WHITEPAPER

aperon

Compliance to **DPDP Act**



Digital Personal Data Protection Act

In August 2023, India enacted the Digital Personal Data Protection (DPDP) Act, its first comprehensive data protection law, establishing a legal framework for the processing of personal data within the country.

The Act defines the responsibilities of Data Fiduciaries (entities collecting personal data) and Data Processors (entities handling or processing the data), while also detailing the rights and obligations of Data Principals (individuals whose data is collected), along with significant financial penalties for non-compliance.

Furthermore, the DPDP Act created the Data Protection Board of India (DPB)—the nation's first regulatory body dedicated to safeguarding personal data privacy. The DPB is tasked with ensuring compliance and enforcing penalties on organizations that fail to meet the prescribed data protection standards.

Non-compliance to the provisions can result in penalties of up to ₹250 crores.

Who is Impacted by DPDP Act?

The DPDP Act applies to businesses that fulfill the following conditions:

1. Process digital personal data capable of identifying the data principal (the individual to whom the data relates).
2. Manage data that is either already in digital form or is intended to be digitized, with non-digitized and offline personal data explicitly excluded.
3. Process digital personal data within India's jurisdiction.
4. Process data outside India that is directly connected to offering goods or services to individuals in India.

The Act impacts a wide range of sectors - including Legal, IT, HR, Sales and Marketing, Procurement, Finance, and Information Security - due to the sheer volume and sensitivity of personal data collected, stored, and processed by them. Consequently, organizations in these and related industries must establish robust data privacy and protection programs to ensure compliance with the DPDP Act.

How Zaperon Helps Organizations Comply to DPDP Act?

Compliance Requirement

1. PROTECT PERSONAL DATA

Data Fiduciary shall implement appropriate technical measures to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

How Zaperon Can Help?

CENTRAL ACCESS CONTROL	CONTEXT-BASED ACCESS	SECURE REMOTE ACCESS	DATA SECURITY
✓ Access to all the enterprise resources (on-premises/cloud applications, servers) is all managed from a single dashboard. ✓ Complete user lifecycle can be managed - onboarding to exit. ✓ Credential phishing attacks can be eliminated via PKI-based passwordless access. ✓ Multi-factor Authentication (MFA) is enforced to block unauthorized access.	✓ Access to enterprise resources is only granted after validating user behavior (user role, location, time of access) and device posture (IP, operating system, antivirus, device lock, disk encryption). ✓ Only authorized devices are allowed access. ✓ Continuous device posture assessment is done to ensure devices are always secure.	✓ Built-in ZTNA ensures secure remote access to all enterprise resources from any location & network without being exposed to VPN vulnerabilities.	✓ All the channels for data leakages from endpoints are blocked - USB, Bluetooth, Airdrop, Screen capture, removable hard disks etc. ✓ User activities on internal & external websites - uploads, downloads and deletions - are monitored to prevent data compromise. ✓ Web applications that users access on their devices are discovered in real-time and malicious or unsanctioned apps can be blocked instantly. ✓ Login to SaaS applications (Google Workspace, ChatGPT, etc.) using unauthorized domains are blocked from corporate devices.

Compliance Requirement

2. DATA LOCALIZATION

Central Government restricts the transfer of personal data by a Data Fiduciary for processing to any territory outside India.

How Zaperon Can Help?

LOCAL DATA STORAGE	ACCESS CONTROL
✓ Zaperon cloud servers are located in India.	✓ Prevent access from users (internal or 3rd party) located in countries not permitted by Govt. of India. ✓ All web traffic of users is monitored, controlled and logged irrespective of their location - in office or outside.

Compliance Requirement

3. DATA MINIMIZATION & RETENTION

Personal data can be processed as long as consent is given by the Data Principal. If a Data Principal withdraws her consent to the processing of personal data or requests for data deletion, Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data.

How Zaperon Can Help?

LEAST PRIVILEGE ACCESS	DATA ACCESS LOG
✓ Grant users access to only those applications that are needed for their roles. ✓ Role-based access and identity verification ensure that only authorized users make changes to the data. ✓ With identity-lifecycle management, remove user data and access easily from a centralized console.	✓ Data transfers from endpoints and cloud apps are monitored and logged to enable timely data deletion or archiving.

Compliance Requirement

4. GOVERNANCE & ACCOUNTABILITY

Data Fiduciary to appoint an independent data auditor to carry out data audit and Data Protection Impact Assessment and evaluate the compliance to the Act.

5. RETENTION OF AUDIT LOGS

On a complaint made by a Data Principal in respect of a personal data breach or a breach reported by Data Fiduciary, Data Protection Board of India shall undertake investigation of the incident and impose penalties.

How Zaperon Can Help?

EVENT LOGGING AND AUDIT TRAILS

- ✓ All user activities - application logins, failed authentications - are tracked and logged in real-time.
- ✓ Any user or device exhibiting suspicious behavior is blocked instantly.
- ✓ User activities on internal & external websites - uploads, downloads and deletions - are monitored & logged to prevent data compromise.

Compliance Requirement

6. ENSURE COMPLIANCE BY DATA PROCESSORS

Data Fiduciary is responsible for any data security lapses by Data Processor that may lead to a data breach.

How Zaperon Can Help?

CONTROL 3rd PARTY ACCESS

- ✓ Least privilege access is given to all users including 3rd-party users of data processor.
- ✓ Enforce Zero Trust policies and restrict data movement from external users and devices.

Zaperon

Zaperon is an Identity-centric Security Service Edge (SSE) platform designed to secure access to applications, data, and cloud infrastructure from any user or device, regardless of location or network. It continuously enforces access policies based on user behavior, device posture, and contextual parameters, ensuring least-privilege access while preventing lateral movement. By minimizing attack surface, proactively detecting anomalies, and providing real-time visibility, Zaperon fortifies hybrid IT environment. Organizations can proactively manage access, reduce risks from credential based threats, and safeguard sensitive information, making security adaptive, scalable, and resilient against evolving cyber threats.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com

© 2025 Zaperon, Inc.
All Rights Reserved.

