FORTRA™

The Digital Personal Data Protection Act, 2023

In early August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023.

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 It was withdrawn in August 2022.

On 18 November 2022, the Ministry of Electronics and Information Technology proposed the Digital Personal Data Protection Bill 2023.

On 11 August 2023, the President of India formally enacted the "Digital Personal Data Protection Bill" following its approval from both houses of the Indian Parliament.

Who does India's Digital Personal Data Protection Act (DPDP Act) apply to?

DPDP Act applies to organisations processing data if the following conditions are met:

- Organisations processing "digital personal data," which is capable of identifying the "data principal." The Data Principal is the individual to whom the data relates.
- The data organisation procesess is either collected in digitised format or will be digitised.
- Organisations processing digital personal data within Indian territory. Alternatively, if you process digital personal data outside of India but the processing is in connection with an activity concerning the offering of goods or services to individuals in India.

What Is Personal Data:

The DPDP Act applies to the processing of digital personal data, which is broadly defined as data in digital form (whether collected in digital form, or in non-digital form and then digitised) about an individual, who is identifiable by such data.

What Personal Data Is Exempt from the Scope of the DPDP Act?

Aggregated data, data used for household/domestic purposes, and publicly available personal data are outside the scope of the DPDP Act.

Key features of the Act

The DPDP Act gives individuals a number of rights with respect to their personal data, including the right to:

- **Know what personal data is being collected about them**: Individuals have 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**: Individuals have the right to access their personal data that is being processed by an organisation.
- **Correct or delete their personal data**: Individuals have 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**: Individuals have the right to object to the processing of their personal data in certain circumstances.
- **Port their personal data to another organisation**: Individuals have 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.

The DPDP Act imposes a number of obligations on organisations that process personal data, including the obligation to:

- **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 access, use, disclosure, alteration, or destruction**: Organisations must take appropriate technical and organisational measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction.
- **Respond to individual's requests for access, correction, deletion, and objection**: Organisations must respond to individual's 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 for non-compliance

The DPDP Act mentions a number of penalties for non-compliance, including:

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 to150 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

Next steps for Organisations

Organisations that process personal data in India should start preparing for compliance with the DPDP Act now. Here are some steps that organisations can take:

- **Assess their data processing activities**: Organisations should assess their data processing activities to identify any areas where they may need to change their practices to comply with the DPDP Act.
- **Develop a data protection policy**: Organisations should develop a data protection policy that sets out their commitment to protecting personal data and outlines their data processing practices.
- **Appoint a data protection officer (DPO)**: Organisations that process personal data on a large scale are required to appoint a DPO. The DPO will be responsible for overseeing the organisation's compliance with the DPDP Act.
- **Implement appropriate technical and organisational measures**: Organisations should implement appropriate technical and organisational measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction.
- **Train employees on data protection**: Organisations should train their employees on data protection so that they understand their obligations under the DPDP Act.

By taking these steps, organisations can help to ensure that they are in compliance with the DPDP Act and that they are protecting the personal data of their customers and employees.

Meet DPDP Requirements with a Suite of Security Solutions

At Fortra, we are creating a simpler, stronger future for cybersecurity by offering a portfolio of integrated and scalable solutions including Data Classification, Data Loss Prevention, Secure File Transfer, Infrastructure Protection, Phishing Protection, and Security Awareness Training.

Complying with DPDP requires a layered approach best met with a suite of security solutions that can be seamlessly integrated across your enterprise to enforce the policies set in place. Fortra's security suite offers a variety of security-focused solutions to help you meet your DPDP obligations.

Data Classification

Fortra's data classification solutions help meet DPDP by applying both visual labels and labelling to a file's metadata to protect and control its use. By adding classification, users can better determine how a given piece of data should be treated, handled, stored, and eventually deleted. Classification adds streamlined functionality as well as enhanced data security and compliance.

Data Loss Prevention

DPDP states that processors must ensure that personal data is not used for any other purpose outside the services it was intended for. Data Loss Prevention from Fortra's DLP aids DPDP compliance by enabling organisations to effectively discover, monitor and control personal data transmitted on the network, in use on workstations, or at rest in workstations, network servers, and cloud storage. Data is appropriately protected against unauthorised transmission, dissemination, use, and storage, while the analytics and reporting functionality can provide key documentation to demonstrate DPDP compliance.

Secure File Transfer (SFT)

Comprehensive SFT solutions can help meet several key DPDP principles, namely securely transmitting personal data through encryption, performing integrity checks of transfers to protect accuracy, and providing detailed audit trails and reporting of all transfers. Personal data is protected in transit and at rest with granular user access roles adding additional security around data.

Secure Collaboration

Fortra's secure collaboration solution encrypts and controls access to sensitive files wherever they go.

Files containing PII, PCI or PHI can only be accessed by authorised users. Digital Guardian Secure Collaboration provides an audit trail of all successful and unsuccessful attempts to access sensitive files. Digital Guardian Secure Collaboration (DGSC) also gives you ability to revoke access to sensitive files, even if they are shared with unauthorised users.

Email Security

Before personal data is ever exchanged through email, Fortra's Email Security solutions apply the optimal security treatment based on your data's content and DPDP privacy policies. It delivers real-time sanitisation/redaction, encryption, and blocking or deleting of sensitive data based on the business rules you define to meet DPDP regulations.

Vulnerability Assessments and Intrusion Protection

Proving DPDP compliance is easier with the security solutions delivered by Powertech. Organisations can automatically identify and quantify their system security vulnerabilities as well as harden their system to intrusion. In addition, robust audit functionality of users and system functions helps meet the audit requirements under DPDP.

Infrastructure Protection

Fortra's infrastructure protection suite includes tools for vulnerability management, penetration testing services and software, adversary simulation, and intrusion detection. These solutions secure sensitive data and ensure compliance by monitoring and assessing your infrastructure to identify and prioritise any risks. With comprehensive reporting capabilities, these solutions can also easily demonstrate compliance to external auditors.

Security Awareness Training

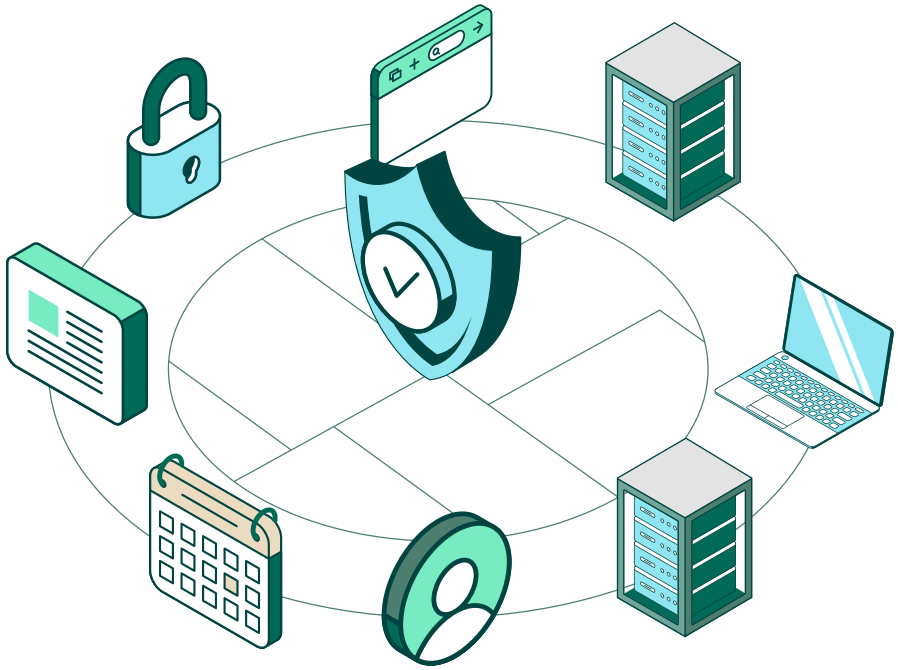
Fortra offers affordable, customisable bundle options for any organisation's size and budget. Implementing effective, scalable training programs and building a cyber-aware culture is easier than ever.

Phishing Protection

Solutions from Fortra for email security and antiphishing can keep emails, brands, and data safe from sophisticated phishing attacks, insider threats, and accidental data loss with minimal business disruption.

Ransomware Mitigation

Fortra provides organisations with the tools to impede ransomware attacks and partners with them at every step to ensure security success. Fortra solutions support rich, deep use cases tailored to unique requirements



Summary

Ultimately, in today's highly regulated data environment, organisations in India need to embrace and build an effective compliance strategy, as those that do will experience positive business benefits and undoubtedly reap the rewards. Those with low levels of data privacy protection and data governance software adoption need to change – and change quickly. But, more broadly, companies need to obtain better visibility of their data before they can consider themselves compliant with relevant data protection regulations. By taking a layered approach to data security and adopting a people, process and technology centric approach, organisations in India can confidently embrace the new DPDP Act and, once compliant, should view this as a competitive advantage.

CONTACT US

FORTRA™

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-1023-r1-db