FORTRA

DATASHEET

Achieving Indonesia PDP Law Compliance with Fortra

Data Security Solutions for PDP Law

In 2022, Indonesia enacted its first comprehensive data protection framework: Law No. 27 of 2022 on Personal Data Protection (PDP Law). The law establishes a unified, rights-based framework governing how personal data is collected, processed, stored, transferred, and deleted across both electronic and non-electronic systems.

The PDP Law balances the fundamental rights of personal data subjects with the legitimate need for organizations to process data for lawful purposes. It introduces clear accountability for personal data controllers and processors, reinforced by strong enforcement mechanisms, including administrative fines of up to 2% of annual revenue and criminal penalties for serious violations.

To comply, organizations must implement verifiable technical and operational controls that demonstrate responsible data handling. Fortra supports these requirements through an integrated data protection portfolio, including Data Classification (DCS), Data Loss Prevention (DLP), Data Security Posture Management (DSPM), Managed File Transfer (MFT), Secure Collaboration, and Secure Email Gateway (SEG).

Together, these solutions enable:

- Data identification and classification
- Purpose-based and risk-based protection controls
- Secure data processing, storage, and transfer
- Data minimization and retention enforcement
- Incident detection and breach notification readiness
- Cross-border data transfer control and auditability

EXECUTIVE SUMMARY

The integrated deployment of Fortra Data Classification, Fortra DLP, and DSPM provides a unified compliance framework supporting PDP Law regulatory requirements via:

- Continuous data discovery and visibility across cloud and data store environments
- Risk-based assessment of personal data exposure
- Impact-based classification
- Persistent metadata enforcement
- Encryption and egress protection
- Lifecycle governance
- Real-time breach detection
- Audit-ready reporting

This layered approach ensures that personal data is continuously discovered, assessed, and protected in alignment with PDP Law obligations. It establishes a defensible, regulator-aligned, and technically enforceable compliance posture for organizations that process the personal data of individuals in Indonesia.

How Fortra Solutions Map to the Indonesia PDP Law

PDP LAW ARTICLE	REGULATORY DOMAIN (TOPIC)	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Article 5, Article 21	Data Identification & Transparency	Organizations must identify Personal Data and provide clear notice regarding purpose, legal basis, and retention.	• Data Classification • DSPM	Data discovery dashboards, classified data inventory
Articles 20–24	Consent Management	Consent must be explicit, informed, recorded, and enforceable across all processing activities.	• Data Classification • DSPM • DLP	Consent-aligned access logs, activity audit trails
Articles 27–28	Purpose Limitation Controls	Personal Data must only be processed according to the stated purpose provided at the time of notice or consent.	• DLP • DSPM	Blocked transactions and purpose enforcement logs
Articles 29–31	Data Accuracy & Governance	Controllers must ensure Personal Data accuracy and maintain records of processing activities.	• Data Classification • DSPM	Processing inventories, version history, audit reports
Articles 34–39	Security Safeguards	Organizations must protect Personal Data from unauthorized access, disclosure, alteration, or loss.	• DLP • DSPM	Security posture dashboards, policy enforcement logs
Article 46	Incident Detection & Breach Notification	Personal Data breaches must be detected, investigated, and reported within 72 hours.	• DLP • DSPM • ARC	Incident timelines, breach investigation reports

PDP LAW ARTICLE	REGULATORY DOMAIN (TOPIC)	REGULATORY REQUIREMENT	FORTRA CAPABILITY	EVIDENCE / OUTPUT
Articles 42–44	Data Retention & Erasure	Personal Data must be deleted or destroyed once retention periods expire or purposes are fulfilled.	• Data Classification • DSPM	Retention tags, deletion workflows, erasure evidence
Article 32	Data Subject Access Rights	Data Subjects may request access to Personal Data and records of processing activities.	• Data Classification • DSPM • DLP	Centralized DSAR reports
Article 56	Cross-Border Data Transfers	Transfers outside Indonesia require equivalent protection or explicit safeguards and consent.	• MFT • DLP • DRM	Encrypted transfer logs, access revocation reports