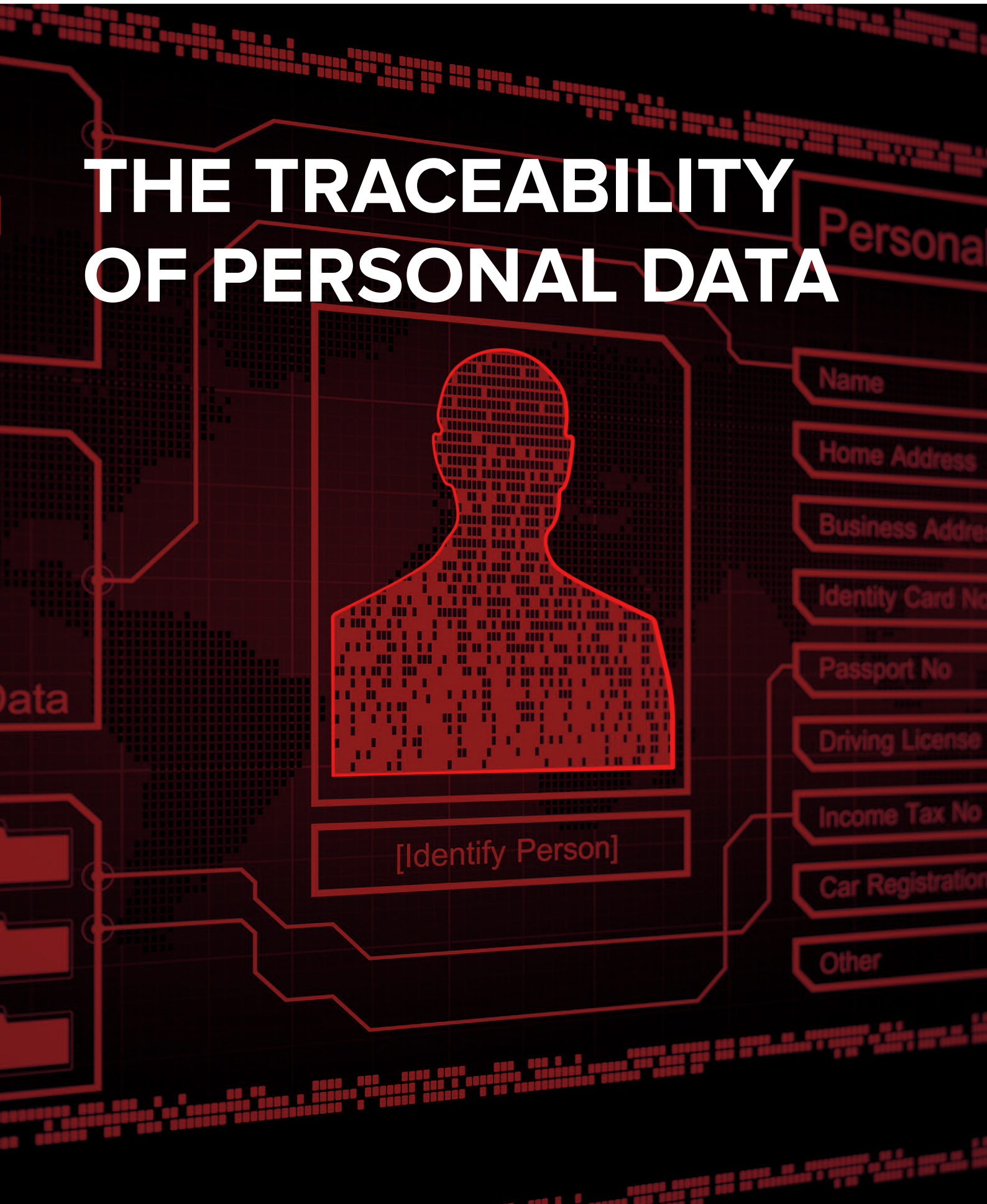
Pridatect
POWERING PRIVACY COMPLIANCE

THE TRACEABILITY OF PERSONAL DATA



Content

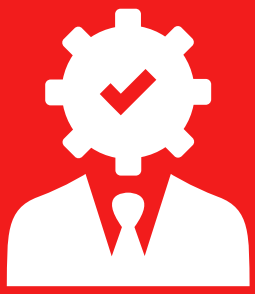
1. Introduction

The evolution of technology in fields as diverse as biotechnology, robotics or artificial intelligence has led to the emergence of what many call the Fourth Industrial Revolution or Digital Revolution. This implies a paradigm shift in the way in which humanity as a whole relates, trades, works and lives. The 21st century has established itself as the digital era, in which advances are made at a previously unimaginable speed and many of these have been carried out thanks to data processing. Consequently, whoever has the data, has the power.

Personal data is now treated as a form of currency and has more value than ever. For this reason the most intelligent thing to do is to carry out a good management of the this, since in many cases organizations are not aware of the large amount of data they own.

On the other hand, it is not unreasonable to say that most people have lost control of their personal data, especially the younger generations that have grown up using the internet. Nowadays, virtually no person would be able to list all the web pages on which they have entered their own personal data. All this makes it necessary for companies and organizations that process personal data, to guarantee their traceability in order to determine what data is available, where it is stored and to whom it has been transferred.

In some cases it has even been declared that personal data should be treated as property of the involved person. In this context, it would be even more important to guarantee the traceability of personal data.



2. What is the traceability of data?

Traceability can be defined as the process by which it is possible to know all the stages, locations or changes through which personal data has passed, in the context of a treatment activity.

Therefore, traceability must consist of having an exhaustive control of the treatment process of personal data, controlling exactly what data is being processed, who is involved in the data processing, which third parties have access and what systems are involved.

3. Traceability and data protection

a) The principle of proactive responsibility or accountability

The principle of proactive responsibility or accountability is one of the pillars for the correct application of the GDPR and all the data protection regulations.

It should be taken into account that it is a branch of preventive law, so t**he most important thing is to comply and be able to prove it, in accordance with Article 5.2 of the GDPR.** Data protection is configured as a series of obligations for organizations to guarantee the rights and freedom of the interested parties and as a series of complementary norms with a soft law character as well, which are not mandatory for the organization but are highly recommended when establishing effective data protection.

All this is related to the traceability of data since, although there is no express obligation in this regard, it is understood as a necessary tool to comply and demonstrate its compliance.

Imagine that an organization collects data through a website registration, which establishes a clause that by registering you are accepting to receive advertising emails. Imagine that the clause is correct but that the acceptance is not recorded or that this data is not maintained. In this case for example, if there were a request for the access rights, the organization could not report how and when the data was collected nor could it prove that the data is not being used for purposes other than its original intended purpose.

This would imply that the organization is not able to demonstrate compliance and consequently, the remaining of the data protection measures would be little or not effective at all. The cause of this problem would be the lack of traceability of personal data.

b) The data flow

As already established, traceability is also related to the data flow, the company must be aware of the context and the processes of data processing.

Article 35 (7) of the GDPR establishes that impact analysis must contain a systematic and detailed description of the treatment. The methodology used to obtain this description is the data flow, which is divided into the following stages:

- **Data capture:** Data collection process, it can be capturing data through online forms, paper, external sources, etc.
- **Classification/Storage:** establishing the data categories for storage in different systems.
- **Use/Treatment:** Set of operations performed on personal data.
- **Session/transfer of data to a third party for processing:** Transfer or communication of data to a third party.
- **Destruction:** Removal of personal data so that it can't be recovered.

In each of these stages the elements involved must be identified:

- **Activities or operations:** Each stage of the data flow involves data processing. In this sense, it should be understood as a processing activity any operation that is carried out on the data, even those that involve only the viewing of data or even its collection.

Each of the activities carried out at each stage of the process must be described in detail.

- **Data:** The personal data processed must be identified, and the data must be categorized according to whether it pertains sensitive data or not.
- **Participants:** All natural or legal persons that are involved in the data flow must be identified. It is important to properly define the roles and responsibilities of each of the participants.

It is vital, in order to guarantee a correct traceability of the information, to have a service that allows the participant to be authenticated and that keeps a record of their access session and of the information accessed.

- **Technology:** Finally, the technology used in each of the stages of the processing must be identified, this is especially relevant in the data session or transfer stage.

In short, the data flow could be represented as follows:

STAGES

ELEMENTS	DATA CAPTURE	CLASSIFICATION	TREATMENT	TRANSFER DATA TO A THIRD PARTY	DESTRUCTION
PROCESSING ACTIVITIES					
DATA PROCESSED					
INVOLVED					
INTERVENING TECHNOLOGIES					

SOURCE: AEPD

c) Responsibilities

The principle of accountability and traceability is directly related to establishing responsibilities. It is not only important to determine if the organization acts in a treatment as responsible, co-responsible or in charge; it is also relevant to define sessions and transfers.

However, it should not be forgotten that every organization is made up of people and therefore, it should also be defined which people have access to the data, maintaining a credential system that records each person's logins.

In addition to guaranteeing the traceability of access and / or modifications of the data with this type of systems, it is recommended to define the structure of responsibilities within the company, since, even though they would ultimately be the ones responsible for the treatment, in practice one or several people will be those who assume the task of complying with the GDPR.

d) Registration of processing activities

Traceability is also apparent in the obligation to keep a record of the processing activities. **This obligation, which is regulated in article 30 of the GDPR, is the responsible of the registration of the files before the AEPD.**

The processing activity log is configured, unlike the old files, as an internal document, which must be made available to the responsible control authority if requested. With this decision the European Legislation demonstrates again the importance of the principle of proactive responsibility. Remember: you must comply and be able to prove its compliance.

The idea of traceability of personal data and treatment processes is also reinforced. At the end of the day, the registration of processing activities aims the objective that the person in charge of the treatment has all his processing activities documented.

The registration of activities, however, is not strictly mandatory for all companies or organizations. It is established that companies that employ less than 250 people are not obliged to have such a registry, "**unless the treatment they carry out may entail a risk to the rights and freedom of the interested parties, it is not occasional, or includes special categories of personal data indicated in article 9, paragraph 1, or personal data relating to convictions and criminal offenses referred to in article 10.**"

The wording of article 30 paragraph 5 of the GDPR has created discrepancies regarding the obligatory nature of the activity log. In practice, most treatments could involve a risk and can be classified as not occasional, so in almost all cases it will be necessary to have a record of such treatment activities.

Even in cases where the requirements of the aforementioned article are not met it is still advisable, in order to maintain adequate traceability of the data, to register the processing activities.

e) The principle of privacy by design

Another principle of the Regulation that has more importance with regards to traceability, is privacy by design.

The privacy by design essentially consists in the application of the appropriate technical and organizational measures both at the time of design of the data processing and at the time of the processing itself.

All this taking into account the state of the technique, the cost of the application and the nature, scope, context and purpose of the processing, as well as the risks that the processing may entail.

Therefore you must select the measures to mitigate the risks that may be more appropriate prior to and during data processing. The measures referred to in the GDPR may consist of different types:

- Monitoring of the regulatory compliance measures
- Management and security against breaches
- Control of treatment managers
- Support and database management
- Access Control
- Continuity and availability
- Access Control (equipment, networks and systems)
- Access Control (physical)

These types of measures are exemplary and different classifications can be established. The most relevant is the importance of traceability in data processing, since traceability measures could be incorporated into virtually all types of technical measures.

For example, permit controls, access controls or support management involve traceability measures such as the registration of the support used, establishing an access record to any equipment or facilities of the organization, etc.

4. Conclusion

In short, traceability can be considered as a measure of compliance, which in some cases will be mandatory and in other mainly highly recommended.

Without being a principle defined in Article 5 of the GDPR, traceability is closely linked to the principle of proactive responsibility and the principle of privacy by design.

Traceability is of great importance as it allows organizations to have a rigorous control of the personal data being handled, as well as to avoid penalties by being able to demonstrate regulatory compliance and define strategies to mitigate the risks detected.

Pridatect
POWERING PRIVACY COMPLIANCE

COMPROMISED TO DATA PROTECTION

For more information:
pridatect.com

Contact:
info@pridatect.com