Data mapping : How to make an inventory of your personal data processing activities ?

An indispensable step to being compliant with Law no. 1.565 of December 3, 2024, the mapping (cartography) of all operations or all operations applicable to personal data (that is, the processing activities) provides an exhaustive view of the personal data processed by the data controller from their collecting to their deletion.

Such an inventory of data seems necessary for all entities wishing to guarantee the protection of personal data that they have in their possession.

This sheet has for objective to guide data controllers in the mapping of data processing activities; mapping comprised of 6 key elements that can be achieved from either a business or technical approach, or even a combination of both, and which above all must face various challenges.

What is a data mapping ?
The mapping of personal data processing activities consists of identifying and inventorying all processing within an entity (company, administration, association, and so forth). Concretely, it enables each data controller to identify, for each processing, the name and contact details of the data controller, the end purpose (that is, the goal) of the identified processing (commercial relations, HR management,...), the categories of people concerned (customers, employees, candidates,…), the internal or external actors (players) who are required to manage these data, the routing of these data flows when these include transfers outside the Principality, the provided delays before deleting the data, and finally, a description of the technical and organisational security measures taken to guarantee their protection. When well conducted, this mapping illustrates a reality that can be both dense and complex, which clearly shows the interactions and interdependencies between the different components and layers of the Information System (IS).

The 6 key elements for a successful data mapping

The 6 key elements are addressed by 6 main questions.

1 – WHO manages the processing?

First, before anything else, it is necessary to know the actors, internal or external, likely to manipulate these data. Thus, it is essential to note the name and contact details of the data controller (and his or her legal representative), to identify the managers of the operational services who are processing the data within the entity, and to establish a list of subcontractors. Particularly for the latter, an updated list will enable them to check and modify, if necessary, the confidentiality clauses contained in their contracts.

2 – WHAT data are collected?

The second important step of the mapping is to determine what data are processed for each actor. To this end, it is necessary to identify the different categories of data that are processed, but also the data likely to raise, because of their sensitivity, specific risks, such as, for example, health-related data.

3 – WHY are the data collected?

After these two steps are accomplished, it is necessary to determine the objectives pursued by this data processing activity, that is, the end purpose, which could be, for example, human resource management, litigation management, or the management of professional messaging systems.

4 - WHERE are the data stored?

An essential step is to decide on the physical location where to store the personal data, but also the country or countries to which these data can be transferred. This question is especially important for data located in the *cloud*. Indeed, such data can move very easily making it difficult to follow the successive transfers.

5 – HOW LONG are the data retained?

Another essential question concerns the length of time that data can be retained. For each category of data, it is necessary to specify the duration the data can be retained (storage period). For example, this can be one month for CCTV images or even until amicable settlement of a dispute as part of the management of litigation.

6 – HOW data security is guaranteed?

Finally, it is essential to outline the different protection measures in place to minimize the risk of unauthorized access to the data, the goal being to limit as much as possible any impact on the privacy of the persons concerned. One of the first measures of protection consists of, for example, setting up personal passwords considered "*strong*" and to regularly change them to access applications.

The different approaches to map the processing activities

Two approaches, often complementary, can be selected to conduct a mapping and to ensure that all operations relating to personal data have been inventoried: A business approach (which start with the individual concerned by the data processing), and a technical approach (which starts with the data management process).

1 – The business approach

This approach consists of the following 4 steps:

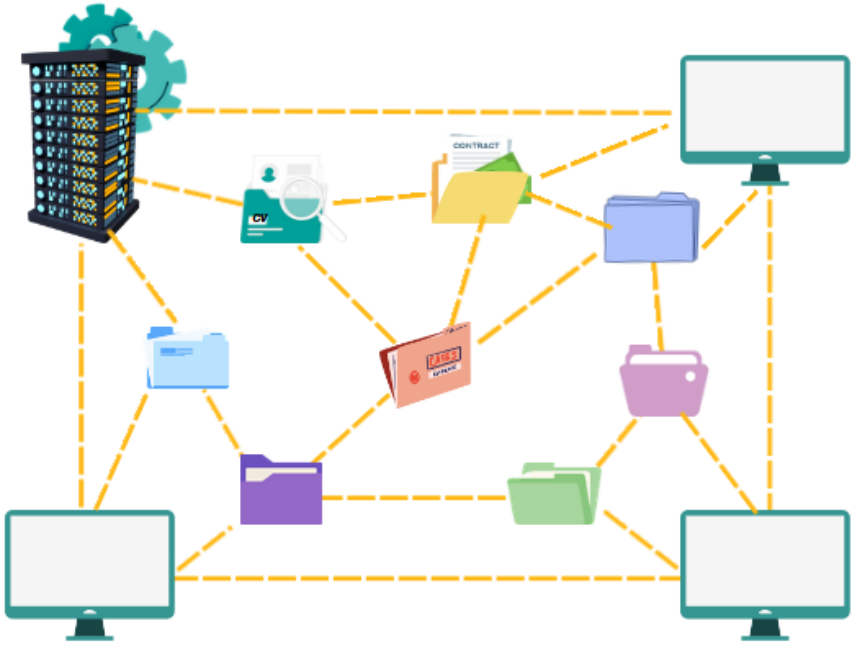
- **IDENTIFY the categories of natural persons who interact with the entity.** These can be employees, customers, prospects, users, suppliers, etc.
- **LIST**, for each category of persons, **the nature of the personal data** collected by the entity concerned
- **FOLLOW the data flows,** namely their entry and transfer points
- **IDENTIFY the processing** performed on these data

Example : Starting with the employees. For these latter, the categories of data such as their wages, their family situations, their social benefits, and the social reasons for their absences can be collected.

After all the categories of data have been inventoried, it becomes easier to identify the responsible departments within the entity, for example, which one is responsible for tracking performance, and which one is responsible for monitoring medical data.

It is then up to these departments to set up data management policy paying particular attention to critical data (for example, bank account numbers) and to establish a retention strategy for these data.

2 – The technical approach



This approach is based on the following procedure :

- **DEFINE internal and external process** interacting with the persons concerned
- **LIST the information systems** on which these processes depend directly
- **IDENTIFY THE FLOWS AND PROCESSING** of personal data supported by these systems
- **RETRACE THE FLOWS AND PROCESSING** of the personal data

Example : Starting this time from the system that manages identity data. These data may originate from the recruitment system since the concerned employee was a candidate before being hired, from the payroll system or even from the expense and travel management system that can contain sensitive information, such as credit card numbers.

Here again, after all these systems have been identified, it becomes easier for the entity to have a complete view of the data lifecycle of its employees, from their arrival in the entity to their departure.

Data mapping over time : challenges and good practices

After its creation, the mapping must live and evolve over time. This inventory meant to be exhaustive must be updated regularly to become the indispensable reference document to enable any entity to ensure compliance with personal data protection.

Faced with the challenge of a subject in constant evolution, it is therefore important for the entities concerned to adopt certain good practices.

1 – A rigorous investigative methodology

An incomplete data mapping exposes the entity to a high risk of vulnerability regarding data protection and may result in the application of corrective actions of disproportionate nature (t high resource costs).

It is therefore important to establish a rigorous investigative methodology, especially when the IS is complex, for example, when:

- processing massive data (big data solutions);
- using virtualization;
- using multiple outsourced IT or business perimeters, especially via the cloud.

2 – A pragmatic and reactive mapping

As previously mentioned, the mapping must show at all times the reality of the SI, whether this reality is that of the existing or a projection of the future (targets).

3 – A mapping in constant evolution

Too frozen (static), a mapping can quickly become useless and costly. Therefore, it is a project constantly in development that must accompany the entity throughout its lifetime, progressively, by reconciling both business and technical visions.

4 – An understandable mapping

A last, the mapping must foster dialogue and understanding of the future by all actors concerned. It must be understandable by all and clearly describe any changes that may need to be made.

In conclusion, a successful mapping is a tool that enables the easy identification by a data controller of all the processing activities (by end purpose) containing personal data that he or she has implemented.