The 6 essential steps for the implementation of the GDPR

The implementation of the General Regulation of Data Protection ('GDPR') has been complex for companies and public institutions in Portugal.

Having entered into force in May 2016, this Regulation, directly applicable in all Member States, will demand that organizations have implemented the necessary legal, technical and organizational measures that can evidence the full compliance of all the obligations set therein, in order to avoid high fines and reputational damages of difficult repair.

Having this complexity in mind, the French Data Protection Authority (CNIL) has issued a 6-step methodology for companies that want to prepare for the changes that will apply under the General Data Protection Regulation ("GDPR"). In place of declarations, CNIL underscores the importance of "accountability" and "transparency", core principles that underlie the GDPR requirements.

"The French Data Protection Authority has issued a 6-step methodology for companies that want to prepare for the changes that will apply under the GDPR. CNIL underscores the importance of "accountability" and "transparency""

According with CNIL, the 6 necessary steps are as follows:

Step 1: Appoint a data protection officer ("DPO") to "pilot" the organization's GDPR compliance program.

Pursuant to Article 37 of the GDPR, appointing a DPO will be required if the organization is a public entity; or if the core activities of the organization require the regular and systematic monitoring of data subjects on a large scale, or if such activities consist of the processing of sensitive data on a large scale. CNIL recommends appointing a DPO before GDPR applies in May 2018.

The Data Protection Officer will be responsible for monitoring and complying with the obligations foreseen in the Regulation by the responsible person for the processing of personal data and will be the contact person for any matter with the competent supervisory authority.

Step 2: Undertake data mapping to measure the impact of the GDPR on existing data processing.

Pursuant to Article 30 of the GDPR, controllers and processors will be required to maintain a record of their processing activities. In order to measure the impact of the GDPR on existing data processing and maintain a record, CNIL advises organizations to identify data processing, the categories of personal data processed, the purposes of each processing, the persons who process the data (including data processor), and data flows, in particular data transfers outside the EU.

To adequately map data, CNIL recommends asking:

- Who processes the personal data?
- What personal data do you process?
- For which purpose?
- Where do you storage the collected personal data?
- What is the data retention period?
- Which security measures do you have in place?

Step 3: Based on the results of data mapping, identify key compliance actions and prioritize them depending on the risks to individuals.

In order to prioritize the tasks to be performed, CNIL recommends:

- Ensuring that only data strictly necessary for the purposes is collected and processed;
- Identifying the legal basis for the processing;
- Revising privacy notices to make them compliant with the GDPR;
- Ensuring that data processors know their new obligations and responsibilities and that data processing agreements contain the appropriate provisions in respect of security, confidentiality and protection of personal data;
- Deciding how data subjects will be able to exercise their rights;
- Verifying security measures in place.

In addition, CNIL recommends particular caution when the organization processes data such as sensitive data and data regarding minors, when the processing presents certain risks to data subjects and/or when data is transferred outside the European Union.

Step 4: Conduct a privacy impact assessment for any data processing that presents high privacy risks to data subjects due to the nature or scope of the processing operations.

Conducting a privacy impact assessment ("PIA") is essential to assess the impact of a processing on data subjects' privacy and to demonstrate that the fundamental principles of the GDPR have been complied with.

CNIL recommends to conduct a PIA before collecting data and starting processing, and any time processing is likely to present high privacy risks to data subjects.

Step 5: Implement internal procedures to ensure a high level of protection for personal data.

According to CNIL, implementing compliant internal procedures implies adopting a privacy by design approach, increasing awareness, facilitating information reporting within the organization, responding to data subject requests, and anticipating data breach incidents.

Step 6: Document everything to be able to prove compliance with the GDPR.

In order to be able to demonstrate compliance, CNIL recommends that organizations retain documents regarding the processing of personal data, such as: records of processing activities, PIAs and documents regarding data transfers outside the EU; transparency

documents such as privacy notices, consent forms, procedures for exercising data subject rights; and agreements defining the roles and responsibilities of each stakeholder, including data processing agreements, internal procedures in case of data breach, and proof of consent when the processing is based on the data subject's consent.

For further information, please contact:

Joana Mota Agostinho I jmagostinho@ctsu.pt

www.ctsu.pt