General Data Protection Regulation and its Impact on Indian Companies

Introduction

General Data Privacy Regulation more commonly known as GDPR came into effect on May 25th 2018 after thousands of proposed amendments to change the data protection laws and a herculean task to replace the outdated legislation preceding it, EU Data Protection Directive 95/46/EC. It is related to the quintessential element around which our modern day life revolves i.e. data and its protection. It covers both the citizen and the businesses in EU allowing them to reap the benefits of digital economy. Firstly, these new set of rules are designed to give EU citizens control over their personal data from uploading and erasing of data to reporting of data breaches. Secondly GDPR emphasizes enhanced supervision over businesses and companies controlling client's data. The law has changed the rule for the companies that are involved in the collection, storage and processing of large amount of data of the residents of the EU. These companies are required to abide by the rules laid down for the data protection and privacy of EU citizens for inter EU transactions. GDPR also covers transaction outside EU relating EU citizens and companies and also exportation of personal data outside EU.

Coverage and Application of GDPR

What does GDPR govern?

The major question creating upheaval amongst businesses or service providers is whether the current law applies to them or not. GDPR applies on Data Controller and Data Processor. It regulates the processing of personal data from the processor by the controller. Personal data means any information that relates to an identified or identifiable living individual. GDPR regulates the processing of information by individual, company or an organization. Examples of personal data include name and surname, home address, an email address such as name.surname@company.com, identification card number, location data, Internet Protocol address, cookie ID, or advertising identifier of a phone and data held by a hospital or doctor, which could be a symbol that uniquely identifies a person. It applies when-:

1. The GDPR applies if a data controller or a data processor has an establishment in the European Union and processes personal data, regardless of whether the processing takes place in the European Union. For example, a company established in European Union and providing services to customers outside the EU and processing and controlling the data of the natural persons.

2. The GDPR also applies if a data controller or a data processor is not established in the European Union and processes personal data of data subjects who are in the European Union, where the processing activities relate to (a) offering goods or services to such data subjects in the European Union, whether for payment or for free or (b) monitoring their behaviour within the European Union.
3. It applies to companies or businesses offering goods and services to data subject of European Union which can be apparent by use of languages used in EU or the mention of the subjects of the EU. Some other apparent indication for implication of GDPR are
4. Using a language in the website indicating connection with EU;
5. Delivering services to EU states;
6. Denoting prices in EU currency in the website;
7. Advertising targeting individuals in EU;
8. Domain name having references to EU;
9. Reference to customer base in EU.

What does GDPR not govern?

1. A company provides services outside EU to subjects outside EU even if the clients use the services while travelling outside the country including within EU;
2. For small and medium-sized enterprises (SMEs) processing personal data with no core activity of creating risk for individuals or processing of personal data, some of the rules of the GDPR does not apply to the it such as appointing a Data Processing Officer;
3. It does not apply to data of legal entities;
4. When an individual flourishes such information for purely individual purposes at his home with no connection to a professional unit;
5. It does not apply to information of deceased persons;
6. It does not apply to activity concerning national security;
7. Processing of data by competent authority for investigation purposes, prevention, detection and prosecution of a criminal offence;
8. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making;

9. Member states diplomatic mission or post.

Obligation and Liability of the Companies

At the core of the GDPR is the value of the fundamental right to privacy provided to every individual in the EU. For this companies and business entities need to abide by certain regulations and fulfill certain obligations.

Obligations of the Companies/ Rights of the data subjects

1. **To establish a representative within the EU-** If a company is not established in the EU and processes the personal data of the members of the EU, the company is required to establish a representative (legal or natural person), in the member EU nation where the data is situated. The obligations of the company must be represented through this representative.
2. **Appointment of a Data Protection Officer –** According to Article 37(1), designation of DPO is required by a data controller or processor when:
3. Processing carried out by public authority or body (except for courts)
4. Processing activity which inherently requires large-scale regular and systematic monitoring of data subjects.
5. Processing activity which consists of large scale processing of data with respect to data on racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic or biometric information identifying the individual, health and sex life or sexual orientation; or personal data relating to criminal convictions and

Protecting the rights of the individuals

Under the rules of GDPR certain rights have been prescribed for the protection of the interest of the individuals for protection of the right to privacy. The rights of the data subjects are contained in chapter 3 Section 1, 2, 3 and 4 of GDPR.

1. Right to transparent information, communication and modalities for the exercise of the rights of the data subject (Art. 12);
2. Information to be provided where personal data are collected from the data subject (Art 13.);
3. Information to be provided where personal data have not been obtained from the data subject (Art 14);

4. Right of access by the data subject (Art 15.);
5. Right to rectification (Art 16);
6. Right to erasure ('right to be forgotten')(Art 17);
7. Right to restriction of processing of personal data(Art 18);
8. Right to be notified regarding rectification or erasure of personal data or restriction of processing (Art 19);
9. Right to data portability (Art 20);
10. Right to object to processing of personal data(Art 21);
11. Right to automated decision making including the right to profiling (Art 22).

Responsibility of the controller

The GDPR has outlined certain general obligations of the controller in respect of personal data under Article 24.

1. To implement appropriate technical and organizational measures to ensure and demonstrate compliance under the GDPR;
2. Implement appropriate data protection policies;
3. Adherence to codes of conduct (Article 40 prescribed under the GDPR or approved certification mechanism (Article 42) to demonstrate

Liabilities of the Companies

There are two categories of fine for non-compliance with the rules of GDPR. These are category A fines and Category B fines.

Category A fines – These fines include failures with the implementation of data protection compliance. These fines relate to administrative or preparedness failures. These includes:

- Not executing a proper Privacy Impact Assessment
- Lacking a designated Data Protection Officer
- Issues with breach notifications to a Data Protection Authority or to data subjects
- Failure to implement GDPR by 'design and default'.

These fines have a cap of £10 million or 2% of worldwide annual turnover, whichever is greater.

Category B fines

These fines address actual breaches and major failures of GDPR compliance. This includes things such as:

Conditions for consent (in obtaining or processing data, etc.)

- Lawful processing of data
- Right of access by the Data Subject (Subject Access Requests)
- Right of erasure (right to be forgotten)
- Right of rectification (accuracy of legally obtain personal data)
- Processing of a National Identification number
- Obligations of Secrecy

Fines can be up to €20 million Euro or 4% of worldwide annual turnover, whichever is greater.

GDPR comparison with its predecessor Data Protection Directives Directive 95/46/EC

GDPR came into force after repealing the obsolete law pre-existing before it. The directive that was existing since 1995. The Data Protection Directive is superseded by the General Data Protection Regulation (GDPR), which was adopted by the European Parliament and European Council in April 2016 and will become enforceable in May 2018. The new regulation expands upon previous requirements for collecting, storing and sharing personal data and requires the subject's consent to be given explicitly and not checked off by default. The major differences between the GDPR and Data Protection Directive, Directive 95/46/EC are that the

1. Data Protection directive being a directive was not binding on the member states and the states can implement these directives accordingly whereas GDPR is a uniform binding regulation;
2. GDPR provides a broad definition of personal data which refers as any information used to identify an individual that can be used individually or in conjunction with some other information. This strict definition was not provided by Data Protection Directives, under which the 28 member can imply the definition of private data according to their own norms;

3. GDPR has a truly global impact in comparison to DPD as GDPR also applies to companies outside EU which deals with storage of information of EU subjects;
4. GDPR has financial repercussions in terms of fines for its non-compliance.
5. Focus on individual rights under GDPR is intense in comparison to DPD.
6. Under GDPR both the data controller as information gatherers and data processors as information managers are jointly responsible for complying with the new rules.

Impact of GDPR on Indian Companies working on global level

GDPR will have impact on organizations if they have

1. Operations in EU.
2. Third parties operating in EU.
3. Serving the EU customers.

These companies need to understand the law and be ready for the compliance otherwise they will face severe penalties, this will simultaneously provide opportunity for growth for companies who comply well with the GDPR. GDPR is a regulation and not a directive and therefore it does not require an enabling statute in each member states and will apply to players whose activities target the EU data subjects.

Impact of GDPR on IT sector / BPOs

Data Protection law of Europe may have critical impact on Indian companies especially the IT sector and the BPOs as it will have a multinational impact on companies all over the world. The EU continues to be a significant market for the IT/BPO industry in India. The top two EU member states—Germany and France—represent nearly half of the European IT Services market, which industry experts conservatively peg at around USD 155-USD 220 billion. IT sector will be the first to be affected by the new data protection law of Europe. Europe caters the need of a larger section of Indian IT sector by providing outsourcing avenue, so if Indian companies comply with the GDPR, it will open up the door of opportunities.

Impact on E-Commerce

Most E-commerce companies having European clients will have to comply with the GDPR If you are an e-commerce company with ties to the EU, it is perhaps time to:

- analyse how you collect data and check if it complies with the GDPR
- re-examine how you process any data that you collect
- ensure that retention periods comply with the new law
- implement systems that protect individual rights over data
- examine whether you need to appoint a representative or a data processing officer or undertake a data protection impact assessment

How compliance can be done?

1. **Updating the user policies –** The first and foremost step required for the compliance of the GDPR will be to update the policies. Companies are now flooding the e-mails of their clients with mails of updated user policies. The effect of GDPR will be seen on big giants such as Facebook, WhatsApp, twitter and various other online portals catering EU subjects and a way forward has already been seen as these giants have already updated their user policies even for non- EU residents. The websites with updated user policies have disclosures such as What kind of information is collected, explicit mention of what the data is used for, who they share it with, and an email ID to which users can write to, to delete their data. For Indian markets legal complications over the “personal data” still exists so it becomes difficult to comply with the law.
2. **Educating and training of the staff-** The companies need to train and educate their staff and make them market ready for any compliance of GDPR. This will require companies to educate and train all its stakeholders and also reassess and significantly redesign its business processes and controls in activities ranging from sales & marketing, pre- sales & project costing to data acquisition, data processing, data management (retention and purging) to compliance and reporting

1. **Policy framework ensuring consent –** Consent is “freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;” There must be compliance by the companies in terms of a policy framework to include the concept of “explicit consent”, i.e., consent has been sought from the customers before uploading any data. It is valid to take eplicit consent under GDPR. It will be a priority for all the organizations to obtain valid consent. In simple terms, here are the conditions of valid consent under the GDPR:

- Consent needs to be freely given.

- Consent needs to be specific, per purpose.
- Consent needs to be informed.
- Consent needs to be an unambiguous indication.
- Consent is an act: It needs to be given by a statement or by a clear act.
- Consent needs to be distinguishable from other matters.
- The request for consent needs to be in clear and plain language, intelligible, and easily accessible.

Reporting personal data breaches – The companies must report the data breaches within 72 hours of breach. In case the data breached is encrypted there will be exemption for breach even if it is done maliciously.

Right to be forgotten aspect of data protection law: Its Implications

Right to forget is a much debatable topic in the light of the right to privacy gaining much highlight in India. The Right to be forgotten allows EU Citizens / residents have the right to obtain from the data controller the erasure of personal information concerning him or her without undue delay. In practice, this means that such data would have to be deleted from the controller's environment and if the controller has made the information public, the controller would have to ensure the erasure of links to the information. Article 17 of the GDPR outlines the different circumstances under which individuals can exercise the right to be forgotten. Individuals can require data to be 'erased' when the personal information is no longer required for the purpose it was collected or there is no legal basis for processing the personal information or where the data subject has withdrawn consent. Controller is liable to perform erasure of the data without delay taking into account the available technology, and cost of implementation even if personal data has been made available to the public.

GDPR will help India in implementing its own data protection law

In India legal principles regarding protection of data are contained in IT Act, 2000 and which prescribes punishment for offenses related to personal data security breach. The security of the personal data comes under the purview of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). In addition to the IT Act and the SPDI Rules, depending on the entity collecting the data and type of data collected, several other India laws can also come into play when it comes to data protection. For instance, collection of financial information (such as credit card, debit card, other payment instrument details) is primarily regulated under the Credit Information Companies (Regulation) Act, 2005 and regulations framed thereunder along with the circulars

issued by Reserve Bank of India, from time to time. In the telecom sector, certain data protection norms can be found in the Unified License Agreement issued to Telecom Service Providers by the Department of Telecommunications, and to deal with unsolicited commercial communications, the Telecom Commercial Communications Customer Preference Regulations, 2010 have been formulated. Data protection norms for personal information collected under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 are also found in the Aadhaar (Data Security) Regulations, 2016, which impose an obligation on the Unique Identification Authority of India (UIDAI) to have a security policy which sets out the technical and organizational measures which will be adopted by it to keep the information secure.

The government of India is further seeking to strengthen its data privacy laws for which a committee of experts under Justice Sri B. N Krishna had been formulated to make suggestions and present a draft Data Protection Bill. It also presented a white paper to the people to present the suggestions and now India is in the verge of formulating a new draft Bill. It is estimated that with the coming into force of the General Data Protection Regulation, it will have an impact on the data protection laws of the nations world including India. India can borrow a larger part of the provisions of the GDPR including the much debatable “Right to be Forgotten” aspect highlighted in Article 17 of the GDPR. The regulatory framework of these regulations become binding on many Indian companies coming in the ambit of the rules for governing of the GDPR and thus will have a greater impact on the data protection regulation legislations of India.

Conclusion

General Data Protection Regulation of the European Union is imperative in nature as it has a global impact, binding not only just member EU states but also such players and companies of the non EU countries who have business or data processing connections with the EU. GDPR has provided an umbrella regulation to govern all processing of personal data and thereby providing universal definition of personal data which was not established yet. This law being a regulation does not need an enabling statute to be binding. Ever since after the coming force of these regulations, there have been haywire all around the world with companies monitoring the behaviour of people within EU. The mails of individual subjects of the companies being flooded with mails of updated user policies. This major flush of mails and stringent abidance by the companies is due to a deterrence of a heavy financial penalty up to 4% of the annual turnover. To be fair, companies in Canada, Singapore and China are even less prepared. Companies in India coming under the ambit of GDPR need to abide by its regulations. There needs to be major policy changes, appointment of a local representative in the member EU states, regulation of data breaches and its reporting within 72 hours. GDPR can have indirect effect on India’s approach toward data protection and security of personal data,

especially with the Aadhar, a 12-digit unique identification number, which is a hot topic of constant debate. The legal challenges in the implications of Aadhar and questions on its being mandatory, actually led to the Supreme Court having to explicitly declare that privacy is in fact a fundamental right. Only time will tell whether Indian companies manage to be out of the woods or fail, all in all GDPR is need of the hour despite it being far from perfect.