



IAPP UK Intensive 2026

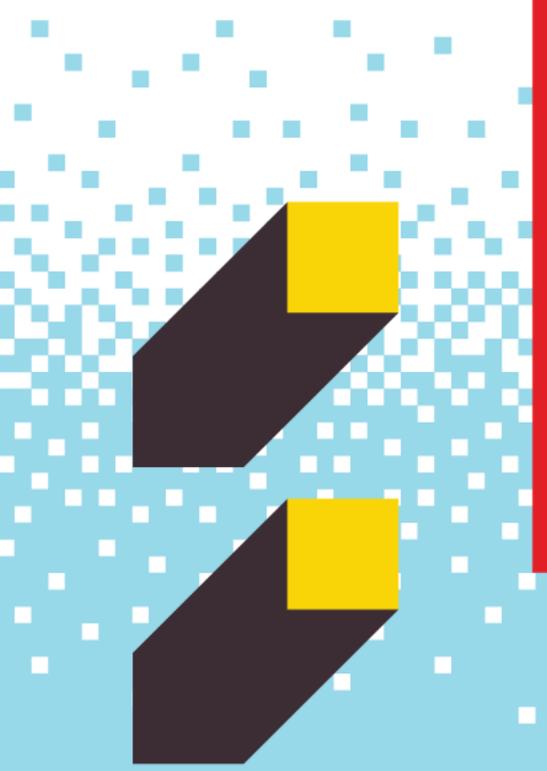
Privacy | AI governance | Cybersecurity law

Training 23-24 February

Workshops 24 February

Conference 25-26 February

LONDON



#IAPPIntensive26

From India to the World

The Rise of a New Data Protection Era



WELCOME AND INTRODUCTIONS



Joe Jones

Director of Research & Insights,
IAPP



Abhishek Tiwari

FIP, CIPP/A, CIPP/E, CIPM,
AIGP

Associate Director,
PWC India



Charmian Aw,

FIP, CIPP/A, CIPP/E, CIPP/US,
CIPM, AIGP

Partner,
Hogan Lovells



Christopher Chew,

FIP, AIGP, CIPP/A, CIPM,

Technical Leader, Security &
Digital Trust - Office of the
CTO, Cisco Singapore



#IAPPIntensive26

Agenda Outline

Introduction

Moderator sets the stage: why India's law matters globally

Deep Dive

Abhishek Tiwari explains the DPDPA's key provisions and enforcement landscape

Comparative Analysis

Christopher Chew, Charmian Aw & Joe Jones highlight cross-jurisdictional implications and lessons from GDPR/UK/Singapore frameworks

Interactive Q&A

Audience engages with panelists on practical compliance strategies

#IAPPIntensive26

How the DPDP Act evolved in India?

Shikrishna Committee

The foundation for India's modern data protection framework was laid by the Justice B.N. Srikrishna Committee, formed in 2017, through its report - "A Free and Fair Digital Economy" released in 2018



2017-2018



24 August 2017

Privacy became a **fundamental right** in India

Personal Data Protection (PDP) Bill

The first draft introduced in parliament included provisions of a Data Protection Authority (DPA) to oversee compliance and introduced individual rights

2019

2022

Withdrawal of PDP Bill

The government withdrew the PDP Bill, citing the need for a simpler, more focused framework



Digital Personal Data Protection (DPDP) Act

The DPDP Act, enacted in August 2023, governs the processing of digital personal data by balancing individuals' right to data protection with the need for lawful data use. It also established the Data Protection Board as the regulator

2023



January 2025

Draft Rules for DDPD Act

The draft DPDP Rules, released for public consultation, provided clarity some of the tenets of the DPDP Act and aimed to provide guidelines for operationalization of the DPDP Act



November 2025



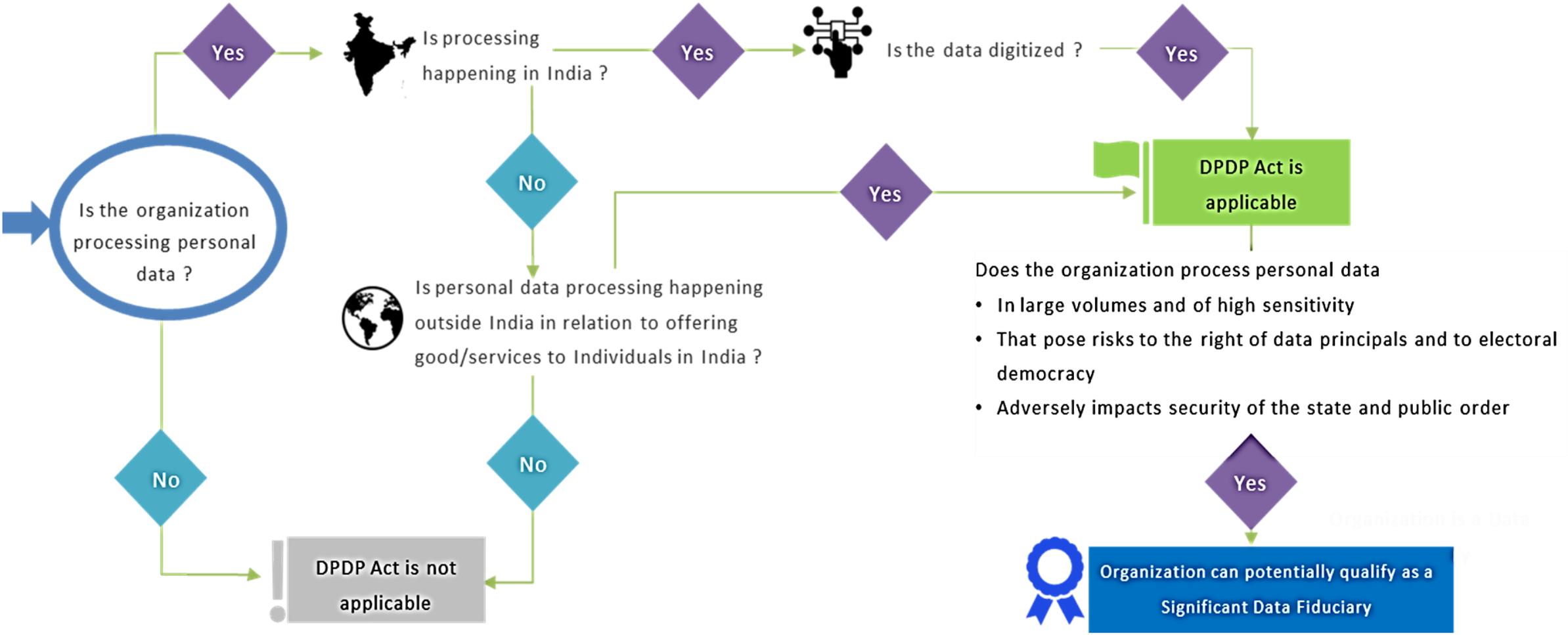
Final Rules for DDPD Act

The Final DPDP Rules, notified the implementation timelines of 18 months for key aspects of the Act and 12 Months for establishment of consent manager



#IAPPIntensive26

Find Out If DPDPA Is Applicable To You...



Key Stakeholders defined in the Act



The Individual to whom personal data relates

Data Principal



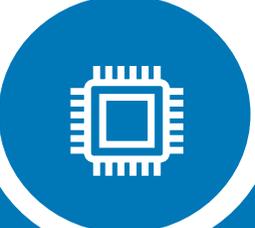
Defines the purposes and means of personal

Data Fiduciary



Organization that processes large volumes of sensitive data sets

Significant Data Fiduciary



Processes personal data on behalf of the Data Fiduciary

Data Processor



Individual appointed by Significant Data Fiduciary

Data Protection Officer



Organization managing the consent of Data Principals

Consent Manager



Your organization can wear multiple hats and can be a **Data Fiduciary, Significant Data Fiduciary, Data Processor** depending upon the context of personal data processing

Do you process your employee's personal data?

You will act as a **Data Fiduciary**

You might act as a **Significant Data Fiduciary**

Do you process large volumes of personal data such as customer data?

Do you process the personal data on behalf of other organizations?

You will act as a **Data Processor**

Scope & Rights defined in the Act

The Act applies to

01

within the Indian territory



processing of digital personal data within the territory of India, where the personal data is collected in a:

01 a) digital form



01 b) personal data collected is in non-digital form and digitised subsequently.

02

outside the Indian territory



processing of digital personal data outside the territory of India:

02 a) any activity related to offering of goods or services to data principals within the territory of India.

The Act doesn't apply to

- personal data processed by an individual for any personal or domestic purpose; and personal data that is made or caused to be made publicly available by the data principal to whom such personal data relates
- person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

01 Right to Grievance Redressal

01

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

02 Right to Access Information about personal data

02

Data principals can request confirmation of data processing, a summary of their personal data, and details of all involved data fiduciaries

03 Right to Nominate

03

Data Principals can nominate someone to exercise their rights in case of death or incapacity

04 Right to correction and erasure of personal data

04

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

#IAPPIntensive26

Grounds for processing

Consent

01

The Data Principal may **give, manage, review, or withdraw their consent** to the Data Fiduciary directly or through a Consent Manager. In case of **children**, consent shall be obtained from the parent or the lawful guardian

Freely
Given

Specific

Unconditional
&
Unambiguous

Who will provide consent?

Data Principal

Who will ask for consent?

Data Fiduciary

How consent should be requested?

- In clear and plain language
- Using itemized notice

How can consent be withdrawn?

By contacting Data Fiduciary or Consent Manager

Legitimate Uses

02

No separate consent is required for certain “legitimate uses” recognized under the Act. This includes where data is **voluntarily** provided or collected for a **legal obligation**

01

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

02

For personal data processed for any function of the state under **any law or judgement issued under law**

03

For responding to a **medical emergency** involving a threat to the life of the Data Principal

04

For maintaining **public order and ensuring safety**

05

For purposes related to **employment**

06

For performing activities in **public interest**

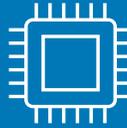
#IAPPIntensive26

Key Obligations defined in the Act

Key Data Fiduciary Obligations

- 01** Take consent from Data Principals where required and implement a **Consent Management** mechanism. (Section 4(1), DPDPA)
- 02** Provide a **privacy notice** to Data Principals at the time of providing consent for processing their personal data. (Section 5, DPDPA)
- 03** Implement appropriate **technical & organizational measures** to safeguard personal data. (Section 8(4), DPDPA)
- 04** Sign a **valid contract** with your Data Processors / third parties to ensure key obligations are abided by. (Section 8(2), DPDPA)
- 05** Review and update the **grievance redressal mechanism** for handling queries from data subjects. (Section 8(10), DPDPA)
- 06** Implement a process for **receiving, acknowledging and honouring** Data Principals Rights (Sections 11, 12, 13, & 14, DPDPA)
- 07** Implement **data retention & disposal mechanism** in consonance with other laws. (Section 8(7), DPDPA)
- 08** Implement a **Data Breach management mechanism** to notify **Data Principals** and **Data Protection Board**. (Section 8(6), DPDPA)

Significant Data Fiduciary* Key Obligations

Data Protection Impact Assessment	 Conduct Data Protection Impact Assessment periodically
Data Protection Officer (DPO)	 Individual appointed to play the role of a DPO within India
Data Audits	 Perform data audits at regular intervals by an Independent Auditor

*Organization can qualify as 'Significant Data Fiduciary' based on the volume, sensitivity of personal data and risks to the rights of Data Principals.

#IAPPIntensive26

Non-Compliance could lead to hefty penalties

**150
Crores /
\$184
million GBP
per instance**

For breach in observance of additional obligations of Significant Data Fiduciary

**200
Crores /
£1.66
million GBP
per instance**

For breach in notifying the board or the affected individuals

**250
Crores /
£2.1
million GBP
per instance**

For violation in taking security safeguards to prevent a personal data breach

**200
Crores /
£1.66
million GBP
per instance**

For breach in observance of additional responsibilities for processing children's personal data

**50
Crores /
£414,000
GBP
per instance**

For breach in observance of any other provisions of DPDPA



Implementation timelines outlined in the Rules

13

November
2025

Rules 1, 2 and 17-21

- Extent and applicability
- Definitions
- Data Protection Board establishment
- Board powers and functions
- Investigation and adjudication
- Appeals to Appellate Tribunal

13

November
2026

Rule 4

- Registration and Obligations of Consent Managers

13

May 2027

Rules 3, 5-16, 22 & 23

- 'Notice, Consent and processing by State
- Reasonable Security Safeguards
- Intimation of breaches and data retention
- Contact information of DPO or equivalent
- Verifiable Consent for Child and PwD
- Obligations of Significant Data Fiduciary
- Data principal Right Management
- Cross Border Data Transfer

#IAPPIntensive26

A summary of the DPDP Act 2023 and the Rules 2025

DPDP Act 2023

22
Clauses

07
Schedule

Notice and Consent

- Provide clear **notices** about collected data and purposes
- Allow data principal to easily give, manage, or withdraw **consent**
- Itemized description of personal data with purpose
- Role of consent managers defined and formalized

Vulnerable User group

- Get verified **parental or guardian consent** for children and PwD data
- Use digital tools to verify identity and age
- Exceptions to creche, educational institutions, clinics and independent doctors are provided

Data Retention & Erasure

- Limits on retention and erasure needed after 3 years from last interaction for certain categories
- Transaction logs to be retained for a period of minimum **one year** by fiduciaries and processors

Final Rules 2025

23
Rules

07
Schedule

Data Principals Rights Mgmt.

- Implement a workflow to enable data principals to exercise their rights.
- Ensure **grievances are resolved within 90 days** of logging the request.

Significant Data Fiduciary

- Conduct yearly **data protection assessments** and audits
- Observe diligence while processing personal data through "algorithmic software"

Breach Notification

- "On becoming aware of a breach", **send notifications** to Data Principals and the Board
- Within **72 hours**, share breach related details including **remedial actions** with the Board

#IAPPIntensive26

Differences Between GDPR and DPDPA 2023

Topic	GDPR (What & How)	DPDPA (What & How)	Action for Indian Clients
Scope & Applicability	Applies to controllers/processors in/out of EU targeting EU data subjects; material scope covers any personal data processing.	Applies to digital personal data processed in India or abroad when offering goods/services to individuals in India.	Map India-facing digital processing; segregate offline datasets governance.
Lawful bases	Art. 6: consent, contract, legal obligation, vital interests, public task, legitimate interests.	Consent + deemed consent/legitimate uses in defined scenarios; narrower formal list vs GDPR.	Create a dual-basis register: GDPR Art. 6 mapping + DPDPA consent/deemed-consent catalogue.
Consent	Arts. 7: freely given, specific, informed, unambiguous; easy withdrawal.	Explicit, revocable, as easy to withdraw as to give; detailed notice requirements under Rules.	Redesign consent UX and logs per Rules; align banners/forms.
Children's data	Child consent for ISS (Information Society Services) 13-16; extra protections.	Child <18; verifiable parental consent; bans on tracking/ads.	Implement age gates + verifiable parental consent+ flows; disable tracking for minors.
Cross-border transfers	Arts. 44-49 adequacy, SCCs, BCRs.	Sec.16: permitted except to government-notified blacklist; Rules may add localization.	Build an India transfer register; prepare contingency if destinations not approved by Central Govt.
Breach notification	Art.33 to Supervisory Authority within 72h; notify users if high risk.	Notify Board + affected individuals without delay; additional info within 72h per Rules.	Embed dual-track playbook (Board + users), templates, 24x7 on-call.
DPO / Grievance Officer	Art.37-39 DPO in certain cases; role defined.	SDFs must appoint DPO (India-based); others must publish grievance contact.	Identify SDF status; appoint India DPO; publish grievance channels.

Gracias!   Spasiba!  
Merci!  Merci!   
Mahalo!    
وناب  عجر تيقوو  

Grazië!     Spasiba! 
Khob Khun Krap!       

Aamsahamnida!     Terima 
Tack!     Kasih!  
Tenã Koutou!    Jannyovaad 
Asante Sana!  Terima Kasih!  धन्यवाद! 
   

How Did Things Go? (We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Intensive 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!



#IAPPIntensive26