Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR

The European Data Protection Board (EDPB) on its first meeting (25th May 2018) endorsed the GDPR-related Article 29 Working Party Guidelines, including the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR.

This document summarises the main aspects of these guidelines.

INTRODUCTION

Controllers must implement appropriate measures to ensure and to be able to demonstrate compliance with the GDPR, considering the risks of varying likelihood and severity for the rights of individuals (art. 24(1) GDPR). A DPIA, then, is required to comply and to demonstrate compliance with the GDPR.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

DPIAs are important accountability tools, because they help controllers to comply with the GDPR and to demonstrate that appropriate measures have been taken to ensure compliance with it.

A DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons (art. 35(1) GDPR)

DPIA SCOPE

A DPIA may concern a single data processing operation. Art. 35(1) GDPR states that 'a single assessment may address a set of similar processing operations that present similar high risks'. A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose and risks.

When the processing operations involve joint controllers, they need to define their respective obligations precisely, and set out which party is responsible.

A DPIA can also be useful for assessing the data protection impact of a technology product.

PROCESSING OPERATIONS SUBJECT TO DPIA

DPIAs are mandatory where the processing is likely to result in a high risk to the rights of individuals.

The GDPR provides a non-exhaustive list in art. 35(3)(a) to (c) GDPR concerning what constitutes a processing operation that is likely to result in high risk:

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 or similar significant effects on individuals

b) processing on a large scale of special categories of data (art. 9) and of personal data relating to criminal convictions and offences referred to in art. 10

c) systematic monitoring of a publicly accessible area on a large scale

The EDPB provided a more concrete criteria to consider whether a processing operation is likely to result in high risk:

- 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 (rec. 71 and 91)
- Automated-decision making with legal or similar significant effects (art. 35(3)(a) GDPR)
- 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 (art. 35(3)(c) GDPR)
- Sensitive data or data of a highly personal nature: special categories of data defined in art. 9 GDPR or personal data related to criminal convictions or

offences in art. 10 GDPR. Also, some categories of data can be considered as increasing the possible risk to the rights of individuals, and thus be deemed sensitive because:

  - They are linked to household and private activities (e.g. private communications);
  - They impact the exercise of a fundamental right (e.g. location data where whose collection questions the freedom of movement);
  - Their violation involves serious impact in the data subject's daily life (e.g. financial data)
- Data processed in a large scale: factors to determine whether the processing is carried out in large scale:
  - The number of data subjects concerned, either as a specific number or as a proportion;
  - The volume of data and/or the range of different data processing activities;
  - The duration, or permanence of the data processing activity;
  - The geographical extent;
- Matching or combining datasets;
- Data concerning vulnerable data subjects (rec. 75GDPR);
- Innovative use or applying new technological or organisational solutions (art. 35(1) and recs. 89 and 91);
- When the processing in itself prevents data subjects from exercising a right or using a service or a contract (art. 22 and rec. 91 GDPR), including operations that allows, modifies or refuse data subjects' access to a service or entry into a contract

A data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In some cases, meeting only one of these criteria would trigger a DPIA.

In cases where the processing corresponds to the criteria and the controller consider that it is not likely to result in a high risk, the controller must justify and document the reasons for not carrying out a DPIA, including the opinions of the DPOs.

The DPIA is not required:

- Where the processing is not likely to result in a high risk to the rights of the data subjects (art. 35(1) GDPR);
- Where the nature, scope, context and purposes of the processing are very likely similar to the processing for which DPIA have been carried out (art. 35(1) GDPR)

- Where the operations were checked by the DPA before May 2018 and the conditions remain unchanged;
- Where a processing operation is based on art. 6(1)(c) or (e), has a legal basis on EU or national law and where the DPIA has already been carried out as part of the establishment of the legal basis (art. 35(10) GDPR);
- Where the processing is included on the optional list established by the DPAs for which no DPIA is required (art. 35(5) GPDR)

A DPIA must be carried out to existing operations likely to result in a high risk to the rights of data subjects and for which there has been a change of the risks, considering the scope, context and purposes of the processing.

CARRYING OUT A DPIA

Timing: The DPIA must be carried out prior to the processing, but carrying out a DPIA is a continual process, not a one-time exercise

Responsible: The controller is responsible for ensuring that the DPIA is carried out (art. 35(2) DPIA), who must be assisted by the DPO (art. 35(2) GDPR) and the processors (art. 28(3)(f) GDPR) and must seek the views of the data subjects or their representatives where appropriate (art. 35(9) GDPR)

Methodology: Different methodologies but common criteria. A DPIA must contain (art. 35(7) and recitals 84 and 90):

- A description of the envisaged processing operations and the purposes of processing;
- An assessment of the:
    - necessity and proportionality of the processing;
    - risks to the rights and freedoms of data subjects;
- The measures envisaged to:
    - Address the risks;
    - Demonstrate compliance with the GDPR

Compliance with a code of conduct, certifications seals and marks, and BCRs have to be considered (art. 35(8) GDPR) when assessing the impact of a data processing operation.

Where necessary, the controller must carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by the processing operation (art. 35(11) GDPR)

Publication of the DPIA: Publishing a DPIA is not a legal requirement of the GDPR, it is the controllers' decision to do so, but they can consider as a good practice publishing at least parts, such as a summary or a conclusion of the DPIA.

CONSULTING THE DPA

Where the identified risks cannot be sufficiently addressed by the controller (ie. residual risks remain high), the controller must consult the DPA (art. 36(1) and recitals 84 and 94 GDPR).

Additionally, whenever national law requires controllers to consult with, and/or obtain prior authorisation from, the DPA in relation to processing by the 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 (art. 36(5) GDPR).

CRITERIA FOR AN ACCEPTABLE DPIA (ANNEX 2 GUIDELINES)

The WP29 proposed the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (art. 35(7)(a) GDPR):
  - ☐ nature, scope, context and purposes of the processing are taken into account (rec. 90 GDPR);
  - ☐ personal data, recipients and period for which the personal data will be stored arerecorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper orpaper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (art. 35(8) GDPR);
- ☐ necessity and proportionality are assessed (art. 35(7)(b) GDPR):
  - ☐ measures envisaged to comply with the Regulation are determined (art. 35(7)(d) and rec. 90 GDPR), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of theprocessing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (art. 5(1)(b) GDPR);
      - ☐ lawfulness of processing (art. 6 GDPR);

- ☐ adequate, relevant and limited to what is necessary data (art. 5(1)(c) GDPR);
- ☐ limited storage duration (art. 5(1)(e) GDPR);

- ☐ measures contributing to the rights of the data subjects:
  - ☐ information provided to the data subject (arts. 12, 13 and 14 GDPR);
  - ☐ right of access and to data portability (arts. 15 and 20 GDPR);
  - ☐ right to rectification and to erasure (arts. 16, 17 and 19 GDPR);
  - ☐ right to object and to restriction of processing (arts. 18, 19 and 21 GDPR);
  - ☐ relationships with processors (art. 28 GDPR);
  - ☐ safeguards surrounding international transfer(s) (Chapter V GDPR);
  - ☐ prior consultation (art. 36 GDPR).

- ☐ <u>risks to the rights and freedoms of data subjects are managed</u> (art. 35(7)(c) GPDR):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. rec. 84 GDPR) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (rec. 90 GDPR);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (rec. 90 GDPR);
  - ☐ measures envisaged to treat those risks are determined (art. 35(7)(d) and rec. 90 GDPR);
- ☐ <u>interested parties are involved</u>:
  - ☐ the advice of the DPO is sought (art. 35(2) GDPR);
  - ☐ the views of data subjects or their representatives are sought, where appropriate (art. 35(9) GDPR).

This briefing was prepared by Federico Marengo for QUBIT PRIVACY

QUBIT PRIVACY is a consultancy firm established in Italy that provides tailor-made services for individuals and companies to comply with the requirements established in the General Data Protection Regulation.

Qubit Privacy

Find more

https://qubitprivacy.com/

Federico Marengo is a lawyer, master in public administration (University of Buenos Aires), LLM (University of Manchester), and PhD candidate (Università Bocconi, Milano).
He currently provides data protection consultancy services for Qubit Privacy and also works as of counsel at Data Business Services.
He is the author of "Data Protection Law in Charts. A Visual Guide to the General Data Protection Regulation", e-book released in 2021, and authored several publications on international data transfers and international trade law.
As a PhD researcher, his research deals with the potential and challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of Artificial Intelligence.
He is also teaching assistant at Università Bocconi.