ONTIER


PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

**14th March 2017**
**#8**

---

## Index



---

## DATA PROTECTION IMPACT ASSESSMENT

Where the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects, in accordance with Article 35 of the GDPR, the Data Controller shall, prior to the processing, carry out a data protection impact assessment (“DPIA”).
A DPIA is a tool to assess the privacy and data protection impacts and risks of a specific product, service or process, taking into account the nature, scope, context and purposes of the processing and the respective sources. The main purpose of a DPIA is to identify appropriate actions to be taken in order to exclude, or at least, minimize those risks, prevent unlawful processing and implement privacy by design and by default.

## Current situation

Under Directive 95/46/EC, there is no legal obligation to carry out a DPIA. However, DPIAs are recommended by some national data protection authorities in the EU (in particular, the United Kingdom) as a helpful tool for organisations to ensure a new project is compliant with privacy law. As such, many organisations have already incorporated DPIAs in their product or service development cycle to ensure compliance with existing principles of data protection.

## What's new?

Under the GDPR, DPIAs will be mandatory every time an organisation is involved in "high risk" processing.

Article 35.1 of the GDPR states that "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*"

The GDPR sets out some non-exhaustive examples of "**high risk processing**", namely:

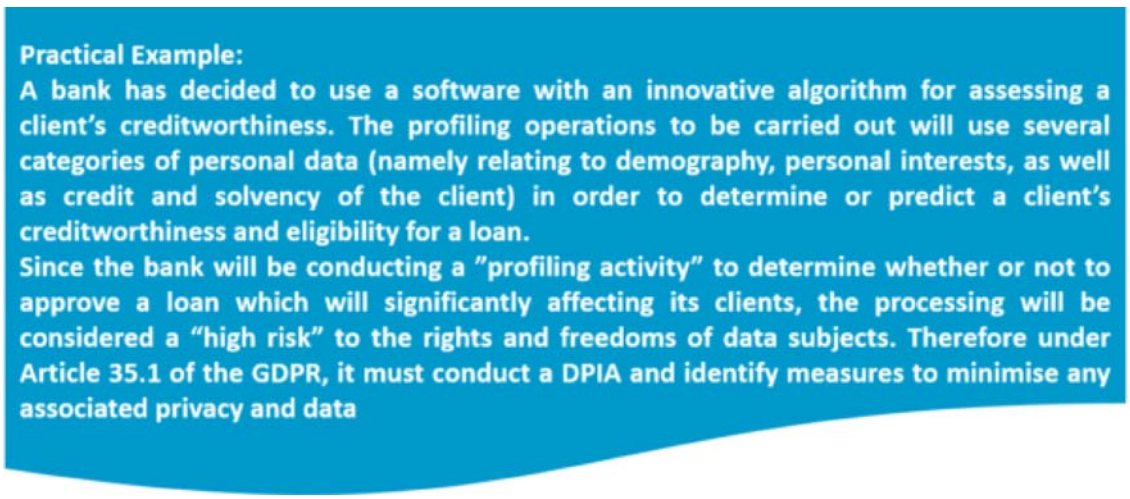
- in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including **profiling**, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a **large scale of special categories of data or personal data relating to criminal convictions and offences**. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are considered, under the GDPR; as "special categories of data"; and
- a systematic **monitoring of a publicly accessible area on a large scale**.(e.g. CCTV).
- It is expected that the Article 29 Working Party will provide further guidance on the concept of "high risk processing" as part of its action plan for 2017.
- Pursuant to Article 35.7 of the GDPR, a DPIA is at least required to include:
- a description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures adopted to mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.
- Where appropriate, Data Controllers should seek the views of the affected data subjects or their representatives (e.g. in the human resources context, work councils or trade unions may have to be consulted). The Data Controller shall also consult the supervisory

authority (i.e. the national data protection authority) prior to the processing if a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk. The supervisory authority should respond within eight weeks of a request for consultation, but can extend this period by a further six weeks if extra time is needed due to the complexity of the processing. These time periods are suspended during the time the supervisory authority is waiting for further information it has requested related to the consultation. Finally, if one has been appointed, the Data Protection Officer should also advise on the DPIA.

## What to do to adapt?

If it is not already doing so, Data Controllers should assess its current and future projects which involves the use of personal data to determine if it is necessary to conduct a DPIA. Such projects could include a new business acquisition, a new service or product, a new process or even a new marketing campaign targeting a certain group. It is important to know what type of data is processed, who can access the data, where the data is located, why the data is being kept and how long the data is being kept for. An action plan on how to implement a DPIA should be in place, addressing who will carry it out and the tasks necessary to remediate the potential risks and ensure compliance.
Existing compliance policies should be reviewed or updated or, in some cases, replaced with new ones. Data Controllers should create and maintain record files of the processing it carries out and establish procedures on its product/service deployment processes to target the necessity of including DPIA, where necessary.
During a product/service lifecycle it may be necessary to carry out a further review to assess if processing is still performed in accordance with the DPIA, at least, when there is a change of risk represented by processing operations.
If a specific project does not require a DPIA, it is good practice to still conduct one to reduce potential risks of non-compliance, resolve any problems at an early stage, reduce costs and limit damage to reputation in the event of a breach of data protection laws and regulations.

---




Practical Example:
A bank has decided to use a software with an innovative algorithm for assessing a client's

creditworthiness. The profiling operations to be carried out will use several categories of personal data (namely relating to demography, personal interests, as well as credit and solvency of the client) in order to determine or predict a client's creditworthiness and eligibility for a loan.
Since the bank will be conducting a "profiling activity" to determine whether or not to approve a loan which will significantly affecting its clients, the processing will be considered a "high risk" to the rights and freedoms of data subjects. Therefore under Article 35.1 of the GDPR, it must conduct a DPIA and identify measures to minimise any associated privacy and data protection risks, before it can commence using the software.

---

## TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

---


---

**Read more:**

about us

---

**Share on:**

Linkedin Twitter

---

**Subscribe:**

our Newsletters

**Contact us:**

Website | LinkedIn

Rua Vitor Cordon Nº 10A, 4º piso - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

-

---

**PORTUGAL** / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / ITALY / MEXICO / PERU / VENEZUELA

---