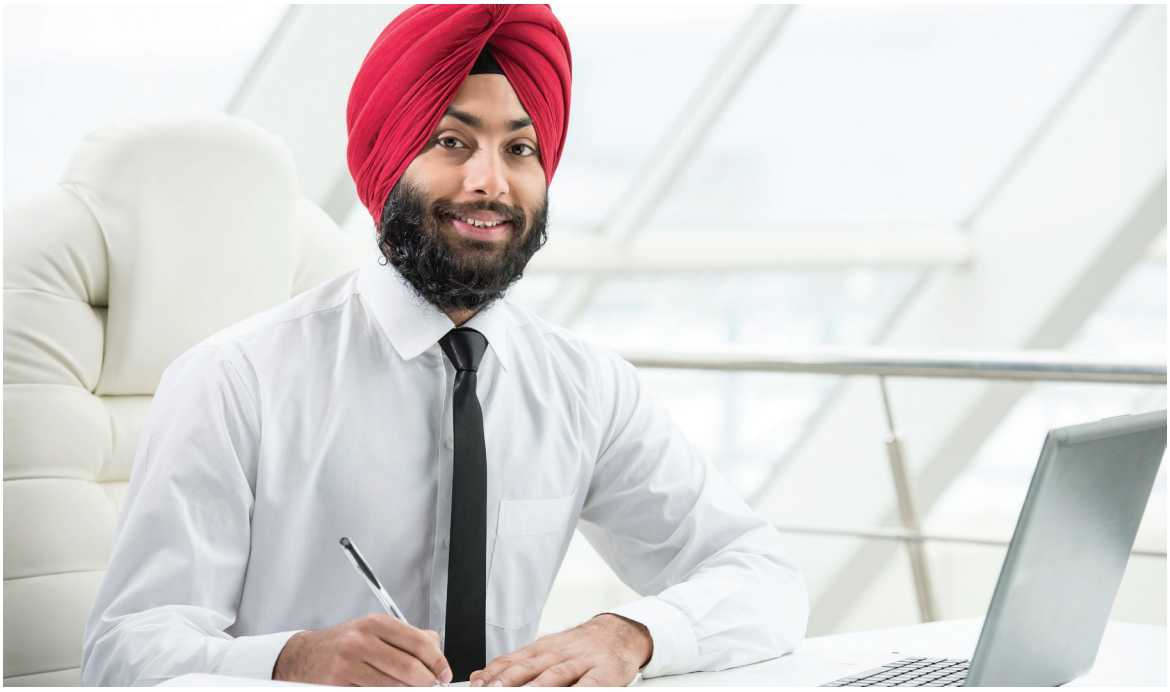
The Personal Data Protection Bill, 2018



What are the 10 things an organisation needs to do?

1. Place privacy at the heart of everything
2. Relook at the mechanism used to collect personal data
3. Refresh consent
4. Provide rights to the data principal*
5. Limit storage of personal data
6. Localise organisational data
7. Perform age verification and obtain parental consent before processing personal data of children
8. Take a data breach more seriously
9. Revisit data security safeguards
10. Meet additional requirements if it is a 'significant data fiduciary'*

pwc

www.pwc.in

From 'body corporate' to 'data fiduciary' – what do organisations need to do?

The much-awaited Personal Data Protection Bill is finally out and organisations across industries are evaluating the impact of the regulation on their businesses. While India-based organisations with global footprints have already taken measures to comply with regulations such as the General Data Protection Regulation (GDPR), entities which operate primarily in the Indian market are anxious to understand the impact of the Data Protection Bill on their day-to-day operations. This document summarises the key impact of the bill on Indian organisations which handle personal information.

Key definitions:

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 personal data.

Data principal means the natural person to whom the personal data refers.

1. *Place privacy at the heart of everything*

In line with many regulations across the globe, the Indian Personal Data Protection Bill also introduces and mandates the concept of 'privacy by design' (PbD).

Organisations will have to embed this concept in the entire data life cycle – collection, processing and use, storage, transmission, archival and disposal. A robust organisation structure and processes supported by technology will have to be established to ensure that the data protection obligations are fulfilled and the data principal is not harmed. Organisations will have to define and establish a data privacy framework as well as privacy controls for the different categories of personal data (personal data and sensitive personal data) at the all the stages of the data life cycle. The framework and controls will need to be published and communicated to all organisational departments by taking a top-down approach. Further, the concept of privacy will have to be introduced to the 'DevOps' and new product development function. This function will assume the role of a privacy toll gate at the planning and go-live stage for any new product, business process or application. For existing business processes and applications managing personal data, organisations will have to perform a 'privacy assessment' and implement the identified privacy controls. Finally, a privacy training and awareness programme will need to be rolled out in the organisation, right from induction to periodic refreshers.

2. *Relook at the mechanism used to collect personal data*

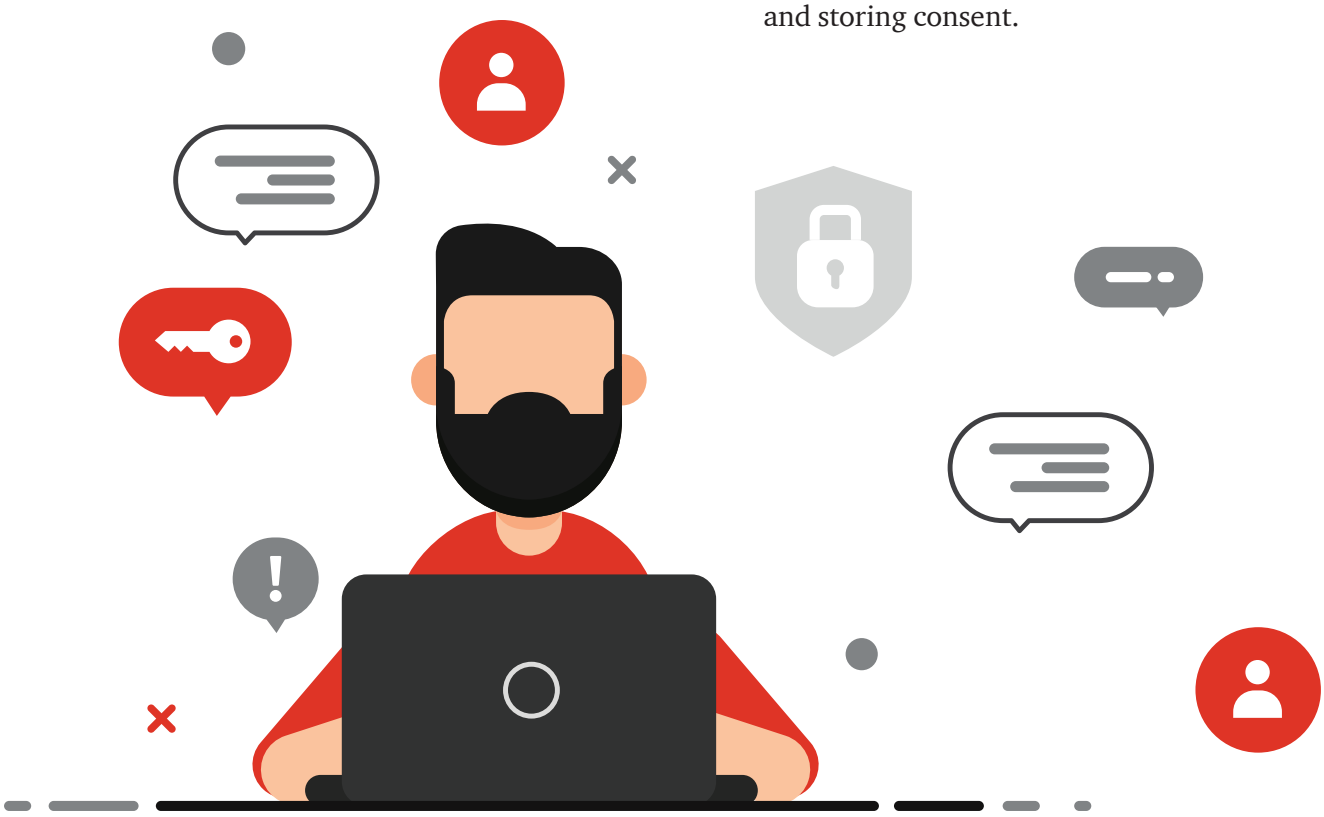
Organisations will need to limit data collection to the minimum required for the purpose of processing.

All organisations, irrespective of their size, turnover or industry, will have to gain visibility into transactions involving the collection and use of personal data. They will have to re-examine the employee on-boarding and customer acquisition process and restrict the collection of personal data only to that necessary for providing the service to the data principal (natural person) or to fulfil the purpose specified. These aspects need to be addressed at the various collection points – physical and digital, including websites, online forms, store and point of sale (POS) locations and mobile applications. Some additional technology interventions will be needed behind the scenes—for instance, with regard to the use of cookies to collect personal data (either intentionally or unintentionally) and prepare a detailed profile of individuals and their preferences. Additionally, data collected for one purpose should not be blindly repurposed without further consent. Organisations need to relook at the testing strategy for their digital initiatives and the use of personal data in the test or development environments.

3. *Refresh consent*

Organisations will have to obtain the consent of the data principal before processing personal data. Explicit consent needs to be solicited before processing any sensitive personal data (e.g. financial data, health data, biometric data, passwords). Valid consent will be one that is freely obtained, explained in detail, specific, clear and capable of being withdrawn equally easily by the data principal.

Organisations will have to refresh the notice and consent forms on all personal data acquisition touchpoints – digital or physical. Notices and consent will have to be reworded to ensure that the purpose of processing, contact details of the Data Protection Officer ([DPO] in the case of a significant data fiduciary), possibility of cross-border transfer of personal data, and the right to withdraw consent are clearly and precisely communicated. All fine print will have to be relooked at to ensure that potentially harmful terms do not escape the attention of the data principal. Consent boxes on the data acquisition touchpoints (physical acquisition forms, online forms, websites, etc.) should not be pre-checked, especially in cases where the organisation is dealing with sensitive personal data. As the responsibility for proving that consent was obtained from the data principal will be with the organisation, organisations will have to resort to identifying the technology enablers for managing and storing consent.



4. Provide rights to the data principal

The right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of information privacy. The data principal (natural person) will have the 'right to confirmation and access' and 'right to correction' of personal data. Further, the data principal will have the 'right to data portability' and 'right to be forgotten'.

The biggest challenge which organisations face today is the multiple versions of the same data stored in different places and different systems such as ERP and CRM. This will require organisations to perform a massive data mapping exercise to understand the collection, storage, processing and transfer of information pertaining to individuals to support the data principal in exercising his rights. Organisations will have to prepare a brief summary of the personal data of the data principal being processed or that has been processed, and this summary will have to be updated and provided to the data principal. Organisations will have to invest in mechanisms and techniques to provide the data principal access to a copy of all the personal data they hold for correction or completion or update of inaccurate or incomplete personal data, thereby aiding data quality. Organisations will also have to take into consideration the data they provide to third parties for any legitimate business purpose. Also, it is imperative to record all requests from data principals and track them to successful closure which means establishing the process, technology and structure to address such requests.

Organisations will also have to acknowledge the receipt of requests from the data principal exercising any of the rights mentioned above within a reasonable time frame. Further, they will need to provide data principals the right to data portability, i.e. sharing of the data with other organisations or deletion of data upon request.

5. Limit storage of personal data

Organisations will need to retain personal data only as long as it is reasonably necessary to satisfy the purpose for which it is obtained. They will have to periodically review the personal data in their possession from a retention point of view.

All organisations, irrespective of their size, turnover or industry, will have to draft a data retention policy. The policy, at a minimum, will have to define the categories of the data it covers, purpose of collection and processing, responsibility and obligations, and conditions under which data needs to be retained and deleted. Apart from the data pertaining to the current period, data governance should also address the type of controls organisations should implement for backed up and archived data. Organisations may also look at anonymising the data, instead of deleting the data once the object of processing has been achieved. The provisions of the bill do not apply to the processing of anonymised data

While formulating policies, the sectoral and other statutory/regulatory requirements also needs to be factored in when determining the retention period. For example, the financial sector will have to look at the same in conjunction with the Know Your Customer (KYC) guidelines issued by the RBI which require information pertaining to the identification of the customer to be retained for at least five years even after the closure of the account.

6. Localise organisational data

An organisation will need to store at least one serving copy of the personal data on a server or data centre located in India. Also, the bill requires organisations not to transfer or store overseas sensitive personal data or certain categories of personal data identified by the Central Government as critical personal data.

For transfer of personal data (other than sensitive personal data or critical personal data) outside India, an organisation will have to agree on standard contract clauses approved by the authority.

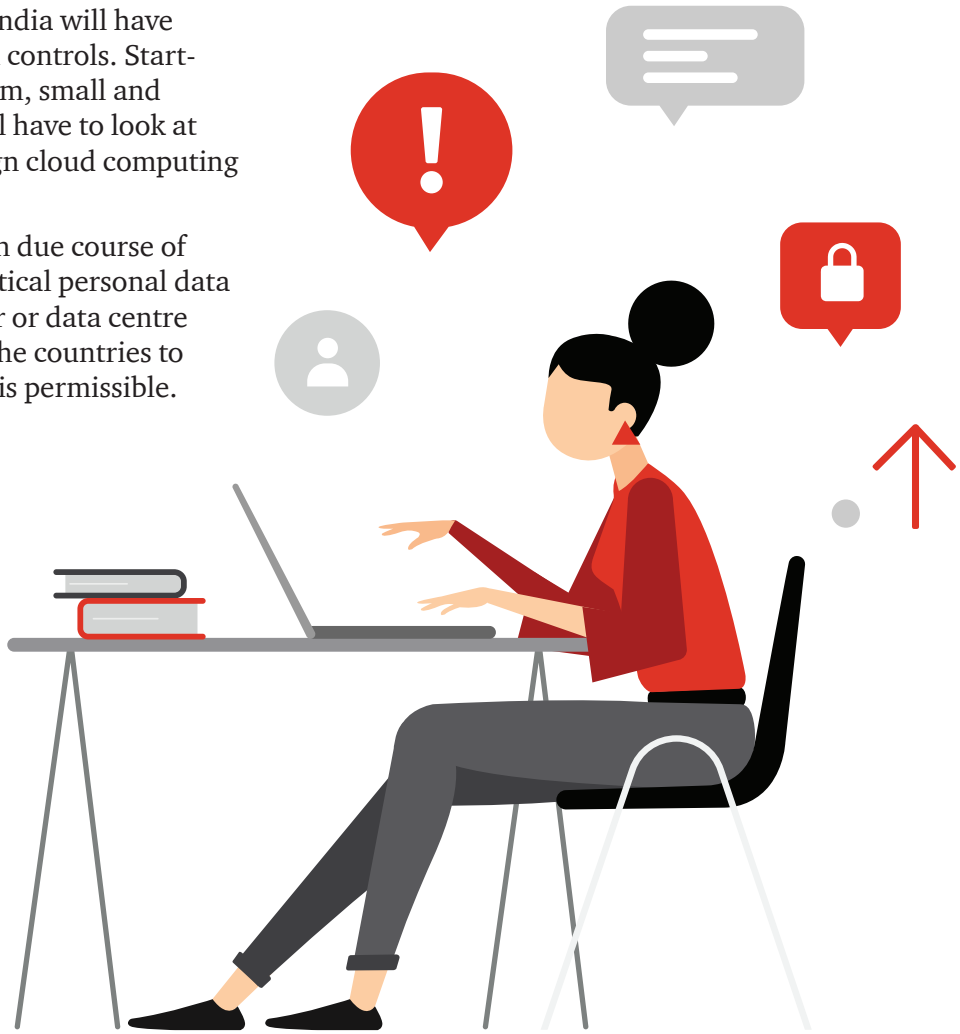
Many organisations have moved to cloud infrastructure services for fulfilling their storage and computing requirements. Organisations will have to relook at their cloud strategy and gain visibility into data storage locations. Global organisations with a presence in India will have to relook at how the personal data of Indian citizens moves across the border and the data centres in which it will be stored. The disaster recovery strategy of global organisations with disaster recovery sites outside India will have to be revamped with additional controls. Start-ups and, to some extent, medium, small and micro enterprises (MSMEs) will have to look at alternative options to the foreign cloud computing services they generally use.

The Central Government may in due course of time notify the categories of critical personal data to be processed only on a server or data centre located in India and prescribe the countries to which data transfer from India is permissible.

7. Perform age verification and obtain parental consent before processing personal data of children

The new data privacy regime requires organisations processing personal data of children to follow due care in protecting the rights and interest of children. Organisations offering services primarily to children, other commercial websites or online services directed at children or those processing a large volume of personal data of children will be identified as 'guardian data fiduciaries'. These fiduciaries will not be allowed to profile, track and perform behavioural monitoring of children, or target them with potentially harmful advertisements.

Organisations with a user base under the age of 18 years will have to make changes to their technology platform to incorporate parental consent and age verification. Advertising-based revenue models, if they involve profiling of children, will have to be modified.



8. Take a data breach more seriously

Organisations will have to notify the Data Protection Authority (DPA) of any personal breach relating to personal data processed by it which can cause harm to a data principal. Failure to notify a breach will make the organisation liable to a penalty under the provisions of this law.

Organisations will have to clearly outline a data breach as one of the possible scenarios in their incident or cyber response plans. They will have to prepare themselves to handle data breaches by performing mock drills. A clear distinction will have to be established between a normal security incident and a data breach. Relevant guidelines will have to be communicated to all stakeholders managing personal data. It will be helpful for organisations to know and map personal data – what data, who all have access to it, where the data is going, where it is stored, the data flows in and out of the organisation, and the potential threats and controls for each area. The process must enable an organisation to identify a data breach and its personal data dumps on the Internet in near real time or at the earliest, before such a breach or leakage is detected by the DPA and general public. Organisations with a humongous amount of data and a large threat landscape may consider identifying suspicious data access by performing behavioural analytics. In case an organisation does not have an in-house forensic or legal team, it should have an external arrangement to ensure that the respective teams are available at short notice to support the investigation in the event of a data breach. Organisations will have to enable data access logs, log administrator activities and monitor them. They will have to identify and nominate a competent person responsible for communicating with the DPA (either a DPO or equivalent) and the communication process he or she needs to follow. Further, organisations will have to be ready to post the details of a personal data breach on their website, at the direction of the DPA.

The DPA will define 'as soon as possible' or the time period for notifying it of any personal data breach.

9. Revisit data security safeguards

Under the proposed bill, organisations are required to implement appropriate security safeguards to protect the personal data handled by them. They should revisit their information security practices and solutions to address the privacy need. Thus far, most organisations have been focused on protecting the integrity and availability of data. In the privacy regime, confidentiality of personal data becomes key, and accordingly, organisations will need to relook at security controls from a data life cycle standpoint (i.e. data capture, transmission, storage, retrieval and destruction). This may call for additional technology investments for security.

10. Meet additional requirements if it is a 'significant data fiduciary'

An enterprise may be classified as a significant data fiduciary (SFD) based on its turnover or the volume or sensitivity of personal data processed by it. Further, if an enterprise uses new technologies for processing personal data or conducting large scale-profiling and if such processing exposes the data principle to risks, the enterprise will be deemed an SFD.

In addition to all of the above requirements, the identified SFD enterprise will have to:

a. Register with the DPA of India;

b. Necessarily perform a risk-based data protection impact assessment (DPIA) for managing, minimising, mitigating and removing the risk of harm to any data principal;

c. Perform annual independent audits of its policies and measures for protection of personal data;

d. Appoint a DPO.

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 2,36,000 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, 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.

Contact Us

Sivarama Krishnan
Leader Cyber Security
sivarama.krishnan@pwc.com

Siddharth Vishwanath
Partner - Cyber Advisory Leader
siddharth.vishwanath@pwc.com

Anirban Sengupta
Partner - Cyber Security
anirban.sengupta@pwc.com

Hemant Arora
Partner - Cyber Security
hemant.arora@pwc.com

Krishna Sastry Pendyala
Executive Director - Cyber Security
sastry.pendyala@pwc.com

Manu Dwivedi
Partner - Cyber Security
manu.dwivedi@pwc.com

PVS Murthy
Partner - Cyber Security
pvs.murthy@pwc.com

Rahul Aggarwal
Partner - Cyber Security
rahul2.aggarwal@pwc.com

Ramanathan (Ram) V. Periyagaram
Partner - Cyber Security
ram.periyagaram@pwc.com

Sangram Gayal
Partner - Cyber Security
sangram.gayal@pwc.com

Sriram Sivaramakrishnan
Partner - Cyber Security
sriram.s@pwc.com

Sundareshwar Krishnamurthy
Partner - Cyber Security
sundareshwar.krishnamurthy@pwc.com

Unnikrishnan P
Partner - Cyber Security
unnikrishnan.padinjyaroot@pwc.com

Venkat Nippani
Partner - Cyber Security
venkat.nippani@pwc.com

Murali Krishna Talasila
Partner - Cyber Security
murali.talasila@pwc.com

pwc.in

KS/AUG2018-13965