

Advent of Privacy Era
in India

The Digital Personal Data
Protection Act, 2023



The better the question. The better the answer.
The better the world works.



Building a better
working world

Salient features of the Act

Journey So Far

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

August 2017

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

December 2019

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

November 2022

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

August 2023

July 2018

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

December 2021

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

July 2023

Union Cabinet approves the draft DPDP Bill, 2023

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 accomplished
- Report Personal Data Breaches 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 electoral democracy



Risk to the rights of data principal



Security of the state



Potential impact on the sovereignty and integrity of India



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

Data Principal Rights



*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 not giving notice of Personal Data Breach



Up to **INR200 Crore**

Breach in observance of additional obligation in relation to children



Up to **INR250 Crore**

Noncompliance of the provisions by Data Fiduciaries

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 Disputes Settlement and Appellate Tribunal

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 responsible for its data processor and taking reasonable security safeguards) under specified circumstances including



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 (GDPR)

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

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

Minors under age 16 need parental consent. Members states of Europe can lower this age to 13 for their regions

Breaches should be notified to the Supervisory Authority within 72 hours and possibly to the affected Data Subjects

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

GDPR lays down specific mechanisms for transferring data to third country such as standard contractual clauses and binding corporate rules

Both Controllers and Processors are under the obligation to appoint a DPO in specific circumstance

Data Controller and Data Processor are required to maintain the records of processing activities (ROPA)

GDPR does not explicitly specify to provide notice to regional languages

Data Protection Impact Assessment (DPIA) is to be conducted by Data Controllers for all the high-risk processing activities

Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act will apply to digitized personal data and non-digitized personal data which is subsequently digitized

Penalties under the DPDP Act extend up to INR250 crore

Children under the age of 18 need consent from parents/ guardian

The Act does not specify a timeframe for Personal Data breach notification

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

The Act has not identified any transfer mechanisms for transferring Personal Data

Only the Significant Data Fiduciary shall have to appoint DPO as a point of contact for the Data Protection Board

The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA)

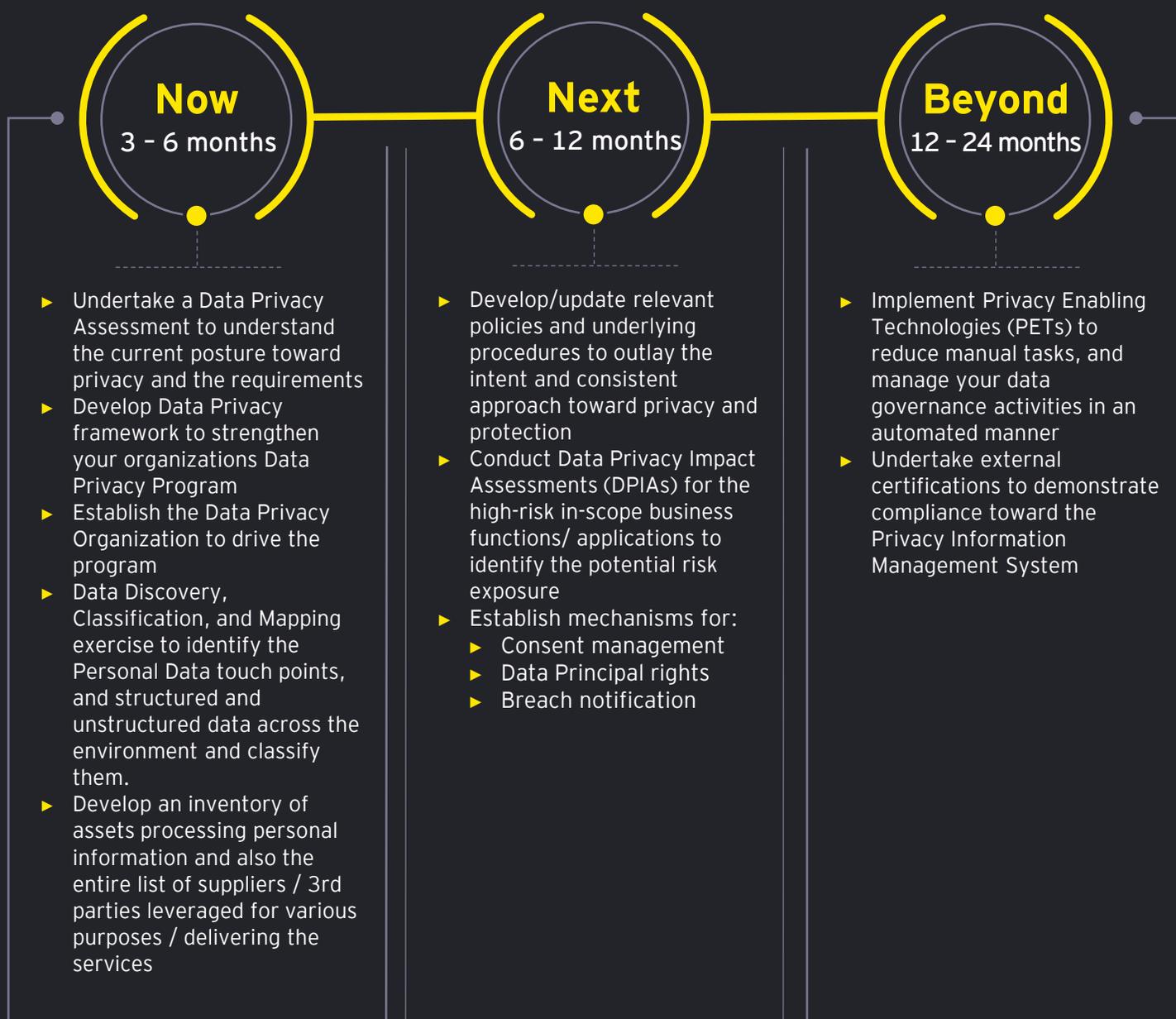
DPDP Act requires the Data Fiduciaries to provide notice in 22 Indian languages in addition to English

Significant Data Fiduciaries are obligated to conduct periodic Data Protection Impact Assessment (DPIA)

What's Now, Next and Beyond

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.



- ▶ **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 EY 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

OUR OFFICES

Ahmedabad

22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru

12th & 13th floor
"UB City", Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
11, Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh

Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai

Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR

67, Institutional Area
Sector 44, Gurugram
Haryana - 122 002, India
Tel: +91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad

THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jamshedpur

1st Floor, Shantiniketan
Building, Holding No. 1
SB Shop Area, Bistupur
Jamshedpur - 831 001
Tel: + 91 657 663 1000

Kochi

9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata

22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune

C-401, 4th floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 9th Floor, Golf View Corporate Tower B, Sector 42, Golf Course Road, Gurugram, Haryana - 122 002.

© 2023 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN2308-011
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RS2

ey.com/en_in

 @EY_India  EY  EY India  EY Careers India  @ey_indiacareers