The Impact of General Data Protection Regulations on Indian Data Processing Companies

Introduction

While European Parliament's General Data Protection Regulation (GDPR) is slated to have global and far-reaching ramifications, a degree of uncertainty looms amongst Indian companies, especially those which are engaged in outsourced data processing activities (whether captive or otherwise) and consequently deal with personal data of data subjects in the European Union (EU). This uncertainty is mainly with respect to the applicability of GDPR and its implications on their businesses. The penalty scheme prescribed under the GDPR is also a cause of concern for such companies since GDPR permits enforceability against a data processor directly.

With a little over six months remaining before GDPR comes into force on 25 May 2018, this is an opportune moment for several companies to revisit their policies and procedures with respect to data privacy and protection and ensure preparedness ahead of time.

Are Indian data processing companies subject to GDPR?

The definition of data processor under GDPR has a very wide connotation. It means any operation performed on personal data such as collecting, recording, structuring, storing, using, disclosing by transmission and even includes erasing and destroying.[1] Article 3 (Territorial scope) of GDPR makes it clear that it will be applicable regardless of whether the processing takes place in EU or not.

Therefore, an Indian company processing personal data in context of activities of an establishment of a controller or processer in EU, in all likelihood will fall within the ambit of GDPR.

What can Indian data processing companies expect?

Prior to undertaking any processing activity, Indian companies will be required to enter into a contract with their customer (generally, a data controller[2]). Such contract will, *inter alia*, stipulate the subject-matter and duration of processing activity, its nature and purpose and the type of personal data and categories of data subjects.

By way of such contract, a customer (the data controller) will seek from an Indian company a flow down of the following obligations:

- Implementation of appropriate organisational measures to ensure (i) pseudonymisation and encryption of personal data; (ii) confidentiality and integrity of processing systems; (iii) restoration of availability and access to personal data after a physical or technical incident; and (iv) regular testing and evaluation of such measures[3];

---

[1] *Article 4(2) – 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[2] *Article 4(7) – "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data…".*

[3] *Article 32 of GDPR.*

- In the event of a personal data breach, the same must be notified to the customer without undue delay after it becomes aware of such personal data breach[4]; and
- Carry out a data protection impact assessment prior to commencement of the processing activity.

Many may feel that this does not change anything substantially as such Indian companies even today have contracts with their customers. It must be noted that GDPR mandates that the contract between data controller and processor will necessarily comprise of the obligations stated above. In addition to the foregoing, an Indian company carrying out data processing will also be obligated to allow the customer to conduct an audit and inspection of its systems to demonstrate compliance with the above. Further, the right of a data processor to subcontract their obligations has been curtailed and made conditional to the data controller's approval. Therefore, the ability of an Indian process outsourcing company to refuse flow-down of contractual obligations has been severely impacted.

Adequacy requirements

A keystone of GDPR is the stipulation of 'adequacy requirements'[5] which restrict the transfer of personal data to any third country or international organisation that does not "ensure an adequate level of protection." In doing so, the European Commission will 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 India, the current legal framework pertaining to data privacy and protection is far from lucid. The recent judgment of the Hon'ble Supreme Court declaring the right to privacy as a fundamental right[6] (Privacy Judgment) has provided much-needed impetus to introducing a long-awaited, all-encompassing data protection legislation in India (Forthcoming Legislation). It will be interesting to see how the Forthcoming Legislation shapes up and whether it will satisfy the criteria laid down under GDPR.

Khaitan Comment

In this era of globalisation and integrated product offerings, the generation, use and flow of personal data has amplified considerably. In the process, both private as well as public entities have acquired access to personal data of individuals, giving rise to concerns with respect to collection, processing, use, storage of such personal data. With the advent of GDPR, many of these concerns in respect of EU citizens will be dispelled to a considerable extent.

Most multinational companies find themselves increasingly dealing with personal data of EU citizens. Indian companies that engage in data processing also gain access to such information as a part of their day to day operations, bringing them within the ambit of GDPR. Simultaneously, GDPR casts some onerous obligations on a data processor. Many of these will entail significant time and capital investment to comply with. Further, data controllers now have a statutory basis for claiming contractual protection from data processors. Earlier, such flow-downs were a subject of commercial negotiation between the parties and could be

---

[4] The data controller in turn has to notify competent authority of such personal data breach within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedom of natural persons.

[5] Article 44 and 45 of GDPR.

[6] Justice KS Puttaswamy (Retd.) v Union of India [Writ Petition (Civil) No. 494 of 2012].

subverted on that ground. Undoubtedly, this will place such Indian companies in a precarious position in comparison to their standing in the period preceding the enforcement of GDPR.

To add to this, whether or not India will meet the 'adequacy requirements' will be discerned by the manner and profundity with which the Forthcoming Legislation deals with these 'adequacy requirements'. While Privacy Judgment has presented several anecdotes for the legislature to consider while framing this legislation, it will be interesting to see to what extent they are adopted. Many experts anticipate that the Forthcoming Legislation will be on the lines of GDPR and this may aid its acceptance by the European Commission.

Notwithstanding, we feel that this presents a golden opportunity to Indian data processing companies to revisit their data protection, information security and confidentiality policies and make them compliant with global standards. This pre-emptive step will not only help them in sustaining their businesses, but also in securing compliance with GDPR, Forthcoming Legislation and other global best practices.

- *Harsh Walia (Associate Partner) and Shobhit Chandra (Senior Associate)*