Retention of Data Under the Indian Privacy Law and GDPR – Practical Challenges

Mr. Shreekanth Katti & Mr. Dipanjan Dey***

Introduction

Data privacy law in India as well as in other jurisdictions of the globe has taken a new momentum in recent years. With the promulgation of the European Union's General Data Protection Regulation ("GDPR") and India's proposed Personal Data Protection Bill ("PDP Bill") making noise since few years, every organization, whether small or big and even the start-up companies have been emphasizing on the compliance to the privacy law. One of the aspects of such compliances relates to storage and retention of the personal information collected by such organizations. In this article, an attempt has been made to understand the current legal framework under Indian privacy law, PDP Bill and GDPR on the retention of personal data and to discuss some of the practical challenges arising out of it.

Legal framework on the retention of personal information

Indian Law

The digital revolution has resulted in a phenomenon where companies are inclined, to the maximum extent, to collect and store the information and documents in electronic form. To encourage and support such a move, the Information Technology Act, 2000 ("IT Act") has an enabling provisions[1] by which if any law provides that any information is

* Associate General Manager -Legal & Regulatory at Syngene International Limited.

** Associate Manager – Legal at Syngene International Limited.

[1] IT Act, Section 4.

required to be in writing or printed form, then the requirement is deemed to have been satisfied if such information is (a) made available in an electronic form; and (b) accessible for a subsequent reference.

The IT Act further enables the electronic storage of documents by providing a provision[2] that where any law required that the documents, records or information have to be retained for any specific period, the requirement is deemed to have been satisfied if such documents, records or information are retained in the electronic form if (a) the information contained therein remains accessible for a subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

While the IT Act enabled the electronic storage of documents in general, the retention of personal information or data is provided under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") which is the only current legal framework on the privacy law of India. SPDI Rules provide[3] that a body corporate holding sensitive personal data or information[4] ("SPDI") shall not retain that information for a period longer than what is required for the purposes for which the information was collected or may lawfully be used or is otherwise required for fulfilment of an obligation under any other law for the time

---

[2] *Supra* 2, Section 7.

[3] SPDI Rules, Rule 5(4).

[4] *Supra 2*, Rule 3, Sensitive personal data or information of a person means such personal information which consists of information relating to;—(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition;(iv) sexual orientation; (v) medical records and history; (vi) Biometric information.

being in force. This is famously termed as the principle of Storage Limitation.

PDP Bill

The proposed PDP Bill, if comes into force in the current form, introduces more stringent compliance requirements for the collection and use of personal data[5]. PDP Bill defines the term "process" to include storage[6]. In line with the current SPDI Rules, the PDP Bill also provides for Storage Limitation principle wherein the data fiduciary[7] can retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed[8]. However, personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation under a law. Further, it imposes an obligation on the data fiduciary that it must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession. If it is not necessary for personal data to be retained by the data fiduciary, then it must be deleted.

PDP Bill further provides for various grounds for storage of the personal data. It may be stored if it is (a) explicitly mandated under any law or (b) for compliance with any order or judgment of any Court or Tribunal in

---

[5] PDP Bill defines the term 'Personal Data' in Clause 3(29) as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information;

[6] PDP Bill, Clause 3(32) – 'Processing' in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

[7] *Supra* Clause 3(13) – 'Data fiduciary' means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

[8] *Supra* Clause 10.

India[9]. The employee data may be stored if such storage is necessary for (a) recruitment or termination of employment of a data principal[10] by the data fiduciary; (b) provision of any service to, or benefit sought by the data principal who is an employee of the data fiduciary; (c) verifying the attendance of the data principal who is an employee of the data fiduciary; or (d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary[11]. However, this provision is applicable where storage on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the storage activities.

Personal data may also be stored in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law is permitted only when such storage is authorised by a law. However, such personal data shall not be retained once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete except where such personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence or class of offences in future[12]. Personal data may be stored where disclosure of such personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding[13].

---

[9] *Supra* Clause 14.

[10] Data principal means the natural person to whom the personal data relates.

[11] *Supra* Clause 16.

[12] *Supra* Clause 43.

[13] *Supra* Clause 44.

The PDP Bill further categorises the personal data into "Sensitive Personal Data" to mean personal data revealing, related to, or constituting, (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority. In order to store and retain the Sensitive Personal Data, in addition to prior explicit consent, it has to be ensured that such storage is (a) explicitly mandated under any law; or (b) necessary for compliance with any order or judgment of any Court or Tribunal in India[14].

General Data Protection Regulation (GDPR)

GDPR has extra territorial jurisdiction to the extent that is it applicable to those entities or organizations not based out of EU but are processing the personal data of individuals based out of EU[15]. Therefore, even the Indian companies dealing with or handling personal data of individuals based out of the EU are required to follow GDPR.

GDPR also defines the term 'processing' to include storage[16]. Similar to SPDI Rules and the PDP Bill, GDPR provides for Storage Limitation principle that the personal data shall be kept in a form which permits identification of data subjects[17] for no longer than is necessary for the purposes for which the personal data is processed[18]. This further

---

[14] *Supra* Clause 20.

[15] GDPR, Article 2.

[16] This 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[17] Data subject an identified or identifiable natural person.

[18] GDPR, Article 5.

comes with an exception wherein the personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

Further, GDPR provides that storage of personal data shall be lawful only if and to the extent that at least one of the following applies[19]: (a) the data subject has given consent; (b) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) for compliance with a legal obligation to which the controller[20] is subject; (d) in order to protect the vital interests of the data subject or of another natural person; (e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

GDPR has further categorized the personal data into special categories of data to include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation[21]. Storage Limitation

---

[19] *Supra* Article 6.

[20] 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

[21] *Supra* Article 9.

principle and the grounds for storage as described above will have to be strictly followed even for special categories of data.

Practical challenges to comply with the data retention obligations

The SPDI Rules, PDP Bill as well as the GDPR does not specify the retention period of personal data but mainly relies on the Storage Limitation principle. The principle of Storage Limitation states that the personal data has to be stored as long as it is required for the purpose for which it is collected, and it can no more be stored once such purpose is fulfilled. However, there are practical difficulties in complying with this requirement particularly when an organization is required to store the documents in order to comply with requirements under other laws as well.

For example, Securities Exchange Board of India ("SEBI") requires the listed entities to have a policy for preservation of its documents in at least two categories as (a) documents whose preservation shall be permanent in nature; (b) documents with preservation period of not less than eight years after completion of the relevant transactions[22]. Now, the Storage Limitation principle under the privacy law which sets out that personal data has to be stored only till the organization needs it does not seem to harmonize with the requirement of SEBI which provides that the documents, which may also include documents relating to personal data, will have stored at least for 8 years even after the transaction. Similarly, various other laws as applicable to an organization may provide for different periods for preservation of documents.

It may be noted that the SPDI Rules and proposed PDP Bill gives an exception to the principle of Storage Limitation for the purpose of complying with any other law or legal obligations. Thereby, one may

---

[22] Regulation 9 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

argue that such a provision may be used to comply with the requirements under other legal provisions such SEBI provisions mentioned above and preserve the documents as required by it. However, it is pertinent to note that the principle of Storage Limitation is the foundation of privacy law to protect the privacy of the individual not allowing the organization to retain the personal data beyond what is required and therefore taking such an interpretation may defeat the basic purpose of having the Storage Limitation principle under the privacy law.

In view of the above, organizations and particularly the public listed companies may find it difficult to draft a single policy on retention of documents applicable for all types of documents of that organization and may in turn end up in having multiple policy documents for various types of documents. While the mood of the nation is towards ease of doing business, the requirements towards retention period does not seem to have directed towards the same.

Conclusion

Storage Limitation principle is an essential principle for the strict compliance with the privacy law in both letter and spirit. It ensures privacy of the individual by mandating that the organization does not retain the personal data anymore once the purpose is fulfilled. Any deviation from the same would defeat the purpose of the principle itself and question the privacy of the individual. While organizations may find a way out to deal with the confusion on the hand, a clarity from the policy makers harmonizing the retention period for all types of documents to be handled by an organization is the need of the hour. It would not only help in reducing the paperwork but also bring clarity in adhering to requirements of retention period.