Digital Personal Data Protection Act

On Aug 11th 2023, the India´s parliament approved the landmark Digital Personal Data Protection (DPDP) Act. This is great news for Wipro, a company that strives to put privacy at the heart of what we do.

Owing to India´s posture and ambition in relation to the digital economy, this legislation is both welcome and necessary, and we are confident that it will support India´s quest for digitalization and innovation moving forward.

Trust,clarity and transparency around the use of personal data is a fundamental drive for digital innovation.

Key concepts

Overall aim of the Act:

The objective of the Bill is to ensure that the processing of digital personal data is carried out in full respect for individual rights and grounded on a transparent, fair and lawful purpose.

Scope of the Act

The Act applies to digital data (including non-digital data which will be digitized subsequently) within the territory of India or outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

Territorial Scope

- Processing within the territory of India
- Processing outside india in connection with an activity related to offering goods and services within India

Material scope

- Personal data that is collected in digitised form
- Personal data that is collected in non-digital form and digitised subsequently.

Grounds for processing personal data

There are two grounds of processing defined in DPDPA under which organisations can process personal data:

Consent

The Data Principle may **give, manage, review, or withdraw their consent** to the data fiduciary directly or through a consent manager. Privacy notice to provided at the time of obtaining consent.

Certain Legitimate Uses

No seprate consent is required for certain “legtime uses” recognised under the Act. This includes where data is **voluntarily** provided or collected for a **legal obligation**. Privacy notice is not required for legitimate uses.

Consent should be

1. Freely given
2. Specific
3. Informed
4. Unconditional
5. Unambigious
6. Requires affirmative action

FAQ

Q. Who will provide consent?
A. Data Principal

Q. Who will ask for consent?
A. Data Fiduciary

Q. How consent should be requested?
A.
- **In clear and plain language**
- **Using itemised notice**

Q. How can consent be withdrawn?
A. By contacting data fiduciary or consent Manager

Scenarios covered under legitimate uses

For personal data provided **voluntarily** by the Data Principal

For personal data prpcessed for function under **any law or judgement isssued uner lay**

For responding to a **medical emergency** involving a threat to the life of the data principal or other individual

For maintaining **public order and ensuring safety**

For purposes related to **employment**

For performing activites in **public interest**

Rights of data principals

Right to grievance redressal

The Data Fiduciary and Consent Manager is required to respond to the grievance of the Data Principal within a time period as may be prescribed

Right to nominate

Data Principal have the right to nominate any other individual, who shall in the event of death or incapacity of the data principal, exercise the right of the data principal

Right to access information about personal data

The Data Principal can excercise their right to obtain confirmation from the data fiduciary regarding data processing, summary of personal data and identities of all data fiduciaries and data processors

Right to correction and erasure of personal data

Data Principal can reach out to Data Fiduciary in order to exercise their right to correct, complete, update and erasure of their personal data.

The key obligations for organizations such as Wipro:

To abide to the new Act, there are certain obligations organizations must adhere to as a data fiduciary (entity that determines the purpose and means of processing of personal data) :

Processes personal data accurately and in line with legitimate uses.

Ensure disposal of personal data retained by organizations as well as it's processors (entity who processes personal data on behalf of a Data Fiduciary) as soon as the data principal withdraws her consent, or when the purpose of processing is fulfilled.

Protect personal data in its possession which is collected directly or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breaches.

Notify the Data Protection Board and the concerned data principal(s) upon discovery of data breach per timelines that shall be stipulated by the Board.

Establish an effective mechanism to redress the grievances of Data Principals.

Implement appropriate technical and organizational measures to ensure effective observance of the provisions of this Act.

Empanel data processors with a valid contract.

Whenever any data is to be shared with other data fiduciaries, it must be accurate, complete, and updated.

Appoint a Data Protection Officer and support the Internal Audits and external Audits/Certifications

Most of these obligations are key KPIs of Wipro's Data Privacy Framework that are implemented, evaluated and monitored on regular basis, these are already part of the foundation privacy principles.

What is Wipro doing?

At Wipro, we adhere to the highest standards of data protection. We pride ourselves on safeguarding our clients and employees data with the utmost respect and care.

Our Privacy framework is GDPR focused with a strong degree of decentralization to meet local requirements. In addition, our privacy Policy is articulated in our Privacy Information Management System (PIMS), which is an ISO standard to provide management direction and privacy support in accordance with business requirements and relevant laws & regulations to ensure confidentiality, integrity, and availability of customer assets, information, data, and IT services.

Below are the salient features of the Privacy framework at Wipro -

- Wipro is certified under the ISO 27701:2019 standard for Privacy Information Management Services including physical security & employee safety.
- Technical (password protection) and organizational (user account management) measures with respect to user identification and authentication have been implemented.
- Through comprehensive physical and logical security controls, unauthorized persons are prevented from gaining access to data processing systems, thereby avoiding any kind of unauthorized access to personal data.
- All aspects of transmitting personal data are regulated.
- Data is protected against accidental destruction or loss by implementing adequate measures like encryption, pseudonymization etc.
- **Personal data processed on behalf of customers are processed strictly in compliance with the controller's instructions dividing responsibilities between the contractor and the client.**
- Wipro has segregated processing (storage, alteration, deletion, transmission) of data for different purposes.
- Wipro has processes for regularly testing and assessing the effectiveness of technical and organizational measures to ensure secure processing while strengthening the internal IT, IT security governance, and management.

In addition to the above, Wipro has structured a DPDP compliance project in lines of –

- **Familiarizing with the DPDP Act:**
  - closely following the updates.
  - continuously understanding the key provisions, latest updates, requirements, and obligations outlined in the act.
- **Assessing and building data privacy:**
  - Evaluating the current on-ground compliance status in all functions.
  - Creating a phased action plan covering governance, technology, people, and processes.
  - Establishing a privacy organization with defined roles, including the DPO.
- **Inventorying of personal data systems:**
  - Identifying critical data storage and processing systems.
- **Identifying data processors:**
  - Listing third parties managing personal data.
  - Updating agreements and communicating responsibilities.
- **Drafting DPDP Act-compliant documents:**
  - Creating approved data privacy policies and processes.
  - Updating necessary documents.
  - Developing privacy notices, consent forms, and standard contract clauses
- **Designing consent mechanisms where applicable:**
  - Defining consent types.
  - Developing user-friendly consent processes.
  - Implementing efficient consent management tools.
- **Evaluating existing data principal rights handling:**
  - Revisit processes for addressing data principal rights.
  - Assessing procedures for request handling.
  - Using tools for efficient rights management to address large volume of requests from individuals as well as Consent Manager
- **Implementing data breach response:**
  - Updating breach management processes.
  - Integrating with incident management.
- **Implementation of data retention periods:**
  - Categorizing data and aligning retention periods with requirements.
  - Evaluating and implementing privacy technologies:
  - Choosing suitable tech solutions for effective and automated DPIA, inventories, vendor risk assessments.
  - Assessing compatibility and scalability.
  - Implementing chosen solutions.
- **Conducting a data audit:**
  - A detailed reassessment to understand the personal data being collected, processed, stored, or transmitted.
  - Identifying the categories of data, the purposes for which it is used, and any third parties involved.
- **Implementing privacy by design:**
  - Incorporating privacy and data protection considerations into your IT systems, products, and services from the design stage.
  - Minimizing data collection, implementing privacy-enhancing technologies, and conducting privacy impact assessments
- **Training employees:**
  - Educating the employees on the DPDP Act's provisions and their responsibilities in ensuring data protection and privacy
  - including training on secure data handling, incident response, and breach notification procedures.
- **Monitor and review compliance:**
  - realigning regular assessment of the data protection practices ensuring ongoing compliance with the DPDP Act.
  - Staying updated on any changes or amendments to the act and adjust your processes accordingly.

How can Wipro gain customer trust and foster innovation culture post DPDP's introduction?

The safety of our client's data is our utmost priority. At Wipro, we are already compliant with GAPP. We ensure ongoing compliance with upcoming regulatory updates such as DPDP.

As per the section 17d, the Act mentions that personal data of Data Principals not within the territory of India, is processed pursuant to any contract entered with any person outside the territory of India. **Hence the existing customer contracts will supersede.**

There may be concerns with respect to the Section 36 of the Act which mention that Government has the power to call for information from any Organization including Intermediary. However, it is important to note that this power applies to processing activities that are aligned **for the purposes of the DPDP** and is hence limited to the scope of the Act that excludes customer data (originating outside of India). Apart from the direct purposes of the State, such as subsidy, surveys, benefits etc., processing of data by government is **limited** to certain legitimate interests such as Sovereignty and integrity of the State or where disclosure of such information is required by any law that is in effect or for judicial purposes as explained in Section 7.

Furthermore the power to enquire, mitigate, penalize the Organizations for their non-compliances is with the Data Protection Board (DPB). In India, the Sovereign power is the Parliament and hence the power to make rules lies with the Central Government and not the subordinate legislation i.e., Data Protection Board. However, DPB is completely accountable and independent of government with respect to execution of the Act. There is also an Appeal and Dispute resolution through an independent body called "Appellate Tribunal" which will uphold the rights of the Data Principals and Organizations by offering an opportunity to be heard and further make changes in the Act, as required

Furthermore, with the new Act coming in, we will be reconsidering the consent mechanism, existing data retention policies, assessment mechanism etc. for ensuring unequalled data security and data privacy proficiency for our customers and clients with the help of tailor-made periodic assessments.

How is Wipro training the employees and customers on the importance of data protection and privacy in the digital economy?

Wipro's Data Privacy Office with the support of relevant departments (Learning and Development, Corporate Affairs & Communication) ensures that there is an ongoing privacy training program in place that involves following –

Regular communications about Data Privacy which includes mandatory annual training.

Mandatory training for New Joiners and annual training refreshers for existing employees.

Role based/ function specific recurring training for existing employees.

Data Privacy awareness campaigns deployed throughout the year.

Ensure all reporting personnels understand the requirements of the Privacy Policy.

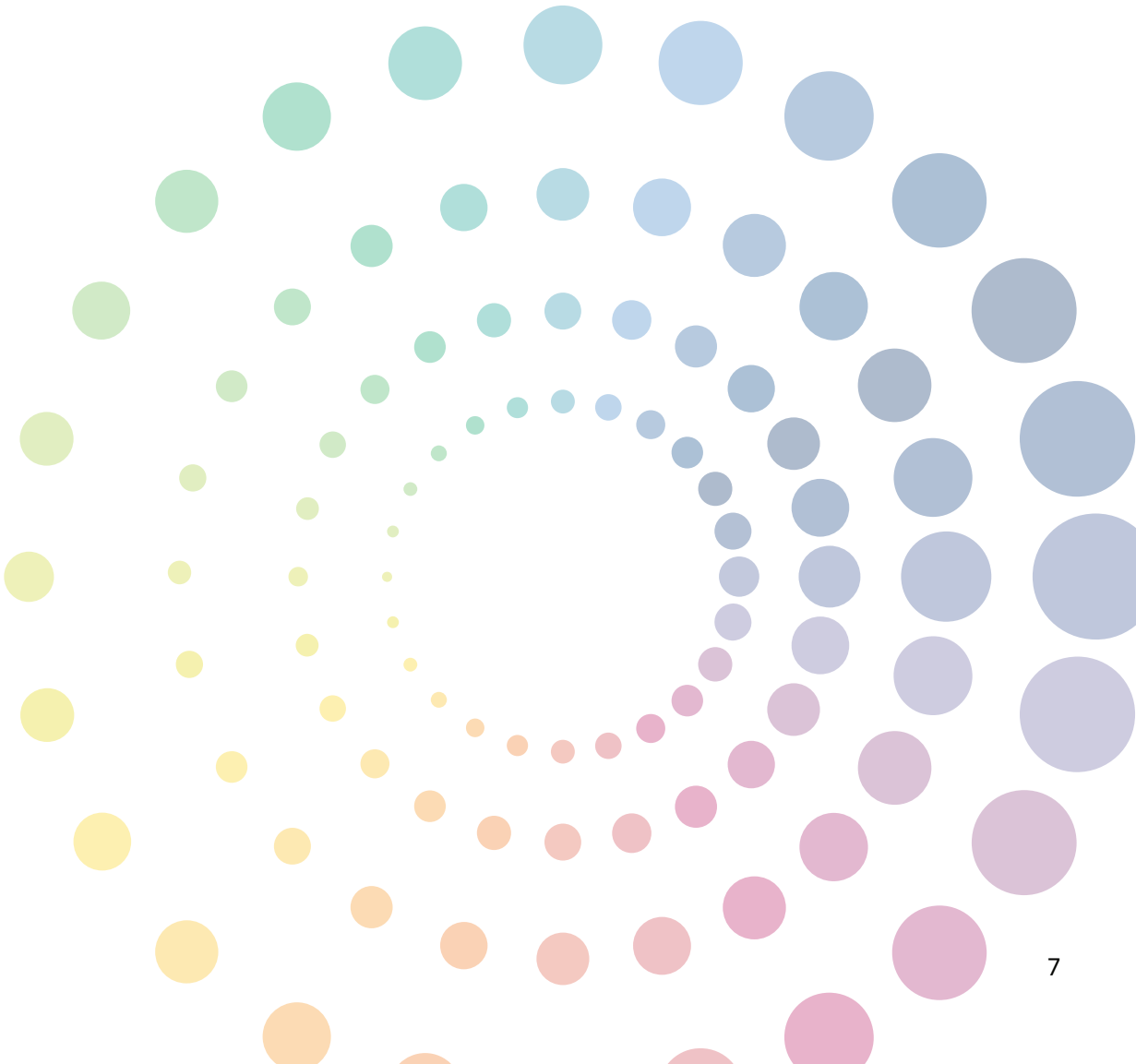
Providing all necessary trainings and/ or guidance to assist with the implementation process, and for monitoring compliance with the Privacy Policy.

The Data Privacy Office has also started to train the internal teams like Legal, CISO, BiTS as to understand the requirements of the DPDP and initiate the implementation.

Does the Act have any impact on the cross-border data transfer?

In DPDP, the Government has embraced an open approach to global data transfers. Unlike the EU adequacy system, which assumes third countries are "inadequate" unless proven otherwise, India's law would render all countries adequate unless otherwise asserted by the Indian government. (It does however leave in place certain existing localization requirements).

With respect to cross-border data transactions, the Act prescribes a simplified process. Under the Act, such transfer may occur with prior approval of the Centre. The government may, while providing such approval, prescribe additional provisions that will have to be followed. However, unlike the GDPR, the Act does not have an elaborative framework for cross-border data transactions.



Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

About Wipro Limited
Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With nearly 245,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at **www.wipro.com**

IND/BRD/NOV2023-DEC2024