Dhir
& Dhir
Advocates & Solicitors

Watershed Year for Data Privacy Laws in India

The European Union's (EU) General Data Protection Regulation (GDPR), which took effect from May 25, 2018 (today), sets out new standards and protocols for handling and storing personal data of EU citizens, granting the data subjects in the EU more rights and control over their data. Any entity based in any country outside the EU but dealing with data subjects in the EU will be necessitated to comply with the GDPR to avoid penalties of up to € 20,000,000 (Twenty Million Euros) or 4% of such entity's global annual revenue, whichever is higher. Given the above, the last few months have seen Indian companies scrambling to update their information security measures and privacy policies in sync with the GDPR.

Interestingly the long arm of the GDPR isn't the only thing that has effected this change in India. The year 2017-18 has been a very important year for data privacy laws in India. Critical developments have taken place in each of the last few months. Listed below are some of the most important developments in the last few months.

The Information Technology (Security of Pre-Paid Instruments) Draft Rules

The Ministry of Electronics and Information Technology (MeitY) on March 8, 2017[1] released draft rules setting out the framework for information security measures for Prepaid Payment Instruments (PPIs) in India. PPIs are governed by the provisions of the Payments and the Settlement Act, 2007 and the RBI is the regulatory authority. Though the Information Technology Act, 2000 and its Information Technology (Reasonable security practices and procedures and

sensitive personal data or information) Rules, 2011, extend protection wherever sensitive personal data is involved, the stepping in of the MeitY particularly for PPIs is one of the first attempts to have dedicated information/cyber security and privacy provisions for a specific sector.

The Privacy Judgment

On August 19, 2017, the Supreme Court of India delivered its verdict in the Justice K. S. Puttaswamy v Union of India[2] affirming the right to privacy as a fundamental right under Article 21 of the Constitution.

That said, it was also clarified that the right to privacy, like other fundamental rights, though fundamental in nature is not absolute and can be denied by means of a 'procedure established by law' for 'compelling state interests'. The denial will however be subject to the 'highest standards of scrutiny' with the test for 'reasonableness' being the minimum benchmark for such scrutiny.

The judgment provides a ballpark for State action in respect of personal data, be it the implementation of its own AADHAR identification systems, or the prospective data protection laws it may bring in for non-state actors.

White Paper by the Committee of Experts

The Justice Shri B. N. Srikrishna led Committee of Experts created by the Government of India to study and suggest a Data Protection Framework for India, released a white paper for public comments on November 27, 2017.[3] The formation of the committee and the release of its observations were the first steps in the creation of a comprehensive data protection framework for both state and non-state actors.

The document which is thoroughly detailed, lists 7 (seven) principles on which the data protection regime in India must be based:

(i) Technology Agnosticism – The law must be flexible and must take into account changing technologies and standards of compliance

(ii) Holistic Application – The law must apply to both private sector entities and government entities, with differential obligations carved out for legitimate state aims

(iii) Informed Consent – The law must ensure that human autonomy is expressed in an informed and meaningful manner

(iv) Data Minimization – The law must ensure that the data obtained and processed is minimal and only to the extent required and necessary

(v) Controller Accountability – The law must hold the data controller accountable for any processing of data, whether done by itself or through any third-party contractors

(vi) Structured Enforcement – The law must provide for a high powered statutory authority with sufficient capacity along with appropriately decentralised enforcement mechanisms

(vii) Deterrent Penalties – The law must provide for penalties that are adequate to create a deterrence

Digital Information Security in Healthcare

The Ministry of Health & Family Welfare notified draft Digital Information Security in Healthcare Act on March 21, 2018, inviting public comments.[4] The draft legislation aims at regulating the generation, collection, storage, transmission, access and use of all digital health data and associated personally identifiable information.

Digital Health Data includes:

(i) information concerning the physical or mental health of an individual;

(ii) information concerning any health service provided to an individual;

(iii) information concerning the donation by the individual of any body part or any bodily substance;

(iv) information derived from the testing or examination of a body part or bodily substance of an individual;

(v) information that is collected in the course of providing health services to an individual;

(vi) information relating to details of the clinical establishment accessed by an individual.

Associated personally identifiable information includes such information that can be used to identify or locate individuals to whom such digital health data belongs.

Reserve Bank of India's Data Localisation Order

On April 6, 2018, the Reserve Bank of India (RBI) issued a notification[5] requiring all payment system operators to ensure that their data was stored in a system in India within a period of 6 (six) months. This was done to grant the RBI "unfettered supervisory access" over end to end transaction data, whether in control or processed by the service providers, intermediaries, third party vendors or other entities in the payments eco-system.

[1]Available at http://meity.gov.in/draft-rules-security-prepaid-payment-instruments-under-provisions-it-act-2000

[2]Writ Petition (Civil) No. 494 of 2012

[3]Available at http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited

[4]Available at https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha

[5]Available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

Dhir & Dhir
Advocates & Solicitors

New Delhi
D -55, Defence Colony,
New Delhi-110 024
T: 91(11) 42410000
E: delhi@dhirassociates.com

Bengaluru
S 402, 4th Floor, South Block, Manipal Center,
47 Dickenson Road, Bengaluru 560042, Karnataka
T: 080-43022997
E: bengaluru@dhirassociates.com

Mumbai
406, 4th Floor, BNG House, D.N. Road, Fort,
Mumbai 400001, Maharashtra, India
T: +91 (22) 67472284
E: mumbai@dhirassociates.com

Hyderabad
105, First Floor,Shangrila Plaza, Road # 2, Opp:
KBR Park, Banjara Hills, Hyderabad-500034, India
T: +91 (040) 42208077
E: hyderabad@dhirassociates.com

Japan
Vent Vert Toyohashi, Centre 302,
1-3-1, Maeda
Minami-machi Toyohashi-shi,
Aichi-ken 440-0851 Japan
T: +81 (0532) 218586
E: japan@dhirassociates.com