MASTT2040

THHINKBV 2024

GDPR

From 25th May 2018 all companies that collect data on citizens across the 28 EU member states had to comply with strict new rules protecting customer data with the introduction of the General Data Protection Regulation. The regulation dictates that by law it is not be allowed to collect data on:

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

This is good for consumers as there are clear rules with respect to their data and it is also good for companies as they only need to comply with a single standard within Europe. However, the requirements to meet and administer the standard require most companies to invest heavily. Large US companies that deal with data had to invest significant amounts to meet the new standard. According to the PwC survey, 68 percent of US-based companies expected to spend between $1 million to $10 million to meet GDPR requirements. Another 9 percent expected to spend more than $10 million leading to some complaints that it put them at a competitive disadvantage with European Companies. As European companies need to abide by the same rules it is not entirely clear where this disadvantage comes from except that the GDPR regulates the exportation of personal data outside of the EU and many US companies have data centres and support staff in the US.

The GDPR requirements forces companies to change the way they process, store, and protect customers' personal data. For example, companies are allowed to store and process personal data only when the individual consents and for "no longer than is necessary for the purposes for which the personal data are processed." Personal data must also be portable from one company to another, and companies must erase personal data upon request enshrining the concept of the "right to be forgotten".

Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR if they have:

- A presence in an EU country, even if they do not have a business presence within the EU
- No presence in the EU, but it processes personal data of European residents
- More than 250 employees

- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data

GDPR takes a wide view of what constitutes personal identification information so the same level of protection for an individual's IP address or cookie data is required as for sensitive data such as name, address and Social Security number. There is also a problem of interpretation. Companies must provide a "reasonable" level of protection for personal data, although what constitutes "reasonable" is not defined.

The GDPR defines three key company roles that are responsible for ensuring compliance: data controller, data processor and the data protection officer (DPO). The data controller defines how personal data is processed and the purposes for which it is processed. The controller is also responsible for making sure that outside contractors comply. Data processors may be the internal staff that maintain and process personal data records or any outsourcing firm that performs all or part of these activities. Notably it is the data processors who are liable for breaches or non-compliance. A DPO needs to be designated to oversee data security strategy and GDPR compliance. Companies are required to have a DPO if they process or store large amounts of EU citizen data, process or store special personal data, regularly monitor data subjects, or are a public authority.

If a company is non-compliant the GDPR allows for penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher. The difference between a major breach that could cause damage and a minor breach needs to be assessed. Here GDPR places a requirement on companies to perform impact assessments to mitigate the risk of breaches by identifying vulnerabilities and how to address them.

Consumers benefit from getting a lot more information about data breaches. A key requirement brought in by GDPR is that companies must report data breaches to supervisory authorities and individuals affected by a breach within 72 hours of when the breach is detected. Customers know a lot more about how safe their data is and also which companies they can trust with their data.