

Privacy by Design and Default Policy

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Changes** | **Reviewed by**  | **Approved by**  | **Applicable from** |
| 1.0 | John Nealon, DPO | 10.08.24 | Initial draft | Michael MurtaghSEO | Senior Management Team |  September 2024 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Purpose

The purpose of this policy is to ensure that data protection by design and by default are embedded in the technical and organisational measures in South Dublin County Council at the design and implementation of processes and systems. **Data Protection by design** means embedding data privacy features into the design of projects at an early stage to ensure better data privacy for individuals. **Data Protection 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 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.

South Dublin County Council will ensure that by default, personal data will be restricted to those individuals required to process such data. South Dublin County Council 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 appropriate and having regard to the data in question:

* Map out personal data, by classification, storage and accessibility in the records of processing activities (ROPA)
* Implementing pseudonymisation and encryption where feasible
* Data Minimisation – only collect necessary personal data
* Risk Management – assess the risks
* Providing individuals with transparency and access
* Only permitted on role-based access
* Provide 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.

Complying with data protection by design and default requirements

At the beginning of any major project, the introduction of new technology or new services or where significant changes are being made to an existing process, South Dublin County Council will undertake an initial assessment to determine whether processing of personal data of individuals is proposed.

A DPIA may then be required to determine whether the processing is inherent high-risk processing. Mitigating measures will be taken into consideration to reduce any identified risks.

Following these assessments, if risks remain high after mitigation measures have been put in place South Dublin County Council may consult the Data Protection Commissioner, prior to proceeding with the new processing/project.

**Review**

The Data Protection Officer within South Dublin County Council will review this policy on an annual basis.