astura
AVOCATS À LA COUR

GDPR: ARE YOU READY?

*Companies operating in France, the European Union, and more generally companies abroad whose processing activities target persons located in the EU, are invited to pay attention to the General Data Protection Regulation n°2016/679 (the "**GDPR**").*

The GDPR will enter into force on May 25th, 2018, in all EU countries. This regulation will replace the European Directive 95/46 on personal data protection and will consequently impact French "Loi Informatique et Libertés" dated January 6th, 1978, by implementing new obligations on every legal entity or natural person processing personal data outside the course of a purely personal or household activity.

Companies must make sure they are in line with the GDPR in due time, all the more so as the GDPR imposes burdensome administrative sanctions for non-compliance, which can amount up to 20 000 000 € or 4% of the firm's global annual turnover.

You will find below an overview of the main requirements to be implemented on May 25th, 2018, which require prior preparation.

1. OBLIGATION TO MAINTAIN A RECORD OF DATA PROCESSING

Most of the formalities to be filed to the French data protection authority (the "**CNIL**") will disappear. Apart from a limited set of exceptions, these formalities will be replaced by the obligation to maintain a record of personal data processing.

- In practice, processings operated by your company should be identified and compiled in a record of personal data processings.

- This procedure requires a strong cooperation between various company departments (IT, legal, HR, marketing …), which shall be dealt with by the DPO or, as the case may be, by a personal data referent (see point 2 below).

2. OBLIGATION TO APPOINT A DPO

The companies under the obligation to appoint a Data Protection Officer ("**DPO**") are the ones whose core activities require:

- large scale processing of personal data on a regular and systematic basis (such as the monitoring of an e-commerce website or the management of customers databases) ; or
- large scale processing of sensitive data (such as health data).

- In practice, the DPO has to be specifically appointed (whether internally or externally) and notified to the CNIL.

- The DPO must be provided with the necessary means to fulfill his tasks, and must be involved in any issues related to personal data. This therefore requires to settle consultation process involving the DPO for any projects relating to personal data processing.

Please note that the CNIL recommends companies which are not concerned by the obligation to appoint a DPO to designate nevertheless a personal data referent in order to centralize information related to personal data processing and to coordinate the actions to be taken.

3. RISK IDENTIFICATION WILL BE MANDATORY, AND WHEN DISCOVERED WILL REQUIRE THE IMPLEMENTATION OF A DATA PROTECTION IMPACT ASSESSMENT

All processing which are likely to result in a high risk to the rights and freedoms of natural persons will have to be addressed by conducting a data privacy impact assessment ("**DPIA**").

- In practice, this requires to identify high risk related processing (for example, credit scoring, due diligence in the context of anti-money laundering, or employees monitoring) and to prepare the PIA accordingly.

4. OBLIGATION TO REVISE CONTRACTS WITH SUBCONTRACTORS

The GDPR imposes to integrate new clauses in all subcontracts involving a personal data processing.

- Existing contracts will therefore have to be amended and contracts under negotiation should include clauses that comply with the GDPR.

5. GETTING READY FOR OTHER OBLIGATIONS

The GDPR imposes many other obligations, such as the requirement of privacy by design and privacy by default, the advisory obligations for subcontractors and the implementation of specific security measures in relation to the relevant risk. All of these obligations require to deeply rethink the company's internal process related to the protection of personal data.

The CNIL is taking many actions to clarify and help companies comply to the new obligations imposed by the GDPR. The CNIL notably issued a method to help companies to adapt their processes, which is summed up in the following link: *https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes.*

ABOUT ASTURA

Astura is an independent law firm specialized in the support of businesses and their related parties. In particular, Astura advises businesses on compliance with data privacy laws, in the structuring of cross-border data flows and in dealing with CNIL controls and proceedings.

More particularly, Astura has appeared in Legal 500 in the following fields:

- **information technology** : *Astura is "an outstanding law firm which has a complete understanding of its clients and is capable of quickly and efficiently solving complex IT matters. Matthieu Mélin is recommended for his expertise,*

his operational knowledge and his ability to smartly protect the interests of his clients."

- **intellectual property**: *Astura delivers "efficient and top-notch work. Matthieu Mélin is in charge, has outstanding expertise regarding patents and complex contracts, and takes great care of his clients."*

- **mergers and acquistions** : "*excellent both in advisory and relational matters", the team has "strong experience in representing groups and foreign investors." Raphaël Dalmas is in charge and "is always dedicated to crafting innovative solutions."*

CONTACTS

Matthieu Mélin
mmelin@astura.fr
T +33 (0)1 84 16 24 31

Raphaël Dalmas
rdalmas@astura.fr
T +33 (0)1 84 16 24 32

Clotilde Chabre
cchabre@astura.fr
T +33 (0)1 84 16 24 36

www.astura.fr