An Roinn Leanaí
agus Gnóthaí Óige
Department of Children
and Youth Affairs

Department of Children and Youth Affairs

Data Protection Policy

The purpose of this policy is to provide a clear statement of the Department's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts. We place a high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom we deal or interact with

June 2019

Document Ownership and Approval

	Name	Grade	Date
Prepared by	Áine Brady	Higher Executive Officer, Data Protection Unit	June 2019
Reviewed by	Gerard Hughes Alan Savage	Principal Officer DPO	June 2019
Approved by	Management Board		June 2019

Date of Issue	Next Review Date
26 June 2019	25 June 2020

Document Change Log Table

Rev. No.	Page No.	Description of Amendment	Approved by	Effective Date

Table of Contents

Data Protection Policy

1. Introduction

1.1. Data Protection is the means by which the privacy rights of individuals (known as "data subjects") are safeguarded in relation to the processing of their personal data. The Department of Children and Youth Affairs ("the Department") is committed to protecting the rights and freedoms of data subjects, and safely and securely processing their data in accordance with legal obligations, including compliance with the General Data Protection Regulation (GDPR).

1.2. We process the personal data of employees, clients, suppliers, and other individuals for a variety of business purposes. This may include the processing of special categories of personal data (also known as "sensitive personal data"). We place a high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom we deal or interact with.

1.3. This policy is a statement of our commitment to protect the rights and privacy of those individuals in accordance with the GDPR and Data Protection Acts. It sets out how we seek to protect personal data and ensure that our employees, joint controllers and third-party data processors understand the rules governing their use of the personal data to which they have access during the course of their work on our behalf.

2. Scope

2.1. This policy applies to all personal data created or received in the course of our business, regardless of format or age, and applies to all locations where personal data is held by us. Personal data may be held or transmitted in paper or other physical and electronic formats.

2.2. All personal and special category data will be equally referred to as personal data in this policy, unless specifically stated otherwise.

2.3. This policy applies to:

- Any person who is employed or engaged by the Department and who processes personal data in the course of their employment or engagement;

- Individuals who are not directly employed or engaged by us but who are employed or engaged by contractors (or subcontractors) and who process personal data in the course of their duties for us.

2.4. The Department may at any time amend this policy.

3. What is Personal Data?

3.1. Personal data is any information that can identify an individual person. This includes a name, an ID number, location data (for example, location data collected by a mobile phone) or a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

3.2. Stronger safeguards and requirements are required for **'special categories of personal data',** which can only be processed under specific circumstances as outlined in Article 9 of the GDPR. The special categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a person's sex life or sexual orientation
- Genetic data
- Biometric data

4. Principles of the General Data Protection Regulation

4.1. The following outlines the principles of the General Data Protection Regulation (Article 5). The Department is required to adhere to these principles.

Lawfulness, Fairness and Transparency

4.2. All data must be processed lawfully, and in a way that is fair and transparent. The data subject will be clearly informed about how their data is being processed at the time it is being captured and who their data is shared with. This data will not be unlawfully disclosed to a third party.

4.3. A general Privacy Notice is available to view on our website and explains how personal data is processed.

Collected for specific, explicit and legitimate purposes

4.4. We will only collect data from data subjects for a specific purpose, and this purpose will be made clear to the data subject at the time the data is collected. Once data is collected for a specific purpose, it will not be processed for any other incompatible purpose.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4.5. The Department will ensure that any data obtained from the data subject will be adequate and relevant to the purpose(s) for which it is being processed. No unnecessary or additional personal data will be processed where the original purpose has been satisfied.

Accurate and, where necessary, kept up-to-date

4.6. Every effort will be made to ensure that all data collected from data subjects is accurate. Where we are made aware of any inaccurate data, we will rectify this subject to appropriate verification.

4.7. It may not always be possible to rectify inaccurate data due to the manner in which the record is held (e.g. a scanned pdf).

Kept in a form which permits identification of data subjects for no longer than is necessary

4.8. Data will be retained for no longer than is necessary in light of the purposes for which that data was originally collected and processed, subject to any relevant archiving obligations.

Processed in a manner that ensures appropriate security of personal data

4.9. All data will be processed safely and securely, to prevent unlawful or unauthorised processing, accidental or unlawful destruction, or accidental loss or damage to the data.

Accountability for the implementation of the above principles

4.10. As a Data Controller, we take responsibility to adhere to the above principles at all times during the course of business. We will keep a record of all personal data collected, held or otherwise processed, known as a 'Record of Processing Activities (ROPA)'. The following details will be recorded:

- The name and contact details of the Controller, and where applicable, the Joint Controller and Data Protection Officer;
- The purposes of the processing;
- Categories of data subjects and personal data;
- Categories of recipients/third parties with whom the data will be shared;
- Retention periods for each category of data;
- Transfers of data to other countries; and
- Details of the technical/security measures in place.

5. Privacy Notice

The Department is required to issue a Privacy Notice where:

- Information is being collected directly from an individual - the Privacy Notice must be provided at the point at which the data is collected;
- Information is obtained from another source - the Privacy Notice must be provided within one month after obtaining the data, preferably at the first point of contact.

A general Privacy Notice is available to view on our website and explains how personal data is processed.

6. Data Subject Rights

We are committed to assisting individuals with the implementation of the following data subject rights:

Right of Access

A data subject can make a formal request for a copy of their personal data being processed by us. There is no fee for such a request, although a fee may be charged for excessive or repetitive requests. A separate ***Data Subject Rights Policy*** provides further details. A Subject Access Request can be made by emailing: sar@dcya.gov.ie

Right to rectification

We are committed to holding accurate data and will work with any data subject to ensure that we rectify any data where inaccuracies have been identified.

Right to erasure (right to be forgotten)

Where we receive a request from a data subject looking to exercise their right of erasure, we will carry out an assessment of whether the personal data can be erased.

Right to restriction of processing

Where a request by a data subject for restriction of processing in certain circumstances is received, we will assess whether the restriction can be applied, and communicate this to the individual.

Right to data portability

Where we have collected personal data by consent or by contract, the data subject concerned has a right to receive the data in a common, machine-readable format to give to another data controller. Exercising this right will depend on the technical feasibility of the request.

Right to object

A data subject has the right to object to the processing of their personal data in specific circumstances. Where such an objection is received, we will assess it on its merits.

Rights relating to automated decision-making, including profiling

A data subject has the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning them. We will ensure that where systems or processes utilise automated decision-making or profiling, an appropriate right of appeal is available to the data subject.

Right to complain

If a data subject is unhappy with the service received, they are welcome to contact the Department's Data Protection Officer (DPO). They also have the right to contact the Data Protection Commission directly. All relevant contact details are provided below.

Right to an effective judicial remedy

A data subject has the right to make a legal claim where they believe they have been affected by the Department (and/or its processors) not complying with relevant data protection obligations.

7. Data Protection Officer

7.1. The Department has a formally appointed Data Protection Officer (DPO).

7.2. The DPO should be included in any matters involving data protection at the earliest possible stage, including privacy impact assessments, data processing activities that may affect data subjects, and incidents which affect their data.

Responsibilities of the DPO

7.3. The DPO will be responsible for the following:

- To act as an advocate for data protection within the Department;
- To inform and advise the Department, its employees, and third-party data processors of their obligations under the GDPR;
- To monitor Departmental compliance with the GDPR, Data Protection Acts and Departmental policies in relation to the protection of personal data, including raising awareness of these policies amongst employees, ensuring relevant and continuous staff training, and auditing and reviewing Departmental systems and procedures;
- To act as a contact point for (i) the Data Protection Commission, and (ii) data subjects regarding the exercise of their data protection rights;
- To ensure confidentiality concerning their role.

Contacting the DPO

7.4. The contact details of the DPO are outlined under ***Useful Contacts*** below.

8. Personal Data Breach

What is a personal data breach?

8.1. A personal data breach is described as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Reporting a breach

8.2. The Department treats data breaches very seriously. The DPO should be notified of a data breach immediately. The DPO will manage any relevant communications with the Data Protection Commission.

8.3. A record of any data breach that occurs, including a description of the breach, its effects and the remedial action taken, will be maintained by the Department.

8.4. Where the data breach results in a high risk to the rights and freedoms of a data subject, the Department is obliged to inform the data subject without undue delay.

9. Training & Information

Training

9.1. The Department will provide access to data protection training to all employees, specific to their role. This training will be periodically reviewed and refreshed to ensure continuing professional development in the area of data protection.

9.2. Employees are responsible to ensure they attend such training and to identify training gaps they feel need to be addressed.

Information

9.3. All employees, joint controllers and third-party processors working on behalf of the Department will be made fully aware of their data protection responsibilities.

10. Freedom of Information

The Freedom of Information Act 2014 (FOI) obliges the Department to publish information on its activities and to make the information it holds, including personal information, available to citizens upon request and in certain circumstances. The Department has a separate FOI policy. There are specific FOI rules covering personal information.

11. Review and Update

This policy may be reviewed from time to time in order to take into account any changes in the organisational structure of the Department, business practices and/or changes in legislation.

Useful Contacts

Department of Children and Youth Affairs	**Data Protection Commission**
Data Protection Officer, Department of Children and Youth Affairs, Block 1 – Miesian Plaza, 50-58 Lower Baggot Street, Dublin 2, D02 XW14.	(i) 21 Fitzwilliam Square Dublin 2 R02 RD28 (ii) Canal House, Station Road Portarlington Co Laois R32 AP23 www.dataprotection.ie www.gdprandyou.ie
Phone: +353 1 647 3183 Email: dpocontact@dcya.gov.ie Subject Access Requests: sar@dcya.gov.ie	Phone: +353 57 868 4800 +353 (0) 761 104 800 Lo-call No: 1890 252 231 Fax: +353 57 868 4757 Email: info@dataprotection.ie

Glossary of Terms

Accountability	**'Accountability'** means being able to demonstrate compliance with GDPR principles. The Department must have appropriate technical and organisational measures in place to be able to demonstrate compliance.
Automated data	**'Automated data'** means any information on computer, or information recorded with the intention of putting it on a computer. It includes not only structured databases but also emails, office documents or CCTV images.
Consent	**'Consent'** is any "freely given, specific, informed and unambiguous" indication of the individual's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed for one or more specific purposes. The affirmative action, or a positive opt-in, means that the consent cannot be inferred from silence, pre-ticked boxes, or inactivity. It should also be separate from terms and conditions, and have a simple way to withdraw it. Public authorities and employers will need to pay special attention to ensure that consent is freely given.
Data Controller	'**Data controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data Processor	'**Data Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller but does not include an employee of the data controller who processes such data in the course of his/her employment. In the context of the Department, this would include the National Shared Services Office (Peoplepoint & the Payroll Shared Services Centre), Financial Shared Services and Pobal.
Data Protection Officer	A **'Data Protection Officer'** must be appointed in accordance with the regulations where either (a) processing is carried out by a public authority; or (b) the "core activities" of a data controller / data processor either require "the regular and systematic monitoring of data subjects on a large scale," or consist of processing of special categories of data or data about criminal convictions "on a large scale."
Data Subject	A natural person (individual) who is the subject of the personal data.
Joint Controller	Joint Controllers as defined in Article 26 of the GDPR jointly determine the purposes and means of processing of personal data.
Personal Data	**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the

	physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	**'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	**'Profiling'** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to an individual, or to analyse or predict in particular that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.
Sensitive personal data	See **'Special Categories of Personal Data'**
Special Categories of Personal Data	**'Special categories of data'** include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Subject access	'**Subject access'** is the data subject's right to obtain from the data controller, on request, certain information relating to the processing of his/her personal data.
Supervisory Authority	The **'Supervisory Authority'** is the national body responsible for data protection. The supervisory authority for the Department of Children and Youth Affairs is the Data Protection Commission. See www.dataprotection.ie
Territorial scope	**'Territorial scope'** of the GDPR includes the European Economic Area (EEA – all 28 EU member states), Iceland, Lichtenstein, and Norway, and does not include Switzerland.
Third party	A **'third party'** is any natural or legal person, public authority, agency, or any other body other than the data subject, the controller, the processor, and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
Transfer	The **'transfer'** of personal data to countries outside the EEA or to international organizations is subject to restrictions. Data does not need to be physically transported to be transferred, for example viewing data hosted in another location would amount to a transfer for GDPR purposes.