Volume II Issue II ISSN NO : 2582-6034

LEGALFOXES LAW TIMES

IMPACT OF GENERAL DATA PROTECTION REGULATION (GDPR) ON INDIAN COMPANIES

By Evlyn Nisha Hamshavarshini

INTRODUCTION

GDPR stands for General Data Protection Regulation. It is a legal framework that sets guidelines for protection and processing of personal data and information. It also contains principle for the data management and the rights of an EU citizen/individual, while imposing fines which can be revenue based in nature. General Data Protection Regulation adds to the general policy of protecting its citizen's privacy. It incorporates stringent and binding regulations, backed by sanctions and finesup to 4% of a company's annual global revenue. This regulates within the territories of 28 European States which are the member states of the European Union. The GDPR was approved by the EU Parliament on 14th April, 2016 and it was enforced on 25th May, 2018. Data helps every company differentiate itself from other and gain a competitive edge over others. Every person who has data and information of an EU citizen, shall/must comply with the regulations of General Data Protection Regulation.

The guidelines and regulations in General Data Protection Regulation are mostly similar to those of EU's Data Protection Directive, 1995. The former data protection law was brought into force before the age of instant internet and social media, which now has a greater impact and importance in every individual's life. So, the basic motive of bringing GDPR into force was to protect every EU individual's personal data and information in the recent modern times of internet and social media. The nature of GDPR is of regulation and not of directive, that means it applies directly and automatically without needing to be changed into law.

WHO IS GENERAL DATA PROTECTION REGULATION APPLICABLE TO?

It applies to almost every organization and individual who deal, control or process with data related to EU citizens. The EU individual who's data is involved does not necessarily need to be a consumer, the individual can be anybody's own staff too. It is automatically applicable to every EU citizen in or out the territories of European States. Organizations don't have to be based in Europe to be in compliance with GDPR. It is sufficient to process and hold data related to EU residents. Based on your role in collecting or processing data, the data regulation will classify you as either the data controller or data processor.

DATA CONTROLLER : A data controller as the name suggest , controls the overall purpose of this data protection regulation. He emphasizes and defines the "how and why" of data processing but it is not necessary for him to carry out all these activities by himself, as there may be situations where he needs to use an external service to process the data. In such cases, the data controller allows another company to process the data which does not mean that the over all control is also transferred, as the main control and power remains with the data controller.

DATA PROCESSOR : On the other hand, data processor is the organizations that process data on behalf of the data controller. The data processor does not get to change the purpose of the data and does not have control over the data as it lies with the data controller.

IMPACT ON INDIAN FIRMS AND COMPANIES

Article 3(1) of the General Data Protection Regulation clearly states that:

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. [1]

The territorial scope of the General Data Protection Regulation clearly states the meaning of GDPR to Indian companies and companies of other countries by virtue of Article 3. Hence,

[1]General Data Protection Regulation

companies and organizations outside the European Union, are bound to enhance and refurbish their regimes as well as their technologies which includes introduction of new practices and encryption system to protect the privacy of data. Refurbishing and upgradation of policies are to meet up the standards of the new Data protection regime of European Union.

According to the European Commission, the law applies to a company or an entity which processes personal data as part of the activities of one of its branches established in the EU[2], regardless of the fact that where the data is processed. Non-compliance of General Data Protection Regulation rules can cost to a fine of20 million Euros or 4% of annual turnover. It also applies to any company which provides goods to any entity based in EU. If any Indian company happens to monitor the behaviour of any EU entity or EU resident, it has to follow the GDPR as it is automatically binding. This can not only be looked upon as a risk bearing and resource exhausting factor but most importantly an advantage to the companies with GDPR compliance as it secures an trustworthy business process.

The few things the companies have to consider as an integral part of their compliance to the General Data Protection Regulation are:

- The policies and strategies should be thoroughly reviewed and upgraded according to the requirement of the European Regime.
- The usage of latest technology which is the minimum requisite of the GDPR, like Pseudonymisation[3] and encryption codes which are required to process the data. The European Union Agency for Cybersecurity has given a detailed guidelines [4] for shaping technology according to the provisions of the GDPR separately.
- Provide the necessary training to the employees in regards to the data privacy standard requirement.

[2]Who does the data protection law apply to? | European .... https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

[3]Pseudonymisation is a well-known de-identification process that has gained additional attention following the adoption of GDPR, where it is referenced as both a security and data protection by design mechanism. In addition, in the GDPR context, pseudonymisation can motivate the relaxation, to a certain degree, of data controllers' legal obligations if properly applied

[4]https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport#:~:text=Pseudonymisation%20is%20the%20processing%20of,and%20organisational%20measures%20to%20ensure

- Proper set of documents have to be maintained to show transparency of the personal data that are processed by the companies.
- A better understanding of the rights of the Data subjects ought to be imparted to the employees and subcontractors if they are planning to process the data of the citizens of the European Union.

CHALLENGES FACED BY INDIAN COMPANIES

The EU has been one of the biggest outsourcing sector for India and the enforcement of General Data Protection Regulation results in a weak data protection law which is less competitive than other outsourcing sectors in the world. Moreover the is a large inflexibility in transferring data outside the EU, until India upgrades to sufficient safeguard measures. As an alert to Indian organizations, Article 3 of the General Data Protection Regulation makes it clear that GDPR is applicable regardless of whether or not the processing takes place in EU. That being said, it is quiet evident that there is no business to Indian organizations until they comply with GDPR or increased compliance costs for those who do and the risk of huge penalties on failing to do so.

The basic idea of introducing General Data Protection Regulation is to protect the control and process of personal data of EU residents. This regulation proves to be a challenge to Indian companies and entities as the majority of them deal with EU organizations. If any organization is dealing with any of the data related to EU residents, they have abide with the regulations of GDPR, failing to do so can cost a huge fine to the entity. One of the main aspect is portability of customer data i.e. what can be shared and what cannot be with/without the consent of the person to who the data is related to.General Data Protection Regulation is both an advantage and disadvantage to the Indian business sector. It has risk bearing factor as well as opportunity providing factor. Compliance with GDPR gives the companies an opportunity to stand out among other companies. Not only the business sector but this helps in the development of India's legal frame work for privacy related laws, as a new data protecting framework has been proposed in SrikrishnaCommittee.'

One of the main concern about the Indian company is that the data protection law in India is comparatively weaker. India's outsourcing industry, which is estimated to be worth over 150

billion USD, contributes nearly 9.3% of the GDP.[5] Europe has one of the biggest outsourcing industry and the weaker law of data protection in India is less competitive than other markets.

SOME IMPORTANT TERMS

These terms are in reference to consider while looking for matching up to the requirements of the general data protection regulation. Few of the terms are:

1. **Personal Data** – This is the broad term used for any details and information related to an individual or a Data Subject, which will be used directly or indirectly to identify the person involved. This can be anything, for say a name, an address, a fingerprint or banking details.

2. **Binding Corporate Rules (BCRs) -** The bundle of internal norms adopted by the multinational companies to define and expound their global policies on international data transfers within the same corporate group and then with the countries which doesn't have the same level of data protection regulation system.

3. **Processing** – An automated or manual action performed on personal data, for example collection, organization or recording.[6] For processing of personal data to be lawful under the GDPR, businesses must identify a lawful basis for this action.

4. **Data Controller** - This is the person who decides the objective for which the personal data has to be processed. Along with this the way in which the data has to be processed is decided by the data controller. The data controller can either be one person or a group combined.

5. **Data Processor** –The data processors are the third parties that are entitled to process personal data on behalf of the Data controller and this entirely includes the Information Technology services

6. **Consent** - The concept of "consent" is foundational to EU data protection law. In general, the validly obtained consent of the data subject will permit almost any type of processing activity, including Cross-Border Data Transfers.

[5]https://blogs.dsci.in/eu-gdpr-part-i/
[6]Privacy Policy | Pixomondo. https://www.pixomondo.com/privacy-policy/

7. **Data Protection Officer -** A Data Protection Officer is someone who is given formal responsibility for data protection compliance within a business. Not every business will need to appoint a data protection officer – you need to do so if:

- Your organization is a public authority; or

- You carry out large-scale systematic monitoring of individuals (for example, online behavior tracking); or

- You carry out large-scale processing of special categories of data or data relating to criminal convictions and offenses.

8. **Data Protection Authority (DPA)** – Every country will have its own DPA, a national authority responsible for the protection of data and privacy as well as implementing and enforcing data protection law.[7]For example, in France it's the Commission nationale de l'informatique et des libertés (CNIL) and in the UK it's the Information Commissioner's Office (ICO).

9. **Biometric Data -** Personal data that resulted from specific processing related to physical and behavioral features of a person, which allows the identification of that person.

10. **Data Subject** – When a piece of data relates to an individual, then they are known as the data subject. This could be you, me or anyone as long as they can be clearly identified from the data in question.

11. **Right to be Forgotten -** The right to erasure of personal data or 'the right to be forgotten' enables an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

12. **Pseudonymous Data -** Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data to be re-identified. A good example of pseudonymous data is coded data sets used in clinical trials.

[7]GDPR key terms and facts uncovered | W1 Virtual Office. https://w1virtualoffice.com/gdpr-key-terms-and-important-facts-uncovered/

13. **Cross-Border Processing -** Processing of personal data when the controller or processor is established in more than one Member State, and the data processing takes place in more than one Member State, OR processing activities that take place in a single establishment in the Union, but that affects data subjects from more than one Member State.

CONCLUSION

The European Union has introduced a stronger enactment to protect the personal data of its citizen which happens to be their own privacy rights. This new enactment has restricted the processing of personal data which has a good chance of restricting trade and cause serious damage to the trade markets. The Indian standards of data protection in comparison to the European regime is weaker and needs a serious upgrade. The Indian companies have a strong base of customers in the European Union, which can injure the Indian markets if the companies fail to meet up the requirements of the General Data Protection Regulation. The main challenge is the fear of losing business and to retain business and trade the Indian government has come up with new set of personal data protection laws which might improve and further boost the international trade.