iapp

The Act Unpacked: Fundamentals of compliance under India's Digital Personal Data Protection Act 2023

Monday, 16 March
06:00–07:00 PST
09:00–10:00 EST
15:00–16:00 CET

Welcomes and Introductions

Supratim Chakraborty

Partner, Khaitan & Co

Nivedita Nivargi

Partner, Samvād: Partners

What will we cover in this webinar:

- DPDPA scope, key definitions, and legal grounds for processing
- Obligations for data fiduciaries and significant data fiduciaries
- Comparative analysis with GDPR throughout

Scope

The DPDPA covers any entity that processes **digital** personal data within the territory of India

Extraterritorial scope: covers data processed outside of India, if such processing is in connection with offering of **goods or services** to data principals within India

Exemptions:

- **Non-digital** personal data unless subsequently digitized
- **Publicly available** personal data if it was made public by the data principal to whom such personal data relates to or by someone who is under a legal obligation to publish such personal data
- Personal data necessary for **research or statistical** purposes and processed according to standard data protection principles, unless used to make "any decision specific to the data principal"
- Broad exemptions for notified **government entities** for specific purposes such as security of the State and public order
- Government may exempt any category of data fiduciaries, such as **startups**, from certain compliance obligations
- **Offshore entities** in India when processing data that relates to foreign data principals on behalf of a foreign data fiduciary

Key Definitions

Personal data: any data about an individual who is identifiable by or in relation to such data

Data principal: an individual to whom personal data relates. In relation to children and persons with disabilities, definition includes the parent or lawful guardian

Data fiduciary: any person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data

Significant data fiduciary: data fiduciaries classified as such based on factors such as volume and sensitivity of the personal data they process, and other prescribed criteria

Data processor: any person who processes personal data on behalf of a data fiduciary

Consent manager: a single point of contact to enable data principals to give, manage, review and withdraw consent for personal data processing through an accessible, transparent and interoperable platform

Sensitive data: Not applicable

Legal grounds for processing

Consent: must be “free, specific, informed, unambiguous and unconditional with a clear affirmative action”; should be limited to such personal data as is necessary for the specified purpose in the request for consent (i.e., no “bundled consent”)

Certain legitimate uses: complying with legal obligations and judicial orders, performing state functions, responding to medical emergencies, maintaining public safety and order, voluntary provision for a specific use, and employment purposes

*Contractual necessity and legitimate interest are **not** available*

Obligations of Data Fiduciaries

In general:

- Fulfill data principals' rights to access, correct and delete personal information, or withdraw consent for processing personal information. Method for withdrawing consent must as easy as giving consent
- Adopt reasonable security safeguards, including encryption, obfuscation, use of virtual tokens, access controls, and retention of data and logs for a period of one year to prevent recurrence of data breaches
- Obtain "verifiable consent" from the parent or lawful guardian of children and persons with disabilities and refrain from certain activities harmful to children
- Notify DPBI and affected data principals of personal data breaches

Notice:

- Inform data principal about personal data and purpose of its processing, how to exercise individual rights under the DPDP Act, and provide process for filing a complaint with the DPBI
- Notice must be presented in clear and plain language and include a detailed description of the personal data, specified purposes for which personal data will be used, and specific description of goods or services to be enabled / provided by such processing.
- Provide an easily accessible link to website and/or app, along with a way for the data principal to withdraw consent, exercise their rights under the DPDPA, and file a complaint with the DPBI

Regarding data processors:

- Execute valid contract for transferring personal information to a data processor, including provisions on reasonable security measures to be adopted by the data processor
- Review indemnity and limitation of liability clauses to ensure responsibility can be transferred onto data processor if data fiduciary is held liable for the data processer's violations of the law
- Ensure data processors erase any data for which consent has been withdrawn
- Perform periodic audits on data processors, implemented through appropriate contractual arrangements

Additional obligations of Significant Data Fiduciaries (SDFs)

- Appoint an India-based DPO to represent the SDF under the provisions of the Act, to serve as the point of contact for data principals' grievances, and be responsible to the board of directors or similar governing body of the SDF
- Appoint an independent data auditor to carry out annual data audits; SDF to cause the auditor to report findings to DPBI, highlighting their observations
- Auditor must also conduct annual DPIAs that consider the impact of processing on data principals' rights, the purpose of processing, the assessment and management of risks to data principals' rights, and other prescribed matters.
- Adhere to any data localization mandates

Further comparisons with GDPR

- Consent managers
- Individual Rights
- International Data Transfers
- Data retention/erasure

Questions and Answers

Supratim Chakraborty

Partner, Khaitan & Co

Nivedita Nivargi

Partner, Samvād: Partners

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ8CTs

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: **livewebconteam@iapp.org**