FORTRA

Achieving Compliance with India's Digital Personal Data Protection (DPDP) Act

In July of 2024, India's Digital Personal Data Protection (DPDP) Act came into force, following its approval from both houses of the Indian Parliament in August of 2023. This ground-breaking legislation balances the rights of individuals to protect their personal data with the necessity of processing such data for lawful purposes. The act:

- Outlines the rights and duties of Data Principals (data owners).
- Imposes obligations on Data Fiduciaries (data processors).
- Introduces financial penalties for breaches.

Below is a high-level overview of India's DPDP Act, to whom and what it applies, penalties for non-compliance, and the Fortra solutions that can help you meet the DPDP requirements.

What is the History Behind the India's Digital Personal Data Protection Act (DPDP Act)?

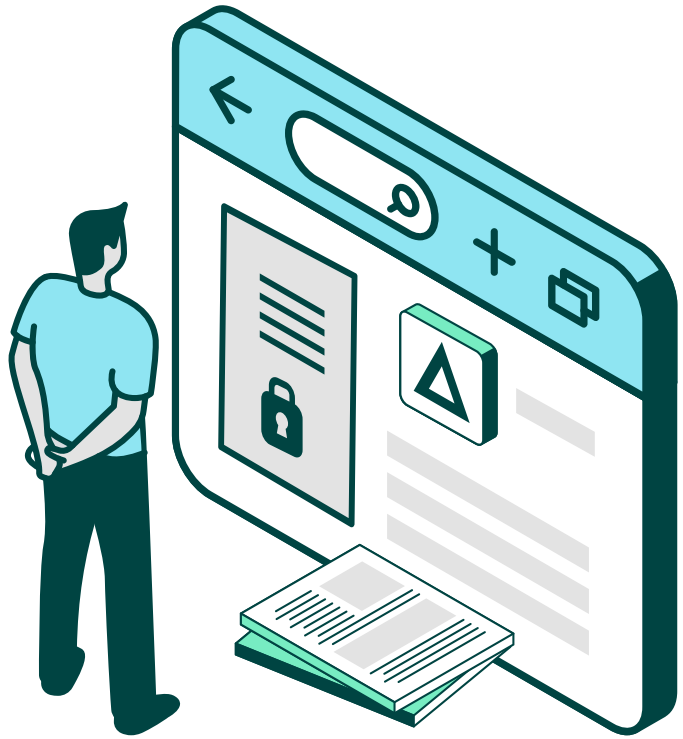
India's Digital Personal Data Protection Act is a ground-breaking legislation that balances the rights of individuals to protect their personal data with the necessity of processing such data for lawful purposes. The Act imposes obligations on Data Fiduciaries, those processing data, and outlines the rights and duties of Data Principals, individuals to whom the data pertains. It also introduces financial penalties for breaches.

The 2023 act is the second version of the bill introduced in Parliament and fourth overall.

In 2017, the Supreme Court of India recognised the right to privacy as a constitutionally protected right in the Puttaswamy Judgement, also known as the Right to Privacy verdict. The court also noted India's lack of a comprehensive privacy law and the limitations of the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules or SPDI Rules, implemented in 2011.

Following the Right to Privacy verdict, the government of India developed draft legislation designed to protect the privacy of Indians. Earlier versions of the Personal Data Protection Act received significant scrutiny and were ultimately unsuccessful, including the Data Protection Bill 2021, which bore some similarities to the European Union's General Data Protection Regulation (GDPR). It was withdrawn in August 2022.

- In November 2022, the Ministry of Electronics and Information Technology proposed the Digital Personal Data Protection Bill 2023.
- In August 2023, the President of India formally enacted the "Digital Personal Data Protection Bill" following its approval from both houses of the Indian Parliament.
- In July 2024, the DPDP Act went into full force.



Who must adhere to the DPDP Framework?

India's DPDP Act covers all digital personal data processed in India and excludes non-digitised and offline personal data. Specifically, it applies to:

- Organisations processing data that could ultimately identify an individual.
- Data that is collected or stored digitally.
- Organisations processing data within Indian territory, or external third parties processing data that involves goods and services offered to those in India.

"Digital personal data" is defined as data in digital form (either via collection or storage) that could identify an individual. Exempt are aggregated data, data used for household/domestic purposes, and publicly available personal data.

Rights Protected by the Act

The DPDP Act protects individuals' rights in respect to their personal data in the following ways:

- **Know what personal data is being collected about them**: The right to be informed about the personal data that is being collected about them, the purpose for which it is being collected, and third parties with whom it is being shared.
- **Access their personal data**: The right to access any personal data that is being processed by an organisation.
- **Correct or delete their personal data:** The right to correct any inaccuracies in their personal data or to delete their personal data in certain circumstances.
- **Object to the processing of their personal data**: The right to object to the processing of their personal data in certain circumstances.
- **Port their personal data to another organisation**: The right to port their personal data to another organisation in certain circumstances.
- **File a complaint with the Data Protection Board (DPB)**: Individuals have the right to file a complaint with the DPB if they believe that their personal data has been processed in a manner that is not in compliance with the DPDP Act.

Organisational Obligations Under the Act

The DPDP Act requires that organisations:

- **Obtain consent from individuals before processing their personal data**: Organisations must obtain consent from individuals before processing their personal data, unless an exemption applies.
- **Use personal data only for the purposes for which it was collected**: Organisations must use personal data only for the purposes for which it was collected, unless they have obtained consent from the individual for further processing.
- **Protect personal data from unauthorised use**: Organisations must take appropriate technical and organisational measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction.
- **Respond to individuals' requests**: Organisations must respond to individuals' requests for access, correction, deletion, and objection within a reasonable time.
- **Report data breaches to the DPB**: Organisations must report data breaches to the DPB within 72 hours of becoming aware of the breach.

Penalties of non-compliance

The penalties for non-compliance under the DPDP Act include the following:

Breach of Provisions	Penalty
Failure to prevent a personal data breach	Up to 250 crore INR/$30 million
Failure to give notice of a personal data breach to Board or affected Data Principal	Up to INR 200 crore/$25 million
Failure to meet additional obligations in relation to children	Up to INR 200 crore/$25 million
Failure to meet additional obligations of significant data fiduciary	Up to 150 crore INR/$18 million
Breach in observation of duties	Up to 10k INR/$120
Breach of any term of voluntary undertaking accepted by the Board	Up to the extent applicable for the breach
Breach of any other provision of this Act	Up to 10k INR/$6 million

Achieve DPDP Compliance with Fortra

Because digital data can hide in a number of places across your network, complying with DPDP requires layered solutions that can be seamlessly integrated across your entire enterprise. Fortra's security suite offers a variety of such integrative, stackable solutions to help you meet your DPDP obligations.

Securing personal information requires a strong suite of data protection solutions. That includes:

Data Loss Prevention (DLP) | Apply data protection policies that will help ensure no digitised personal data falls through the cracks. To help, Fortra's Digital Guardian will:

- Deploy rapidly for immediate visibility into your organisation's assets.
- Discover, monitor for, and block threats to sensitive data.
- Give you out-of-the-box dashboards and guide users on next-best security steps.

Data Classification | Create custom rules based on each classification and sensitivity level, so a public data store will receive a different (and less resource-intensive) level of cyber security than a repository of private personal data. And with Fortra, you can:

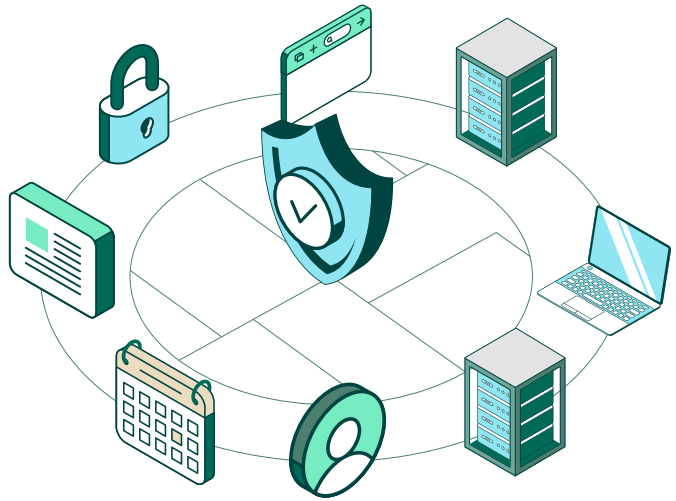
- Apply visual and metadata labels that simplify and support your DLP policies.
- Get AI engine suggestions for quick label application.

Secure Collaboration | Safely do business across Indian territory lines while complying with DPDP policies, no matter if you are an Indian organisation or external third party. Fortra's secure collaboration solution:

- Encrypts files to secure them no matter where they go.
- Revoke file access at any time (even after the file is sent).
- Supports a zero-trust approach to file sharing and collaboration.

Identity and Access Management (IAM) | Protecting personal data means protecting all access points into the organisation – including those of supply chain partners. Fortra's IAM and privileged access management (PAM) solutions:

- Provide informed provisioning.
- Improve identity governance with actionable data insights.
- Simplify access management to reduce complexity and improve mitigation.



Summary

In today's highly regulated data environment, nothing less than a person's identity and fundamental rights are at stake. In 2017, the Supreme Court of India recognised the Right to Privacy in a landmark verdict and India's Digital Personal Data Protection Act is a direct product of that.

While mandatory, compliance with the new DPDP Act will grant adopters a competitive advantage, both with partners and customers, and serve as a business initiative as much as a security boon.

Fortra supports initiatives like these around the world by bringing our best to the table, enabling those striving to meet even the most stringent compliance requirements to meet the needs of their customers, protect the privacy of their citizens, and continue to advance towards complete privacy and security maturity.

For more, check out Fortra's suite of data protection solutions.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-eb-1024-r2-db