Data Protection Regulations, 2018 - Key highlights

August 1, 2018

In brief

The committee of experts under the chairmanship of Justice BN Srikrishna, submitted its Report titled "*A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians* ("**Report"**), to the Ministry of Electronics and Information Technology **(Ministry)** along with a draft Personal Data Protection Bill, 2018 ("**Bill**") on 27 July, 2018

The Report and the Bill aims to bring about a regulatory framework for data protection by granting autonomy to individuals in relation to their personal data to specify the extent of usage of personal data and its processing and to create obligations for implementing organisational and technical measures in processing and protecting such data. In this regard, an independent authority – the Data Protection Authority ("**DPA**") – is proposed to be set up for creating an ecosystem system for responsible data handling.

In detail

Applicability

- Applicable to the Government and private sector.
- Personal data collected, disclosed, shared or otherwise processed within the territory in India.
- Foreign entities, processing personal data in connection with any business carried on in India or involving profiling of Indian individuals within India.

Definitions

- Personal Data means 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
- Sensitive Personal Data means personal data revealing, related to, or constituting, as may be applicable— (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;
- 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;
- 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

Processing personal data and sensitive data

- Personal data and sensitive personal data to be processed for specified purposes; consent to be obtained for the same.
- Consent to be free, informed, specific clear and capable of being withdrawn.

- Personal data including sensitive personal data to be retained only for such duration as is necessary to meet the purpose for which it is processed. Data fiduciary obligated to undertake periodic reviews for the same.
- For the purposes of performing functions of the State, ensuring compliance with a law or court order or responding to a medical emergency or for any other reasonable specified purposes (prevention of unlawful activity, credit scoring, recovery of debt etc.), the data can be processed without prior consent.
- In addition, the Bill also provides that any sensitive personal data may be processed only for (i) explicit consent, (ii) functions of state, (iii) compliance with a law or order of a court/tribunal, (iv) for prompt action in case of emergencies for passwords, financial data, health data, official identifiers, genetic data and biometric data.
- With respect to processing of personal data of children (under 18 years of age), appropriate mechanisms for age verification and parental consent to be incorporated by data fiduciaries.

Transparency and accountability measures

- Data fiduciary to implement policies and measures that ensure that business practices and technical systems are designed to protect the personal data of individuals; business practises followed are transparently disclosed; and adequate measures are in place for security safeguards and reporting data breaches.
- Mandatory appointment of a data protection officer (*even if data fiduciary is outside India),* conducting periodical data audits including maintaining accurate and up-to-date records and providing an effective mechanism for grievance redressal.
- Data protection impact assessment necessary where processing involves new technologies or large-scale profiling or use of sensitive personal data or any other processing that carries a risk of significant harm to individuals.

Transfer of personal data outside India

- With respect to personal data, data fiduciary to store at least one serving copy on a server or data centre located in India.
- Such personal data may be transferred outside India subject to conditions - contracts or intra-group schemes, approved by the DPA, data to be subject to adequate level of protection in jurisdictions approved by the Central Government, etc.
- Critical personal data, to be notified by the Central Government, to be processed only in a server or a data centre located in India.
- Sensitive personal data notified by the Central Government may be transferred outside India for provision of health services.

Exemption

- In certain specific cases, processing of personal data has not been allowed unless it is authorised by specific laws and procedures laid down by the Central Government. For instance: personal data in the interest of the security of the State.

Data Protection Authority of India

- The power and functions of the DPA *inter alia* include the following:
  - monitoring and enforcing the proposed law ;
  - taking prompt and appropriate action in response to a data security breach);
  - maintaining a database of significant data fiduciaries along with their data trust score;
  - examination of data audit reports and taking appropriate action;
  - registration of data auditors ;
  - monitoring cross-border transfer of personal data;
  - issuing codes of practice in accordance;
  - receiving and handling complaints;
  - conducting inspections and inquiries;

Penalties and remedies

- Penalties ranging from INR 50 million or 2% of total worldwide turnover to INR 150 million or 4% of the total turnover.
- Certain offences have been categorised as cognizable and non-bailable.
- The Central Government shall constitute an appellate tribunal to hear and dispose of any appeal against any order of the DPA.

The takeaways

- "The Report and Bill have presently been submitted to the Ministry. As the next step, the Bill will be tabled in Parliament before going for Cabinet approval.

- It is expected that the Bill, once passed, will be implemented in a phased manner with the constitution of the DPA being the first step as this will be important to put in place the promulgation and implementation of codes of practices and other necessary rules, regulations and procedures.
- The Bill introduces an overarching law on data privacy. However, specific sectoral norms/ laws, if issued by sectoral regulators for compliance, would also need to be aligned to the Bill as the Bill envisages precedence over other sectoral laws in case of conflict. For e.g. TRAI has recently released their recommendations for a data protection framework in the telecom sector. Similarly, the Ministry of Health and Family Welfare has issued guidelines regarding the protection of digital health data.
- In addition, the promulgation of data protection would need to be complemented by amendment of several other laws. For e.g. Right to Information Act, 2005, Indian Telegraph Act, 1885, Information Technology Act, 2000 etc.
- Also, mirroring of data in India shall entail significant investments in setting up data centres. Based on newspaper reports relating to the upcoming e-commerce framework, it seems that the Government will incentivise the creation of data centres by giving them the status of 'infrastructure' and possibly some tax exemptions. This would be an interesting space to watch."

Let's talk

For a deeper discussion of how this issue might affect your business, please contact your local PwC advisor

Our Offices

Ahmedabad

1701, 17th Floor, Shapath V,
Opp. Karnavati Club,
S G Highway,
Ahmedabad – 380051
Gujarat
+91-79 3091 7000

Bengaluru

6th Floor
Millenia Tower 'D'
1 & 2, Murphy Road, Ulsoor,
Bengaluru – 560 008
Karnataka
+91-80 4079 7000

Chennai

8th Floor
Prestige Palladium Bayan
129-140 Greams Road
Chennai – 600 006
Tamil Nadu
+91 44 4228 5000

Hyderabad

Plot no. 77/A, 8-2-624/A/1, 4th
Floor, Road No. 10, Banjara Hills,
Hyderabad – 500034
Telangana
+91-40 44246000

Kolkata

56 & 57, Block DN.
Ground Floor, A- Wing
Sector - V, Salt Lake
Kolkata – 700 091
West Bengal
+91-033 2357 9101/
4400 1111

Mumbai

PwC House
Plot No. 18A,
Guru Nanak Road(Station Road),
Bandra (West), Mumbai – 400 050
Maharashtra
+91-22 6689 1000

Gurgaon

Building No. 10, Tower - C
17th & 18th Floor,
DLF Cyber City,
Gurgaon – 122002
Haryana
+91-124 330 6000

Pune

7th Floor, Tower A - Wing 1,
Business Bay, Airport Road,
Yerwada, Pune – 411 006
Maharashtra
+91-20 4100 4444

For more information

Contact us at
pwctrs.knowledgemanagement@in.pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Jamshedpur, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

Follow us on: