General Data Protection Regulation (known as GPDR)

Introduction:

The General Data Protection Regulation (known as "GDPR") adopted on April 14, 2016 and entered into force on May 25, 2018 has been perceived and felt as a real revolution in the protection of personal data and, more broadly, of privacy.

However, the GDPR replaces or completes already old texts whose principals were already very similar: the Directive 95/46/EC of October 24, 1995 at the European level or, for example, the Data Protection Act in France dating from January 6, 1978.

What makes the GDPR a particularly innovative and impactful text for companies in the broadest sense is, on the one hand, its desire to standardize the regulatory framework for data protection throughout the European Union, and even beyond, and on the other hand, the strengthening of the obligations weighing on companies with very strong penalties.

This extended scope of application is reflected in the fact that the GDPR concerns all companies and all public or private organizations that collect or process personal data in Europe: law firms, but also legal professionals such as notaries or bailiffs are therefore all concerned by the GDPR in their activities that involve the processing of large volumes of personal data.

With regard to our professional and ethical obligations, we must be particularly vigilant and ensure that our activities comply with these new requirements.

What's new in the GDPR

1. A broader scope of application

The main objectives of the GDPR, namely the harmonization of national regulations and the strengthening of personal data protection in the globalized context in which they are processed, have resulted in a significantly expanded scope of application:

The notion of "personal data" is extremely broad, since it concerns "*any information relating to a data subject*" that corresponds to "*an identified natural person* [...] *or who can be identified, directly or indirectly, by means that are reasonably likely to be used by the controller or by any other natural or legal person [...*]". Thus, personal data is no longer defined solely in terms of the identifying nature of the information held by the data controller itself, but also in terms of the possibility that this information may be cross-referenced with any other information held by a third party and giving it an identifying nature.

In addition, the definition of anonymous or pseudonymous data within the GDPR is extremely restrictive. In essence, as soon as a data is likely to be individualizing, even without directly identifying a person, it falls within the scope of personal data.

For example, by making pseudonymized statistics on the preferences of its customers or by keeping documents related to a case that do not show the name or the first name of a person ... one processes a priori personal data, and one must respect the GDPR.

The territorial scope of application of the GDPR is extensive: as soon as a processing operation is carried out in the context of the activities of an establishment located in the territory of the European Union, concerning a European resident, or is linked to an offer of goods or services to persons located in the territory of the European Union, the GDPR applies. Similarly, the transfer of data outside the European Union or access to data from outside this territory is subject to very strict rules which tend to be reinforced under the influence of the European Commission.

It is understandable, in the context of the constant use of digital tools and new technologies and where personal data is becoming a strong economic stake: the GDPR applies everywhere and all the time!

2. Reinforced obligations

The GDPR requires companies to rethink their organization of personal data management and protection through, in particular:

The obligation for all companies, except in certain cases, **to keep a register** listing the processing operations they carry out. This register must show a certain amount of information that requires knowing exactly what data is being processed and how. This work may seem tedious but often allows for an in-depth analysis that facilitates compliance with the GDPR later on.

The obligation to define the **division of responsibilities with its service providers or partners:** the GDPR provides for different qualifications (controller, joint controller, or processor) which depend on who decides on the means and purposes of the personal data processing. The distribution of these responsibilities must be contractualized within a document respecting a certain number of provisions imposed by the GDPR.

- It may be mandatory or recommended to appoint a "**Data Protection Officer**", the famous "DPO" which is the cornerstone of compliance with the GDPR.

- The principles of minimization and proportionality introduced by the GDPR also require defining for **what periods of time data is kept** (regardless of the medium: paper or digital). These "data retention policies" must be reliable and based on clear criteria, such as the purposes for which the data is used (I should not keep data I do not need), legal obligations or applicable limitation periods.

The GDPR also strongly emphasizes the implementation of the **necessary measures, whether technical or organizational, to ensure a sufficient level of security of the processed data**. This also includes an obligation to notify the national supervisory authority of serious personal data losses and breaches within 72 hours of the discovery of the breach, which is generalized to all organizations. In addition, where the breach is likely to affect the privacy of data subjects, they will also have to be notified.

The GDPR has changed the expectations of companies and organizations processing data: where previously, as in France, it was sufficient to make simple declarations to the Commission Nationale Informatique et Libertés, it is now required to have a thorough knowledge of the processing operations that are implemented and to document the way in which the regulatory requirements are met.

3. Increased protection of the rights of the persons concerned

The protective nature of the GDPR is reflected in a strengthening of the rights of data subjects. Thus, to the existing rights such as the right of access or the right of rectification have been added new rights that data subjects can exercise with companies:

Extended **right to information** (Articles 13 and 14 of the GDPR): In addition to the information already provided for in the previous regulation, the information provided to individuals must, in particular, also cover "the duration of the retention period" and "any other information necessary to ensure fair processing of the data", which is very broad.

Consent (Articles 4 and 7 of the GDPR): When required, consent will need to be explicit and separate. That is, individuals must give consent for each use of their data for which it is required. In addition, the GDPR introduces specific consent requirements for children under 16 for the provision of certain services.

The right to **erasure** or "right to be forgotten" (Article 17 of the GDPR): Data subjects may request the erasure of their data in multiple cases, including when the data will no longer be necessary for the purposes for which it was collected or processed or when individuals wish to withdraw their consent or object to the processing.

The right to **portability** (Article 20 of the GDPR): Controllers must allow a data subject's data to be provided to another controller in a "structured, commonly used and readable" format.

The management of requests for the exercise of rights by data subjects must be anticipated in order to be able to respond to them in a complete manner and within the deadlines imposed by the GDPR. This includes, for example, for the right to information, reviewing the information notices or the privacy policy on its website or any other medium through which data is collected. Similarly, in order to be able to respond to a request for access rights, it is recommended to anticipate a procedure aimed at identifying which data must or can be transmitted and how to extract volumes of data from its information systems that may be significant.

To ensure compliance with these obligations and to provide protection authorities with real leverage against the companies they control, the GDPR has added **administrative sanctions,** the amount of which has been greatly increased. Depending on the type of violation, a fine can reach 20,000,000 euros or up to 4% of annual worldwide turnover, whichever is higher. The arsenal of sanctions also contains the possibility for the supervisory authorities to make their decisions public, which is very impactful and therefore dissuasive for the sanctioned companies.

<u>The main compliance actions</u>

What are the major steps?

1. **Define governance**: to approach compliance in a proper and rational manner, it is recommended to :
    - Define whether it is mandatory or relevant to appoint a DPO and identify the internal and/or external strategic actors to ensure compliance;
    - Conduct internal awareness campaigns to disseminate good practices and ensure the effectiveness of the approach.

2. **Inventory the processing operations**: this step is essential in order to adapt the compliance measures and to ensure that a complete register is created. To do this, it is often useful to start by gathering and analyzing any existing documentation (register, old CNIL declarations, etc.) before proceeding with an inventory of the main categories of processing by project and/or purpose (customers, human resources, IT service providers, etc.).

3. **Prioritize the actions to be carried out**: it is necessary to **set a schedule taking into account:**
    - The activities, size and structure of the teams involved
    - Possible external factors that could impact the priority actions to be taken (e.g. new project underway or to come)

4. **Ensuring compliance**:

All these actions can be implemented as and when required, according to the specific priorities of each activity.