October 2025

Impact assessment on personal data protection

A new instrument introduced by Law no. 1;565 of December 3, 2024, the data protection impact assessment (DPIA) is a study whose purpose is to identify and analyze the risks that data processing may pose to individuals' privacy.

Need for a high risk to the rights and freedoms of the data subjects

Not every operation that could pose a risk to the rights and freedoms of individuals automatically requires an impact assessment. The law only requires an impact assessment when processing is likely to result in a **high risk to rights and freedoms**, particularly when **new processing technology** is used.

What is meant by new processing technology?
According to the Guidelines on Data Protection Impact Assessment adopted on April 4, 2017 by the Article 29 Data Protection Working Party[1], 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, and 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* ». Conducting an impact assessment will enable the data controller to understand and address this risk.

[1] Independent European working group that dealt with issues relating to privacy and personal data until 25 May 2018 (before the General Data Protection Regulation - GDPR came into force).

In which cases is there a high risk to the rights and freedoms of the data subjects?

Article 35 of the Law provides that a **high risk** exists in four cases:

Case 1: **the systematic and thorough assessment of personal aspects** concerning natural persons, including profiling, and on the basis of which decisions are taken, which produce binding legal effects to a natural person or likewise significantly affect him or her.

Case 2: **the large-scale processing of sensitive data** or personal data relating to offences, criminal convictions, and security measures, or relating to suspicions of unlawful activities.

Case 3: the large-scale systematic monitoring of areas accessible to the **public**.

Case 4: **the widespread use of a digital identifier**.

This list is not exhaustive, as indicated by the use of the word « *including* ». Therefore, other processing operations not listed in these four cases may nevertheless present an equally high risk and therefore require an impact assessment.

What criteria are used to determine whether a processing is likely to result in a high risk to the data subjects?

Article 1 of Ministerial Order no. 2025-361 of July 14, 2025 implementing Article 35 of Law no. 1.565 of December 3, 2024 on the protection of personal data establishes the list of criteria for determining whether a processing is likely to result in a **high risk to the rights and freedoms** of natural persons. Most of these criteria have been clarified by the Guidelines of the Article 29 Working Party.

There are eight criteria in total:

- **Criterion No. 1: systematic and extensive evaluation of personal aspects, including profiling**

According to the guidelines of the Article 29 Working Party, this refers to assessments relating in particular to « *aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements* ».

Examples :

- a company analysing usage or browsing on its website to create behavioural or marketing profiles
- a financial institution screening its customers against a credit rating database or a database dedicated to combating money laundering and terrorist financing

- **Criterion No. 2: automated decision-making producing legal effects concerning a natural person or significantly affecting them in a similar manner.**

For the Article 29 Working Party, automated decision-making is the ability to make decisions using technological means without human intervention.

Automated decisions can be based on any type of data, for example:

• data provided directly by the data subjects (such as responses to a questionnaire);
• data observed about individuals (such as location data collected through an application);
• derived or inferred data, such as a profile of an individual that has already been created (e.g., a credit rating).

These automated decisions may be made with or without profiling and must **produce legal effects** on the data subject or **significantly affect them** (e.g. by resulting in exclusion or discrimination).

Example: creation by a banking institution of a database specialising in credit ratings

- **Criterion No. 3 : systematic monitoring**

According to the guidelines of the Article 29 Working Party, this refers to personal data « *that 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)* ».

This applies to all processing operations involving the observation, monitoring or control of data subjects, including the collection of data via social networks.

Examples:

- the use of a camera system in a shopping centre
- monitoring by an employer of all outgoing emails through alert notifications

- **Criterion No. 4: the processing of sensitive data or data relating to offences, criminal convictions and security measures or relating to suspected illegal activities**

In accordance with Article 2(9) of Law no. 1.565 of December 3, 2024, sensitive data are defined as *« personal data that directly or indirectly reveal political opinions or affiliations, racial or ethnic origins, religious or philosophical beliefs, trade union membership, or genetic data, biometric data that can be used to uniquely identify a natural person, or data concerning the health, sex life or sexual orientation of a natural person* ».

Example: healthcare treatments provided by a healthcare facility

- **Criterion No. 5: cross-referencing or combining data sets**

For the Article 29 Working Party, these data sets may result from two or more data processing operations carried out for different purposes and/or by different data controllers in a manner that would exceed the reasonable expectations of the data subject.

Example: the collection of data on public social networks for the purpose of generating profiles.

- **Criterion No. 6: processing of data concerning vulnerable persons**

According to the explanatory memorandum to Law No. 1.565 of December 3, 2024, vulnerable persons should be understood to include, in particular, « *in addition to children, employees, persons with disabilities, elderly persons, etc.* ».

Example: collection of pseudonymised data from patients participating in clinical research

- **Criterion No. 7: innovative use or applying new technological or organisational solutions**

The use of new technology may involve new forms of data collection and use, the personal and social consequences of which may be unknown at the time of deployment. A DPIA will therefore enable the data controller to understand and address such risks.

In its guidelines, the Article 29 Working Party gives the example of the combined use of fingerprint and facial recognition systems to improve physical access control.

- **Criterion No. 8: processing that prevents the data subject from exercising a right or benefiting from a service or contract**

For the Article 29 Working Party, such processing includes, in particular, operations aimed at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

Example: a bank screening its customers against a credit rating database before deciding whether or not to grant them a loan.

Where processing meets **at least two of these criteria**, the data controller must consider that the processing is **likely to result in a high risk** to the rights and freedoms of data subjects and that **an impact assessment is therefore necessary**.

In some cases, however, the data controller may consider that, given the context of the processing, only one criterion is sufficient.

Special case of large-scale processing

Article 2(24) of Law no. 1.565 of December 3, 2024 defines large-scale processing as « *any operation that aims to process a* ***considerable volume of personal data****, which may affect a* ***significant number of data subjects****, assessed in absolute terms or in relative terms in relation to the population concerned, and which is* ***likely to result in a high risk****, taking into account, in particular, the* ***duration or permanence of the processing activity*** *and its* ***geographical scope*** ».

In this regard, Ministerial Order no. 2025-361 of July 14, 2025 specifies that an operation which:

- aims to process a **considerable volume of data** and
- may affect a **significant number of data subjects** (assessed in absolute terms or in relative terms in relation to the population concerned), taking into account in particular:
    - the **duration or permanence** of the activity and
    - its **geographical scope**

is likely to pose a **high risk** if:

- it meets **at least one of the criteria** set out in Article 1 of the same order (Article 3 of Ministerial Order no. 2025-361).

- it involves the **use of a digital identifier** (Article 4 of Ministerial Order no. 2025-361).

If the data controller considers that the processing in question is **unlikely to result in a high risk** to the rights and freedoms of natural persons and therefore does not require an impact assessment, they **must be able to demonstrate this**. (Article 18 of Sovereign Order no. 11.327 of July 10, 2025 implementing Law no. 1.565 of December 3, 2024 on the protection of personal data).

If there is any doubt as to whether an impact assessment is necessary, it is **recommended that one be carried out regardless**. Impact assessments are useful tools that enable data controllers **to ensure that the operations they are planning to carry out comply with personal data protection requirements**.

Impact assessments are not required for processing operations that remain subject to prior approval by the APDP or the Special National Security Commission established by Article 16 of Law no. 1.430 of July 13, 2016.

When and how should the impact assessment be carried out?

The impact assessment must be carried out **before the data controller implements the processing operation**.

If **a data protection officer** has been appointed, the data controller must seek their **advice** and instruct them to **verify that the impact assessment has been carried out**.

Furthermore, if a data processor is involved in the processing, they must provide their **assistance** and the **information necessary** to carry out the impact assessment.

A single impact assessment may cover a **set of similar processing operations, provided that they present similar high risks.**

The data controller must also **reassess** its impact assessment in the event of a change in risk.

Finally, the impact assessment must be **kept as evidence** by the data controller and communicated to the APDP **upon request**.

What must the impact assessment contain?

Pursuant to Article 35 of Law no. 1.565 of December 3, 2024, all impact assessments must include at least the following elements:

- a **systematic description of the processing operations envisaged and the purposes** of the processing, including, where applicable, the **legitimate interest pursued** by the data controller;
- an assessment of the **necessity and proportionality of processing operations in relation to the purposes**;
- an **assessment of the risks** to the rights and freedoms of the data subjects;
- the **measures envisaged** to address the risks, including safeguards, measures and security mechanisms to ensure the protection of data subjects and other persons affected by the envisaged processing operations.

Mandatory prior consultation with the APDP in the event of high residual risks

If, when carrying out the impact assessment, the data controller realises that the **identified risks cannot be sufficiently reduced** and that there are **high residual risks that cannot be controlled**, Article 36 of Law no. 1.565 of December 3, 2024 stipulates that they **must** first consult the APDP.

The data controller shall provide the Authority with the following information:

- the **respective responsibilities** of the data controller, joint controllers and data processors involved in the processing, and the contact details of the data protection officer, where one has been appointed;
- **the purposes and means** of the proposed processing;
- **the measures and safeguards** envisaged to protect the rights and freedoms of data subjects;
- the **impact assessment** carried out;
- any other information requested by the Authority.

The APDP will then have a maximum of eight weeks to issue a **written opinion** to the data controller; this period may be extended by six weeks in the case of complex processing operations.

If the Authority considers that the processing constitutes a violation, it will impose **appropriate measures** on the data controller and may carry out the **verifications and investigations** provided for in Article 46 of Law no. 1.565 of December 3, 2024.

What is the penalty for failing to comply with impact assessment requirements?

Any failure to comply with impact assessment obligations, whether it is the obligation to conduct the impact assessment under Article 35 of the Law or the duty to consult the APDP beforehand pursuant to Article 36 of the Law, is punishable by an administrative fine of up to **5,000,000 Euros or, in the case of a company, up to 2% of the previous year's total worldwide annual revenue, whichever is the highest.**