THE GENERAL DATA PROTECTION REGULATION AND ITS COMPLIANCE

The General Data Protection Regulation ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It is also meant for dealing with the export of personal data outside the EU and EEA areas. The main objective of GDPR is to give control to individuals over their personal data and to simplify the regulatory environment for international business.

GDPR replaces the earlier Data Protection Directiveand the regulation contains provisions and requirements pertaining to the processing of personal data of individuals inside the European Union, and applies to any company or enterprise that is established in the EU orthat indulges in processing the personal data of people inside the EU. The ones who control personal data must have the required technical and organisational measures to implement the data protection principles.

According to the regulation, business processes that handle personal data must be designed and built in order to provide safeguards to protect data and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed without lawful basis specified by the regulation or unless the entity processing or controlling the data received consent from the owner of the data, however consent can be revoked at any time.

A processor of personal data must clearly disclose that data is being collected, declare the lawful basis and purpose for it, and state how long data is being kept and if it is being shared with any third parties or outside of the EU. Data subjects have the right to request a copy of the data collected by a processor and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities are based around processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

The GDPR was adopted on 14 April 2016, and became enforceable beginning 25 May 2018. As the GDPR is a regulation, not a directive, it does not require national governments to pass any enabling legislation and is directly binding and applicable.In certain cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

The regulation applies if an organisation that collects data from EU residents, or that processes data on behalf of a data controller like cloud service providers, or the data subject is based in the EU. Under certain circumstances, the regulation is also applicable toorganisations based outside the EU if they collect or process personal data of person located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity."

According to the European Commission, "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical

information, or a computer's IP address." The precise definitions of terms such as "personal data", "processing", "data subject", "controller" and "processor", are stated in Article 4 of the Regulation.

Since the regulation covers all the EU member states and citizens, all global enterprises with operations or customers in EU must comply. Europe is a significant market for the ITeS, BPO and pharma sectors in India, therefore companies in India in relation to the EU must satisfy the GDPR compliance.

In order to show compliance with the GDPR, the data controller must implement measures that satisfies principles of data protection as a defaultoption. Dataprotection by design and by defaultmandates data protection measures to be designed into the development of business processes for products and services. Such measures include using fictitious names for personal data. It is the responsibility and the liability of the data controller to implement efficient methids and be able to show the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller

In order to collect data, data subjects must be told clearly about the extent of data collection, the legal basis for processing of personal data, how long data is retained.If the collected data is being transferred to a third-party and/or outside the EUthis must be clearly told to the data subjects and disclose any automated decision-making that is made on a solely algorithmic basis.Controllers should also make the data subjects aware of their privacy rights under the GDPR, including their right to revoke consent to data processing at any time, their right to view their personal data and access an overview of how it is being processed, their right to obtain a portable copy of the stored data, the right to erasure of data under certain circumstances, the right to contest any automated decision-making that was made on a solely algorithmic basis, and the right to file complaints with a Data Protection Authority.

Data protection impact assessments have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the data protection authorities is required for high risks.

Europe is a substantial marketplace for the ITeS, BPO and pharmaceutical industry in India. The size of the IT industry in the top two EU member states is estimated to be around 155–220 billion USD. 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 penalty structure of 20 million EUR or 4% of global turnover in cases of non-compliances.The regulation requires a programmatic approach to data protection and a defensible programme for compliance will be required to prove that you are acting appropriately.

India’s outsourcing industry, which is estimated to be worth over 150 billion USD, contributes nearly 9.3% of the GDP. The EU has been one of the biggest markets for the Indian outsourcing sector and India’s relatively weak data protection laws make us less competitive than other outsourcing markets in this space.

Also largely inflexible, the GDPR reduces the extent to which businesses can assess risks and make decisions when it comes to transferring data outside the EU. Indian companies would need to implement sufficient safeguards, as required under the GDPR, in order to transfer personal data outside the EU, thereby further increasing compliance costs.

Article 3 of the GDPR makes it clear that the regulation will be applicable regardless of whether or not the processing takes place in the EU. This means no business for Indian companies that do not comply

with the GDPR or increased compliance costs for those who do and the risk of huge penalties on failing to do so.

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