General Data Protection Regulations

General Data Protection Regulations or GDPR is the new Privacy Protection Regulation adopted on 27th April 2016 by the European Union in replacement of the earlier Data Protection Regime. The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue-based. The new Data Protection Act 2018 replaces the 1998 Data Protection Act.

The nucleus of the GDPR is to protect the personal data and privacy of all citizens in the EU. It makes companies accountable for the data it collect, store, analyse and use. The development will not only change the business landscape in the EU but also influence global markets and multinationals.

These privacy regulations which come with restrictions on non-transferability of EU data to non-compliant countries make it highly relevant for countries outside EU also as it could make or mar the data processing industry.

What distinguishes GDPR from the earlier regulations is the high level of penalties envisaged under the regulation which may go upto Euro 20 million (approximately Rs 140 crores) or 4% of global turnover of a company and will be applicable even for Non EU based companies.

7 Key principles for GDPR

- Lawfulness, fairness and Transparency
- Purpose Limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity & Confidentiality
- Accountability

Advantage of GDPR

Improved Cybersecurity: Organisations have been in a continuous battle for almost as long as the internet has existed. Security upgrades in networks, servers and infrastructures have been a primary source of cyber protection along with other policy and security changes until recently. Cybersecurity is not something a business can ignore any longer, and it is not something that they can put on the back burner and "get to later". The GDPR makes sure that increased cybersecurity is made very important for companies to get right, and that is why they have large fines for those who do not get on board.

Business opportunity rather than compliance burden: Indian IT companies serving the EU market, their second largest after the US, would be required to comply with the GDPR. However, rather than seeing this as an additional burden in terms of compliance, Indian companies should see it as a massive business opportunity knocking at their doors.

Provide customer and clients more control over their data : The regulations provide the customers with some measure of peace of mind that they did not have before. It might not be a perfect system, but it is going to be better than what it was. Additionally, companies need to think about the GDPR benefits for businesses. Having leaks and data breaches at a company is going to be bad for business. Not having any breaches will be a sign of trust.

Opportunity to stand out: Over the years, India has become a technology hub equipped with deep expertise and a talented resource pool. The GDPR could be an opportunity for Indian companies to stand out as leaders in providing privacy compliant services and solutions.

Developments in India's privacy landscape: The 'adequacy requirements' under the GDPR allow the European Commission to consider whether the legal framework prevalent in the country to which the personal data is sought to be transferred affords adequate protection to data subjects in respect of privacy and protection of their data. In the wake of recent developments and the Supreme Court verdict, a data protection framework has been proposed by the Srikrishna Committee. It will be interesting to see how the forthcoming legislation shapes up and whether it will satisfy the criteria laid down under the GDPR.

Impact of GDPR on Indian Entities

Europe is a substantial marketplace for the ITeS, BPO and pharmaceutical industry in India. Thus, for the Indian IT industry to keep continuing to do business in Europe, it needs to comply with the GDPR. The GDPR imposes a substantial penalty structure in cases of non-compliances. Clearly, the GDPR would impact the service sector, especially sectors like data entry, customer care, advertising, banking and IT among others. These services cannot be provided to a European client unless the Indian data protection laws are considered adequately rigorous by EU standards or on par with GDPR.

The regulation requires a programmatic approach to data protection and a defensible programmed for compliance will be required to prove that we are acting appropriately. Due to India's relatively weak data protection laws Indian e- services industry would become less competitive and lose its European Market. Indian companies would be required to implement sufficient safeguards, as per the GDPR, to prevent transfer of personal data outside EU geographies.

Preparation for GDPR

Things which are essential for GDPR compliance:

- Review policies, procedures and existing privacy programmes;
- Conduct data discovery exercises and maintain documentation in order to demonstrate visibility of the personal data processed;
- Impart data privacy training to employees or subcontractors;
- Review / Update contracts signed with third – party vendors
- Equipping the security ecosystems with effective identity and access management
- Reviewing data retention schedules, cross-border data transfers, privacy notices, consent, etc.;
- Logging monitoring and incident management solutions;

What are the challenges Associated With the GDPR

The decision to implement the GDPR came with criticism. Those opposed to the new regulation said that the position of the DPOs could be an administrative burden for many EU countries. The guidelines were set to include social networks and cloud provider but did not consider how to deal with employee data. In addition, data cannot be transferred to another country outside the EU - unless it guarantees the same kind of protection - so companies that didn't have this kind of privacy protection would be required to change their business practices. Furthermore, the costs associated with the proposed regulation could also increase over time due to the need for more investment, and general education in data protection is also sometimes required. There was also concern that data protection agencies across the EU would need to agree to a standard level of protection, something that may not be easy as they may disagree in the interpretation of the guidelines.

Accountability & Compliance

Companies covered by the GDPR are accountable for their handling of people's personal information. This can include having data protection policies, data protection impact assessments and having relevant documents on how data is processed. The draft Protection Bill, 2018 has borrowed several provisions from GDPR to ensure that protection laws do not hamper ecommerce transaction between India and EU member countries. For companies that have more than 250 employees, there's a need to have documentation of why people's information is being collected and processed, descriptions of the information that's held, how long it's being kept for and descriptions of technical security measures in place. Organizations covered by GDPR have to hire staff, the person shall report to senior member of staff , monitor GDPR compliance and be a point of contact for the employees and customers. Even if Indian companies do not directly interact with European citizens , they would still require GDPR compliance. This is so because personal data of European citizens have the potential to be exploited for other related data processing activities. If so Indian companies would attract heavy penalty for noncompliance. Apart from convergence between the GDPR and Indian Data protection Bill 2018, the divergence relates to issues like data localization or data stored in an Indian server is mandatory.

GDPR Fines

One of the significant elements of the GDPR has been ability for regulators to fine businesses that don't comply with it. If an organisation doesn't process an individual's data in the correct way, it can be fined. If there's a security breach, it can be fined.

Conclusion :

Today, the information technology Act, 2000 (amended in 2008) provides for data protection through Sections 43A, 72 & 72A. These provisions, along with Information Technology Rules 2011, provides the legal framework to govern data privacy in India. GDPR specifically confers protection to citizens and rights to decide on how their data is processed which is not included in the IT Act. The principles under IT Act 2000 apply to collect of information and its use. Principles listed in the GDPR but not mentioned in IT Act are data integrity, protection from unlawful processing, accountability, fairness and transparency.