| **Date:** 5.6.2018 | **Publication:** Moneycontrol.com |
|---|---|

# A look at what GDPR entails and changes in compliance risk

To understand the risks associated with how information is processed, stored and transferred, an organisation must fully understand the data it collects and processes

Rajeev Kumar

Data is the most valuable asset and the biggest driving force in the digital economy. For most companies and individuals breach of data is their biggest fear. The General Data Protection Regulation (GDPR) that came into effect on 25th May 2018 is arguably one of the greatest shake ups in privacy legislation which seeks to address these issues of data privacy and protection.

All of us have recently started getting notifications to update and check our privacy policy on various social media platforms. We can now choose whether our personal information available on that application can be used further by the company to customise advertisements, share feeds, etc.

All this is mainly due to the GDPR, a comprehensive and strictest European Union Privacy regulation. Let's dive further into what exactly is GDPR and its implication in India.

The GDPR is a landmark piece of legislation in the EU, giving the people enough power necessary to take on the erring corporates having custody of their personal data, by providing stronger data protection and digital privacy laws for EU citizens. It replaces the 1995 Data Protection Directive, the GDPR is an attempt to give internet users more of a say in how their data is used and mandates companies to adhere to strict guidelines on how it is collected, stored, and leveraged.

**Key Areas of Regulation**

This clearly defines data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It also defines "personal data" as any data that can be directly or indirectly associated with a living individual – a very broad scope that now includes, for example, IP addresses.

It provides safe harbour for organisations with strong security measures by providing that "if appropriate technical and organisational measures" were in place to protect the data – specifically calling out data encryption – the company does not need to report the breach.

Notification of breach is applied in the strictest form in GDPR. Companies experiencing a notifiable breach of EU personal data after May 25, 2018, must make notifications without any delay not later than 72 hours after having become aware of it. Recognising companies may not know many definitive facts within 72 hours of detecting an incident, it also allows notifications to be provided in phases.

On whom to notify the GDPR establishes a simpler, two-track model. If a breach of EU personal data poses a risk to the rights and freedoms of individuals, the company must notify its lead data-protection authority (DPA). If the breach poses a high risk to individuals, the company must also notify them.

It prescribes unprecedented fine by penalising failure to comply with the regulation's requirements with fines of up to €20 million or 4% of the offending company's annual global revenue, whichever is higher.

On the post-mortem documentation GDPR require companies who have experienced a data breach to document the facts relating to the breach and remedial action taken to prevent a reoccurrence.

**Action Plan for organisations dealing in EU data**

Raise awareness enterprise-wide

The first step is to raise awareness of the GDPR at all levels of organization. Develop record-keeping and monitor best practices, engage in ongoing training outlining breach scenarios and causes, and create a culture of security across the entire organisation. Ensure that employees not only understand the impact of these new regulations, but that they feel comfortable raising alerts and know whom to approach if there is cause for concern.

Designate a Data Protection Officer (DPO)

The GDPR outlines specific organizations that must formally designate a DPO, including public authorities (except for courts) and private organizations where the core activities consist of processing operations that require regular and systematic monitoring of personal information on a large scale or large-scale processing of sensitive data or data relating to criminal convictions or offenses. EU or member-state law may require the designation of DPOs in other situations as well.

Create a data inventory

To understand the risks associated with how information is processed, stored and transferred, an organisation must fully understand the data it collects and processes. Once a detailed inventory list of data types has been created, each data set should be mapped end-to-end throughout the organisation's technology infrastructure to identify all physical and virtual places where data is held.

Evaluate risk and perform gap analysis

Next step will be to take inventory of data and processes and compare it to the GDPR requirements. Be sure to include third-party suppliers and vendors. Where are the gaps in compliance? Are there areas at risk of non-compliance in the future? What are the most immediate needs the company must satisfy to move toward GDPR compliance?

Develop a roadmap

Having identified all potential GDPR compliance gaps, organization should develop a roadmap outlining required changes to processes and systems to conform with GDPR requirements. Some of these changes may result in the tightening of existing controls, while others may require new controls and processes to be developed.

Monitor and report progress and compliance

The GDPR regulations require "security by design," which mandates that all IT professionals build compliance into the design of future business operations that capture, process or store data. The DPO should work with all necessary business and IT teams to ensure that operational systems and data management workflows remain compliant and stay up-to-date with any GDPR announcements or changes.

**What it means to us in India?**

The world is much more integrated than we think it is. Internet has made it look even smaller. Hence, we have now ITES companies in India rendering the services to customers of foreign companies on real time basis in far off Europe and America. This wouldn't be possible without data sharing by the those fronting organizations and here will be the impact majorly felt with the new regulation coming in force.

Based on the risk appetite, the companies need to review their limits under the E&O and D&O policies and those not having must go for it without any further delay.

Further, as we have seen that such issues of privacy are already being debated and implementation of newer stricter regulations back home is only a matter of time. This clearly would mean that companies dealing with customer data back home need to gear up fast.

Irrespective of whether an organisation is dealing with data of European or Indian citizens, it is important to increase the privacy awareness of employees to ensure they can recognise and respond appropriately to requests from data subjects. Any process for responding to these rights should be clearly documented and embedded into business practices.

- Risk and Compliance department has an agenda clearly cut out for them;
- Review current data-processing activities
- Perform impact assessments to establish whether there is a risk of infringement
- Establish necessary policies and processes to meet all privacy requirements (e.g. security, complaints handling, data accuracy, breach reporting, etc.);
- Update current policies regarding personal data and make the necessary changes to business operations.

Therefore, rather than waiting for a strict regulation to be promulgated, it's important that necessary steps be initiated right away shedding the lax attitude that Indian companies adopt and imperilling the fortunes of the organisation even if one doesn't deal with data of EU customers.

*(The writer is Chief Risk Officer, Bajaj Allianz General Insurance)*