Read this post online

GDPR: How to ensure compliance by May 25, 2018?

The EU General Data Protection Regulation will take effect on May 25, 2018. Companies must take steps to ensure an enhanced protection of personal data, failing which they will face heavy fines of up to 4% of their annual turnover. The GDPR – that includes 99 articles and 173 recitals – combines both legal and technical provisions that promote an accountability approach. What are the key practical implications for businesses?

Who does the GDPR apply to?

Any and all companies (startups, micro-businesses, small- and medium-sized businesses, intermediate-sized businesses and large companies) based in the EU, but also those based outside the EU, that target EU residents through the offering of goods or services, or through profiling.

What changes does the GDPR bring about?

The RGPD implies a radical cultural change. Companies will have to apply a new principle of data protection at the time the processing is conceived (*Privacy by design*) and by default (*Privacy by default*). As such, they will have to take into account the golden rules for data protection from the earliest stage of development of the product, service or processing. This includes in particular minimizing in every respect the processing carried out. These principles are part of the more general principle of accountability according to which businesses must implement internal mechanisms and procedures to be able to demonstrate compliance with the new rules governing the protection of personal data. As such, companies will have to elaborate and formalize data confidentiality policies, consent management procedures, request forms for the exercise of the data subject's rights, data breach procedures, and adapt their contracts accordingly. In some cases, they will even have the obligation to maintain a record of their processing activities, carry out privacy impact assessments or appoint a data protection officer.

How to proceed?

Companies must adopt a structured approach. For this purpose, they should be assisted by experienced lawyers and IT consultants. The first thing to do is to perform an audit to analyze the current situation (How are data and consents collected? For what purposes? What are the collected data? Is the minimization principle complied with? Where are the data stored? Are the data transferred and, if yes, where are they transferred? What is the level of security of storage bases and data flows (encryption, pseudonymization, etc.). What are the applicable procedures if a breach occurs?). The audit is designed to identify compliance gaps as well as the tasks to be performed to ensure compliance. The third step is to elaborate an action plan that will list and plan the actions and measures to be taken. The project team must be a multi-disciplinary team that brings together the internal and/or external resources that are required to take into account all of the issues at stake: Legal organizational, technological, commercial and marketing.

Our firm is ready to work hand-in-hand with you to ensure that your organization will be compliant-with the new rules imposed by the GDPR.