an individual has a right to be informed of and maybe object to the purpose for which you hold his/her data and that you must be able to identify that purpose?
3. Use and disclose information only in ways compatible with these purposes

Fiona meets with an irate individual who has called to the office to complain. The complainant had earlier sent her CV to Discreet Industries. Before they had considered making her a job offer and without her consent, Fiona contacted her current employer for a reference. Her employer didn’t know she was looking for a new job and the complainant’s relationship with her employer has been damaged. She is going to make a complaint to the Data Protection Commissioner.

4. Keep information you have about people safe and secure

During the discussion on the use of CCTV footage, it emerges that Derek has computer access to the employee personnel records, which he does not need.

Security measures relating to the disposal of manual records also come into question following the discovery of staff pay records in a builder’s skip outside the office.

Relate this to your own organisation

1. The key word in relation to security measures is ‘appropriate’. Have you examined what personal information you hold and what level of security should be applied to it?
2. Is access to information restricted to authorised staff on a need to know basis?
3. Are your servers protected from unauthorised access?
4. Are appropriate security measures applied to desktop PC’s?
5. Do you have back-up procedures in place?
6. What measures do you have in place for securely disposing of waste paper, printouts, etc.?
7. Are your premises secure when unoccupied?
8. How often do you review your security measures and do you have a written policy in place?
5. Ensure that the information is adequate, relevant and not excessive. *(This is shown as Rule 6 in the Guide for Data Controllers)*

On examining the types of information held on personnel files, Joanne notices that they record the religious beliefs of staff without any apparent reason. According to Cormac, it is a throw back to the early days of the company.

**Relate this to your own organisation**

1. Is all the information you keep relevant and necessary for your purposes?
2. Have you specific criteria to judge what is adequate, relevant and not excessive – ask yourself, ‘do I really need to keep all this personal information’?

6. Keep information accurate, complete and up to date. *(This is shown as Rule 5 in the Guide for Data Controllers)*

A customer, Mr Mullins, was refused credit when making a purchase from one of the Company agents, because his record showed that he had defaulted on a previous finance agreement. Joanne subsequently discovered that Mr Mullins’ record was incomplete; the goods purchased had been returned because they were faulty.

**Relate this to your own organisation**

1. Are your clerical and computer procedures adequate to ensure high levels of data accuracy?
2. Do you have appropriate procedures in place to ensure that information is kept up to date?
3. What are the advantages of people being able to ask for a correction or to include their version of the facts into your record?
4. Do you need to carry out periodic reviews and audits of information held, to assist in complying with your obligations?
5. When staff become aware of inaccuracies, what should they do?
On examining Mr Mullins’ file Joanne noticed that his bank account details are still held on file. Further checking revealed that the company retains customer bank details indefinitely even where there is no purpose for holding them. Helen then relates that she has had issues in the past with her credit card details being retained indefinitely when booking tickets for shows.

Following the conversation about inaccurate information held on Mr Mullins’ file, Cormac asks what an ‘access request’ is. Joanne explains that Mr Mullins is entitled, on request, to get a copy of any information they hold on him.

Relate this to your own organisation

1. Do you have procedures in place for dealing with an access request and is there somebody responsible for this?
2. What are the legal requirements on your organisation in complying with an access request? (eg. reply within 40 days, can charge a setup fee.)
3. In what circumstances can you refuse to release information on an access request? (In very limited cases such as where information is legally privileged; also note special procedures for release of medical or social work data.)
4. Would you be happy with what a person might see if they accessed their own file?
5. Will this affect the way you process information?
Summary of discussion points:

1. What are the main issues in our organisation?

2. Which rules are particularly relevant to us?

3. What questions do we need to ask?

4. Do we need to consult the Data Protection Commissioner’s Office?

5. What do we need to do differently to make sure we comply?

6. Who will be responsible for data protection compliance in our organisation?