Compliance Solutions for India's Digital Personal Data Protection (DPDP) Act

Overview

The idea behind data privacy is that people should have control of their personal data — including the right to determine how organizations collect, store, and use that information. It's an especially significant concept in today's digitally driven world, where technology has paved the way for an unprecedented flood of information.

India's *Digital Personal Data Protection (DPDP) Act* (2023) aims to protect the personal data of citizens, replacing the Personal Data Protection Bill of 2019, which was withdrawn in 2022.

Key Features of India's DPDP Act

- **Data Protection Authority:** Oversees and enforces data protection regulations
- **Consent:** Requires explicit consent from individuals before their data can be processed
- **Data Processing:** Defines lawful purposes for data processing to ensure it's done transparently and securely
- **Rights of Individuals:** Grants individuals rights such as access to their data, correction of inaccuracies, and the right to be forgotten
- **Cross-Border Data Transfer:** Sets guidelines for transferring personal data outside India
- **Penalties:** Imposes penalties for non-compliance to ensure accountability

Key Features and Benefits

- Broad portfolio that helps secure identities, data, network, applications, and workloads — and integrates with a broad partner ecosystem
- User authentication and access management helps you enforce strong authentication and access control policies
- Data-at-rest encryption and key management protect data stored on databases, servers, and in cloud environments
- Data-in-transit encryption safeguards data as it moves across networks using encryption protocols like TLS (Transport Layer Security)
- Maintain visibility of critical data assets
- Mitigate exposure to data breaches
- Facilitate compliance with data security regulations and stringent auditing and risk-reporting requirements

Compliance Solutions for India's Digital Personal Data Protection (DPDP) Act

Our Solutions

Entrust provides a range of digital security solutions that help organizations secure user identities and ensure sensitive data is secure from unauthorized access and breaches, aligning with the DPA's mandate for data protection and confidentiality.

DPDP Directive Measure	Entrust Solutions
Identify data principles accurately to prevent impersonation	Entrust Identity and Access Management Our identity platform provides user authentication, authorization, and access control to the right resources anytime, anywhere. Entrust Identity Verification Get trust at every stage — user ID verification, onboarding, and beyond — with a complete digital identity solution.
Protect personal data securely to prevent data breach and misuse	Application-Level Encryption Entrust KeyControl Vault for VM Encryption Entrust KeyControl Vault for Databases Keys and secrets underpin the security of cryptographic processes. Managing their complete lifecycle is critical for comprehensive security. nShield HSMs and nShield as a Service nShield hardware security modules (HSMs) offer FIPS-certified hardware roots of trust, available on-premises or as a service, enabling you to implement and enforce best practices in generating and protecting the cryptographic keys that underpin your encryption strategy.
Informing of data breaches to the Board and each affected data principal	Entrust KeyControl Compliance Manager Documents how keys and secrets are used for risk mitigation and regulatory compliance. Facilitates key audit and reporting information to authorities.
Securing data during transmission	Entrust PKI Digital certificate solutions (private and public) for communication encryption with TLS technology — used for web servers, applications and VPNs.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223