COURTS SERVICE
*An tSeirbhís Chúirteanna*

# Courts Service

# **Data Protection** General Policy

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

COURTS SERVICE
*An tSeirbhís Chúirteanna*

# **Data Protection** General Policy

# Table of Contents

Introduction . . . . . 2

Data Protection . . . . . 2

Purpose of this Policy . . . . . 2

Definitions . . . . . 2

Obligations of the Courts Service . . . . . 4

Right of Access - Accessing Personal Information . . . . . 6

Exceptions to the Right of Access . . . . . 6

What if the Courts Service refuses to respond to an access request? . . . . . 7

Description of data held by the Courts Service which contains personal data registered on the Data Protection Commissioner's website – www.dataprotection.ie . . . . . 8

Security Measures . . . . . 10

Data Compliance Officer . . . . . 10

Good Practices . . . . . 12

Appendix . . . . . 14

## Introduction

The Courts Service has overall responsibility for ensuring compliance with data protection legislation where it is the controller of personal data.

## Data Protection

Data protection is about a person's fundamental right to privacy. A person has a right to access and correct data about themselves. Those who keep data about individuals must comply with data protection rules. This policy gives information on the organisations responsibilities in relation to data protection.

## Purpose of this Policy

This policy is a statement of the Courts Service's (as a Data Controller) commitment to protect the rights of individuals in accordance with the data protection legislation.

## Definitions

**Data** means information 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.
>
> **Manual data** means any information that is kept as part of a relevant filing system. Data received and not yet filed also comes under the provisions of data protection legislation.

**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 the data;
- collecting, organising, storing, altering or adapting the data;
- retrieving, consulting or using the data;
- disclosing the data or information 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 Controller** is a person who, either alone or with others, controls the contents and use of personal data. For the purposes of this policy the Courts Service is the Data Controller.

All employees of the Courts Service who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation. To ensure compliance with data protection legislation arrangements will be put in place for regular audits to be carried out by the Internal Audit Unit. The Courts Service will provide support, assistance, advice and training to all offices and staff to ensure it is in a position to comply with the legislation.

**Data Compliance Officer** is a person appointed by the Data Controller (Courts Service) to oversee the implementation of the data protection legislation in respect of the Service.

**Data Processor** is a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment e.g. Shared Services Centre in Killarney.

**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.

# Obligations of the Courts Service

The policy of the Courts Service in relation to the implementation of the Data Protection Acts 1988 and 2003 is to implement the key responsibilities contained in the data protection legislation.

These responsibilities are:

1. Obtain and process information fairly.
   The Courts Service will obtain and process personal data fairly in accordance with the fulfilment of its functions and its legal obligations.

2. Keep information only for one or more specified, explicit and lawful purposes.
   The Courts Service will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

3. Use and disclose information only in ways compatible with these purposes.
   The Courts Service will only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

4. Keep information safe and secure.
   The Courts Service will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The Courts Service acknowledges that high standards of security are essential for processing all personal information.

5. Keep information accurate, complete and up-to-date.
   The Courts Service will endeavour to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up-to-date.

6. Ensure that information is adequate, relevant and not excessive.
   Personal data held by the Courts Service will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

7. Retain information for no longer than is necessary.
   The Courts Service will have a defined policy on retention periods for personal data and appropriate procedures in place to implement such a policy.

8. Give a copy of personal data to an individual, on request.
   The Courts Service will have procedures in place to ensure that data subjects can exercise their rights under the data protection legislation.

**These responsibilities are binding on all officers dealing with personal data. Any failure to observe them is a breach of the Act.**

## Right of Access – Accessing Personal Information

Under section 4 of the Data Protection Act, 1988 and amended by section 5 in the 2003 Act, an individual or group has a right to:

1. Determine whether the Courts Service holds any personal information relating to them.

2. Be supplied with a copy of this data, clearly explained, of any information relating to them kept on computer or in a structured manual filing system.

3. Have this data amended or erased if it is incorrect.

4. Complain to the Data Protection Commissioner.

All applications must be in writing and include any additional details that may be necessary to enable the Courts Service to locate the data/record e.g. case number, reference number etc. A fee is payable but it cannot exceed €6.35.

Once a request has been made and the appropriate fee paid, the information must be given within 40 days.

## Exceptions to the Right of Access

Section 5 of the Data Protection Act 1988 sets out a small number of circumstances in which individual rights to see personal records can be limited. This is necessary in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand. For example, a criminal suspect does not have a right to see the information held about him by An Garda Síochána, where that would impede a criminal investigation; and a person does not have a right to see communications between a lawyer and his or her client, where that communication is subject to legal privilege in court.

## What if the Courts Service refuses to respond to an access request?

If the Courts Service does not comply with an access request made, it is open to a person to make a complaint to the Data Protection Commissioner. The Commissioner will investigate the matter to ensure that the rights of the individual are fully upheld. The Commissioner has wide powers to investigate complaints made to him/her and will take appropriate action against any persons or organisations who are not complying with the provisions of the Acts.

# Description of data held by the Courts Service which contains personal data registered on the Data Protection Commissioner's website – www.dataprotection.ie

| | |
|---|---|
| **Description of data held by the Courts Service :** | Supreme & High Court Operations<br>• High Court case tracking;<br>• Basic case information;<br>• Records of probate applications;<br>• Higher Court judgements;<br>• Court Lists;<br>• Wards and Committee accounts in the Office of the General Solicitor for Minors and Wards of Court;<br>• Enduring powers of Attorney Register in the Wards of Court Office;<br>• Database of all solicitors' firms in Ireland in relation to personal injuries cases for the purposes of complying with section 30 of the Civil Liability & Courts Act 2004. |
| | Corporate Services Directorate<br>• Applications for judicial appointments;<br>• Personal information in relation to advertisements, tenders and published material most particularly Courts Service News. |
| | Circuit & District Court Operations<br>• Circuit Court case tracking;<br>• Basic case information;<br>• Criminal and legal aid applications;<br>• Court Lists;<br>• Family Law summons applications and Orders;<br>• Jury summonses and Jury Lists; Court Orders;<br>• District Court - charge sheets, summonses, registers, accounts, appeal papers, copy orders, disqualifications, any endorsements (under Road Traffic Acts), notices, family law accounts. |

| | |
|---|---|
| | Finance Directorate<br>• Court Office Accounts;<br>• Accounting System financial transactions resulting from court orders and rules of court;<br>• Court fee payments;<br>• Fines Collections tracking system. |
| | Human Resources Directorate<br>• HRMS System;<br>• Personnel records for staff employed by the Courts and the judiciary or paid from the Courts Vote. |
| | *Any or all of the above mentioned offices may hold data relating to tender and/or advertisement documents.* |
| **Purpose for which the data is held:** | • Administration of the Courts Service. |
| **Parties to whom data may be disclosed:** | • Persons to whom data refers;<br>• Interested parties in accordance with the District Court Rules 1997 (as amended and extended), rules of the Circuit Court 1950 (as amended and extended), Superior Court Rules 1986 (as amended and extended);<br>• Minister for Justice and other officers designated by him/her;<br>• Garda Siochána; other government departments;<br>• Computer maintenance personnel;<br>• Revenue Commissioners. |
| **Sensitive data (categories held, if any):**<br>Racial origin; Political opinions; Religious beliefs; Other beliefs; Physical or mental health; Sexual life; Criminal convictions. | • Health and sick leave records;<br>• Certain court records held in the Courts may contain sensitive data. |

## Security Measures

The Courts Service is committed to implementing the following security measures:

Physical Safeguards

- Human Resource records - Access confined to HR staff only, records under lock and key.
- Premises are alarmed and secured when not occupied.

Technical Safeguards

- All PC's are password protected - Access to system terminals requires system password.
- Anti-virus software installed.

Staff Awareness

- All staff are made aware of the obligations of the Courts Service under the Data Protection Acts.
- The Data Protection Compliance Officer is available to give support and guidance to Courts Service staff on data protection matters.

## Data Compliance Officer

The Data Protection Compliance Officer must:

- ➔ Register Courts Service data annually on the Data Protection Commissioner's website;
- ➔ Collate and respond to requests for information from individual members of the public and groups;
- ➔ Provide support and guidance to Courts Service staff on any data protection matters.

All Staff must be aware of their obligations under data protection legislation and must:

- Forward any Data Protection requests to the Data Protection Compliance Officer immediately;
- Be vigilant when recording comments about individuals and/or groups;
- Maintain information accurately;
- Observe computer security procedures;
- Contact the Data Protection Compliance Officer before forwarding any personal data to persons outside of the Courts Service;
- Ensure any outsource companies, consultants and/or contractors have signed a Confidentiality Agreement prior to issuing any Courts Service data.

## Good Practices

The Courts Service is committed to developing best practice in respect of the personal data it collects and/or controls. In carrying out good practices the Courts Service will:

- Implement the key responsibilities contained in the data protection legislation;
- Safeguard the privacy rights of individuals;
- Protect the personal data that it collects, processes and retains;
- Release personal data under the Data Protection Acts only when permitted by law;
- Manage, co-ordinate and develop, in an effective manner, the implementation of Data Protection legislation in the Courts Service. This includes the management of responses to access requests, the restriction of access where required, and the on-going communication between the Data Protection Unit and offices to ensure that particular practices, proposals and developments are fully compliant with Data Protection legislation;
- Liaise and co-operate with and support the Data Protection Commissioner's Office on issues affecting Data Protection in the Courts Service;
- Liaise with other Government Departments/Offices on Data Protection matters of mutual interest;
- Ensure that the Courts Service staff are aware of their responsibilities under the Data Protection Acts;
- Liaise with the Data Protection Commissioner's Office for guidance on specific cases;
- Be vigilant when recording comments about individuals and/or groups;

- Make sure that any data displayed on PC screens, papers and computer print-outs is not legible to the public unless they are entitled to see relevant details;

- Ensure all outsource companies, consultants and/or contractors have signed a confidentiality agreement to comply with the Courts Service's obligations in relation to Data Protection legislation. (See example in Appendix).

* **This Policy will be reviewed regularly in light of any legislative or other relevant regulations.**

# Appendix

## Data Protection

The successful tenderer shall be prohibited from transferring or assigning, directly or indirectly, to any person or persons, corporation or other legal entity, any part of the whole of the contract without the prior written approval of the Courts Service. At the time of applying for prior written approval the successful tenderer will submit a copy of the proposed contract/agreement that it intends to enter into by way of the transfer or assignment of its obligations. The proposed contract/agreement will contain a similar restriction to that outlined above so as to prevent a transfer or an assignment of the obligation so assigned to another party other than that approved by the Courts Service. Successful tenderers will be required to comply and ensure that all sub-contractors comply with the general conditions of contract and in particular the terms relating to compliance with relevant legislation in relation to the Organisation of Working Time, the Health and Safety and the Data Protection legislation.

The service provider shall comply with, and ensure that all the service provider's personnel and any sub-contractors are aware of and comply with the Data Protection Acts 1988-2003 as amended.

Produced by the Courts Service
Information Office
Phoenix House
15 / 24 Phoenix Street North
Smithfield
Dublin 7