The General Data Protection Regulation: What it means and what to do…

Facing the General Data Protection Regulation (GDPR) is somewhat daunting, particularly for organizations based outside of Europe and less familiar with its requirements. Even for those companies that complied with the Safe Harbor regulations previously in effect, the differences are substantial and important.

First, the GDPR requires that those subject to its rules stop thinking in terms of PII (personally identifiable information) or other, older views of what makes data about individuals sensitive. The concept of personal information used in the new regulation is much broader – it can include many things that would not previously have been considered sensitive, such as a person's email address, cell phone number or internet connections.

The GDPR is also much more explicit about specific roles and responsibilities that those under its control must define. A Data Protection Officer (DPO) must be identified, though the role may be assigned to someone who is also holding a more traditional role such as Chief Information Security Officer or Chief Privacy Officer; the role can also be one contracted from an outside resource with specialized skills.

In much of past privacy or data protection law, there was an emphasis on contractual relationships and agreements. The GDPR is much less concerned with the role of the data subject as a consumer, a business partner or as an employee, though there are some specific considerations for those roles. The focus on data subjects is also clear in the regulation's scope, since it extends to the information of and data subject in the UE regardless of where that data may be collected, stored, processed or transmitted.

Most of all, the core concept of the GDPR's purpose is in the regulation itself: "Natural persons should have control over their own personal data." Mechanisms must be put in place to ensure that organizations that collect and maintain records about natural persons also provide those subjects with the means to control collection, maintain accuracy, and withdraw permission for use of the information.

Steps towards GDPR compliance

Several models have been put forward by privacy organizations, EU privacy regulators, and EU member governments. One of the most straightforward is issued by CNIL, the French regulatory body for information privacy. They set out six steps for compliance:

Step 1: Appointing a data protection officer or leader

The appointment of a DPO is first in the process because it's assumed that whoever holds this role (whether on an interim or permanent basis) will lead the remainder of the project.

Step 2: Data mapping

The next key step is understanding and documenting exactly which data is within the GDPR's governance requirements, and what data is not. Organizations that fail to carry out this step are in extreme danger of incorrectly scoping their projects – either missing critical data that should be addressed, or allowing an over-large and uneconomic growth in scale and increasing the likelihood of project failure.

Step 3: Prioritizing compliance actions

CNIL breaks the third step down into six critical points to establish compliance priorities:

- You've ensured that your organization is only collecting and processing personal data that is strictly necessary.
- You've identified the legal basis for the data processing.
- You've reviewed existing privacy notices for compliance with the GDPR notice requirements.
- You've verified that all vendors are aware of their new obligations under the GDPR and appropriately revised service agreements.
- You've defined a procedure for handling data subjects' requests for exercising their data protection rights.
- You've verified data security measures have been implemented.

Step 4: Managing risks

In managing risks, the GDPR introduces another often unfamiliar concept – the Privacy Impact Assessment (PIA), sometimes also called the Data Protection Impact Assessment (DPIA). A carefully crafted PIA/DPIA can fulfill not only the initial need to understand and communicate risks and guide their management – it can also provide evidence to satisfy the record-keeping requirements of GDPR Article 30 and other elements (see Step 6).

Step 5: Organizing internal processes

To organize internal processes, CNIL lays out the following components:

- Data protection principles must be taken into account when designing an application or a data processing activity.
- Develop a training and communications plan to increase employee awareness and ensure information is escalated to relevant employees or directors when appropriate.
- Handle all data subjects' requests related to individual data protection rights.
- Be prepared for data breaches by ensuring the organization communicates appropriately with the data protection authority (sometimes within 72 hours), and the affected data subjects.

Step 6: Keeping documentation on compliance measures

Finally, CNIL notes the following as key elements of documentation that must be created and updated:

- A record of data processing activities (controllers) or the categories of data processing activities (processors).
- DPIAs for high risk data processing.
- Any data transfer mechanisms.
- Privacy notices.
- Consent forms, including evidence of individual consent where consent is the legal basis for processing.
- Procedures for handling data subjects' data protection rights.
- Contracts with vendors/data processors.
- Internal procedures for responding to a data breach.

Summary

GDPR compliance is neither trivial nor something to be ignored – but it is also not as difficult as it may at first appear. The steps can be simply stated, and the complexity of the effort will be consistent with the value of that data to the organization and the complexity of its use.

- Identify internal and/or external expertise and give them a mandate
- Know what you need to protect
- Set priorities for the project
- Use risk assessments and risk-based management to govern your efforts
- Build privacy awareness and protection into your organization's efforts
- Keep track of what you do