Legislative Summary: Data Protection Overview

Making sure it's secure.™

The Data Protection Act (Ireland)

Enacted: 1998; Modified: 2003 – under Office of the Data Protection Commissioner

1 What the law covers:

Eight principles governing the:

- Protection of the processing and use of personal data against unauthorised or unlawful use, disclosure, accidental loss, destruction or damage
- Rules on the processing of personal data including obtaining, recording, storing, organising, updating, adapting, altering, using, disclosing and destroying it

2 What is "personal data":

Information that allows the identification of a living individual – whether direct from that data or from that data in conjunction with other information. Examples are name, date of birth, address and Personal Public Service Numbers.

It includes both manual and automated data.

3 DPA and information management:

The DPA requires that appropriate technical, organisational and security measures be documented and taken to prevent:

- Unauthorised or unlawful processing of personal data
- Accidental loss, destruction or damage to personal data

It is critical to note that even if organisations use third party "data processors" to conduct any part of the processing on their behalf, including destruction, **the organisation remains responsible for the protection of the personal data and not the third party.**

4 Who must adhere to the regulations:

The DPA applies to both "data controllers" and "data processors" that are resident, incorporated or maintain a presence in Ireland.

Data controller: An organisation, individual or legal person who controls and is responsible for the keeping and use of personal information on a computer or in structured manual files.

Data processor: An organisation, individual or legal person who holds and/or processes the personal data on behalf of a third-party data controller. Examples include payroll companies, accountants and market research companies.

5 Offences/penalties for non-compliance

Failure to register with the Data Protection Commissioner's Office, when obligated to do so, is an offence under Section 19(6) of the DPA.

A person who obtains unauthorised access to personal information and then discloses it to another person, also commits an offence under section 22 of the DPA.

The maximum fine on summary conviction for any of the offences under the DPA is €3,000, and for a conviction on indictment is €100,000.

There is no legal obligation for breach notifications but the Personal Data Security Breach Code compels organisations to notify the Data Protection Commissioner's office in the event of a security breach, except in some limited circumstances. They may also need to contact the individuals whose data was breached.

For more information:

Data Protection Commissioner – dataprotection.ie

Data Protection Act 1988/2003 – irishstatutebook.ie

Companies Act 1990 – irishstatutebook.ie

6 How to comply:

All data controllers must comply with certain important rules about how they collect and use personal information. Some data controllers must also register annually with the Data Protection Commissioner, in order to make transparent their data handling practices.

Organisations need to periodically review their internal information management systems to ensure that the personal data in their possession is:

- Only collected, kept, used and disclosed for explicit and legitimate purposes
- Adequate, relevant and not excessive
- Subject to the appropriate security measures
- Securely destroyed as soon as no longer needed
- Accessible to the subject of the information, if they request to see it

Recommended security management and information controls:

- Use passwords to control and restrict access
- Train staff on data protection principles and their responsibilities
- Create audit trails and incident response plans to deal with a data security breach
- Ensure facilities are secure
- Properly dispose of printed material

When using third party "data processors":

- Establish a written contract outlining what can be done with the personal data and how it will be protected
- Ensure the level of protection is sufficient to meet your organisation's compliance with the DPA
- Take reasonable steps to monitor that the security measures are put into practice

7 Secure document retention and disposal requirements:

The DPA requires data controllers to securely destroy personal data as soon as the legitimate purpose for its processing no longer exists. However, the requirement must take into account other legislations that govern the rules for document retention prior to its secure disposal, and the penalties for non-compliance.

Examples of areas where regulatory document retention periods are in place:

- Employment records
- Health and safety records
- VAT records
- Corporate tax records
- Transaction records and formal company documents (Companies Act 1990)

Organisations subject to pending litigation will need to disclose documents to the other side but measures can be taken to protect personal information. Litigants must not destroy documents with intent of avoiding disclosure.

Recommended inclusions for a document retention policy:

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of "document" and the format and length of time in which it is to be retained (electronic or hard copy)
- ☐ Guidance on creation of documents
- ☐ Members of staff designated to deal with the document management system
- ☐ Methods of document destruction, including those carried out by third parties
- ☐ How to keep an accurate record of documents destroyed

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a free Data Security Survey at your organisation
- Helpful resources available at shredit.ie/resource-centre

For peace of mind, contact Shred-it today

1800 747 333 (ROI)
0800 028 1164 (NI)
shredit.ie

Making sure it's secure.™