The Digital Personal Data Protection Act, 2023

Advent of Privacy Era in India

DPDP CONSULTANTS

Salient features of the Act

Journey So Far

August 2017 — Hon'ble Supreme Court of India declared Right to Privacy as a fundamental right in K.S. Puttaswamy judgement

July 2018 — Committee formed under the chairmanship of Justice Srikrishna submits report along with draft of PDP Act, 2018

December 2019 — The PDP Act, 2019 introduced in the Lok Sabha and was referred to Joint Parliamentary Committee (JPC)

December 2021 — JPC releases its report and a new version of the Act as Data Protection Act (DPA)

November 2022 — Ministry of Electronics and Information Technology (MeitY) releases draft Digital Personal Data Protection Bill (DPDPB) for public consultation

July 2023 — Union Cabinet approves the draft DPDP Bill, 2023

August 2023 — The President of India assents to the Bill to make Digital Personal Data Protection (DPDP) an Act

Applicability of the Act

Processing of digital and digitized personal data

- Processing of personal data within the territory of India and outside India
- Activity related to offering goods and services to Data Principals within India

Does not apply to

- Processing for domestic or personal purposes by individuals
- Personal data made publicly available

Key Terminologies

Consent
Organizations should seek a consent, which is freely given, specific, informed and unambiguous indication of the Data Principal's wishes, by a clear affirmative action

Consent Manager
A consent manager represents the Data Principal and takes action on their behalf when granting, managing, reviewing and revoking consent

Notice
Should be clear, itemized and in simple language. Data Principals should have the option to access information in English or in any of the 22 languages (as per Eight Schedule of Indian Constitution)

Data Fiduciary
Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data

Processing outside India
Government to notify countries to which transfer is not permissible unlike the whitelisting approach under the General Data Protection Regulation (GDPR)

Data Principal
• An individual to whom the personal data relates | • A child, includes the parents or lawful guardian of such a child
• A person with disability, includes their lawful guardian acting on their behalf

Children's Data
For children < 18 years of age, consent from Parents/Guardians is required. Behavioural monitoring and Targeted Advertising is prohibited

Data Processor
Any person who processes personal data on behalf of a Data Fiduciary

Legitimate Uses
Consent is not expressly needed for situations such as
• Voluntary disclosure by data principal | • Reasonable expectation by data principal | • Performance of function under the law
• Medical emergency among others | • Compliance with any judgment issued under any law | • Threat to public health
• Ensure safety in case of any disaster

Salient features of the Act (Contd.)

Obligations of the Data Fiduciary

- Engage with a Data Processor to process personal data on its behalf through a valid contract only
- Provide a clear, concise and comprehensible notice to Data Principals
- Obtain verifiable parental consent before processing children's personal data
- Abstain from processing personal data that may cause harm to children or undertake behavioral monitoring of children or targeted advertising directed at children
- Implement technical and organizational measures to ensure effective adherence with the Act
- Delete and cause its Data Processor to erase data as soon as the purpose is accomplishedipsum
- Report Personal Data Beaches to Data Protection Board and Data Principals

Significant Data Fiduciary

Significant Data Fiduciary will be determined based on an assessment which include

The volume and sensitivity of personal data processed

Risk to the rights of data principal

Potential impact on the sovereignty and integrity of India

Risk to electoral democracy

Security of the state

Public order

Obligations of the Significant Data Fiduciary

Appoint a Data Protection Officer (DPO) based in India

Appoint an Independent Data Auditor for evaluating compliance

Conduct Data Protection Impact Assessment (DPIA) & periodic audits

Data Principal Rights

Right to information
Data Principals have the right to seek information on how their data is processed, available in clear and understandable way

Right to grievance redressal*
Individuals have the right to readily available means of registering a grievance with a Data Fiduciary

Right to correction and erasure
Individuals have the right to correct inaccurate / incomplete data and erase data that is no longer required for processing

Right to nominate
Individuals can nominate any other individual to exercise these rights in the event of death or incapacity

**Timeline to respond to grievances raised by Data Principals shall be notified by the Central Government*

Salient features of the Act (Contd.)

Personal Data Breach

- A Data Fiduciary is required to protect personal data, including any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent Personal Data Breach.
- In the event of a Personal Data Breach, the Data Fiduciary needs to notify the Board and each affected Data Principal of such breach.

- No specific timeline for reporting the breach
- Data Fiduciaries to inform about the breach in prescribed form

Penalties

Up to **INR10,000**
Breach in observance of duty of Data Principal

Up to **INR200 Crore**
Breach in observance of duty of Data Principal

Up to **INR200 Crore**
Breach in observance of duty of Data Principal

Up to **INR250 Crore**
Breach in observance of duty of Data Principal

The Data Protection Board

The Central Government may, by notification shall appoint and establish, an independent board to be called the Data Protection Board of India (Board).

- This Board should consist of a chairperson and other members, who should be appointed by the Central Government
- The Board is entrusted with the task of enforcement, including determining non-compliances, imposing penalties, issuing directions and mediation (to resolve dispute between parties) to ensure compliance with the law
- The Board is enshrined with powers of a civil court and appeals against its decisions lie to Telecom

Amendments to Prevailing Laws

Existing IT Act, 2000 and Right to Information Act 2005 are amended as following:

Article 43(A) (Compensation for failure to protect data) of IT Act 2000 is omitted

Section 8 (1)(j) RTI Act 2005 is amended to exempt the personal information which allows disclosure for public interest

Salient features of the Act (Contd.)

Key Highlights

Considering the volume and nature of personal data processed, the Central Government may by notification exempt certain provisions of the Act for a Data Fiduciary or a class of Data Fiduciaries including startups

When the consent for processing Personal Data was provided before the commencement of this Act, Data Fiduciary needs to provide detailed privacy notice describing the Personal Data collected and the purpose as soon as practicable after the enactment of this Act

Certain provisions* of the Act will not be applicable for the processing of Personal Data in India of a Data Principal not based in India pursuant to a contract signed with a person outside India

The Central Government may upon ensuring if the processing is verifiably safe, notify the age above which a Data Fiduciary shall be exempt from applicability of children's personal data obligations

The Data Principal shall exhaust the opportunity of redressing her grievance with Data Fiduciary before approaching the Data Protection Board of India

Exemptions

The DPDP Act exempts Data Fiduciary from certain obligations (except for being esponsible for its data

- Processing for enforcing any legal right or claim
- Processing for performance of any judicial or quasi-judicial functions by any Indian court/tribunal or other body
- Processing in the interest of prevention, detection, investigation or prosecution of any offence of any law
- Processing of Data Principals outside the territory of India pursuant to any contract entered into with any person outside the territory of India by any person based in India
- Processing necessary for a merger / amalgamation or similar arrangement as approved by a court or other authority competent

Ambiguities

Below mentioned are the ambiguities in the Act:

01 ***Children's Data***
The definition of detrimental effect on well-being of a child as a result of processing their Personal Data has not been specified.

02 ***Breach Notification***
Absence of defined timeline for notifying a Personal Data breach to the Data Protection Board and the affected Data Principal(s).

03 ***Publicly available data***
The Act exempts any Personal Data that is made available publicly, but it does not clarify if the information is made available to public can be used for processing or can be for view-only purposes.

04 ***Data Principal Request timeline***
The Act has not specified a timeframe for Data Fiduciaries to respond to any Data Principal requests.

GDPR v/s DPDPA

Difference

Below mentioned are the key differences between DPDPB 2023 and the General Data Protection Regulation (GDPR):

General Data Protection Regulation		Digital Personal Data Protection
GDPR applies to processing of Personal Data wholly or partly by automated means and to Personal Data which form or will form a part of a filing system		The DPDP Act will apply to digitized personal data and non digitized personal data which is subsequently digitized
Penalties under GDPR extend to 20 million euros, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher		Penalties under the DPDP Act extend up to INR250 crore
Minors under age 16 need parental consent. Members states of Europe can lower this age to 13 for their regions		Children under the age of 18 need consent from parents/ guardian
Breaches should be notified to the Supervisory Authority within 72 hours and possibly to the affected Data Subjects		The Act does not specify a timeframe for Personal Data breach notification
GDPR does not include right to nominate however provides for the right to portability Organizations have 30 days to respond to a Data Subject request		The Act comprises of an additional right to nominate while omits the right to portability and timeline to respond to the Data Principal requests has not been specified
GDPR lays down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules		The Act has not identified any transfer mechanisms for transferring Personal Data
Both Controllers and Processors are under the obligation to appoint a DPO in specific circumstance		Only the Significant Data Fiduciary shall have to appoint DPO as a point of contact for the Data Protection Board
Data Controller and Data Processor are required to maintain the records of processing activities		The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA)
GDPR does not explicitly specify to provide notice to regional languages		DPDP Act requires the Data Fiduciaries to provide notice in 22 Indian languages in addition to English
Data Protection Impact Assessment (DPIA) is to be conducted by Data Controllers for all the high risk processing activities		Significant Data Fiduciaries are obligated to conduct periodic Data Protection Impact Assessment (DPIA)

Salient features of the Act (Contd.)

Journey to Compliance

As organizations embark on the journey toward compliance with DPDP Act 2023, there are multiple facets and requirements as per the Act and could be phased in 3 24 months for an effective and sustainable Data Privacy and Protection Program.

Now
3 - 6 months

- Undertake a Data Privacy Assessment to understand the current posture toward privacy and the requirements
- Develop Data Privacy framework to strengthen your organizations Data Privacy Program
- Establish the Data Privacy Organization to drive the program
- Data Discovery, Classification, and Mapping exercise to identify the Personal Data touch points, and structured and unstructured data across the environment and classify them.
- Develop an inventory of assets processing personal information and also the entire list of suppliers / 3rd parties leveraged for various purposes / delivering the services

Next
6 - 12 months

- Develop/update relevant policies and underlying procedures to outlay the intent and consistent approach toward privacy and protection
- Conduct Data Privacy Impact Assessments (DPIAs) for the high risk in scope business functions/ applications to identify the potential risk exposure
- Establish mechanisms for:
- Consent management
- Data Principal rights
- Breach notification

Beyond
12 - 24 months

- Implement Privacy Enabling Technologies (PETs) to reduce manual tasks, and manage your data governance activities in an automated manner
- Undertake external certifications to demonstrate compliance toward the Privacy Information Management System

- Technical safeguards
- Training and awareness
- Periodic audits
- Establish and drive cyber culture in the enterprise
- Strong cyber governance mechanism sponsored by the Board
- Continuous monitoring of the notifications and amendments by the Data Protection Board / Central Government

**Note: Conducting DPIAs is a mandatory requirement for a Significant Data Fiduciary*

How DPDPA can help?

Journey to Compliance

Our broad transformation approach considers the key facets of the Act across organization's data management lifecycle

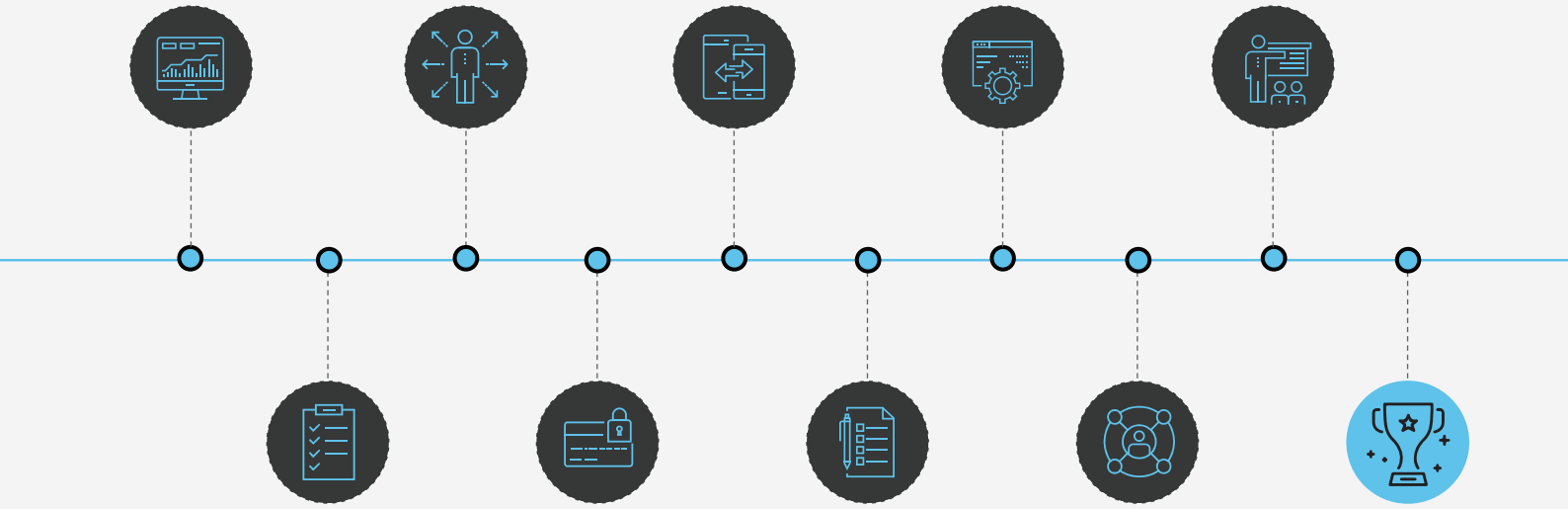
Data Privacy Assessment
Assess the current Data Privacy posture, working practices and documentation against the requirement of DPDB

Data Discovery and Mapping
Identify the Personal Data touch points and conduct data discovery and mapping activities

Third Party Risk Management
Identify the third party ecosystem, ensure organizational and technical security measures are implemented through inclusion of the same within valid contracts

Technical Safeguards
Identify the critical business processes/assets/ applications which processes large volume of Personal Data and implement technical security measures

Training and Awareness
Socialization workshops for employees, management personnel and third parties to promote a privacy inclusive culture throughout the organization



Data Privacy Framework Development
Develop Data Privacy framework to strengthen your organization's data privacy program

Privacy Risk Assessment
Perform Data Protection Impact Assessment (DPIA) for the high risk in scope business functions/ applications to identify the potential risk exposure*

Privacy Enhancing Technologies
Reduce manual tasks with integrated workflow through Privacy Enhancing Technologies and manage your data governance activities in an automated manner

Internal Audit Assistance
Independent Data Privacy audits to identify the gaps and risks on a periodic basis

Connect with us!

Landline: 0120-6930999
Toll Free: 1800-5711333

info@dpdpconsultants.com

DPDP Consultants is your trusted partner in ensuring Digital Personal Data Protection (DPDP) act 2023 compliance for businesses in India.

About DPDP Consultants

We understand that DPDP regulations are complex and time-consuming for businesses, so we empower our clients with skills, tools, and knowledge to navigate and comply with these regulations successfully. Our experience in implementing privacy policies in different geographies has enabled us to create customised solutions for businesses of all sizes.

Who We Are

DPDP Consultants is the forerunner in the digital personal data protection space. Our team boasts of industry experts specialising in data protection and privacy compliance.

Our Mission

Our mission is clear and resolute: to empower Indian businesses to safeguard the personal data of their customers and stakeholders while complying with the DPDP Act 2023. We believe that DPDP consulting is not just a legal requirement but also an essential aspect of building trust and maintaining the integrity of your brand.

Our Vision

We envision a future where proper handling and processing of people's personal data is not just a legal obligation but a fundamental aspect of a fair digital society. Our goal is to initiate a change where personal data compliance is integrated into every business operation, improving legal compliance and building trust among customers and stakeholders.

What We Do

DPDP Consultants offer a comprehensive suite of DPDP services tailored to your unique compliance needs. We work closely with businesses of all sizes and industries, offering a personalised approach to address their specific challenges.

Our services include:

- Compliance Assessment
- Policy Development
- Training and Education
- Data Protection Impact Assessments (DPIA)
- Incident Response Planning

DPDP CONSULTANTS
Empowering Privacy in Digital World