LexArticle March 29, 2018, New Delhi, INDIA

AN OVERVIEW OF DATA PROTECTION LAWS IN INDIA AND EUROPEAN UNION

This article has been co-authored by the team of LexCounsel Law Offices in collaboration with Ms. Magdalena Jacolik of Aliant Krzyżowska International Law Firm, Poland.

If you have questions or would like additional information on the material covered in this Newsletter, please contact the authors.

LexCounsel Law Offices:

By: Seema Jhingan, Partner (sjhingan@lexcounsel.in)

AN OVERVIEW OF DATA PROTECTION LAWS IN INDIA AND EUROPEAN UNION

Communication, transfer, storage and use of data (and often sensitive, confidential and personal data) has become part and parcel of today's digital transactions. While electronic transactions are quickly becoming an easier and efficient way of transacting as opposed to the traditional offline paper work, they are not without the risk of hacking, data theft and other cybercrimes. Data protection has therefore become a multi-jurisdictional issue in this borderless digital world, and countries around the world have developed regulatory frameworks to specifically address and protect against loss of privacy.

India is still at a relatively nascent stage when it comes to data protection regulations, as compared to other jurisdictions such as the highly developed (and often stringent) guidelines prescribed by the European Union ("**EU**") on data protection. Comparison of the two legal regimes offers certain interesting insights on data protection laws, as discussed below.

A. Regulatory Framework in India.

(i) Information Technology Act, 2000 and SPDI Rules:

The legal principles regarding data protection are contained in the Information Technology Act, 2000 ("**IT Act**") and the rules framed thereunder *inter alia* on matters relating to collection, storage, disclosure and transfer of electronic data.

Neha Yadav, Principal Associate (nyadav@lexcounsel.in)

Monica Benjamin, Associate (mbenjamin@lexcounsel.in)

Aliant Krzyżowska International Law Firm, Poland:

By: Magdalena Jacolik (Master in European Law), Associate (aliant@aliantlaw.pl)

LexCounsel, Law Offices C-10, Gulmohar Park New Delhi 110 049, INDIA.
Tel.:+91.11.4166.2861
Fax:+91.11.4166.2862

The IT Act also prescribes punishment of imprisonment and/or fine for offences involving illegal downloading, destruction, alteration or deletion of data, introduction of viruses into computer systems, illegal access to computer systems, data theft, identity theft, cheating by personation, cyber terrorism, breach of confidentiality, privacy and disclosure of information in breach of lawful contract, to name a few.

Specifically with respect to personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**"), mandate adherence to specified procedures and measures by a body corporate, which processes, deals with, stores or handles sensitive personal information or data in a computer resource which it owns, controls or operates. Some of the key compliances under the SPDI Rules are as follows:

- Obtaining prior written consent from the provider for collecting information, while providing an option to the provider to not provide such information sought from it and to also withdraw his/her consent given earlier in this regard.
- Taking of reasonable steps to ensure that the information provider has knowledge of the fact of collection, purpose of usage, intended recipients of the information and details of the agency that is collecting and that will retain the information.
- Personal information should not be retained for longer than is necessary for achieving the corresponding purpose or as is otherwise required under applicable law.
- Formulation and communication of a privacy policy for handling of or dealing in personal information.
- Non-disclosure of personal information to any third party without prior permission (unless such disclosure is required by law or has been contractually agreed with the information provider).
- Designation of a grievance officer for addressing discrepancies and grievances.
- Implementation and maintenance of reasonable security practices and procedures. The international standard IS/ISO/IEC 27001 on "Information Technology -Security Techniques - Information Security Management System - Requirements" is deemed to be reasonable security practice subject to certification by independent auditors.
- Information may be transferred to any other person that ensures the same level of data protection as provided under the SPDI Rules, provided that it is necessary for performance of lawful contract with the information provider or where such provider has consented to data transfer.

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.

(ii) A New Data Protection Law on the Horizon:

With the gamut of laws regulating collection and usage of various types of data, the data protection regime in India is still not exhaustive enough, and several concerns are being raised to further secure and adequately deal with the complex issues including loss of data and consequent privacy.

The Indian Government is however, seeking to further strengthen and equip its regulatory framework for data protection and privacy. Accordingly, a Committee of Experts under the chairmanship of former Supreme Court Justice, Shri B. N. Srikrishna ("**Committee**"), has been formed to study various issues relating to data protection in India, make specific suggestions on principles to be considered for data protection and suggest a draft Data Protection Bill. The Committee has accordingly released a white paper on November 27, 2017, on a data protection framework for India, seeking public comments. In January earlier this year, the Committee in collaboration with the Indian Ministry of Electronics & Information Technology has also conducted stakeholders' consultation meetings at various Indian cities, to obtain their opinions and concerns regarding the issues raised in the white paper.

This white paper has come on the heels of the Supreme Court's landmark judgment of August 24, 2017 in the case of ***Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., 2017 (10) SCALE 1***, where the Court recognized the right to privacy as an intrinsic part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India. The Court observed that 'informational privacy' is a facet of the right to privacy and recognized that dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. The Court referred to how "'Uber' owns no vehicles, 'Facebook' creates no content, 'Alibaba' has no inventory and 'Airbnb', the world's largest accommodation provider, owns no real estate, but entities like these and other social network providers, search engines, e-mail service providers and messaging applications, are all further examples of non-state actors that have extensive knowledge of our activities, financial transactions, conversations, health, mental state, shopping habits, etc. With increase in people's reliance on internet based services, deeper and deeper digital footprints are being created and there is an unprecedented need for regulation regarding the extent to which such information can be stored, processed and used by non-state actors and also by the State. Since the Government had informed the

	Supreme Court of the constitution of the Committee to review *inter alia* data protection norms in the country, the Court felt it was appropriate to leave the matter for expert determination so that a robust regime for the protection of data is put into place. The Committee in the white paper, has suggested that the data protection framework should be based on seven principles: (i) law should be flexible to take into account changing technologies, (ii) law must apply to both government and private sector entities, (iii) consent should be genuine, informed, and meaningful, (iv) processing of data should be minimal and only for the purpose for which it is sought, (v) entities controlling the data should be accountable for any data processing, (vi) enforcement of the data protection framework should be by a high-powered statutory authority, and (vii) penalties should be adequate to discourage any wrongful acts. The Committee has sought public comments on questions relating to territorial applicability of data protection laws; extent to which the law should apply outside India such as inclusion of measures to ensure compliance by foreign entities; definition of personal data; categories of exemptions of entities from certain obligations (e.g., certain actions taken by the state during investigations); conditions of valid consent; exposure of online risks for children, purpose of collection; participation rights of data provider in its processing (such as right to confirm, access and rectify data); enforcement models/tools to be used for code of conduct, breach of personal data, categorization of different data controllers, and creation of a separate data protection authority. The Committee has also noted that the provisions of the IT Act are limited in their applicability and do not appear to take into account the wide range of instances of data protection violation which may occur due to advancement in technology used towards processing of personal data. Moreover, the quantum of penalty prescribed under the provisions of the IT Act appear to be inadequate and may not act as a deterrence to emerging e-commerce and other technology based players in India. The white paper has accordingly discussed penalties for offences under the proposed law, and adjudicating authorities for complaints; and noted that awarding compensation to an individual who has incurred a loss or damage due to the data controller's failure is an important remedy to be specified under the law. **B. <u>Regulatory Framework in EU.</u>** A significant development in the data protection regime in the EU, has been the introduction of the Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC ("**General Data Protection Regulation**" or "**Regulation**").

	This provisions contained in the Regulation are applicable from 25th May 2018. It is worth mentioning, that in accordance with Article 288 of the Treaty on the Functioning of the European Union, the Regulation is binding in its entirety and is directly applicable in all Member States of the EU. Therefore this Regulation does not require additional implementation of acts of national law, as the **provisions included in it are binding from the date of its entry into force**. An important feature of the Regulation is also its direct effect, which means, that both the Member States and the units can rely directly on the measures contained in the Regulation. The Regulation concerns "*the protection of individuals with regard to the processing of personal data and (...) the free movement of such data*". Certain fundamental features of the Regulation are specified below: ➢ Key Definitions: Article 4(1) of the Regulation, defines the concept of "**personal data**" as, "*the personal information means information about an identified or identifiable natural person (" the data subject"); an identifiable person is a person that can be directly or indirectly identified, in particular on the basis of the ID such as first and last name, , identification number, location data, online ID or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the natural person".* Article 4(2) defines the concept of "**processing**", as *"the processing means an operation or set of operations performed on personal data or sets of personal data in an automated or not-automated way, such as collection, organization, ordering, storage, adaptation or modification, downloading, viewing, using, disclosure by sending, dissemination or another type of sharing, matching or connecting, limiting, deleting or destroying".* ➢ It is also worth emphasizing that as per clause (15) the protection concerning the processing of personal data should not be dependent on forms used for the processing of data. Also the Regulation is not applicable to the processing of personal data by the relevant authorities in order to e.g. protect the public or national safety under Article 2(d), and to the processing of anonymous information including for statistical or research purposes under clause (26). ➢ Extra-Territorial Application: The question of territorial application of the Regulation, is dealt with in Article 3, according to which the Regulation is applicable to: (i) processing of personal data in connection with the activities carried out by the administrator's organizational unit or by the processor in the European Union, regardless of whether the processing takes place in the European Union; (ii) the processing of personal data of the persons to whom the data relates, staying in the European Union by the administrator or the processing unit without organizational units in the Union, if the processing operations are related to: a. offering goods or services to such persons to whom the data relates, in the European Union - regardless of whether the payment from such persons is required; or b. monitoring of their behaviour, unless the behaviour occurs in the European Union.

	(iii) the processing of personal data by the administrator not having any organizational units in the EU, but having an organizational unit in a place, where under the public international law the law of the Member State of EU applies. ➢ Fair and lawful processing: Personal data must be processed fairly - in accordance with clause (60) of the Regulation i.e. that the administrator should inform the person that such data relates to, about the context, purposes and circumstances of information processed and to be within the limits of the law - in accordance with clause (40) i.e., on the basis of consent expressed by the person to whom the data relates or on the different legal basis. ➢ No Misleading Information: Any misleading information and those that are invalid from the point of view of the purpose of the processing, should be corrected or deleted in accordance with Article 5(1)(d) of the Regulation. ➢ Processing of Special Categories of Personal Data: It is not permitted to process the personal data of a particular category i.e. including sexual orientation, political opinions, religion, racial/ethnic origin or health (Article 9). ➢ Processing not requiring identification: When the information is not sufficient to identify the person, the administrator is not required to obtain further information necessary for the identification of such natural person, if the objectives of processing do not oblige to do that (Article 11(1)). ➢ Purpose of Collection: Personal data should be processed in accordance with the purpose for which these data were collected. However, if the administrator intends to process this data for other purposes, he's obliged to inform the person to whom the data relates and also provide necessary information (Clause (50) and Article 14(4)). ➢ Right of Access: The natural person should have access to information it relates to. The administrator, who receives data from that person, should inform the person about the purposes of the processing of such data, about the recipients and also about the right to claim deletion, correction or objection by the administrator (at any time) (Article 15). ➢ Right to be forgotten: Article 17 establishes the "*the right to be forgotten*", i.e. a natural person to which the data relates, may claim the right to delete data by the administrator in designated circumstances, i.e.: in a situation where personal data are no longer needed for the intentions in which they were collected, were processed in an unlawful manner, or the person withdrew his consent or objected. ➢ Permitted Profiling: Making decisions on the basis of profiling should be permitted where it is expressly permitted by European Union law or the law of the Member State to which the administrator is subject, including the purposes of monitoring and prevention - in accordance with the regulations and standards and recommendations of the institutions of the European Union or national supervisory authorities - of fraud and tax evasion and to guarantee the safety and reliability of the services provided by the administrator, or where it is necessary for the conclusion or performance of a contract between a person the data relates to and the administrator, or where the person the data relates to agreed explicitly (Clause (71)).

	➢ Restrictions: Restrictions in individuals' rights to the protection provided with regard to the processing of personal data are justified if they are for protection of the public security, public health, national security or crime prevention (Article 23). ➢ Safety: The administrator and the processing subject shall implement appropriate methods to ensure the safety of data processing (Article 32). ➢ Duty to report breach: Article 33 relates to the duty of reporting breaches in the protection of personal data, in accordance with which, the administrator should inform the supervisory authority about the breach of personal data protection (within 72 hours).The processor is required to inform the administrator of personal data breach without undue delay. ➢ Data protection impact assessment: Under Article 35, the administrator estimates the effects of the planned data processing and assesses the possible risks that are associated with the processing of such data. ➢ Data Protection Officer: Under Article 37(1) the administrator and the processor designates a Data Protection Officer (DPO), in the situation when: a) processing is carried out by the authority or a public body with the exception of the courts in the exercise of the justice; b) the main activity of the administrator or the processor is based on processing operations, which due to their nature, scope or purposes require regular and systematic monitoring of persons the data relates to, on a large scale; or c) the main activity of the administrator or the processor is to process special categories of personal data on a large scale, referred to in Article 9(1) and personal data on convictions and infringements of the law as referred to in Article 10. It should be noted that the principle of designation of the Data Protection Officer is based on professional qualifications which officer directly reports to the top management of the administrator or processor. Its tasks include: a) informing the administrator, the processor and the employees who process personal data about the their obligations under this Regulation and about other provisions of the EU or the Member States about data protection and advising them on this matter; b) monitoring the compliance with this Regulation, the other provisions of the European Union or the Member States on data protection and administrator's or processors' in the field of protection of personal data, including the responsibilities, actions aimed to raise awareness, training of staff involved in the processing operations and the associated audits; c) cooperation with the supervisory authority. ➢ Codes of Conduct: The Commission, the European Data Protection Board, the Member States and supervisory authorities encourage the development of codes of conduct that are to promote relevant application of the Regulation (Article 40).

	➢ Certification: The Commission, the European Data Protection Board, the Member States and supervisory authorities encourage the introduction of certification systems, quality labels and markings that prove that the processing of personal data is adjust to provisions of this Regulation. ➢ Supervisory Authority: In each Member State there is to be an independent supervisory authority (at least one), that cares, i.e.: for the appropriate data protection of individuals in relation to its processing and the appropriate use of the Regulation (Article 51). ➢ European Data Protection Board: Article 68 of the Regulation provides for establishment of European Data Protection Board ("**EDPB**"). The EDPB consists of the Chairman of one supervisory authority of each Member State and the European Data Protection Supervisor or their representatives. Importantly, the Commission can participate in meetings or EROD activities, but without the right to vote. It includes the chairman, who represents it, and two vice-chairmen (Article 73). The EDPB is an independent body and settles disputes (Article 65), monitors and supports the proper application of the Regulation, makes recommendations, guidelines and provides opinions on the European Commission on certification, etc., and it also plays an advisory role (Article 70). ➢ Penalties: The provision under Article 83 of the Regulation provides for financial penalties for infringement of the provisions. These penalties shall be proportional, but above all effective and dissuasive. ➢ Adequacy Requirements: Transfers of personal data to third countries which have not been recognized by EU as countries with adequate level of data protection (such as India), can take place only on one of the following conditions as specified under Article 49, such as: a) explicit consent of the data subject to the proposed transfer, after being informed of the possible risks; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request or for conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; c) the transfer is necessary for important reasons of public interest; or for establishment, exercise or defence of legal claims; or in order to protect the vital interests of the data subject; d) the transfer is made from a register of public information as prescribed therein; or e) on certain other conditions as specified therein. ➢ Binding Corporate Rules: Article 47 of the Regulation also provides for the concept of "Binding Corporate Rules" (BCR), which can be a viable alternative in cases where the adequacy requirements are not met for transfer of data to third countries/organizations outside EU. Binding corporate rules are defined as personal data protection policies adhered to by a controller or processor established on the territory of a Member State for transfers of personal data to a controller or processor in third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. As per Article 47 of the Regulation, the competent supervisory authority is to approve binding corporate rules in accordance with the mechanism set out in the Regulation.

Following the rapid development of the collaboration between EU and Indian companies, especially in the IT field, it should be stressed that the data protection requirements on the similar level between the parties are be expected. It is also important to note, that according to the Regulation, processing of personal data located in the EU by the administrator or the processor, even if it does not have an organizational unit in the EU, is subject to the Regulation even where it involves monitoring the behaviour of those whose data is concerned, if this behaviour takes place in the EU. Therefore, in order to be able to legally secure, without the risk of administrative penalties or civil liability towards the customer, at the time of entrusting personal data to third-country entities providing IT services, it seems that it is easiest and safest to conclude a data transfer contract with the service provider that will contain standard contractual clauses on the protection of personal data, approved by the European Commission. In case of international capital groups, whose members often cooperate in a manner requiring the transfer of personal data, an attractive alternative to the transfer agreements mentioned above may be to use appropriate binding corporate rules as mentioned above.

C. <u>The Future ahead.</u>

As opposed to the stringent EU model, the current Indian regulatory framework on data protection is not sufficiently adequate to address the growing concerns arising on account of collection and linking of data including biometrics by the Government under the Aadhaar Act and the exponential advancements in technology and digital transactions, which increases the risk of data violations. Recognizing these issues, the Government of India is working on a more effective legal framework for data protection which initiative is being led by the above stated Committee. However, the devil lies in the details, and it remains to be seen as to how far appropriate changes and global concepts will be introduced, implemented and enforced in the Indian context.

Further, in the meantime, the EU's new General Data Protection Regulation which is coming into effect in May 2018 is expected to have far-reaching implications even in the Indian context, due to its applicability to Indian entities who deal with data of EU nationals (as discussed above). As on date, India is not recognized by EU as a country with adequate level of data protection, which therefore requires additional compliances for transfer and processing of data by such Indian entities. Therefore, from an Indian perspective, it becomes imperative for such Indian entities to implement the data protection requirements stipulated in the EU Regulation within their systems, particularly as their EU counterparts are likely to insist on compliance with the Regulation as part of their standard contractual clauses, given the heavy penalties associated with non-compliance with the Regulation.

Bibliography:

1. Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
2. *White Paper on Data Protection Framework for India*: [http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited].
3. Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC(General Data Protection Regulation)
   EU official journal of 04.05.2016, L119, page 1.
4. Treaty on the Functioning of the European Union, official journal of 2012, C 326, page 1.
5. P. Justyńska, *Zasady prawa Unii Europejskiej, [w:] J. Galster (red.) Podstawy prawa Unii Europejskiej z uwzględnieniem Traktatu z Lizbony*, Toruń 2010, page 251 i n, 326 i n.
6. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM%3Al14522, as at 02.01.2018.
7. *Public consultation on White Paper – Data Protection Framework for India*, Press Release dated December 28, 2017: [http://meity.gov.in/writereaddata/files/public_consultation_on_white_paper.pdf].

Feedback