An Roinn Leanaí, Comhionannais,
Míchumais, Lánpháirtíochta agus Óige
Department of Children, Equality,
Disability, Integration and Youth

Department of Children, Equality, Disability, Integration and Youth

Data Protection by Design and Default Policy

February 2021

Purpose
The purpose of this policy is to ensure that data protection by design and data protection by default are embedded in the technical and organisational measures in the Department at design and implementation of processes and systems. By default, only personal data necessary for each specific purpose will be collected and processed.

Objective
The objective of this policy is to ensure, at the time of determining the means of processing as well as when actually processing, appropriate technical and organisational measures are implemented. The primary objectives of implementing data protection by design and data protection by default are to ensure the following are considered:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Fundamental rights and freedoms of individuals
- GDPR obligations and mitigation of the risk of breaches.

The Department will ensure that by default, personal data will be restricted to those individuals required to process such data. The Department will adopt internal policies and technical and organisational measures to meet the principles of data protection by design and data protection by default, to include the following as may be appropriate and having regard to the data in issue:

- Map out personal data, by classification, storage and accessibility in the records of processing activities
- Implementing pseudonymisation and encryption where feasible
- Data Minimisation
- Risk Management
- Integrating data privacy into IT policies
- Providing individuals with transparency and access
- Forbidden unless permitted role-based access
- Providing an audit trail of access controls
- Ability to restore availability of, and access to data in the event of an incident
- Regular testing of the effectiveness of security measures.

Scope
To implement data protection by design and data protection by default to ensure only personal data necessary for each specific purpose are processed.

The concept of "necessity" informs the amount of data collected, extent of processing, and retention and accessibility of data as documented in the Record of Processing Activities.

Complying with data protection by design and default requirements
At the beginning of any major project, the introduction of new technology or new products or where significant changes are being made to an existing process, the Department will undertake an initial assessment to determine whether processing of personal data of individuals is proposed.

A second assessment is then required to determine whether the processing is inherent high-risk processing i.e. where the processing meets more than two of the following criteria

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data

- Data processed on a large scale
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects
- Innovative use or applying technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”

Following these assessments, the Department may conduct a Data Protection Impact Assessment (DPIA) and where the DPIA does not identify mitigating safeguards against residual high risks, the Department will consult the Data Protection Commissioner.