Privacy laws of digital India: Need to gear up to EU's GDPR

1. Introduction

"Privacy" has become the buzz word these days. From the recent Cambridge Analytica scandal or Aadhar linkage to third party sharing of users' data by WhatsApp, every issue related to invasion of privacy is making news. Innumerable transactions require extensive personal information. Data banks are increasingly being created and used to understand the market in the most optimum way. In fact, the way market is shaping up, a lot of personal information is available with various disconnected businesses. Globally too, economic and social integration of markets require substantial amount of cross-border flow of data. So, when data has become such an integral part of day to day dealings, there is need for laws to protect privacy. The current laws dealing with technology is Information Technology Act, 2000 and the different rules framed thereunder. One such set of rules are contained in the stand-alone Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**IT Regulations**") which have a very limited scope; they only protect an individual's "*sensitive personal data*." In the newsletter of February 2017[1], this issue was discussed where it was highlighted that it is high time when India takes a cue from the EU's exhaustive General Data Protection Regulations ("**GDP Regulations**").

This newsletter gives a brief overview of the GDP Regulations and underscores how the legal framework of India is deficient as compared to these regulations.

2. Brief overview

The GDP Regulations harmonize various data privacy laws across Europe and reshape the way organizations, including those in India, will have to approach data related to people in the EU.[2] They were approved and adopted by the EU Parliament on April 27, 2016 and will come into effect after a two-year transition period i.e., from May 25, 2018. Basically, EU's current data protection regime is set out in directives which are akin to guidelines which require member states to interpret and transpose them into their laws. Inevitably, multiple interpretations by different member states has created inconsistency with respect to data protection compliances across the continent and organizations doing business in the EU find it difficult to deal with such complexities. GDP Regulations address this issue by removing the need for national implementation and introduce an element of consistency in EU's data protection regime.

Article 3(1) of the GDP Regulations limit their scope to processing personal data of people in the EU and in the context of any commercial activity in the continent. This means that the regulations protect personal data of people[3] in the EU and extend protection to data within EU. So, for instance if an EU citizen gives his credit card details for a transaction in the US, the GDP

[1] See http://psalegal.com/E%20Newsline%20February%202017.pdf
[2] On March 29, 2017, UK notified EU of its intention to withdraw from the Union. As per European Commission's notification dated January 9, 2018, the GDP Regulations cease to apply to the United Kingdom from March 30, 2019
[3] In this article, the word "people" refers to every data provider within the territory of EU, irrespective of their nationality and citizenship

Regulations will not trigger. However, if a U.S citizen in the EU gives his credit card details for a transaction in the EU, then the company taking his information will have to ensure that the privacy of the details is maintained as per the GDP Regulations. In other words, in this instance the situs of the company assumes importance. The Regulations prescribe a heavy penalty of up to USD 2.4 million[4] or up to 4% of the total global annual turnover of the preceding financial year, whichever is higher for any breach of data privacy of EU citizens.

3. GDP Regulations vs. IT Regulations

Both GDP and IT Regulations are supposed to safeguard data of people from misuse by the companies who collect or deal with such data. The former is a much better drafted piece of legislation. Some differences between the two regulations are discussed below.

3.1 Definition of personal data and its ambit

The Preamble to the GDP Regulations states that "…*the principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data*."

The GDP Regulations treat the right to protection of personal data as a fundamental right and, therefore, to safeguard this right in the most optimum manner, the definition of "personal data"[5] is kept quite vast. Almost every kind of information with which a person can be identified viz. name, national identification number, location, online identifiers (such as IP address, cookies, radio frequency, information on social media), identification tags etc. health records, sexual orientation, biometric[6] or genetic data,[7] bank details etc. is covered. Basically, the GDP Regulations do not protect a person's data which has no connection with some professional or commercial activity. In fact, Article 18 specifically excludes data processed in the course of a personal or household activity. However, there is some data which though not connected to professional or commercial activity, is still accorded protection under the GDP Regulations. Article 9 states that data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership information, and data concerning sex life shall be treated as sensitive data.

On the other hand, under the IT Regulations, the definition of protected data does not have as wide a scope as the GDP Regulations, even though there are some similarities. The IT Regulations only protect "sensitive personal data" of a person in India. Section 7 defines sensitive personal data as information regarding password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information or any other related information provided to a body corporate. This leaves Indians vulnerable since there is no legal protection against leakage of their data that is outside the purview of sensitive personal data. The Supreme Court has time and again stressed on the need for the state to protect privacy rights of people which must culminate into codified laws. Enactment of appropriate

[4] This is about INR 160 million, applying a rate of USD 1= INR 66
[5] Under Article 4 of the GDP Regulations
[6] As per Article 9 of the GDP Regulations, biometric data relates to personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a person, which provide their unique identification such as facial images, retina map etc.
[7] Article 4 of the GDP Regulations define this a data related to inherited or acquired genetic characteristics of a person

amendments to the law that caters to the evolving business methods will not happen overnight as the legislative process has to be followed. In short, the need for widening the scope of protected data cannot be ignored. In the context of e-transactions at least, consumers must be given an option to either allow the sellers to retain their information or direct them to erase it after every transaction.

3.2 Data subjects

Under Article 30(5) of the GDP Regulations, the mandate of protecting the privacy of personal data of EU citizens is on every organization in the EU which has 250 or more employees. These also apply to organizations with less than 250 employees provided **(i)** the data controlling or processing[8] by companies with less than 250 employees is not occasional; or **(ii)** the processing may pose a risk to the rights and freedoms of data providers in the EU; or **(iii)** they process sensitive data or data relating to criminal convictions and offences. In India, there is no such employee headcount limit under the IT Regulations which are binding on every company which deals in sensitive personal data. The GDP Regulations do not explain the ambit of anticipated risk to data privacy rights or what would occasional processing mean. Further, there seems no logic behind categorizing the applicability based on employee head count. Putting a blanket obligation on an organization with 250 employees, but limiting the obligations when employees are below that figure and the organization collects personal data occasionally, appears to be unreasonable. Loss of personal data puts a person in a vulnerable position, be it by a company with 250 or 100 employees.

3.3 Extra territorial scope

As per Article 3(1) the GDP Regulations, organizations outside the EU too are obligated to protect personal data of people in the EU. So, organizations in India too, who either control or process personal data of the EU people, will have to adhere with them. The legislative intent of GDP Regulations is to protect personal data of people in the EU irrespective of *their nationality or residence;* every person in the EU is protected. The IT Regulations do not have extra territorial scope. They only regulate companies in India who collect and process sensitive personal information of Indian citizens. They exclude foreigners living in India, which seems rather strange. Given the impetus on promoting medical tourism there is no reason why their medical records should not be protected. Similarly, an Indian e-wallet company could have data of Indian citizens as well as expats. Unless there is a legal mandate, companies will not come forward and execute contracts to impose obligations on them for protecting data of foreigners living in India. It is, therefore, essential to extend the same protection to all persons in India, regardless of nationality.

3.4 Pre-conditions for data processing

Under rule 5, the IT Regulations mandate that the data subjects must know the reason and end purpose for such collection. However, once the data is collected the information providers do

[8] Basically, the regulations revolve around "controlling" and "processing" of personal data. As per Article 4 (2), data controlling refers to determining the purpose of processing data and data processing means any operation which is performed on personal data whether via automated means or otherwise. Article 4 (7) provides that activities like collection, recording, organizing, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction can be categorized as data processing.

not know if the data can be used for any other purpose apart from the one informed to them. They also do not have any idea on the intended recipients of their data. The GDP Regulations treat "consent" in a more responsible manner and go a few steps ahead of the IT Regulations. These enlist principles for data collection under Article 5. These provide that at the time of taking consent, the data controller must provide its ID and contact details along with the identity of the data recipients or category of the recipients, the period for which the personal data will be stored and the criteria for determining that period and information on the right to lodge a complaint with a supervisory authority in case the information provider anticipates breach of their data privacy rights. So, the consent is sought for every stage; be it for collection, recipient's identity, purpose of collecting data, forwarding to other recipients etc.

3.5 Child's consent

The IT Regulations having nothing specific with respect to seeking consent of children before collecting their data. In contrast, Article 30 the GDP Regulations mandate that consent from the holder of parental responsibility over the child is sought and reasonable efforts are made to verify that such holder has tendered consent on the child's behalf. But, the word "reasonable" is very subjective; and, the regulations do not explain what "reasonable efforts" would mean. It is left to the interpretation of data collectors and processors. This is a very tender issue and both the regulations need to address the issue in an effective manner.

3.6 Right to be forgotten

Rule 5 of the IT Regulations gives an option to the information provider to withdraw consent for using his data. The company cannot, thereafter, use the information of such provider. So, right to give consent for usage of certain information comes with the right to withdraw such consent too. The GDP Regulations also provide for this. Additionally, Article 17 grants a right to the information provider to ask the controller to erase his data from the company's records without any undue delay. This ensures that the controller cannot retain the data any longer with it and rules out access to the same to any third party in the future. The information cannot even be used for any purpose, including studying behavioral characteristics of a data subject.

4. Conclusion

The GDP Regulations are global in their scope and applicability. These have been drafted to ensure that the people in the EU are able to exercise their right to protection of personal data in the best possible manner and without any fritters. However, it is yet to be seen whether it would be practical to really enforce these in letter and spirit. For instance, ensuring that every entity who does business in the EU shall, regardless of its location, be equipped to take well informed consent in a uniform manner from EU subjects before seeking their personal data seems impractical. The regulations require that every entity must ensure that "appropriate technical and organizational measures" are implemented to secure personal data of "data subjects in the EU" but no parameters are prescribed with respect to these "measures." So, open issues remain. For instance, who will verify if a company doing business in EU has adequate tools to seek consent of the information providers, whether the data is really erased when consent is withdrawn, how will the high quantum of penalty for data breach be imposed, especially on a small enterprise who does not have that kind of worth to bear it, how will that penalty be collected, what are going to be the

implications for non-payment of penalty etc. So far, these questions have no answer and the hope is, in due course, adequate clarity will be provided.

Author
Mansi A. Gambhir