General Data Protection Regulation: A Summary Guide

What is the GDPR?

Recognizing and harmonizing the fundamental right of individual with respect to the protection of their personal data, the General Data Protection Regulation("GDPR") is the new set of privacy laws that have come into force in the European Union since 25th May, 2018.

GDPR has been envisaged as the regulation that brings under its ambit all matters concerning personal data of individuals within the Union, and prescribes the need for an explicit consent, lawful and transparent processing, notification for personal data breach and increased fines, in the event of breach of the regulation and accordingly, has a huge impact on the organisations collecting, processing and storing personal data.

Who are covered by GDPR

GDPR is applicable on all entities that conduct business within EU, are established in the EU or have presence in the EU via subsidiaries etc. Further, even companies that collect process and hold personal data of individualswho are in EU at the time of collection and processing of such personal data, even if they are established outside of the EU, need to comply with GDPR.

Various multi-national companies (MNCs) have their backend offices or development centres established in India, which access data of customers globally, including that of EU residents.Further, Europe also serves as a customer for the Indian IT companies. As such these companies and offices hold and process delicate personal data of individuals in Europe, they too need to be compliant with such norms.

Hence, under the GDPR, an organisation, irrespective of its geographic location, offers goods and services to individuals in EU or where it monitors the behaviour of individuals in EU, it needs to ensure compliance with it. In light of the above, Indian companies need to comply with GDPR wherever they undertake the aforementioned activities in relation to residents in EU.

Therefore a company that falls within the ambit of the above has to ensure that they are in compliance with the GDPR or risk paying hefty fines as penalties,as prescribed under the regulation,which could be as high as €20 million or 4% of the global annual turnover, whichever is higher. This is the highest fine that could be imposed under the GDPR for serious violations such as lack of customer consent or violation of an individual's rights. However, for violations such as not conducting an impact assessment or not maintaining proper records of the processing activities undertaken, amongst others, the amount of fine prescribed is 2% of the global annual turnover or €10 million, whichever is higher.

Compliance: GDPR has introduced the definition of the term "**consent**" which plays a pivotal role in redefining the functions of the corporations that collect and process data. Consent has been emphasised upon greatly in GDPR so as to ascertain the fact that the individual whose data is being collected knows what data is being collected, what is the purpose of the collection of the data as well as for how long this data will be used or stored. Only when the individual is aware of all the related facts canand the company can prove that the individual has consented to all the terms and conditions in accordance with which the company can use such data. This in turn means that all the data previously collected without such consent from the individuals cannot be used for any sort of processing or even be stored. Companies require fresh consent to be taken from each individual whose data is being stored or processed and this consent needs to be in line with the definition of consent provided in GDPR.

GDPR also provides for a further classification of data into specialised categories of personal data which includes, *inter alia*, racial or ethnic origin, biometric data, and health data, genetic data that should not be processed except without obtaining the explicit consent of the individual concerned or in accordance with the provisions laid down in this behalf in GDPR. This ensures that the sensitive data of an individual is not encroached upon by the organisation and the individual can protect his privacy and data.

The Regulation also provides certain principles that need to be kept in mind while conducting activities such as collecting, processing or storing personal data of individuals in the Union. These include the following:

- **Lawfulness, fairness & accountability** - The data being processed should be done lawfully, fairly and in a transparent manner;
- **Purpose limitations -** The data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

- **Data minimization -** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are being processed;
- **Accuracy** - Every reasonable step should be taken to ensure that the data processed is accurate and kept up to date;
- **Storage limitation** - The data shall not be permitted to be stored for a period longer than necessary for the purpose for which the data is being processed.
- **Integrity & confidentiality** - Utmost security and confidentiality shall be maintained with respect to the data which is being processed to protect it against any unauthorized or unlawful processing.

These principles should be incorporated within the companies' policies' in order to integrate data protection and **privacy by design**. Over and above these principles GDPR also provides for certain Code of Conduct that can be looked at for guidelines as to ensuring the company has an airtight system to prevent any data breaches. Further, the appointment of a **Data Protection Officer** could be another way to not only safeguard, but also to demonstrate compliance, which again is a major part of GDPR. A Data Protection Officer acts as the point of contact between the individuals whose data is being collected and the company collecting the data as well as the company and the governing bodies in the Union.

While acknowledging and maintaining the sanctity attached with the personal data of individuals, the regulation also empowers competent authorities to process such personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In view of this the GDPR seeks to maintain a balance between individual rights and legitimate requirements of using personal data.

Rights of individuals:

Rights of individuals have been emphasised greatly in GDPR and the following rights can be exercised by an individual in relation to his personal data under GDPR:

- **Right to erasure of personal data**: If an individual whose data was collected while he or she was in the Union wishes to get the data removed from the database of the company, then the company is bound to remove such data as soon as possible. Further, where there is no legal ground available with the organization for undertaking processing, it shall be obligated to erase the individual's personal data. However, an individual's right to erasure of personal data is not absolute and is subject to certain exceptions such as

exercising right to freedom of expression and information, for compliance with a legal obligation, establishment or exercise or defence of legal claims etc.;

- **Right to withdraw:**Withdrawal of consent is also something that needs to be understood properly. The consent given by an individual can be withdrawn at any time. GDPR has made it very clear that withdrawal of consent needs to be as easy as giving consent. Essentially, if consent is being given by the way of sending an email or ticking a box, then withdrawal should also be just as easy;

  Right to information and access to personal data: The individual has a right to be informed about the purpose of processing, categories of personal data being processed; period for which the personal data shall be stored etc. by the organizationand shall have a right to access such personal data. The information provided to the individual must be concise, transparent, easilyaccessible and it must be in a clear and plain language. Additionally, the individual also has a right underGDPR to be provided with the contact details of the data protection officer and the details of the organization processing such data;
- **Right to rectification**: The individual has a right to get the inaccurate personal data in relation to him/her corrected or to get the incomplete data in relation to him completed;

- **Request the restriction of processing of personal data:** A right to ask the company to suspend the processing of personal data; where the individual is of the opinion that the personal data is not accurate or such processing is unlawful. Upon exercise of this right by an individual, an organization must stop processing an individual's data; however, it can continue to store such data;

- **Right to data portability:** An individual has a right to transmit or request the transmission of the data stored with an organization to another organization in a structured, commonly used and machine-readable format;

- **Right to object:** An individual shall have a right to object to the processing of personal data and the organization shall not continue with such processing unless it shows certain compelling legitimate grounds for continuing with it.

The GDPR also provides for a breach notification to be made to the supervisory authority by the organisation concerned, within 72 hours of becoming aware of such breach, wherever a data breach is likely to result in a risk to the rights and freedom of individuals.

Further, for children under age of 16, a person holding parental responsibility must consent to the processing of personal data of such a child. Moreover, to extend sufficient safeguard to the processing of an individual's personal data, the regulations also provide for 'Data Protection Impact Assessment' to be undertaken wherever the data is subjected to high risk arising out of such processing.

Essentially, GDPR is a regulation that not only brings aboutchanges in the Union but affects businesses outside of the Union greatly too. All in all, GDPR seems to bring a big change in the world of data protection & privacy laws and could have a far reaching impact on organisations globally.