Department of Justice and Equality

Data Protection Policy

Contents

Foreword

The objective of this policy is to support our obligation to comply with Data Protection Legislation. There are related legal obligations arising from Freedom of Information, National Archives and Official Secrets legislation.

A data breach can have serious consequences for the person whose data is breached, for the organisation responsible for the breach and, in some circumstances for individuals who may be responsible for the breach. Breaches can be due to systems failure, individual error or deliberate breaches by internal or external people using a range of techniques.

The Department of Justice and Equality is responsible for having a policy and systems in place to support it and to audit for compliance. Each year the Secretary General makes a Statement of Internal Controls to the Office of the Controller and Auditor General which is subject to the Public Accounts Committee. This policy is one of those controls.

You have personal responsibility to make yourself aware of this policy and if you are handling personal information to ensure that you comply. It is in your interest to ensure that colleagues who are holding data about you also comply.

Data Protection Rules

Below are the eight rules of Data Protection that describe the requirements and responsibilities of the Department under Data Protection

1. **Obtain and process the information fairly**
2. **Keep it only for one or more specified and lawful purposes**
3. **Process it only in ways compatible with the purposes for which it was given**
4. **Keep it safe and secure**
5. **Keep it accurate and up-to-date**
6. **Ensure that it is adequate, relevant and not excessive**
7. **Retain it no longer than is necessary for the specified purpose or purposes**
8. **Give a copy of his/her personal data to that individual, upon request.**

Your responsibility is to ensure that you are familiar with these rules, comply with them.

If you become aware of any issue – potential or actual - you must raise it within your Division and also with the Data Protection Compliance Officer.

It is our overarching aim to prevent data breaches.

1. Introduction

The Department of Justice and Equality is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Acts 1988 and 2003. These Acts give effect to the Council of Europe Data Protection Conventions.

Data Protection is the manner in which the privacy rights of individuals are safeguarded in relation to processing their Personal Data. Personal Data covers **any** information that relates to an identifiable, living individual. The data can be electronic, manual and images and may be held on computers or in manual files. The policy applies to all Data Subjects whose personal data is held by the Department, from staff details to clients and members of the public.

This policy applies to the Department of Justice and Equality and is available to all agencies and executive offices to apply.

The development of this Data Protection Policy took account of best practice in the area using resources available on the website of the Data Protection Commissioner. We also considered Data Protection Policies in other Government Departments in particular those which have been formally approved by the Data Protection Commissioner on their website.

This policy applies to all data held by the Department of Justice and Equality. This includes all electronic and paper records, it also includes all CCTV images in the Department.

2. Key definitions used in the Data Protection legislation

Below are definitions of the key terminology, from the website of the Office of the Data Protection Commissioner

Data means information in a form which can be processed. It includes both automated data and manual data.

Automated data means any information on computer, or information recorded with the intention of putting it on computer. It includes not only structured databases but also emails, office documents or CCTV images.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system – this includes temporary folders.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in or is likely to come into the possession of the data controller.

Processing means performing any operation or set of operations on data, including;

- Obtaining, recording or keeping data
- Collecting organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the information or data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking erasing or destroying the data.

Data Subject is an individual who is the subject of personal data.

Data Controllers are those who either alone or with others control the contents and use of personal data. Data Controllers can either be legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as GPs, Pharmacists or Sole Traders. In our context this means information being submitted to the Department for a specific purpose, for example applications submitted to Irish Naturalisation and Immigration Service.

Data Processor is a person who processes personal data on behalf of a Data Controller, but does not include an employee of the data controller who processes such data in the course of his/her employment. Again individuals such as GPs, Pharmacists or Sole Traders are considered to be legal entities. In our context this means information that is being processed for the Department by Peoplepoint or Financial Shared Services for example when a new staff member joins.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

3. The Eight Rules of Data Protection

Rule 1 - Obtain and Process Information fairly.

The Department of Justice and Equality is committed to collecting information fairly and ensuring that it is processed fairly. We are committed to only collecting personal data necessary to allow us to carry out our functions as set out in legislation. To comply with this rule, all forms whether electronic or paper requesting information from a member of the public should only request information for which there is a specific business need and legislative basis.

Rule 2 - Keep it only for one or more specified, explicit and lawful purposes.

The Department will only keep data for purposes that are specific, lawful and clearly stated and data will only be processed in a manner compatible with that purpose.

In order to comply fully with the rule, the Department must let the person know the reason why we are collecting and retaining their data. The purpose for which data is being collected must be a lawful one. The Department will retain a list of its Data holdings and it will also be recorded in their registration on the Data Protection Commissioners website. If the Data collected is to be used for statistical purposes, this should also be stated on any forms.

Rule 3 - Use and disclose it only in ways compatible with these purposes.

The Department will ensure that personal information collected for a particular purpose will not be used for any other purpose. We must also ensure that personal data is not divulged to any third party, except in ways that are specifically allowed within the stated purpose. To comply with this rule we must ensure that data is only transferred to another department or body on the basis of a statutory requirement where there is a legal basis for this sharing. When data sharing is being considered the following principles should also be considered Demonstrable Justification, Explicit Legal Basis, Authorisation, Transparency,

Data Minimisation, Access and Security and Retention[1]

Where Data is being transferred abroad it must always be done in accordance with specified international agreements. Specific guidance will be issued as the "Safe Harbour" and related cases come to finality.

If you require guidance on this please contact Gillian McGuire, the Data Protection Compliance Officer - dataprotectioncompliance@justice.ie

Rule 4 - Keep it safe and secure.

The Department will maintain the highest standards of technical and physical security to ensure that we protect the confidential personal data while we hold and process it. This responsibility is discharged in structural terms by IT Division but primarily by the actions of staff members. This will be done by ensuring;

- Access to the information is given to staff at the appropriate authorised level and this is done in accordance with an outlined ICT policy
- All computer systems are password- protected, you must never disclose your password to any individual including other employees in the Department
- All portable devices used to transport data are encrypted
- Where sensitive personal data is being sent via email please take measures to ensure it is sent securely – such as a password protected attachment – consult the Acceptable Usage Policy or discuss the options with ICT Division
- All premises will be kept secure in particular when they are unoccupied
- Regular awareness sessions are arranged for staff to ensure that they are aware of their responsibilities under the Data Protection Acts

[1] https://dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/Data_Sharing_in_the_Public_Sector.htm

- Individual staff members have a key role in keeping data safe and secure through this policy in conjunction with the Acceptable Usage Policy. It is currently being redrafted to ensure that it supports this policy and will be available on Justinfo.

Rule 5 - Keep it accurate, complete and up to date.

The Department must ensure that all personal data is kept fully up to date and accurate.

If you hold personal data you must ensure that all clerical and computer procedures are adequate to ensure the highest levels of data accuracy. It is the right of every individual to have any inaccurate data held by the Department updated or erased as appropriate.

Procedures/Systems in Divisions will be reviewed by the Data Protection Compliance Officer or by Internal Audit. A catalogue of systems is under development which will, among other reasons, identify holding of personal information.

Rule 6 - Ensure that it is adequate, relevant and not excessive.

In order to comply with this rule the Department will put measures in place to ensure that the data held and sought by us is the minimum amount required for the specified purpose. The data held must be adequate, relevant and not excessive in relation to the purpose for which it is sought. All requests for data must clearly state the Department's business need for the collection of such data.

Rule 7 - Retain it no longer than is necessary.

Data must not be retained for longer than necessary and must not be retained once the initial purpose has ceased. As long as personal data is retained by the Department the full obligations under the Data Protection Acts are attached to it. The Department should be clear in regard to the length of time data is kept for and why it is being retained.

In this regard, the Department has limited control in terms of record disposal as we are also subject to the National Archives Act, 1986 and Freedom of Information Act, 2014. Our Department, together with others, is proposing to adopt a standard Data Classification system to categorise data to support decisions on how specific records must be created, held and eventually disposed of.

A formal Data Retention Policy for the Department will be put in place which will involve consultation with Divisions across the Department. Pending the development of this policy all Personal data should be treated as Confidential subject to these eight rules.

Rule 8 - Give a copy of his/her personal data to that individual, on request.

Under the Data Protection Act, the Department has a responsibility on receipt of a written request to provide an individual with the following:

- A copy of the data being kept about him/her
- A description of the purpose for which it may be held
- A description of those third parties to whom the Data may be disclosed
- The source of the Data unless this would be contrary to public interest.

Please note that a Data Protection Request does not need to refer to the Data Protection Acts in order to be a valid request.

4. Roles and Responsibilities

The table below sets out the roles and responsibilities.

All employees	You have a personal responsibility to ensure compliance with the principles of the Data Protection Acts and to adhere to the Department's Data Protection Policy.
Line Managers	Managers are responsible for ensuring compliance with the Department's Data Protection Policy within their unit. They are also responsible for ensuring that staff in their area are aware of the policy and have received Data Protection Awareness Training as part of their Performance Management and Development System.
Data Protection Compliance Officer	The development and implementation of the Data Protection Policy.
Internal Audit	The Internal Audit Unit is responsible for providing reasonable assurance that the accounting systems, procedures and controls operated by the Department are adequate and are being complied with. It is not the primary role of Internal Audit to ensure that Divisions are Data Protection compliant; however, as part of its audit work it may carry out periodic Data Protection Audits in relation to the Department as a whole or to specific Units of the Department.
Human Resources	A Data Protection Module is currently being delivered by HR to new staff as part of their online Induction programme.
Audit Committee	To review and assess how the policy is working and to make recommendations on areas as appropriate.
Secretary General	The Secretary General in his/her role as Accounting Officer has overall responsibility for the Department's data and implementation of the policy in terms of Data Protection.

i. Responsibilities of all staff in the Department

- It is your responsibility, as an employee of the Department of Justice and Equality to ensure that you are fully aware and complying with the contents of this policy on a daily basis.

ii. Responsibilities of the Data Protection Compliance Officer

- Responsible for the development and implementation of, and support arrangements for, the Department's Data Protection Policy.
- Ensuring that the Department's registration with the Office of the Data Protection Commissioners website is current and accurate.
- Deal with any Data Protection queries that arise and available to provide guidance to divisions on how to comply with Data Protection rules and to advise where specific issues arise.
- Responsible for reporting Data Protection Breaches (if any occur) to the Office of the Data Protection Commissioner and advising Internal Audit of same. The view of the Commissioner is that breaches should be reported to the individuals concerned.
- Promoting Data Protection Awareness across the Department.

5. Training and Awareness

Data Protection information sessions will be held for staff across the Department and will be augmented by online material and information notices. If you are involved in handling personal information you must attend one of these sessions in order to familiarise yourself with the policy. In the meantime the Data Protection Commissioners website is an invaluable resource - see www.dataprotection.ie

A group of Data Protection decision-makers will be established in the Department similar to that currently being implemented for Freedom of Information. A new catalogue of systems will clearly identify data holdings with personal information to support our efforts in this area.

It is also our intention to establish a Data Protection Officers network. This will be for all Data Protection Officers working in the Department's offices and agencies and will provide an opportunity to update information and share experiences within our sector and with colleagues in other sectors. This will be progressed in parallel with arrangements being put in place to implement the new Data Protection Regulation and Directive.

6. Audits of Data Protection in the Department

The Internal Audit Unit in the Department carries out periodic reviews of the Department's Data Protection procedures as part of their ongoing review process.

The Office of the Data Protection Commissioners may also carry out audits and inspections on a periodic basis.

7. What to do in the event of a breach

A data protection breach can occur for a number of reasons:

- Failure of protective systems or equipment
- Theft or loss of data/equipment/paper that data is stored on
- Human error
- Department systems being deliberately hacked by staff or outsiders wrongly getting access by technical means or by fraud or misplaced curiosity to personal information
- Fire or flood
- Access levels to systems or buildings not being properly monitored and controlled.

In the event of a data breach you must immediately notify the relevant business unit and the Data Protection Compliance Officer. The Data Protection Compliance Officer will contact the Internal Audit Unit when advised that a breach has occurred.

In all cases, the Office of the Data Protection Commissioner will be contacted and also if necessary the data subjects affected by the breach.

Remedying breaches has significant cost in time, money and reputation. Prevention is always better.

8. Registration with the Office of the Data Protection Commissioner

The Department of Justice and Equality is registered as a Data Controller under the Data Protection Acts 1988 & 2003. This is renewed on a yearly basis by the Department. A list of the data holdings and disclosees for the Department can be found on the Data Commissioners Offices website[2].

If your unit holds data that is not included in this description, you should contact Gillian McGuire at dataprotectioncompliance@justice.ie to have the description amended.

[2] Website address: https://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/display.asp?ID=0725%2FC

9. Office of the Data Protection Commissioner

The Office of the Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the acts and ensuring that the data controllers comply with their obligations. The Office operates independently of the Department and has full rights of audit of the Department.

10. Useful Contacts

Data Protection Compliance Officer
Gillian McGuire
VOIP: 608246
Phone: 01-6028246

If you have any queries, she can provide assistance, advice and awareness training to staff in the Department to ensure that they are aware of the contents of this policy document and in a position to comply with the legislation.

Alternatively email: dataprotectioncompliance@justice.ie

Individuals seeking personal data under the Data Protection Acts should write to:

Information Access Unit
Department of Justice and Equality
51 St. Stephens Green
Dublin 2
D02 HK52

Subject Access Requests can also be emailed foi@justice.ie

You can also log onto the website of the Office of the Data Protection Commissioner for further information and guidance at www.dataprotection.ie

Appendix 1: Requesting Personal Data under the Data Protection Acts

A request for a copy of Personal Data under the Data Protection Acts is called a **Subject Access Request (SAR).**

These apply to all manual and electronic records held at the time the access request was received regardless of when the record was created.

The information must be provided in permanent form unless otherwise agreed by the Data Subject.

Please be aware of these key points when responding to Subject Access Requests under the Data Protection Acts:

- The request must be received in writing however it does not need to state that the request is being made under the Data Protection Acts.
- The Data subject must provide sufficient information to enable the Data Controller to clearly identify them and to locate the relevant data or information.
- The Data subject must also provide proof of identity, such as copy of a drivers licence or passport.
- The Data Controller has 40 days to comply with the request.
- A fee of €6.35 may be charged.

What must be disclosed in an access request?

- Personal Data held
- Outline the purposes for processing data
- The persons to whom the data has been disclosed
- The source of the data – while taking account of any confidentiality safeguards

- The logic involved in any automated decisions

For details on exemptions under the Data Protection Acts [3]

If the Data Subject is enquiring as to whether or not an organisation holds data on them and a description of what is held – they must receive a response within 21 days.

[3] https://www.dataprotection.ie/viewdoc.asp?m=r&fn=/documents/rights/2di.htm

Appendix 2: Subject Access Request Form

Full Name	
Address	
Telephone Number	
Email Address	
Please advise us as to the nature of contacts you have had with the Department. *(letters, reps to Ministers, emails, applications to INIS)*	
Reference Number you have received in your dealings with the Department *(where applicable)*	
Approximate date when this contact took place	
Please outline the details of the information you are seeking	

In order to assist us in ensuring your data is protected you must submit photographic evidence of your identity (Passport/Drivers Licence) with this form.

I declare that the information I have provided in this form is true and accurate to the best of my knowledge.

Signature: _____ **Date:**_____

Please send this form to:
Information Access Unit
Department of Justice and Equality
51 St. Stephens Green
Dublin 2
D02 HK52

Subject Access Requests can also be emailed foi@justice.ie

Appendix 3: Acknowledgement letter to Subject Access Request

SAR ref no:

Dear_____

I wish to acknowledge receipt of your request to access information held by this Department under the Data Protection Acts 1988 & 2003.

Your request has been sent onto the relevant Division within the Department who will deal with your request.

Under the terms of the Data Protection Acts, a reply must issue to you within 40 days of receipt of your request. Therefore the response should be issued to you by dd/mm/yy.

Yours sincerely

_____

Name

Information Access Unit

Appendix 4: Decision Letter for Subject Access Request

SAR ref no:

Dear_____

I refer to your subject access request under the Data Protection Acts 1988 & 2003 for all data relating to_____

I wish to advise you that a decision has been made by XXX XXX, XXX in XXX Division and they have provided the following schedule of records to be released.

Schedule of Records

Date of Record	Description of Record	Granted/Refused	Reason for Refusal

If you are not satisfied with the decision you have the right to appeal in writing by contacting the Office of the Data Protection Commissioners, Canal House, Station Road, Portarlington, Co. Laois R32 AP23.

Yours sincerely,

_____

Name
XXXXX Division

Appendix 5: CCTV

Purpose of the CCTV Systems in the Department

The Department of Justice and Equality has CCTV in its offices at 51 St. Stephen's Green and 94 St. Stephen's Green. CCTV is also installed in INIS Offices in Burgh Quay, Timberlay House and in 6/7 Hanover Street. While CCTV is in place in Reception in Bishops Square and Montague Court it is operated by the building managers and the Department has no access to, or control of recordings. If you have any queries regarding the CCTV you should raise this with the staff on the reception desks in the relevant building and they will advise you who to contact.

Justification for CCTV

The primary purpose of the CCTV cameras in use by the Department of Justice and Equality is for Security and Health and Safety. As an ancillary use, the Department of Justice and Equality may also have regard to CCTV footage where it is reasonably required to assist with establishing facts in an investigation. This could include a security event, a trip and fall or a health and safety concern. In the event that the Department has need to investigate an incident involving a member of staff, either as a result of a complaint being brought by that employee or by another party, CCTV would be used where reasonably necessary to assist in the investigation and resolution of any such issue.

Under the Data Protection Acts 1988 & 2003, the eight rules apply to CCTV images as to all other Data held within the Department of Justice and Equality.

Appropriate signs are in place in Department and INIS Offices advising staff and visitors to the buildings that CCTV is in use for the purposes of security and health and safety.

Employee personal data

There are no CCTV cameras internally on the work floor and the Department of Justice and Equality confirms that CCTV is not used for remote management of employees. Recorded images will be viewed in exceptional circumstances such as when a security breach, employee personal protection or health and safety incident occurs or where recourse to the

CCTV images is necessary in the course of any investigation carried out by the Department to prove or disprove any concerns regarding an employee or employees, any third party or the work place itself.

The Organisation Unit, Corporate Services and INIS Shared Services are responsible for the installation and operation of the CCTV cameras and equipment. All footage is stored securely on the hard drive within each system. The retention period for the images is 28 days, and after this period they are deleted unless the images are required where they identify an issue and are retained for investigative purposes. The CCTV is monitored live by the Service Officers manning the reception desks, however they do not have access to download any of the images. A select number of EOs and COs with Corporate Services/INIS Shared Services have been trained to download images from the systems when required.

Training in regard to accessing the system is given on the job within Corporate Services Organisation and within INIS Shared Services Organisation Unit. Staff are fully aware of what these images can be used for and the sensitive nature of personal data and requests for same.

Requests for CCTV footage from An Garda Síochána must be made in writing. Details of the images released are recorded in the access log.

The same process applies to the CCTV within INIS/ORAC/RAT which is managed by the INIS Shared Services Organisation Unit.

As with all other Subject Access Requests, requests for CCTV footage should be sent in writing to:

Information Access Unit
Department of Justice and Equality
51 St. Stephens Green
Dublin 2
D02 HK52

Subject Access Requests can also be emailed to foi@justice.ie.

Appendix 6: Good Practices to comply with Data Protection Rules (Think if this was your personal data).

- Keep your work area clear of confidential data when not in use.

- Do not walk away from the printer when you have a document printing as this could be picked up by another staff member and it may contain personal data.

- Ensure that you never leave documents/files/notebooks behind in a meeting room or other office following a meeting.

- Always keep paperwork together and on relevant files.

- Ensure that files are registered and are placed in relevant cabinets/filing areas when not in use.

- Follow computer security procedures – Acceptable Usage Policy.

- If you need to send sensitive personal data by email, please use an attachment and password protect it. Please ensure you transmit the password in a separate email or by phone to the recipient. It should also be noted that where a document is password protected there is no guarantee that ICT Division will be in a position to unlock it. If you need further information on other options available contact ICT Division.

- Be sure that you have established the identity of an enquirer prior to disclosing any personal data and make sure that the enquirer has the right to the information (The requester should always submit ID with their request for data).

- Discuss it with your supervisor if you are unsure about giving the information out.

- Keep a record of the disclosure on the relevant file.

- If there are difficulties locating a record/file carry out an exhaustive search* and discuss the issue with the Information Access Unit in regard to Subject Access Requests.

- Ensure mobile devices are never left unattended and that they are secured by a strong password.

*** Exhaustive search – check within your area, checking filing cabinets where the file would normally be kept, other filing cabinets in the area. Email your colleagues asking that everyone check their desks. Check with Registry in case the file has been sent there in error.**

Appendix 7: Self-help checklist on Data Protection Policy

This checklist will help you to assess your compliance with this Data Protection policy[4].

Rule 1: Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? *[Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]*
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal

[4] Data Protection Website - https://www.dataprotection.ie/docs/Self-Assessment-Data-Protection-Checklist/y/22.htm

data? *[Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]*

Rule 4: Security

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 5: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 7: Retention time

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?
- Registration
- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*
- Is a named individual responsible for meeting our registration requirements?

Training and Education

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- Has a data protection co-ordinator and compliance person been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?

Department of Justice and Equality
51 St. Stephen's Green
Dublin 2 D02 HK52
Lo-Call: 1890 221 227

Web: www.justice.ie