PERSONAL DATA

WHAT ARE THE CHANGES IMPLIED BY THE GENERAL DATA PROTECTION REGULATION (the "GDPR") AS FROM THE 25TH OF MAY 2018

- **The European parliament has adopted a new regulation regarding data protection. This regulation will be applicable in France from the 25th of May 2018.**

- **This regulation is applicable to all organisations which process personal data on behalf of another body, as part of a service performance. Therefore it applies to all European based organisations, but also to foreign companies that process Europeans citizens' personal data.**

- **The purpose of this new regulation is to increase the rights of European citizens regarding the processing of their personal data.**

- **Organisations have new responsibilities with regards to the General Data Protection Regulation.**

- **The regulation implements new penalties in the event that organisations do not comply with the GDPR.**

Summary table of the new obligations companies are subjected to

	Less than 250 employees	More than 250 employees
Collecting individuals' prior consent to the data processing activities	**Yes**	**No**
Prior declarations to the CNIL	**No**	**No**
Setting up of processes in order to deal with individuals' exercise of rights	**Yes**	**Yes**
Keeping a register of processing activities	**No**	**Yes**
Appoint a DPO	**In the event of processing of sensitive data**	**Yes**
Conducting impact assessments	**In the event of processing of sensitive data**	**In the event of processing of sensitive data**
Information of the CNIL in the event of a breach of data security	**Within 72h after the breach occurs**	**Within 72 hours after the breach occurs**

The European parliament has adopted on the 27th of April 2016 a regulation n°2016/679 regarding the protection of personal data; the general data protection regulation or "GDPR" which will be applicable in France from the 25th of May 2018.

The GDPR will replace the previous provisions resulting from the directive 95/46/CE from the 24th of October 1995.

The purpose of the GDPR is to normalize the rules regarding data protection across the whole European Union. The personal data are defined in the article 4 of the GDPR as any information relating to an identified or identifiable natural person, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name and identification number, location date, an online identifier or to one or more factors specific to the physical physiological, generic, mental, economic, cultural or social identity of that natural person.

The GDPR is applicable to all organization which process personal data on behalf of another body, as part of a service performance, it can be large corporations, startups, public authorities or even associations.

Will come within the scope of the GDPR all data processor if they are established in the European Union. Also come in the scope of the GDPR processors, which are not established in the European Union but which processing activities are related to the offering of goods or services to data subjects in the EU, or the monitoring of their behavior as far as their behavior takes place within the EU[1].

Moreover, the GDPR implements new penalties in the event that a processor does not comply with the regulation.

Therefore, a processor that is not compliant with the GDPR regulations may be held liable for the damage suffered and be subjected to major administrative penalties of up to €10m or €20m depending on the category of offence, or, in the event of an undertaking, up to 2% or 4% or the total worldwide annual turnover of the preceding financial year whichever is higher[2].

In France, it is also considered to be a criminal offence not to comply with the GDPR regulations, therefore processors can be sentenced to up to 5 years jail time and a fine of €300.000 for the natural persons and €1.500.000 for companies.

We will first study what are the new obligations for companies as from the 25th of May 2018 **(I)** and then which steps shall companies undertake in order to comply with the GDPR provisions **(II).**

[1] Article 3 of the GDPR
[2] Article 82 and 83 of the GDPR

I) New obligations for companies as from the 25th of May 2018

1) The accountability principle

Until now, under French law, companies had to make declarations or ask for permission to the *Commission Informatique et Libertés* (the CNIL) before processing personal data.

Under the new regulation, companies are no longer under the obligation of asking permission to the CNIL, they must take all the necessary steps to ensure that they are complying with the GDPR regulations, it is called the "**accountability principle**".

Companies must set in place processes, means and tools in order to protect the personal data.

This accountability principle also applies to companies processing sensitive personal data. Now the person in charge of the processing of personal data has to perform impact assessment in order to determine the risks the processing has on the individuals' private lives, and in order to find out what are the most effective means in order to guarantee the highest level of security while processing personal data.

2) The obligation to appoint a Data Protection Officer "DPO"

Under the previous French regulations, companies had, in some cases, to appoint a "*Correspondant Informatique et Libertés*".

The article 37 of the GDPR requires companies to appoint a DPO in the following circumstances:

- The processor is a public body or authority,
- The processor employs more than 250 persons,
- The core activities of the processor involve conducting, on its clients' behalf, regular and systematic monitoring of data subjects on a large scale,
- The core activities of the processor involve processing on a large scale, on its clients' behalf, sensitive data or data relating to criminal convictions and offences.
- Over and above these compulsory cases, designation of a DPO is recommended as it ensures that the companies are provided with an expert, tasked with the practical implementation and management of compliance with the GDPR.

The DPO can be a person working inside the company having special skills in order to perform this duty. It can also be someone from outside the company, like a lawyer.

The DPO performs the following tasks:

- Advisory and information of the data processor;

- Management of the compliance with the GDPR;
- Implementation of the GDPR;
- Giving advises regarding the performance of impact assessment.

The DPO will also be the contact with the authorities in the event of a breach of the data protection regulation.

3) Recording of the processing activities

The processor is under the obligation of maintaining a record of processing activities, in the event that the company employs more than 250 persons.

This record must be maintained in writing and contain:

- The name and contact details of each client on behalf of which data is being processed,
- The name and contact details of each sub processor, where applicable,
- The name and contact details of the DPO,
- The categories of processing carried out,
- The transfers of data outside the EU that is carried out by the processor
- Where possible, a general description of the technical and organizational security measures set up by the processor.

4) Strengthening of individuals' rights

The GDPR sets up new rights for the individuals subjected to processing activities. It is therefore essential for companies to take into account these new rights while collecting and processing personal data.

French law already provided individuals with safeguards regarding their personal data procession. For instance French law granted individuals with:

- The right to access to personal data processed by the company;
- The right of correction regarding the data processed;
- The right of opposition to the processing;
- The right to transfer the data.

The GDPR establishes the right for individuals to transfer their data in a form that can be easily reused by another processor.

While processing personal data companies are now under the obligation to ensure that the individuals gave an express consent for their personal data to be processed. The express consent is defined as the expression of one person's will to have its data processed.

Therefore the silence of the inactivity of one person is not sufficient to consider that the person consented to the processing.

It is essential for the processor to make sure that the individuals gave their consent for their data to be processed and to record this consent in the event of an inspection.

5) New obligations in the event of a data breach

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

In the event of a data breach, the company is under the obligation to notify its client of the breach without undue delay after having become aware of it.

On the basis of this notification the company must notify within 72 hours following the breach, the competent supervisory authority.

II) Actions to be implemented by companies in order to comply with the GDPR

When a company operates as a processor in the implementation of personal data processing operation it must provide its client with sufficient guarantees to implement appropriate technical and organizational measures in such manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

It there is essential for companies to comply with the GDPR before it enters into force, on the 25th of May 2018.

Therefore it is necessary to set up internal processes, and a general policy regarding personal data processing within the company.

Moreover, it is necessary to bring awareness to all the employees within the company on the new regulation regarding the processing of personal data.

In France the "CNIL" as set the following guidelines for the processors to comply with the GDPR.

1) Appoint a controller

This controller can be the company's DPO. This controller is in charge of ensuring that the company takes all the necessary steps in order to comply with the GDPR. The controller must advise the persons in charge of the data processing and also the company's employees.

2) Identify and map the data processing activities

The controller must precisely identify the data processing activities and more precisely (i) the different personal data processing activities, (ii) the different categories of personal data that are being processed, (iii) the reasons why the data are being processed (i) the persons in charge of the data processing activities (v) the data flows and more precisely the origin and the destination of the data, in order to determine whether or not they are being transferred outside from the EU.

3) Prioritize the actions that need to be taken

It is necessary to identify which steps the company must take in order to comply with the GDPR.

It is also necessary to identify on which legal basis data are being processed. Companies must only process data they need to and check that the informational measures set up within the company comply with the GDPR.

The companies processing personal data must also set up internal process in order to insure that it can respond to the individuals' will to exercise their rights (right of opposition to the processing).

4) Management of the risks

Where a processing is likely to result in a high risk to the rights and freedoms of natural persons, the processor shall carry out a privacy impact assessment. This data protection impact assessment is supposed to show the characteristics of the treatment, the risks and the measures adopted.

The compliance approach implemented by carrying out a privacy impact assessment is based on two pillars:

- Fundamental rights and principles, which are "non negotiable", established by law and which must be respected, regardless of the nature, severity and likelihood of risks;
- Management of data subjects' privacy risks, which determines the appropriate technical and organizational controls to protect personal data.

Therefore, to carry out a privacy impact assessment it is necessary to:

- Define and describe the context of the processing of personal data under consideration;
- Analyse the controls guaranteeing compliance with the fundamental principles : the proportionality and necessity of processing and the protection of data subjects' rights;
- Assess privacy risks associated with data security and ensure they are properly treated;
- Formally document the validation of the privacy impact assessment in view of the previous facts to hand and decide to revise the previous steps.

This is a continuous improvement process. Therefore it sometimes requires several iterations to achieve an acceptable privacy protection system. It also required a monitoring changed over time (in context, controls, risks, ect) for instance every year and updates whenever a significant change occurs.

The approach should be implemented as soon as a new processing of personal data is designed.

5) Organization of the internal process in order to ensure a high level of personal data protection

In order to ensure a high level of personal data protection companies are under the obligation of setting up internal processes in order to ensure a high level of data protection at all times.

These internal processes must take into account all the events that can affect personal data during their lives, for instance security breach or editing of the personal data.

The organization of internal processes supposes to:

- Take into account the data protection issue since the beginning of the conception of any activity that would result in the processing of personal data,
- Inform the employees and organise the reporting of information by building a training plan for the employees,
- Deal with all claims made by individuals regarding their rights related to personal data processing activities,
- Anticipate the data breaches.

6) Document the compliance activities

In order to prove that companies comply with the GDPR provisions, they are under the obligation of keeping and compiling all documents that can prove that they took all the necessary steps to comply with the regulation.

The following must be gathered:

- The register of processing activities,
- The impact assessment on sensitive data processing activities,
- Documents related to policies regarding transfers of personal data outside from the EU,
- The consent forms,
- Informational measures,
- The process set in place in order to ensure that individuals can exercise their personal rights,
- The internal processes applicable in the event of a security breach,
- Proofs that individuals whom data are being process gave their express consent to the processing activities.

CONTACT: + 33 1 42 27 05 38

Arnaud Roiron - Partner Attorney at law (France) – arnaud.roiron@wtsf.fr

Marielle Tyranowicz – Senior Associate – marielle.tyranowicz@wtsf.fr

Bérengère Tosani - Associate lawyer – berengere.tosani@wtsf.fr

---

WTS

WTS SELARL (France), a member of the WTS International Network, is a law firm offering global services in taxation and business law assisting our clients in all types of operations, at local and international level.

Combining the strength of the WTS international network with the local knowledge of the Paris office, the WTS France team is able to assist clients in all day-do-day and exceptional operations, such as external growth in particular...

WTS
57 avenue de Villiers,
75017 Paris - France
Tél. : +33 1 42 27 05 38
Fax : +33 1 42 27 05 39
arnaud.roiron@wtsf.fr