Coimisiún
Cosanta Sonraí
Data Protection
Commission

Public Consultation

Draft list of types of Data Processing Operations which require a Data Protection Impact Assessment.

June 2018

Introduction

Article 35 of 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.

The GDPR further requires national data protection authorities to adopt and publish, under Article 35(4) of the GDPR, a list of the kind of processing operations for which a DPIA is required.

Prior to adoption, this list must be 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.

In accordance with the requirements of the GDPR, the Irish Data Protection Commission ("**DPC**") has prepared a draft list of processing operations for which it considers it is mandatory to conduct a DPIA. The list is intended to encompass both national and cross-border data processing.

With a view to finalising the proposed list for submission to the EDPB for approval, the DPC is issuing its draft DPIA list for public consultation.

The submissions received by the DPC from this consultation will be used for the purposes of finalising the draft DPIA list for submission to the European Data Protection Board and for the purposes of any future guidance materials which the DPC may produce. The submissions may also be shared with other supervisory authorities and other members of the European Data Protection Board.

Stakeholder submissions are welcome by 4 July 2018 by email to consultation@dataprotection.ie.

When is a DPIA required?

Processing operations that do not result in a high risk to the rights and freedoms of individuals will not require a DPIA. However, 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.

As a controller, under the GDPR an organisation will need to assess and evidence whether a DPIA is necessary for each proposed data processing operation.

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/data-protection-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:

- uses systematic and extensive profiling with significant effects;
- processes special category or criminal offence data on a large scale; or
- systematically monitors publicly accessible places on a large scale
- processes personal data in way that is likely to result in a high risk to the rights and freedoms of an individual

In addition, the DPC is proposing that a DPIA is required where an organisation is planning to:

1) use personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to Article 6(4) of the GDPR;

2) profile vulnerable persons including children to target marketing or online services at such persons;
3) use profiling or special category data to determine access to services;
4) monitor, track, or observe individuals' location or behaviour;
5) profile individuals on a large-scale;
6) process biometric data to identify an individual;
7) process genetic data;
8) indirectly source personal data where GDPR transparency requirements are not being met;
9) combine, link or cross-reference separate datasets where such linking contributes to profiling or behavioural analysis of individuals;
10) process personal data based on legislative measure under the Data Protection Act 2018 where suitable and specific measures are required to safeguard the fundamental rights and freedoms of individuals;
11) further process personal data for archiving purposes in the public interest, scientific or historical research or statistical purposes.

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).

Frequently Asked Questions

These questions and answers should be read while taking into account the nature, scope, context and purposes of proposed processing operations.

What does "High Risk" mean?

GDPR mentions risk in many places but does not define "risk" or "high risk". In the context of DPIA, risk is talked about in relation to rights and freedoms of individuals.

This may include non-data protection rights and freedoms. Risk in this context is about the potential for any significant physical, material or non-material harm to individuals.

Threats are different than risks. For instance a *threat* of loss of data will have a *risk* of actually occurring that varies depending on circumstances, nature and scope of processing. A threat is a statement concerning the possibility of damage or harm. A risk quantifies that threat in terms of its likelihood and impact.

Risks can be multi-dimensional and variable over time and environment or the domain of processing. A low risk in one kind or processing operation or environment may be high risk in another. Risks can be managed or remediated with suitable "controls" or measures. Controls and measures can be organisational or technical and may be fully effective in mitigating risk, or partial.

Considering the likelihood and severity of potential harm to an individual arising from some kind of threat, "High Risk" includes risk that is may lead to a more severe or harmful outcome for an individual than an outcome in other circumstances.

Screening for a DPIA involves determining at a high level if an intended processing operation is likely to result in a high risk. A DPIA then objectively explores, assesses and documents that risk, what it means for data subjects and how it may be mitigated and managed.

What does "significantly affect" mean?

GDPR does not define the term "significantly affect" but it is used alongside the term "legal effect". Both are outcomes that have a detrimental or discriminatory affect on an individual or that cause a change in behaviour, decision making, circumstances or ability to avail of their rights or entitlements. The significance of processing is closely related to the vulnerability of the data subject affected.

Significant and legal effects include and relate to:

- legal effect or limitation of rights - for example:
  - loss of entitled to a particular social benefit conferred by law, such as child or housing benefit;
  - refusal of entry at the border;
  - being subjected to increased security measures or surveillance;
  - being refused employment or access to goods or services (e.g. insurance, credit, housing);
  - being charged more for goods or services than he or she would otherwise be charged;
  - prevents exercise of rights under contract, using a service or contract;
  - affects a person's legal status or their legal rights.
- damage, interference, loss or distress to individuals health or wellbeing;
- affects, or is likely to affect, individuals' financial or economic status or circumstances;
- causes, or is likely to cause individuals to change their behaviour in a significant way;

- creates embarrassment or other negative outcomes, including reputational damage;
- has unlikely, unanticipated or unwanted consequences for individuals;
- deprivation of control over one's own personal data or identity
- loss of confidentiality of data protected by professional secrecy

What factors can lead to "high risk" processing?

A DPIA is a tool that is used to determine whether processing is likely to result in a high risk to rights and freedoms of individuals. During screening there are certain factors that can be considered at a high level to help guide whether a DPIA should be conducted in order to work out in detail whether a high risk exists. 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 (see below);
- Data processing at a large scale (see below);
- Profiling/Evaluation - Evaluating, scoring, predicting of individuals' behaviours, activities, attributes including location, health, movement, interests, preferences;
- Any systematic (see below) 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 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. These include 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;
- Ex-EEA data transfers depending on the envisaged country of destination and the possibility of further onward transfers;
- 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;
- Insufficient protection against unauthorized reversal of pseudonymisation.

What does "New technology" mean?

The term "New Technologies" is not defined in GDPR but includes:

- An organisation's first time or novel use of an existing advanced, automated or innovative collection or processing technologies – for instance this could include a first time use of artificial intelligence technologies.
- Use of newly "coined", immature, unproven or "bleeding edge" technology
- Use of technology that is an alternative "in-house" or self-created instance of an otherwise existing technology – for instance a custom encryption method known only to the data controller
- Processing in novel or unexpected ways that may involve unknown or new risks, or because a technology is newly applied to a processing category or sector.

What does "Large Scale" mean?

GDPR does not define the term large scale but it includes:

- duration, or permanence, of the data processing activity
- number or proportion of data subjects
- volume of data and/or the range of different data items being processed
- geographical extent of the processing activity

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a supermarket chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.

Individual professionals processing patient or client data are not processing on a large scale.

What does "Regular" processing mean?

GDPR does not define the term "regular processing" but it includes:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly taking place
- Periodically occurring over an extended time frame

What does "Systematic or extensive" processing mean?

GDPR does not define the terms "Systematic" or "extensive" processing but it relates to:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy
- Extensive implies that the processing covers a large are or involves a large range of data or data subjects.

Are there any exemptions to the requirement for a DPIA?

A DPIA is NOT required where

- Processing was previously found not to be at risk by DPIA
- Processing has already been authorised by supervisory authority
- Processing already has an existing clear legal basis
- Performed as part of an impact assessment arising from a public interest basis and where a DPIA was an element of that impact assessment
- Where a supervisory authority chooses to enumerate the processing operation in accordance with Article 35(5)