Anonymisation or pseudonymisation

Article 31 of Law no. 1.565 of December 3, 2024 stipulates that the data controller and the processor must take **appropriate technical and organisational measures** to guarantee a **level of security appropriate to the risks** to the rights and freedoms of individuals, including the **pseudonymisation of data**.

Similarly, pseudonymisation is one of the **appropriate safeguards** that may be put in place in the event of **further processing of personal data** for purposes other than those for which the data were originally collected, as well as the appropriate technical and organisational measures mentioned in the explanatory memorandum to enable the data controller to comply with the principle of **data protection by default** or to carry out processing for **archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes.**

It therefore seems appropriate to clarify this concept, which is often confused with "*anonymisation*".

Définitions

Anonymisation

Anonymisation is a technique that consists of "*removing any identifying character from a set of data*".

According to the standard ISO 29100, it corresponds to the "*process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party*". (ISO 29100: 2011).

Anonymisation is therefore recognisable by the **irreversibility** of the **loss of any identifiable individual characteristics**.

Pseudonymisation

Pseudonymisation is defined in point 16 of article 2 of Law no. 1.565 of December 3, 2024 as "*the processing of personal data in such a way that these data can no longer be attributed to a specific data subject without recourse to additional information, provided that this additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

Also know as "*reversible anonymisation*", " it consists of **replacing one attribute by another** in a record.

Hence, the physical (natural) persons may still be likely to be identified indirectly.

For example, the codification of a client's name will not prevent his/her individualisation if it is possible to gain access to other characteristics, such as, for example, gender, postal address, or date of birth.

As such, pseudonymisation may reduce the risk of direct correlation between personal data, but may not completely eliminate, in any way, the personal nature of the processed data.

As a result, the pseudonymisation is not a watered-down form of anonymisation, but a simple **security measure**.

Whereas pseudonymisation acts as a bulwark against direct access to personal data, anonymisation irreversibly neutralises the personal nature of the data.

Distinct objectives

The choice of anonymisation or pseudonymisation is less a technical choice than the need to retain or not personal data.

Pseudonymisation lends itself to situations that necessitate or allow to go back from the encoded personal data to the original personal data. For example, the processing of personal data may require, due to legal obligations, to be able to go back to a specific person.

On the other hand, anonymisation is not part of a subsequent **re-identification process** and is not intended to allow such a step backwards.

Pseudonymisation and anonymisation therefore serve different purposes: to preserve or not the personal nature of information. As a result, anonymisation that may be undermined by particularly advanced techniques (IT for example) is not the same as pseudonymisation.

Pseudonymisation is not a '*low-cost'* anonymisation, but an appropriate method designed to achieve a **specific goal**.

The challenges of qualification

Point 5 of Article 2 of Law no. 1.565 of december 3, 2024 states that a personal data is « *any information relating to a natural person identified or identifiable" and that "an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

The data may therefore be **directly identifying** (a person's first and last name, for example) or **indirectly identifying**, either by **reference to an identification number** (telephone number, number plate or IP address, for example) or by **elements specific to the physical identity** of the person concerned (photo, voice or fingerprint, for example).

Similarly, when it is possible to identify a person by **cross-referencing several pieces of information** such as gender, age, occupation and place of residence, the data are **always** considered personal.

It is consequently clear to note that the legislator privileged the result over the intention: as long as the person is determined or determinable, directly or indirectly, the law no. 1.565 of December 3, 2024 applies.

Therefore, by eliminating the specific characteristics of a natural person, anonymisation enables the data to be **removed from the scope of application** of this law.

On the other hand, the pseudonymised data whose identifiable nature has only been **mitigated** are still subject to the law no. 1.565 of December 3, 2024.

The choice of de-identification method is therefore not neutral in that it dictates the rules applicable to the processed data.

Let's take a look at a concrete example

Point 5 of Article 4 of Law no. 1.565 of December 3, 2024 stipulates that personal data must be "*kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which they are processed*".

Anonymisation of personal data, in that it removes the identifiable nature of the data subjects, allows the anonymised information to be retained after the purpose of the processing has been achieved.

Pseudonymisation, on the other hand, does not allow personal data to be kept **beyond the retention period specified for the processing operation.**

Unlike pseudonymisation, anonymisation is more of a **denaturing measure than a security measure.**