General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), is a law enforced by the European parliament in European Union (EU) and European Economic Area (EEA) which allows the owners to have full control on their data by assigning obligations on service providers who manage and process personal data. First implemented on 25 May 2018, the law simplifies the regulatory environment for international business by unifying the regulation within the EU.

The provisions are consistent across all 28 EU member states and as per the law, the companies have just one standard to meet within the EU to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. However, that standard is quite high and requires most companies to make a large investment to meet and to administer.

Personal data includes any information related to a person such as a name, a photo, an email address, bank details, updates on social networking websites, location details, medical information, or a computer IP address and all these data are protected through GDPR.

After the implementation of the law, any resident of the EU can demand the following:

- Right to access
- Right to be forgotten
- Right to data portability
- Right to be informed
- Right to have the information corrected
- Right to restrict processing
- Right to object
- Right to be notified

These are some cases which aren't addressed in the GDPR specifically,

- Personal or household activities
- Law Enforcement
- National Security

A company must be GDPR compliant to avoid the penalties attached to it. Companies appoint a data collector, a data protection officer, and a data processor who manage the collection, storage, and distribution of the data and are also responsible for the compliance.

The data protection officer or data controller is in charge of GDPR compliance. Data processors maintain and process personal data records. The GDPR holds processors liable for breaches or non-compliance. They are also responsible for the security measures taken to avoid piracy.

Penalties for those companies and organizations who don't comply with GDPR fines of up to 4% of annual global revenue or 20 million Euros, whichever is greater.

To be a compliance, a organization must::

- Map the company's data
- Determine what data should be kept
- Put security measures in place
- Review the documentation
- Establish procedures for handling personal data

The GDPR places equal liability on data controllers and data processors. All the existing contracts with processors (e.g., cloud providers, SaaS vendors, or payroll service providers) and customers need to spell out responsibilities.

Any freely given, specific, informed, unambiguous, and clear affirmative action by which a person gives permission for their personal data to be processed in a particular way should be asked before accessing the data.

India has followed the EU's General Data Protection Regulation (GDPR) in allowing global digital companies to conduct business under certain conditions, instead of following the isolationist framework of Chinese regulation that prevents global players like Facebook and Google from operating within its borders.

According to recent reports, the Indian government looks set to legislate a Personal Data Protection Bill (DPB), which would control the collection, processing, storage, usage, transfer, protection, and disclosure of personal data of Indian residents.

Indian DPB carries additional provisions beyond the EU regulation. There are a number of features of the DPB that will require companies to change their business models, practices, and principles. Many others will add operational costs and complexity.

Data is a valuable currency in this new world. And while GDPR does create challenges and pain for the businesses, it also creates opportunity. When first announced in 2016, it felt like there was plenty of time for new businesses to take the necessary steps. But the time has flown by and many companies are still scrambling, even after the deadline has passed. Companies who show they value an individual's privacy (beyond mere legal compliance), who are transparent about how the data is used, who design and implement new and improved ways of managing customer data throughout its life cycle build deeper trust and retain more loyal customers.

By:

Prashant

Anjali Singh

MCA 1st Year