Personal Data Protection Bill, 2019: What Indian citizens can expect

April 2020

pwc

Introduction

India is one of the world's largest democracies, but here is no 'singular piece of legislation' in India currently to address the very important issue of privacy. In 2018, a draft of a new law – the Personal Data Protection (PDP) Bill – to monitor data privacy in India was introduced in the Parliament. Post the Supreme Court's ruling in 2017, which classified privacy as a fundamental right (in relation to the concerns about Aadhaar), the Government of India (GoI) rightly took a step towards forming stricter data protection and privacy laws in India. The bill underwent a few changes and the 2019 version was passed by the cabinet in December 2019, after which it was referred to a joint committee (comprising of members of the Lok Sabha and Rajya Sabha), which is to present a final report before the next budget session for final deliberation before it becomes a law.

The PDP Bill primarily focuses on the people of India and protecting their privacy. It seeks to provide more control to Indians over their personal information and create a culture towards respecting informational privacy of individuals. At the same time, it tries to balance the importance of personal privacy and new technological innovation to help people gain ethical and fair advantages from data they choose to share and thus create an environment of trust around processing of personal information.

In this article, we will discuss our views and perspective on the impact of the PDP Bill on Indian citizens.

Protect and empower the vulnerable classes

01

Children: Children are curious by nature, psychologically impressionable, vulnerable to abuse and easily swayed. The experiences they undergo during childhood form the basis of their adult life. They lack the maturity to understand the threats in cyberspace and the impact of risks posed by online sources. Currently, it's only the Information Technology (IT) Act, 2000, along with other small sectoral laws (e.g. RBI laws), which addresses some aspects related to cyberspace and its risks. The PDP Bill has provisions for internet use by children and how data related to children is used by organisations. Some of the provisions in the bill are:

- The PDP Bill talks about 'parental consent' when processing personal data of a child. This would help in creating more awareness, along with an additional layer of safeguard to protect children from online risks.
- Since the processing of data is based on principles, it would make governments (state and Central) and the private sector more accountable when personal data of children is processed for educational apps, biometric usage, social media usage, etc.
- The GoI would be able to take steps against social media companies and other organisations if data connected to children is misused in any form, especially since social media platforms, known to be fraught with cyber bullying or abuse of children, may fall under the category of significant data fiduciary.
- Profiling of data related to children is prohibited, thus safeguarding children from biases or discrimination threats.

It has been observed that Indian children are buying goods and products like alcohol, gaming products and medicines, whose purchase is prohibited online. There is a robust age verification process mandated by the GoI and the Data Protection Authority (DPA) would formulate rules on this and it would no longer be left to the discretion of the organisations to implement them. This would further help the cause of protecting Indian children in the digital space and having a standard practice and level of security

Data privacy and employer-employee relationship: Privacy has been recognised as a fundamental right and the Supreme Court's 2017 ruling emphasises individual choice as an important aspect of privacy. The PDP Bill, unlike the General Data Protection Regulation (GDPR) in the European Union (EU), provides for a separate legal ground for organisations to process employee personal data that is necessary for purposes of employment, but allows employee-sensitive personal data to be processed only on the basis of consent, which in turn would go a long way in creating trust and confidence in employees and protecting their privacy Companies will be responsible for data collected even for hiring purposes, which means that all the information collected about candidates before they are offered employment would require higher degree of control and transparency. It also means that information that is no longer needed for employment purposes would need to be eradicated in a safe and non-recoverable manner.

The bill would thus also be helpful in addressing the issues of employee and workplace monitoring, as currently employee surveillance is not dealt with under the IT Act.

LGBT community: Indian society continues to be conservative in its acceptance of lesbian, gay, bisexual and transgender (LGBT) people. The PDP Bill would ensure that data related to LGBT people is treated responsibly, sensibly and adequately protected by adding 'personal information' about them in the sensitive personal data category, which would also mitigate the risk of discrimination to a great extent.

Patient data: The market for patient data is growing worldwide, including in India. Obligations like privacy by design, data privacy impact assessments (DPIAs) and individual rights provided by the proposed bill could privacy concerns of the patient community. Further, the range of justifiable reasons for collection of personal data may be restricted to limited and disclosed purposes only. Requirements related to consent, cross-border data transfer restrictions and technical safeguards would add an additional layer of protection and prevent misuse of patient data. It would be mandatory for hospitals and entities managing personal data of patients to keep track of patients' records. Usage of data for secondary purposes such as marketing would also get regulated with the help of the bill.

Enhanced control to consumers

02

The PDP Bill would provide more control and transparency to consumers, enabling them to become 'owners' of their information. Data accumulated on/from a consumer cannot be given to third parties without the consumer's consent. Records of processing, privacy by design and knowledge on the usage of 'personal information' would give consumers control in terms of knowledge of how, where and why their personal data is being processed. The individual rights related to data portability, access and correction, and objection to processing would strengthen consumer transparency and individual choice. Companies/institutions would have to protect an individual's IP address, browsing activity, name, address, financial details, etc. In case of a data breach, it is mandatory for organisations to send notifications to the DPA.

Increased accountability for handling citizens' data

03

The PDP Bill would hold both private and government organisations accountable for how sensitive and personal data is used by them, hence bringing in more transparency in terms of how the government (one of the largest data collectors in the country) handles citizens' data. This measure may even indirectly help the government in putting up mandatory additional security measures to protect this category of data, as this volume of data surely needs regulation and better control. Although there are exceptions carved out for the GoI to exempt some of the processing by the state from the applicability of the PDP Bill, these are not without certain conditions and in addition to this, such exemptions would have to pass the tests of proportionality

Enhanced security for personal data of not only citizens but any processing activity within India

04

The applicability of the bill is extraterritorial, which means that it seeks to protect the data of not only Indian citizens but any data principal within the territory of India whose data is being processed by Indian companies or MNCs situated in India or outside. Data audits, trust scores, security parameters, etc., introduced by the PDP Bill would surely pave the way for a uniform data protection structure in our country and result in stronger security measures to protect citizens' data.

Enhanced rights to the citizens on their personal information

05

The PDP Bill, 2019, has further enhanced the data principals' rights in terms of a) deletion of data which is no longer required, making this provision a requirement by law, and b) giving citizens the right to know what data is shared with the data fiduciary and to what extent the data has been shared by the fiduciary with others. All these rights add to the transparency aspects of data privacy for citizens.

The 2019 bill introduces the provision of sandbox to pave the way for responsible and more regulated methods of scientific research and innovation with reduced risks and transparency, thus balancing individual privacy with technological advancement. Also, anonymised data is kept out of the purview of the bill, which may further help in experiments without compromising privacy. The GoI has also proposed a jail term for de-identification of anonymised personal data as a deterrent to add an additional layer of protection for individuals and instil a sense of accountability for various bodies processing personal data.

MeitY notification on non-personal data vs personal data

06

On 13 September 2019, the Ministry of Electronics and Information Technology (MeitY) announced the setting up of an expert committee to discuss aspects of community data. Community data is defined as any anonymised, non-personal or public data, which is not private. The 2019 version of the PDP Bill also defines the term non-personal data.

Ownership of community data, including non-personal data, is questionable, as there are debates on who owns it – the government or the individual. Data belonging to an individual may be used along with other data like traffic records and usage of electricity, which may also belong to the individual but has a larger impact.

There are definite benefits of regulating community data but these have to be balanced with individual rights, and care should be taken to not dilute the traditional concept of 'privacy' vis-à-vis 'community data'. Thus, it needs more analysis and probing into the usages and risks attached to non-personal data or even deidentified data.

Two clear takeaways from the PDP Bill

The PDP bill seems to have a clear focus on empowering citizens by giving them considerably more control over their data. The bill would certainly change the way Indians deal with and perceive their own personal data and that of others.

Once the bill becomes a law, it would also help in better data management practices and data-related awareness in society. For example, businesses would also have to deal with personal data more seriously, and would have to relook at all their data processing activities. It would pave the way for a stronger data security and privacy control framework and guidelines in India, similar to those established globally.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in 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, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

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

Acknowledgements

This article has been researched and authored by Dhrtimaan Shukla, Sonali Saraswat and Harbani Gill

Contact us

Dhritimaan Shukla
Partner and Privacy Leader
PwC India
dhritimaan.shukla@pwc.com
+91-9899038326

Sonali Saraswat
Associate Director, Privacy
PwC India
sonali.saraswat@ pwc.com
+91-9620701515

pwc.in

Data Classification: DC0

SG/April2020-M&C5393