List of Types of Data Processing Operations which require a **Data Protection Impact Assessment.**

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Introduction

Article 35 of the General Data Protection Regulation ("GDPR") prescribes that a Data Protection Impact Assessment ("DPIA") shall be conducted by a controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers must conduct a DPIA. If required, a DPIA must be completed prior to the commencement of the relevant data processing.[1]

Pursuant to Article 35(4) of the General Data Protection Regulation (GDPR), the Irish Data Protection Commission adopts the following list specifying the types of processing operations subject to the requirement for a Data Protection Impact Assessment (DPIA). This list further specifies the requirement set out in Article 35(1) GDPR and, as such, this list is not exhaustive of the instances in which a DPIA will be required. The list is also without prejudice to the requirement to conduct a DPIA pursuant to Article 35(3) GDPR.

The list is intended to encompass both national and cross-border data processing and reflects feedback received during public consultation. The list has also been approved by the European Data Protection Board (EDPB) where it includes processing operations relating to the provision of goods and services to individuals or the monitoring of their behaviour in several Member States or which may substantially affect the free movement of data within EU.

When is a DPIA required?

The GDPR defines several situations when a DPIA is mandatory:

1. GDPR Article 35(1) requires a DPIA to be conducted in cases where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, taking into account the nature, scope, context and purposes of the type of processing. This is likely to be the case if the processing involves new technologies.

2. GDPR Article 35(3) states that DPIAs are mandatory in a number of processing scenarios. These arise where a data controller performs automated decision-making based on personal data profiling, large scale processing of special categories of data or systematic monitoring of publicly accessible areas on a large scale.

3. Where required by a data protection supervisory authority who in accordance with GDPR Article 35(4) has established a list of specific kinds of processing operation that are likely to result in a high risk to the rights and freedoms of data subjects.

[1] *The Irish Data Protection Act 2018, Section 84 transposing Article 27 of the Law Enforcement Directive also requires that a DPIA shall be conducted where certain processing, in particular using new technology, is likely to result in a high risk to the rights and freedoms of individuals, and when conducted for law enforcement purposes.*

In addition, the Working Party 29 Guidelines WP248 (WP29 DPIA Guidelines which were endorsed by the European Data Protection Board on 25 May 2018) state that in most cases, a data controller will require a DPIA when processing meets two of the criteria listed in the WP29 DPIA Guidelines (as set out on pages 9-11). However, in some cases, the WP29 DPIA Guidelines considers that processing meeting only one of these criteria requires a DPIA. The criteria developed in the WP29 DPIA Guidelines were applied in the development and approval of this list to support the consistent application of the GDPR.

As a controller, under the GDPR an organisation will need to assess, decide and document whether a DPIA is necessary for each proposed data processing operation. Records of processing operations should include relevant risk information including reasons why a DPIA needs to be carried out, or not.

If an organisation does need to complete a DPIA, the DPC has published guidance on the steps to follow. The guidance is available at http://gdprandyou.ie/dataprotection-impact-assessments-dpia/

It is important to remember that it is a data controller's obligation to ensure a DPIA is carried out when required, at the appropriate time and contains all the detail required by the GDPR. In particular, all DPIAs should include all the elements listed in Article 35(7) of the GDPR. It should be noted that the requirement to carry out a DPIA applies to processing operations, meeting the criteria in Article 35 and initiated after the GDPR became applicable on 25 May 2018.

List of types of Data Processing requiring a DPIA

The GDPR states that a DPIA is necessary where an organisation, in particular where using new technologies, processes personal data in way that is likely to result in a high risk to the rights and freedoms of an individual.

In particular, a DPIA is required where an organisation:

- uses systematic and extensive profiling with significant effects; or
- processes special category or criminal offence data on a large scale; or
- systematically monitors publicly accessible places on a large scale.

In addition, in accordance with GDPR Article 35(4), the DPC has determined that a DPIA will also be **mandatory** for the following types of processing operation where a documented screening or preliminary risk assessment indicates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals pursuant to GDPR Article 35(1):

1) 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).
2) Profiling vulnerable persons including children to target marketing or online services at such persons.
3) Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.
4) Systematically monitoring, tracking or observing individuals' location or behaviour.
5) Profiling individuals on a large-scale.
6) Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines.
7) Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.
8) Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.
9) Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.
10) Large scale processing of personal data where the Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals.

This list does not remove the general requirement to carry out proper and effective risk assessment and risk management of proposed data processing operations nor does it exempt the controller from the obligation to ensure compliance with any other obligation of the GDPR or other applicable legislation. Furthermore, it is good practice to carry out a DPIA for any major new project involving the use of personal data, even if there is no specific indication of likely high risk.

With reference to point 1 above, where an organisation wishes to use personal data for purposes other than for which it was originally collected, Article 6(4) of the GDPR requires the organisation to do a compatibility test. That test should take into account any links between the original and new purposes, the context in which the data was collected (in particular the relationship between the individual and the organisation, the type of personal data involved (i.e. special categories of data), the possible consequences for individuals of the further processing, and if appropriate safeguards exist (i.e. encryption or pseudonymisation).

Further information and references

Factors influencing DPIA preparation

The GDPR makes use of several terms in relation to the obligation to undertake a DPIA for high risk processing. In particular, and as discussed in the EDPB opinion on DPIAs, the concept of high risk is influenced by several factors. Where these factors are involved in the proposed processing operation, there is a chance they are likely to result in a high risk, particularly where more than one is a factor. However, these factors are not prescriptive, and a data controller ultimately is responsible for determining if there is a high risk. Where there is a doubt, conducting a DPIA is advised.

These factors include:

- Uses of new or novel technologies;
- Data processing at a large scale;
- Profiling/Evaluation - Evaluating, scoring, predicting of individuals' behaviours, activities, attributes including location, health, movement, interests, preferences;
- Any systematic monitoring, observation or control of individuals including that taking place in a public area or where the individual may not be aware of the processing or the identity of the data controller;
- Processing of sensitive data including that as defined in GDPR Article 9, but also other personally intimate data such as location and financial data or processing of electronic communications data;
- Processing of combined data sets that goes beyond the expectations of an individual, such as when combined from two or more sources where processing was carried out for different purposes or by different data controllers;
- Processing of personal data related to vulnerable individuals or audiences that may have particular or special considerations related to their inherent nature, context or environment. This will likely include minors, employees, mentally ill, asylum seekers, the aged, those suffering incapacitation;
- Automated decision making with legal or significant effects (see below). This includes automatic decision making where there is no effective human involvement in the process; and
- Insufficient protection against unauthorised reversal of pseudonymisation.

Reference information

The EDPB have published guidelines and opinions on related concepts and terms. The DPC advises data controllers to consult these when considering the nature, scope, context and purposes of their intended processing operations and the need to carry out a DPIA.

- Further information on risk, systematic processing, vulnerable data subjects and new technology is available in EDPB Guidelines WP 248 rev.01 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679"

- Further information on large scale, significant or legal effects, systematic or regular processing is available in EDPB Guidelines WP 243 rev.01 "Guidelines on Data Protection Officers ('DPOs')"

- Further information on profiling, automated processing and significant or legal effects is available in EDPB Guidelines WP 251 rev.01 "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679"

Are there any exemptions to the requirement for a DPIA?

A DPIA is NOT required where:

- Processing operations do not result in a high risk to the rights and freedoms of individuals;
- Processing was previously found not to be at risk by DPIA;
- Processing has already been authorised by supervisory authority;
- Processing pursuant to point (c) or (e) of Article 6(1) already has an existing clear and specific legal basis in EU or Member State law and where a DPIA has already been carried out as part of the establishment of that legal basis as per Article 35(10);
- Performed as part of an impact assessment arising from a public interest basis and where a DPIA was an element of that impact assessment (Art 35(10)); and/or
- Where a supervisory authority chooses to enumerate the processing operation in accordance with GDPR Article 35(5).