DATA PROTECTION AND PRIVACY
University of Genoa

Lesson 3: Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment (DPIA)

When a processing may entail a high risk for the rights and freedoms of the data subjects (due to systematic monitoring of their behaviour, or due to the large number of interested parties whose sensitive data is perhaps processed, or even due to a combination of these and other factors), art. 35 GDPR obliges data controllers to carry out an impact assessment before starting it, consulting the supervisory authority if the technical and organizational measures identified by them to mitigate the impact of the processing are not considered sufficient - that is, when the residual risk for the rights and freedoms of the interested parties remains high (“prior consultation”).

When DPIA is mandatory?

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale

When processing may present risks to the rights and freedoms of natural persons? (1/9)

Working Party art. 29 (WP29) has identified some specific criteria:

- 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 behavior, location or movements”.

Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website

When processing may present risks to the rights and freedoms of natural persons? (2/9)

Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person". For example, the processing may lead to the exclusion or discrimination against individuals

When processing may present risks to the rights and freedoms of natural persons? (3/9)

Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area".

This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s)

When processing may present risks to the rights and freedoms of natural persons? (4/9)

Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10

When processing may present risks to the rights and freedoms of natural persons? (5/9)

Data processed on a large scale: the GDPR does not define what constitutes large-scale. In any event, the WP29 recommends that the following factors be considered when determining whether the processing is carried out on a large scale:

a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

b. the volume of data and/or the range of different data items being processed;

c. the duration, or permanence, of the data processing activity;

d. the geographical extent of the processing activity

When processing may present risks to the rights and freedoms of natural persons? (6/9)

Matching or combining datasets, 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

When processing may present risks to the rights and freedoms of natural persons? (7/9)

Data concerning vulnerable data subjects: the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified

When processing may present risks to the rights and freedoms of natural persons? (8/9)

Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear that the use of a new technology, defined in "accordance with the achieved state of technological knowledge", can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy and therefore require a DPIA

When processing may present risks to the rights and freedoms of natural persons? (9/9)

When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”. This includes processing operations that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan

When isn’t a DPIA required? (1/4)

When the processing is not "likely to result in a high risk", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required

When isn’t a DPIA required? (2/4)

WP29 considers that a DPIA is 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 DPIA have been carried out. In such cases, results of DPIA for similar processing can be used

When isn't a DPIA required? (3/4)

- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed;
- where a processing operation has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis, except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities

When isn’t a DPIA required? (4/4)

- 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 authorizations, compliance rules, etc. In such cases, and subject to re-assessment 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 all the relevant requirements of the GDPR

At what moment should a DPIA be carried out?

Prior to the processing. This is consistent with data protection by design and by default principles. The DPIA should be seen as a tool for helping decision-making concerning the processing

Who is obliged to carry out the DPIA?

The controller, with the DPO and processors.
The controller is responsible for ensuring that the DPIA is carried out. Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task

What is the methodology to carry out a DPIA?

Different methodologies but common criteria.
The GDPR sets out the minimum features of a DPIA:
- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to:
(i) address the risks;
(ii) demonstrate compliance with this Regulation

Is there an obligation to publish the DPIA?

No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA

When shall the supervisory authority be consulted? (1/2)

When the residual risks are high, for example:

- an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy, and/or
- when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well known vulnerability is not patched)

When shall the supervisory authority be consulted? (2/2)

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health