WHITE PAPER

proofpoint.

Navigating India's Digital Personal Data Protection Act

A practical, human- and AI-centric approach to data security with Proofpoint

Executive summary

Proofpoint's *2025 Voice of the CISO* report highlights the scale of data exposure in India. 99% of Indian CISOs reported a material loss of sensitive data, the highest rate globally. This was significantly above the global average of 66%. Incidents involving sensitive data often include personal data and can arise from scenarios such as misdirected communications, compromised accounts, or everyday employee actions. As a result, personal data exposure has become an operational challenge for organisations in India and globally. This challenge has become magnified as governments across the U.S., the EU, Asia-Pacific, and other regions strengthen personal data protection frameworks.

India's Digital Personal Data Protection Act, 2023 (DPDPA)—together with the Digital Personal Data Protection Rules, 2025 (DPDPR)—marks a major milestone in India's privacy and data protection journey. The Act reflects a global shift toward outcome-based data protection. It gives organisations flexibility in how they design security controls while raising expectations around safeguards, incident readiness, and accountability in day-to-day operations.

Most data breaches today are caused by human interaction with digital systems. Phishing, impersonation, misdirected communications, misuse of access, and accidental exposure are common causes. Proofpoint research shows that 85% of organisations experienced at least one data loss incident in the past year. In addition, a very small number of users accounted for the majority of exposure events. These findings expose the limitations of traditional, perimeter-based or content-only data protection approaches.

These risks are now being amplified by AI-driven attacks, as well as the rapid adoption of shadow AI tools and agentic workflows. AI increases the speed, scale, and sophistication of both external threats and internal misuse. This exposes the limitations of traditional, perimeter-based or content-only data protection approaches. In an agentic workspace, organisations require integrated, context-aware controls that can adapt to evolving human and machine-driven risk.

This whitepaper examines the DPDPA and DPDPR as catalysts for data security transformation.

The paper explains why a people-focused security strategy is critical to reducing real-world personal data protection risk. It also outlines how Proofpoint's human- and AI-centric data security platform helps organisations strengthen personal data protection, support regulatory outcomes, and build long-term resilience.

Understanding the DPDPA and DPDPR

Scope of application

The DPDPA and DPDPR apply to the processing of digital personal data of individuals ("Data Principals"). Within this scope, organisations acting as Data Fiduciaries and Data Processors must meet core operational and accountability obligations.

This framework applies when personal data is processed in India. It also applies when personal data is processed outside India in connection with offering goods or services to individuals in India. The regulation focuses exclusively on digital personal data, including data collected online or subsequently digitised.

This means Data Fiduciaries and Data Processors must manage personal data that is stored and processed across multiple cloud services, third-party environments, and digital communication channels. This distribution increases exposure and complexity. It also makes consistent and scalable protection essential.

Core regulatory principles

The DPDPA is principle-based rather than prescriptive. However, it establishes clear regulatory expectations centred on:

- Lawful and consent-based processing of personal data
- Purpose limitation and data minimisation, ensuring data is processed only for specified and legitimate purposes
- Protection and enablement of Data Principal rights, including transparency and grievance redressal
- Accountability of Data Fiduciaries, including responsibility for preventing, detecting, and responding to personal data breaches

Together, these principles shift compliance from policy declarations to demonstrable operational accountability.

Key obligations of Data Fiduciaries

Under the DPDPA and the DPDPR, Data Fiduciaries must implement technical, organisational, and procedural measures to protect personal data and uphold the rights of Data Principals.

Key obligations include:

- **Implementing reasonable security safeguards** to prevent personal data breaches and mitigate associated risks. These must take into account the nature, volume, and sensitivity of the personal data processed. *(DPDPA, Section 8(5); DPDPR, Rule 6)*
- **Ensuring lawful, consent-based processing of personal data**. This includes maintaining valid consent records and honouring the withdrawal of consent where applicable. *(DPDPA, Sections 4, 6, and 7; DPDPR, Rules 3, 5, and 8)*
- **Notifying the Data Protection Board of India and affected Data Principals of personal data breaches** without delay. This must be done in accordance with prescribed procedures and timelines. *(DPDPA, Section 8(6); DPDPR, Rule 7)*
- **Respecting and enacting Data Principal rights**. These include the rights to access information, seek correction or erasure of personal data, withdraw consent, or raise grievances, within the timelines specified under the Rules. *(DPDPA, Sections 11 to 14; DPDPR, Rule 14)*
- **Providing enhanced protection for children's personal data**. This includes restrictions on certain forms of processing and the requirement to obtain verifiable parental or guardian consent. *(DPDPA, Section 9; DPDPR, Rule 10)*

These obligations apply across the entire personal data lifecycle, from collection and use to storage, retention, and erasure. They reinforce the need for continuous oversight rather than one-time compliance efforts.

Penalties and enforcement

The DPDPA adopts a civil penalty–based enforcement model. Penalties of up to INR 250 crore (over USD 27 million) may be imposed for serious failures. Examples are inadequate security safeguards, unmanaged data breaches, or failure to meet notification obligations.

Regulatory exposure is compounded by the financial impact of data breaches. According to the IBM *Cost of a Data Breach Report 2025*, the global average cost of a data breach was USD 4.44 million. In high-penalty regulatory environments, breach costs can be much higher.

For example, the United States reached an average breach cost of USD 10.22 million, driven in part by regulatory fines and enforcement actions.[1] When combined with potential penalties of up to INR 250 crore under the DPDPA, these figures send a clear message to organisations operating in India: investing in effective, risk-based, and auditable data protection measures is not only a compliance requirement, but a critical business imperative.

Experience from other mature privacy regimes suggests that the main intent of such penalty frameworks is not to maximise fines, but to drive organisational focus and behavioural change. Under laws such as the EU General Data Protection Regulation (GDPR) and Australia's Privacy Act, large penalties are relatively rare and typically reserved for serious or systemic failures. Far more common are regulatory inquiries, corrective orders, and reputational consequences. In this context, the DPDPA's penalty structure should be viewed less as a revenue mechanism and more as a strong signal.

Organisations are expected to take protection of personal data seriously, invest in safeguards, and demonstrate accountability before breaches occur.

[1] IBM. *Cost of a Data Breach Report*. 2025.

Practical challenges

While the DPDPA establishes clear legal obligations, the DPDPR translate those obligations into enforceable operational expectations. To meet these expectations in a sustainable way, organisations must address a number of key practical data protection challenges.

Ambiguity of reasonable security safeguards

Like the EU GDPR, Singapore's Personal Data Protection Act (PDPA), and Australia's Privacy Act, the DPDPA avoids prescribing specific technologies. Organisations must prove that their safeguards are appropriate to the data they hold and the risks they face. They must support this with evidence such as monitoring, incident records, and measurable outcomes.

Maintaining breach readiness

The Rules impose explicit expectations for timely breach detection, investigation, and notification. These put increased pressure on organisations to maintain continuous visibility and incident readiness rather than reactive response capabilities. People-centric attacks shorten detection and response windows, leaving organisations less time to contain incidents before data is exposed. By forcing teams to correlate signals across siloed systems, fragmented security tools and manual processes further slow detection and containment. For example, IBM reports an average of 241 days to identify and contain a breach.[2] In contrast, organisations that adopt integrated, AI-enabled detection and response capabilities materially shorten breach lifecycles and reduce overall cost and regulatory impact.

Knowing where personal data resides

Today, data is widely distributed across cloud services, software as a service (SaaS) platforms, collaboration tools, and AI-enabled workflows. Proofpoint research shows that data sprawl across cloud and SaaS platforms is a top challenge for nearly half of organisations. At the same time, everyday human actions, such as sharing, copying, and responding to messages, as well as interacting with AI tools, introduce risks that static controls can't adapt to.

Managing insider and accidental risk

Proofpoint's *2025 Data Security Landscape* report shows that most data loss incidents are driven by human activity, with a small subset of users responsible for a large share of exposure. And according to Proofpoint's *2025 Voice of the CISO* report, 96% of CISOs in India who experienced data loss said departing employees played a role. Both of these findings underscore the impact of insider-related risk. Everyday actions by trusted users, such as misdirected communications, unsafe sharing, or misuse of access, remain among the most common triggers for reportable incidents.

Addressing AI-related data exposure

The rapid adoption of AI is reshaping the personal data protection landscape. According to IBM's *Cost of a Data Breach Report 2025*, 16% of breaches involved attackers using AI-driven techniques. At the same time, unapproved "shadow AI" tools were involved in 20% of breaches, increasing average breach costs by approximately USD 670,000.[3]

AI also amplifies traditional insider risk. Careless users might unintentionally expose personal data through AI prompts. Compromised accounts can weaponize AI access for rapid discovery and exfiltration. And agentic AI systems introduce a further challenge: without strong guardrails, they can behave like over-privileged insiders, with the ability to access, reproduce, or disclose sensitive data at scale.

2. IBM. *Cost of a Data Breach Report*. 2025.
3. Ibid.

Proofpoint's human- and AI-centric approach to data security

For decision makers, the key question under the DPDPA is not simply whether controls exist, but whether those controls reduce real-world personal data protection risk. As an outcome-based regulation, the DPDPA emphasises effectiveness, evidence, and accountability.

Proofpoint helps organisations translate legal obligations into measurable, enforceable security outcomes by focusing on the intersection of people, data, and threats. This is where personal data exposure most often occurs.

From Proofpoint's perspective, effective personal data protection must account for how people access, use, and share data across everyday digital workflows. While the DPDPA is technology-neutral, Proofpoint's approach is shaped by long-standing market insights and observed breach patterns. Industry data consistently shows that a small subset of users and behaviours account for a significant share of

Proofpoint reduces personal data exposure by addressing how people actually work and how data is most often compromised in modern organisations. Its unified data security solution protects personal data across email, cloud applications, collaboration platforms, endpoints, and AI-driven workflows using a single, consistent policy framework.

Proofpoint's unified solution combines Enterprise DLP, Data Security Posture Management (DSPM), and Insider Threat Management (ITM). It applies context-aware controls that consider user behaviour, data sensitivity, and threat signals, rather than relying on static content rules. This approach enables organisations to identify and prioritise real risk, prevent both accidental and malicious data exposure, and reinforce secure handling of personal data through continuous behavioural insight and awareness.

The following table shows how Proofpoint's human- and AI-centric security platform helps organisations address and translate DPDPA and DPDPR requirements into measurable, operational controls.

Requirements/Obligations	Limitations of traditional data security solutions	Proofpoint solutions	How Proofpoint solutions help
Reasonable security safeguards Prevent personal data breaches and mitigate associated risks through effective technical and organisational measures *(DPDPA Section 8 and DPDPR, Rule 6)*	Rely on static, content-only rules that lack behavioural context, generate high amounts of false positives, and fail to stop data loss during everyday user activity.	• Enterprise DLP • Data Security Posture Management (DSPM) • Collaboration Security Protection • ZenGuide (Security Awareness Training & Phishing Simulation)	Proofpoint protects personal data where people work: email, SaaS, collaboration, and endpoints. **Enterprise DLP** enforces consistent controls for data in motion and at rest. **DSPM** provides agentless discovery and classification of sensitive data across cloud and hybrid environments. Behavioural analytics, threat intelligence, and user context prioritise real risk and prevent both accidental and malicious data exposure before it becomes a breach.
Managing emerging, AI-driven personal data risk Ensure reasonable safeguards continue to prevent personal data breaches as new technologies change how data is accessed, shared, and exposed *(as part of reasonable security safeguards)*	Legacy tools lack visibility into AI usage, shadow AI tools, and AI-assisted data sharing. Static data loss prevention (DLP) rules and siloed controls can't detect sensitive data flowing into GenAI prompts, training data, or AI agents. This increases accidental and insider-like exposure.	• Enterprise DLP • Data Security Posture Management (DSPM) • Insider Threat Management (ITM) • Secure Agent Gateway • AI Data Governance • ZenGuide (Security Awareness Training & Phishing Simulation)	**DSPM** protects sensitive data across cloud and on-premise environments and secures how data is used by AI, copilots, and large language models (LLMs). **Enterprise DLP** prevents sensitive data loss by controlling how employees use AI tools, prompts, uploads, and endpoints. **ITM** detects risky insider behaviour by monitoring abnormal access to, or use of, sensitive data. **Secure Agent Gateway** governs the access of AI agents to data, enforcing policies and blocking or redacting sensitive information. **AI Data Governance** enables safe GenAI adoption by identifying AI usage and enforcing controls to prevent data exposure and compliance risks. **ZenGuide** changes employee behaviour with adaptive security training that reduces human risk over time.

Requirements/Obligations	Limitations of traditional data security solutions	Proofpoint solutions	How Proofpoint solutions help
Consent-based and purpose-limited processing Ensure personal data is accessed and used only for lawful and authorised purposes *(DPDPR, Rule 5 & Rule 8)*	Limited visibility after data enters SaaS and cloud platforms, making purpose limitation difficult to enforce in dynamic environments.	• Data Security Posture Management (DSPM) • Enterprise DLP	**DSPM** continuously discovers and classifies personal data in place, giving organisations clear visibility into where sensitive data resides and how it is accessed. **Enterprise DLP** implements risk-based DLP policies that govern data use based on user role, behaviour, and context. This enables practical enforcement of purpose limitation without disrupting business workflows.
Data Principal rights Enable timely, secure, and auditable execution of access, correction, and erasure requests *(DPDPA Chapter III & DPDPR, Rule 14)*	Manual searches across disparate systems slow response times and increase the risk of unauthorised access or misuse during sensitive processes.	• Data Security Posture Management (DSPM) • Insider Threat Management (ITM)	**DSPM** accelerates data discovery and scoping across cloud and hybrid environments, reducing uncertainty during rights fulfilment. **ITM** adds behavioural visibility for high-risk and privileged activity, helping organisations complete rights requests securely and with audit-ready evidence.
Breach detection and notification readiness Detect, investigate, and report personal data breaches without delay *(DPDPA Section 8 & DPDPR, Rule 7)*	Disconnected security tools require manual correlation, delaying detection, investigation, and regulatory notification.	• Collaboration Security Protection • Threat Intelligence • Insider Threat Management (ITM) • Automated logging & reporting	Proofpoint correlates threat intelligence, user behaviour, and data movement across email, cloud services, and endpoints. Automated investigation and response reduce time to containment, while structured dashboards, logs, and forensic evidence support accurate breach notification and post-incident regulatory review.
Accountability of Data Fiduciaries and Processors Demonstrate ongoing oversight, governance, and accountability *(DPDPA, Section 8)*	Periodic compliance reporting provides limited insight into real exposure, insider risk, and data misuse.	• Human Resilience Workbench • Insider Threat Management (ITM) • Data Security Posture Management (DSPM) • Enterprise DLP • ZenGuide (Security Awareness Training & Phishing Simulation)	Unified risk dashboards provide visibility into personal data exposure, identity risk, and insider activity. Proofpoint provides executive-level visibility into personal data exposure, identity risk, and insider behaviour. DSPM prioritises data risk by sensitivity and business impact, highlights overexposed or over-permissioned data, and guides remediation. Policy enforcement and forensic audit trails support Data Protection Impact Assessments (DPIAs), internal reviews, and regulator-facing accountability.

Why Proofpoint is unmatched for the DPDPA era

Traditional data protection tools focus primarily on content and infrastructure. They rely on static, policy-driven controls that inspect data patterns and locations, with limited visibility into user behaviour, intent, or changing risk conditions. As a result, these tools often generate large volumes of alerts while struggling to prevent data loss where it actually occurs.

Proofpoint is different because it's designed for the realities of the modern workplace. It applies people-focused controls across the channels where personal data is most frequently exposed. These include email, cloud, collaboration, and AI-driven workflows. By correlating user behaviour with data sensitivity and threat context,

Proofpoint reduces false positives and prioritises the activity that matters most. Its integrated approach brings together prevention, detection, response, and user awareness. This enables organisations to address both traditional data exposure and emerging, AI-driven risk with a single, coherent security strategy.
Proofpoint's approach addresses the real-world ways that personal data is exposed and misused, which aligns with the DPDPA and DPDPR's focus on outcomes and accountability. It helps organisations reduce personal data exposure and demonstrate effective, ongoing protection.

Conclusion

Together, the DPDPA and DPDPR represent a positive and timely transformation for data protection in India. They signal the country's commitment to building trust in the digital economy by shifting focus from formal compliance to demonstrable protection and accountability.

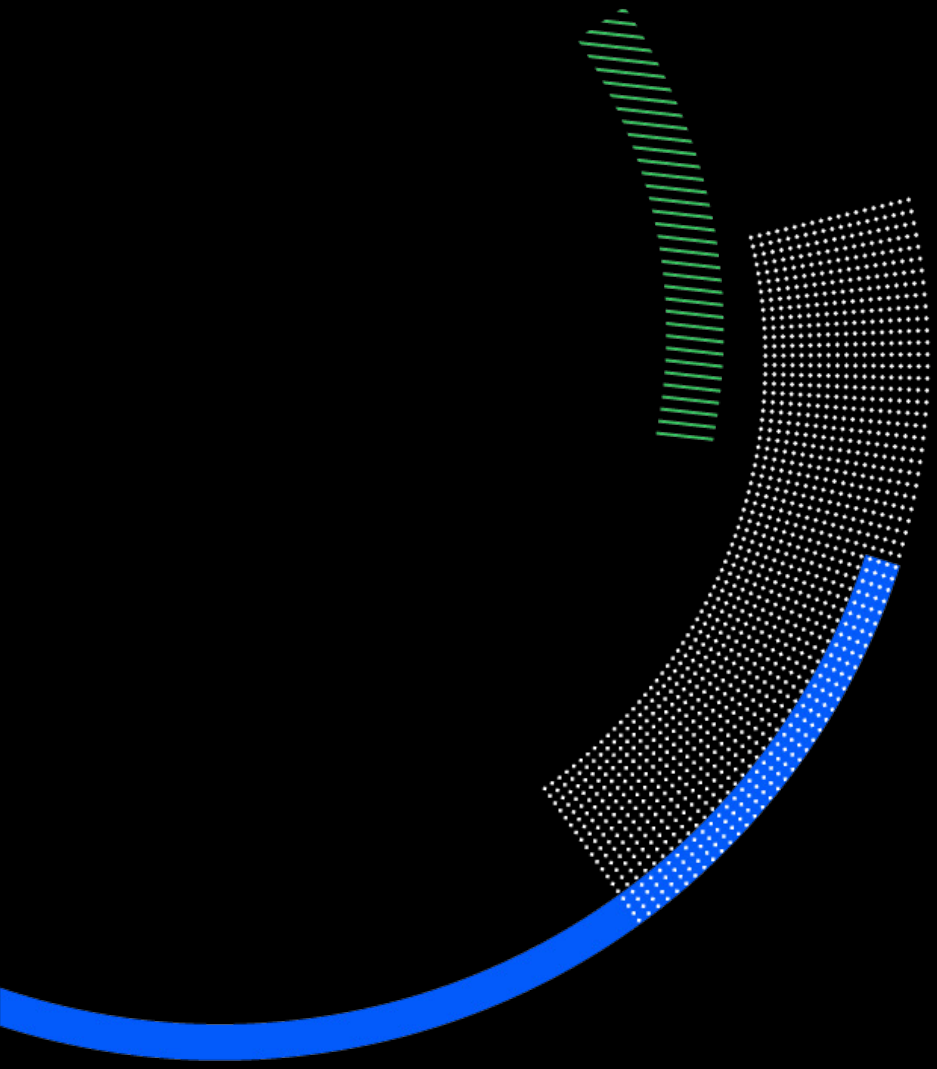
For organisations, this moment goes beyond regulatory alignment. The DPDPA provides a valuable opportunity to reassess data security strategies, modernise controls, and strengthen resilience against evolving threats. By reassessing data security through a people-focused lens, organisations can reduce personal data protection risk. What's more, they can reinforce customer trust, support innovation, and build long-term confidence in how personal data is handled.

Proofpoint enables this transformation by helping organisations protect people, data, and digital communication channels together. This helps organisations move beyond compliance checklists toward sustainable and defensible personal data protection in the DPDPA era.

Your next steps

To understand how Proofpoint can help your organisation align with DPDPA expectations and strengthen personal data protection, contact your Proofpoint representative or request a consultation. As your strategic partner, Proofpoint will collaborate with you to assess current data security risks, identify compliance gaps, and design a future-proof, people-focused strategy that delivers measurable protection outcomes.

To learn more about our unified data security solution, explore Proofpoint Data Security solutions or contact your Proofpoint representative to schedule a demo.



proofpoint®

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn