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 Impact Assessment Policy

February 2021

Purpose

The Department has responsibilities as a data controller to assess the impact of processing operations on the protection of personal data, where the processing is likely to result in a high risk to the rights and freedoms of data subjects. This is done by conducting a Data Protection Impact Assessment (DPIA).

Objective

The objective of conducting a DPIA is to improve awareness of the data protection risks associated with a project, and to identify and mitigate those risks. This will help to improve the design of a project and enhance the communication about data privacy risks with relevant stakeholders. Some of the benefits of conducting a DPIA are as follows:

- Protecting individual's rights
- Enabling data protection by design into new projects
- Risk Management
- Proactive Management

Scope

The Department will conduct a DPIA for defined projects. A particular function of the Department, or a programme of changes to the Department's operations, may be viewed as a project.

The Department will carry out a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of data subjects, in the following cases but not limited to:

- In the event of use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4).
- Large scale processing of special categories of data referred to in GDPR Article 9 (e.g. health, data).
- In the event of implementing new IT systems that infringe on data subject rights.
- In the event there is a change to the risks posed to personal data by the processing operation(s).

The Department may re-visit a DPIA if new processing activities or if the risks posed by the processing change. In such instances a review will be conducted to assess whether processing creates addition risk which must be mitigated.

A DPIA is generally not required in the following cases:

- Where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons".
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, the results of a DPIA for similar processing can be used.
- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis.
- Where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required. Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorisations, compliance rules, etc. In such cases, and subject to reassessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned

in the list and continues to comply fully with the relevant requirements

Assessment Criteria (for high-risk processing):

Evaluation or scoring, including profiling and predicting, especially "from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

- Automated decision-making with legal or similar significant effect, or processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person".
- Systematic monitoring, being processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area".
- Sensitive personal data, which includes special categories of data (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offenses.
- Data processed on a large scale, taking into account the following factors:
    1. The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
    2. The volume of data and/or the range of different data items being processed
    3. The duration, or permanence, of the data processing activity
    4. The geographical extent of the processing activity

- Datasets that have been matched or combined for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- Data concerning vulnerable data subjects, which can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data.
- Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.
- Data transfers 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".

Timing of a DPIA

The DPIA will be carried out by the Department prior to the processing, in the design phase of the proposed processing operation. For some projects the DPIA may need to be a continuous process and be updated as the project moves forward.

Roles and Responsibilities

The Department is responsible for ensuring the DPIA is carried out. It may be delegated to an external provider, but the Department is ultimately accountable.

The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team.

If a data processor is involved in the processing, the data processor should assist with the DPIA and provide any necessary information.

The Department must seek the views of data subjects or their representatives "where appropriate" in carrying out the DPIA. In some cases, the data subjects may be people within the Department.

Seeking the views of data subjects will allow the Department to understand the concerns of those who may be affected, and to improve transparency by making individuals aware of how their information is intended to be used.

The views of data subjects can be sought through a variety of means, depending on the context. If the Department's final decision differs from the views of data subjects, the reasons should be recorded as a part of the DPIA. If the Department does not feel it appropriate to seek the views of data subjects, the justification for this should also be recorded.

In the event that a DPIA is required, including where the processing is underpinned by a legislative basis, the following features will be present in the DPIA:

- a systematic description of the processing operations and purposes of the processing
- an assessment of the necessity and proportionality of the processing operations
- an assessment of the risks to the rights and freedoms of data subjects
- the Department if appropriate may seek the views of the affected data subjects
- measures envisaged to address the risks
- a description of the measures the Department will take to address these risks, including the safeguards, security measures and mechanisms that the Department will implement to ensure compliance with the GDPR.

Key Stages of a DPIA

1. Identifying whether a DPIA is required.
2. Defining the characteristics of the project to enable an assessment of the risks to take place.
3. Identifying data protection and related risks.
4. Identifying data protection solutions to reduce or eliminate the risks.
5. Signing off on the outcomes of the DPIA.
6. Integrating data protection solutions into the project.

The Department will consult with the Data Protection Commission if a DPIA does not identify mitigating safeguards against residual high risks.