FORTRA

DATASHEET

Achieving DPDP Act Compliance with Fortra Solutions

In 2023, India introduced its first comprehensive data privacy law: the Digital Personal Data Protection (DPDP) Act. The Act became operational in November 2025 with the notification of the DPDP Rules, replacing a previously fragmented regulatory landscape with a unified framework for the digital age.

The Act establishes a rights-based framework for the processing of digital personal data, covering both data collected online and offline data that is subsequently digitized. Its primary objective is to balance individuals' right to protect their personal data with organizations' legitimate need to process it for lawful purposes..

Unlike earlier regulations in India, the DPDP Act introduces significant financial penalties to deter negligence. For example, failure to prevent a data breach can result in penalties of up to ₹250 crore per instance.

The responsibility for data privacy — including collection, consent management, storage, and deletion — now rests entirely with the organization, referred to as the Data Fiduciary.

Achieving DPDP Act compliance can be complex. Fortra simplifies this challenge through an integrated approach, delivering technical controls that align directly with DPDP Act requirements.

EXECUTIVE SUMMARY

India's DPDP Act establishes a rights-based framework for protecting personal data, with heavy penalties for noncompliance.

Fortra's integrated solutions help organizations achieve compliance in three core areas:

- **Discover & Classify:** Identify sensitive data across files, databases, and cloud assets.
- **Protect & Monitor:** Prevent leaks, enforce policies, and secure transfers.
- **Audit & Report:** Generate defensible evidence for access, consent, and transfers.Simplify compliance, reduce risk, and maintain full control over personal data.

By automating notice, consent, access, and transfer controls, Fortra helps organizations meet DPDP Act obligations, reduce risk, and maintain a defensible audit trail for regulatory compliance.

Fortra's Data Security Solutions that Support DPDP Act Compliance

Fortra Data Classification Suite

DPDP Mapping: *Applicable in Section 5 (Notice), Section 6(1) (Consent), Section 8(3), 8(7) (Accuracy), and Section 11(1) (a) and 11(1)(b) (Right to Access)*

Fortra DCS serves as the "foundational layer." An organization cannot protect or report on data that has not been identified. For example:

- **Metadata Tagging for Purpose Limitation:** By tagging files with "Purpose" metadata, Fortra DCS ensures data is only used for the reason it was collected.
- **Visual Markings for Awareness:** Fortra DCS applies headers/footers to documents, ensuring employees handle data according to its DPDP sensitivity.
- **Automated Discovery:** Scans unstructured data to identify digital personal data that otherwise would be hidden, making it available for "Right to Access" requests from Data Principals.

Fortra DSPM

DPDP Mapping: *Section 5 (Notice), Section 6(1) (Consent), Section 8(3), 8(4),8(7) and Section 8(7) (Obligations of Data Fiduciary), Section 11(1)(a), 11(1)(b) (Right to Access), Section 16 (Transfer of Personal Data)*

Fortra DSPM focuses on visibility, risk, and protection across cloud environments. It addresses the "where" and "who" of data through automated discovery, classification, and protection against data leaks in cloud assets. For example:

- **Eliminating "Shadow Data:"** Identifies forgotten databases or cloud buckets containing Indian citizen data.
- **Security Posture Monitoring:** Finds misconfigurations before a breach occurs.
- **Access Governance:** Maps who has access to PII. For example, if a marketing intern has access to the core customer database, DSPM flags this as a compliance risk.

Fortra DLP

DPDP Mapping: *Section (5) (Notice), Section 6(1), 6(4), 6(6) (Consent), Section 8(4), 8(6) (Obligation of Data Fiduciary) and Section 15 (Duties of Data Principals), Section 16 (Transfer of Personal Data)*

Fortra DLP is the enforcement engine as it stops data from leaving an authorized environment. For example:

- **Real-time Exfiltration Blocking:** If a user tries to upload a CSV of Indian customer IDs to a personal cloud drive, Fortra DLP blocks and logs it.
- **72-Hour Breach Readiness:** Under Section 8(6), organizations must notify the Board of a breach within 72 hours. Fortra DLP provides the forensic "paper trail" — what was taken, by whom, and when —for rapid, accurate reporting.
- **Data Masking/Redaction:** Can automatically redact PII in transit, ensuring even if a file is shared, the sensitive personal data is protected.

How Fortra Solutions Map to the DPDP Act

DPDP Requirement: Notice and Transparency, Section 5

Data Fiduciaries must provide clear "Notice" to Data Principals before or during collection of personal information. "Notice" for data processing requires a structured approach integrated with data classification to ensure transparency and compliance.

ACT SECTION	REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
Section 5	Data Discovery and Classification (The "Itemization" Requirement)	Requires organizations to provide an itemized list of personal data collected. Accurate inventory of collected data is impossible without knowing where it resides.	• Fortra DCS • Fortra DSPM	By automatically identifying data types, Fortra helps build the "Data Inventory" needed for an accurate, itemized Section 5 notice. By tagging data at creation, it ensures processing aligns with the stated purpose in the notice.
	Purpose Limitation and Enforcement	Intrinsically linked to Purpose Limitation — users must be informed of the reason their data is being collected.	• Fortra DLP • Fortra DSPM	Once a user is notified their data is for "Service A," Fortra DLP enforces this. If an employee tries to move that data to a department or application unrelated to "Service A," DLP can block the action.
	Data Minimization (The "Necessary" Requirement)	Specifies notices must be limited to data necessary for the stated purpose.	• Fortra DLP • Fortra DSPM • Fortra SEG	The noted Fortra solutions use "Actionable" policies to redact or block out-of-scope sensitive data, preventing scope creep and ensuring alignment with user notices.

DPDP Requirement: Consent, Section 6

Defines the characteristics of Valid Consent. Mandates consent must be free, specific, informed, unconditional, and unambiguous, provided through a clear affirmative action.

ACT SECTION	REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
6(1)	Specific and Informed	Requires consent is limited to a "specified purpose." If data is collected for "Shipping," it cannot legally use it for "Marketing" without new consent.	• Fortra DCS	When a user provides consent for a specific purpose, Fortra can automatically apply a metadata tag to that data. Because the metadata stays with the file, other systems recognize the data is "Purpose-Bound," preventing it from being accidentally pulled into unauthorized processing activities.
6(1)	Purpose Limitation and Enforcement	Consent must be a "clear affirmative action." Organizations must maintain a "Consent Artifact" to prove this if audited.	• Fortra DCS • Fortra DSPM • Fortra DLP	The noted Fortra solutions track every interaction with sensitive data. If the Data Protection Board asks for proof of how a specific category of data was handled, Fortra provides the forensic trail showing the data was only accessed by applications and users consistent with the "Affirmative Consent" given at collection.
6(4), 6(6)	Unambiguous and Affirmative Action	If a Data Principal withdraws consent, the Data Fiduciary must "within a reasonable time, cease and cause its Data Processors to cease" processing.	• Fortra DLP • Fortra DRM • Fortra Secure Collaboration	Once a user withdraws consent, their unique identifiers can be updated in the DLP policy. The system can then automatically block any further processing or transmission of that user's data across the network, effectively stopping data flow in real time. If the user's data has been shared with a third-party processor, Fortra Secure Collaboration enables remote access revocation. Even if the file remains with the processor, it can no longer be opened.

DPDP Requirement: Obligations of a Data Fiduciary, Section 8

Outlines the General Obligations of a Data Fiduciary. It is the "operational" core of the Act, requiring organizations to ensure data accuracy, implement security safeguards, and manage data breaches.

ACT SECTION	REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
8(3)	Duty to ensure Data Accuracy	Data Fiduciaries must ensure personal data is accurate and complete when it is used to make decisions affecting the Data Principal.	• Fortra DCS • Fortra DSPM	With the noted solutions, duplicate, redundant, or obsolete data (ROT) can be identified. Ensures that "one version of the truth" is correctly labeled across all servers prevents old or inaccurate data from remaining in forgotten silos when a user requests an update.
8(4)	Duty to Implement Security Safeguards	Mandates "reasonable security safeguards" to prevent personal data breaches.	• Fortra DLP • Fortra DSPM	The noted solutions provide automated discovery, deep visibility, and control over sensitive data at the endpoint, on the network, and in the cloud. It prevents unauthorized disclosure, the very definition of a breach under the Act.
8(6)	Duty to Notify of Data Breach	In the event of a breach, the Data Protection Board and each affected Data Principal must be notified within 72 hours.	• Fortra DLP • Fortra DSPM	Fortra DLP, supplemented by Analytics and Reporting Cloud (ARC), makes it quick and simple to investigate and audit any data breaches across the network. This capability extends to the cloud with Fortra DSPM to ensure that any unverifiable activity is promptly highlighted and addressed.
8(7)	Duty to Erase Data	Requires deletion of data once the purpose of collection is fulfilled or consent is withdrawn.	• Fortra DCS • Fortra DSPM	Fortra's advanced discovery functionality helps identify data that has exceeded its retention period. It can automatically tag data with expiration dates, and once those dates pass, the system can flag it for deletion or move it to a "trash" folder for permanent erasure.

DPDP Requirement: Right to Access Information, Section 11

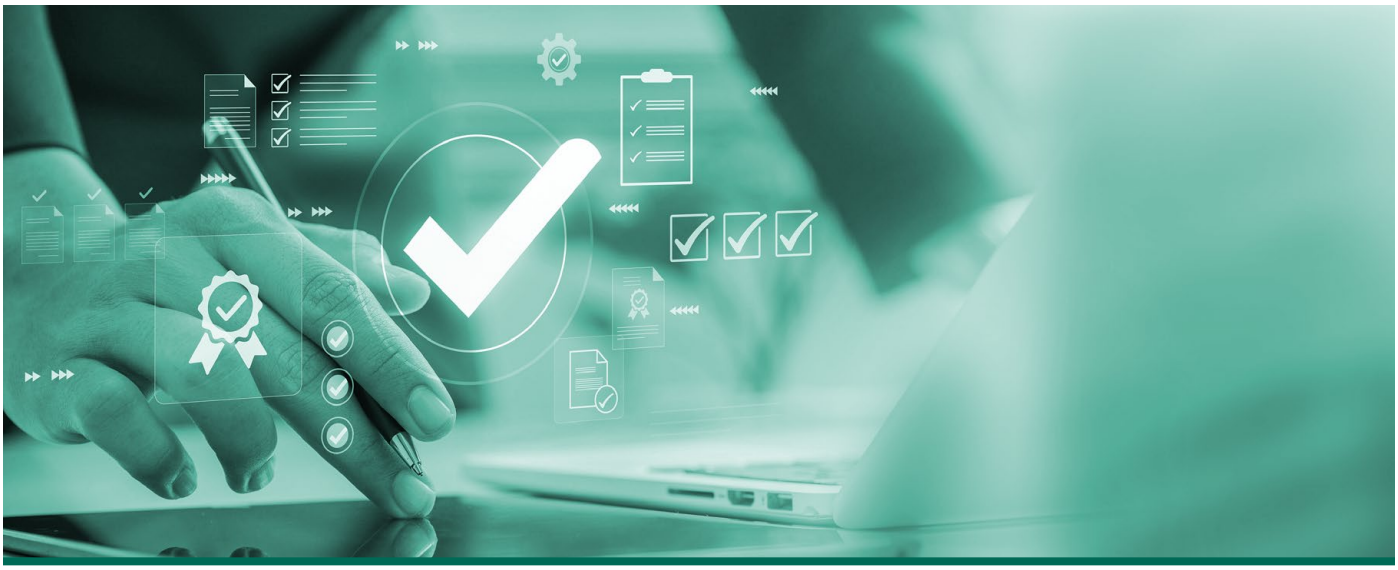
Grants individuals the Right to Access Information. Organizations must provide a summary of the personal data they hold, how it is being processed, and a list of all third parties with whom it has been shared.

ACT SECTION	REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
11(1)(a)	Data Discovery: "Show me what you have"	A user can ask for a summary of their personal data.	• Fortra DLP • Fortra DCS • Fortra DSPM	The noted solutions use discovery engines to scan the entire infrastructure to locate every instance of an individual's data. Fortra's discovery engines create a centralized inventory, simplifying the generation of the legally required "summary."
11(1)(b)	Tracking Data Sharing: "Who did you give it to?"	Requires organizations to disclose the identities of all other Data Fiduciaries and Data Processors with whom personal data has been shared.	• Fortra DLP • Fortra DSPM • Fortra MFT	Fortra DLP with ARC and DSPM monitor and record data movement across endpoints. When data is sent via email or uploaded to a cloud portal, the solution dashboards provide evidence of these "sharing" events. Additionally, Fortra Managed File Transfer (MFT) maintains an unalterable audit log of every file transfer.
8(6)	Purpose and Processing Transparency	Requires informing the user about "all processing activities" related to their data.	• Fortra DCS • Fortra DSPM	Attach metadata to files that describe their purpose. When a user requests information, this metadata helps explain exactly why and how their data is being used, ensuring the response is accurate and detailed.
	Secure Delivery of the Access Request	Returning highly sensitive PII in response to a Section 11 request via standard email could result in a new data breach.	• Fortra MFT • Fortra SEG	Ensures the "Access Report" sent to the Data Principal is encrypted and password protected. Can set these links to expire, ensuring the data doesn't sit in the user's inbox indefinitely.

DPDP Requirement: Transfer or Processing of Personal Data, Section 16

Governs the Transfer or Processing of Personal Data Outside India. Uses a "permissive by default" model.

ACT SECTION	REQUIREMENT	DETAIL	FORTRA CAPABILITY	BUSINESS OUTCOME
16(1)	Geofencing and Transfer Restrictions	If the Indian Government blacklists a specific country or territory, organizations must immediately stop data flows to that region.	• Fortra MFT • Fortra SEG • Fortra DLP	With Fortra MFT and SEG, organizations can configure IP whitelisting and blacklisting at the gateway level. If a country is designated as restricted under Section 16, all automated file transfers to or from IP ranges associated with that territory can be blocked. Fortra DLP can also enforce policies that identify and control data transfers based on geographic destination.
16(2)	Sector Localization Compliance	Since DPDP does not override stricter localization laws, many Indian firms must keep copies of data in India or prevent it from leaving entirely.	• Fortra MFT • Fortra SEG	The noted solutions can scan for specific data types that are legally required to remain in India, such as credit card transaction data. If such data is detected in an outbound email or file transfer to a foreign entity, the system can automatically encrypt, redact, or block the transmission.
16	Maintaining "Equivalent Protection"	Even if a transfer is allowed, the Data Fiduciary remains responsible for the data's safety.	• Fortra Secure Collaboration • Fortra MFT	When data is sent to a foreign processor, Fortra Secure Collaboration encrypts the file itself, ensuring protection under the organization's policies rather than foreign law. Additionally, if a foreign partner's security is compromised or if the Indian government imposes restrictions under Section 16, access to those files can be instantly revoked remotely through Fortra Secure Collaboration.
16	Visibility and Audit for the "Blacklist"	Show exactly where data is going.	• Fortra MFT • Fortra DCS • Fortra DSPM	By labeling data according to its sensitivity or "National Importance," different transfer rules can be enforced. Data labeled as Restricted – India Only is physically barred from cross-border movement by the integrated DLP and MFT systems. Fortra MFT provides a "Transfer Map" and detailed logs showing the destination country for every byte of personal data sent outside the organization.



Ready to simplify DPDP Act compliance?

Discover how you can strengthen your data protection strategy today and comply with the DPDP Act.

CONNECT WITH FORTRA

FORTRA

Fortra.com