HARLAY
AVOCATS

LEGAL UPDATE IN FRANCE

Harlay Avocats | June 2017 | Personal Data | Newsletter N°57

The first actions for complying with the new Data Protection Regulation (GDPR)

Action needs to be taken now in order to be compliant with the GDPR. That is the message contained in the CNIL guidelines, published on March 15th 2017.

The General Data Protection Regulation ("GDPR") will come into effect on May 25th 2018. From this date, companies will need to provide increased protection for personal data. In case of a breach of these rules the French National Data Protection Authority ("CNIL") can impose financial penalties of up to 20 million Euros or 4 % of consolidated annual global turnover (whichever is greater). In its practical guide, the CNIL indicates the following 6 key measures that need to be taken: appointing a pilot; mapping personal data processing; prioritizing action to be taken; risk management; organizing internal procedures; drafting compliance documentation.

In order to comply with the GDPR, a company could structure its approach by setting up a compliance audit, appointing a "CIL" (a future Data Protection Officer) and winning client confidence by securing the Governance Label from the CNIL.

DPO or Data Protection Officer

The role of the DPO is to manage and organize personal data processing inside the company. He could rely on an internal network ("Freedoms and Computer Network") across various business lines of the company to keep him informed about any new data processing that has been introduced.

Appointment of a Data Protection Officer ("CIL" in French) is highly recommended, even before it becomes mandatory or even if the company falls within a category that is not bound to appoint one. Structuring management enables the Company to determine the action that needs be taken and to increase internal awareness. For example, the CIL will keep a register of all data processing, which will become mandatory for all data controllers and data processors under the GDPR.

The DPO can be an existing member of staff with the appropriate level of technical and/or legal expertise in data protection. The company may equally decide to outsource the role to an external consultant or a legal counsel specialized in personal data.

Compliance audit and Risk analysis

Companies are advised to carry out a GDPR compliance audit of the GDPR during this transitional phase.

This audit should be able to help the company to map personal data, identify the purposes for processing, identify users, data recipients and the transfer of personal data outside the EU, to understand the processes related to the use, storage and destruction of data, and to analyse security measures. These internal measures must provide protection for data from the moment of conception (minimising the amount of data processed with reference to the purpose for which it is processed).

In most cases, this involves, at the very least, a consultation with General Management, the CIO, the CISO, the DPO, the Human Resources department, the Marketing department and the Business department.

Risky processing, in data protection terms, will be subject to risk analysis and/or a Privacy Impact Assessment ("PIA"). This analysis will be mandatory for all processing that is liable to create an increased risk to the rights and freedoms of individuals (profiling) or for large-scale processing of sensitive data. Such analysis will enable Companies to assess their risk exposure and put into place the appropriate measures (legal/security) to manage these risks accordingly.

The audit will end with an audit report containing recommendations for presentation to management, together with a suitable action plan with defined priorities.

Finally, Companies must keep records of their internal data management procedures, as evidence of compliance with the GDPR ("Accountability"). This documentation can be drawn in parallel with the audit. In particular, Companies will have to keep a Register of all data processing and supervise data transfers outside the EU (EU Commission Standard Contractual Clauses or Binding Corporate Rules), review sub-contracting agreements. The Companies also have to review their subcontracting contracts, individual consent forms, etc.

CNIL Governance Label

The GDPR strongly encourages the use of compliance labels and certificates for personal data protection. Companies with a DPO are therefore recommended to apply for a Governance Label from the French national data protection authority ("CNIL").

This Label is a mark of confidence for clients and provides a distinct competitive advantage.

As a reminder, the Governance Label includes various document templates that can be useful when implementing internal procedures (for example, exercising access rights, portability, removal or for the management of security incidents).

For further information or queries please, contact us at contact@harlaylaw.com.




Harlay Avocats