



Irish Youth Justice Service

Seirbhís na hÉireann um Cheartas i leith an Aosa Óig

Information leaflet¹

Obtaining, Using and Sharing Personal Data in the Youth Justice Sector

January 2011

¹ This leaflet is for general guidance only and does not purport to be a legal interpretation of the Data Protection Acts

Table of Contents

| | Page |
|--|-------------|
| 1. Introduction | 3 |
| 2. Personal Data | |
| 2.1 What is personal data? | 3 |
| 2.1 What is meant by sensitive personal data? | 3 |
| 3. Obtaining Data | |
| 3.1 What must be done when obtaining personal data? | 4 |
| 3.2 What must take place where disclosure to other organisations is envisaged? | 4 |
| 4. Using Data | |
| 4.1 What must be done to ensure fair use of data? | 4 |
| 4.2 Why must the purpose (or purposes) for which personal data is to be used be specified? | 5 |
| 4.3 Once personal data has been obtained for a specified purpose can it be used for other purposes? | 5 |
| 5. Disclosure to Others | |
| 5.1 Is disclosure of personal data to other organisations permitted? | 5 |
| 5.2 Under what circumstances can personal data be disclosed to another organisation without the consent of the individual? | 6 |
| 5.3 What is the distinction between 'best interests' and 'vital interests'? | 6 |
| 6. Further information | |
| 6.1 Where can more detailed information in relation to data protection in the youth justice sector be obtained? | 6 |
| 7. Summary chart of responsibilities | 7 |

1. Introduction

This leaflet provides brief general information in relation to personal data, sensitive personal data, obtaining data, using data and disclosing data.

There is also a summary chart at the end of the leaflet setting out the main responsibilities of organisations in relation to personal data.

For more comprehensive information, please refer to the Data Protection Guide for the Youth Justice Sector.

2. Personal Data

2.1 What is personal data?

Personal data covers any information that relates to an identifiable, living individual. However, it needs to be borne in mind that data may become personal from information that could come into the possession of an organisation. There are different ways in which an individual can be considered 'identifiable'. A person's full name is an obvious identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms, occupation, address etc. Often a case by case assessment must be made taking account of some of the above considerations as to whether data could be deemed to be personal.

'Personal data' is technology neutral. It does not matter how the personal data is stored - on paper, on an IT system, on a CCTV system, etc.

2.2 What is meant by sensitive personal data?

Sensitive personal data covers any personal data relating to a person's racial or ethnic origin, political opinion or religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence and trade union membership.

Additional conditions are required to be met when using such data. Usually this will be the clear consent of the person about whom the data relates.

3. Obtaining data

3.1 What must be done by an employee of an organisation when obtaining personal data?

The employee must:

- be open and honest about their identity;
- have genuine reasons for collecting and using the personal data, i.e. identify the purpose;
- explain how they intend to use any personal data they collect including disclosures to other organisations;
- collect only personal data necessary for the purpose.

3.2 What must take place where a disclosure to other organisations is envisaged?

Individuals should be able to choose whether or not their personal data is disclosed to others. If the personal data is going to be disclosed, the individual must be informed that their data will be disclosed and given the opportunity to consent to such disclosures.

There are some limited situations where data can be provided to other organisations without the individual's consent (see 5.2 below).

4. Using Data

4.1 What must be done to ensure fair use of data?

Fairness requires the collection and use of personal data to be open, transparent and up-front. The first step is to ensure that the individual is not deceived or misled when the information is obtained. Secondly, the individual's personal data should not be used in ways that they would not reasonably expect.

4.2 Why must the purpose (or purposes) for which personal data is to be used be specified?

The purpose or purposes for holding personal data must be clear to ensure that the data is used in a way that is compatible with that purpose. Specifying the purpose at the outset will help in deciding what information to give individuals to ensure fair use of the data.

Personal data cannot be held unless it is for a specific, lawful and clearly stated purpose.

4.3 Once personal data has been obtained for a specified purpose, can it be used for other purposes?

There is a limitation on the use in that the personal data must not be used for any purpose that is incompatible with the original purpose or purposes.

5. Disclosure to Others

5.1 Is disclosure of personal data to other organisations permitted?

It is important to remember personal data may not be disclosed except in ways that are compatible with the specified purpose for which the data was obtained. In making a disclosure, it should be considered whether the individual would be surprised to learn that a particular disclosure is taking place.

Generally, it is not permitted to make a disclosure to another organisation unless the individual has been informed of the disclosure and has consented. However, there are a number of exceptions that allow disclosure in certain limited circumstances (see 5.2).

A decision to share personal data with another organisation does not take away the duty to treat individuals fairly.

5.2 Under what circumstances can personal data be disclosed to another organisation without the consent of the individual?

These exceptions are where the disclosure is required:

- for the purpose of safeguarding the security of the State;
- for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board;
- in the interests of protecting the international relations of the State,
- urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
- by or under any enactment or by a rule of law or order of a court;
- for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness.

5.3 What is the distinction between the sharing of personal information in the 'best interests' and 'vital interests'?

There is a difference between the sharing of information to protect a child (in their vital interests) and the sharing of personal information without consent where an organisation deems it to be in their 'best interests'.

It is important to note that sharing in someone's 'best interests' where their consent has not been given would need a specific legal basis which, does not currently exist.

6. Additional information

6.1 Where can more detailed information in relation to data protection in the youth justice sector be obtained?

A Guide to Data Protection for the youth justice sector which deals with issues in greater detail is available on the Irish Youth Justice website at www.iyjs.ie.

7. Summary chart of responsibilities

