K7 CYBER SECURITY

A K7 CYBERSECURITY EXECUTIVE BRIEFING • NOVEMBER 2026

Turning DPDP Compliance into a Security-Led Capability

From Endpoint to SOC

For CIOs and CISOs—and the CEOs, COOs, CFOs and boards who depend on them.



www.k7cybersecurity.com

Executive Summary

An auditor asks: **“Can you show that our personal information was protected throughout the last quarter?”** That evening, a supplier-linked cloud folder is found exposed. The CEO asks: **“Whose information is at risk, what did we do, and what must we report?”**

Different moments, much the same answer. The organisation must know where personal data is, who can reach it, whether safeguards are actually working, and what happened when they failed. A policy or a green dashboard cannot answer all four questions.

India’s principal DPDP privacy, security and breach-notification obligations are scheduled to commence on **13 May 2027.** The Act sets maximum penalties of **₹250 crore** for failures relating to reasonable security safeguards and **₹200 crore** for breach-intimation failures, subject to inquiry and the statutory process. These are not automatic fines. A single incident may engage both provisions if both duties are breached. [1–3]

DPDP is bigger than cybersecurity. Product, Legal and Privacy must address lawful processing, notice and rights. Operations must handle requests; Procurement must govern processors; and Security must protect the systems and evidence on which the business relies. One accountable executive must coordinate the programme.

What a connected endpoint-to-SOC approach changes: Security controls, their current state, incident investigations and retrievable evidence become one operating chain. Failures are surfaced earlier; an audit becomes evidence retrieval rather than last-minute reconstruction; and responders work from a common timeline during a breach. This supports compliance—it does not confer it.

Five management actions

- **Assign ownership:** one executive sponsor and named owners across business, Privacy, Product, IT, Security and Procurement.
- **Map one important process:** its personal data, applications, suppliers, access paths and unknowns.
- **Prove the safeguards:** test what is in force today and what can be evidenced across a past period.
- **Rehearse both kinds of breach:** unauthorised exposure and loss of access, with Legal and operations in the room.
- **Challenge the evidence:** use internal audit or independent advisers to test readiness and confirm corrective action.

THE DECISION FOR LEADERSHIP

Fund a cross-functional readiness programme anchored in **measurable protection and credible evidence**, not another collection of disconnected security reports.

In This Briefing

1 DPDP changes the business, not just the security team

2 What Rules 6 and 8 really require you to show

3 Protect information across the digital estate

4 Make security posture current and verifiable

5 Make audit readiness a daily capability

6 Respond to a breach with facts and speed

7 Nine demonstrations to demand from security providers

8 A practical route to May 2027

9 Conclusion: Protection, assurance and response belong together

READING GUIDE : Page one is a stand-alone board briefing. Sections 1–5 explain what management must establish; Sections 6–8 guide Security, IT and implementation teams.

1 DPDP changes the business, not just the security team

DPDP regulates digital personal data, and security scope follows the business processes that use it—not merely a database. Customer and employee information moves through business applications, cloud services, devices, portals, suppliers and test copies.

Across sectors, the implications are tangible. Hospitals and diagnostic laboratories handle identifiable patient information in clinical systems; financial institutions manage customer and payment records across banking platforms and providers; and retailers connect loyalty and transaction data through applications and partners. Controls and evidence must follow that information across the processing chain. Applicable sector-specific obligations still apply.

A Data Fiduciary decides why and how personal data is processed; a Data Processor handles it on the Fiduciary's behalf; a Data Principal is the individual concerned—including an employee. Outsourcing work does not outsource the Fiduciary's legal accountability. [1] The privacy programme has significant non-security work: appropriate notices, consent or specified legitimate uses, withdrawal, individual rights, grievance handling, nomination, retention and erasure. Product teams must make these processes work inside applications, not just in policy documents. Security monitoring of employees may itself process personal data and must have a lawful basis and appropriate safeguards.

For businesses serving children, Section 9 restricts tracking, behavioural monitoring and targeted advertising directed at children, subject to specified exemptions; the Act provides a separate penalty ceiling of ₹200 crore for children's-data obligations. Supplier security clauses are also a contract-by-contract effort—not a single policy update when a business has dozens or hundreds of processors. [1–2]

An organisation becomes a Significant Data Fiduciary (SDF) when notified by the Central Government, not simply when it reaches a particular size. Additional duties include an India-based Data Protection Officer, an independent data auditor, a Data Protection Impact Assessment and a data audit every twelve months, due diligence on algorithmic software, and possible restrictions on transfers of specified personal data and associated traffic data. Monitor notifications and plan scenarios with counsel. [1–2]

Three easy-to-miss distinctions: the November 2026 phase principally concerns the Consent Manager framework; the main enterprise phase is scheduled for May 2027. DPDP does not impose blanket localisation of all personal data. Rule 14 requires a published route for individuals to exercise their rights, including the identifiers needed to verify a requester. It also calls for a grievance-redressal process with a published response period of no more than 90 days and measures to meet it. That grievance period is not a universal deadline for every access, correction or erasure request. [1–4]

THE DECISION

Appoint an executive programme owner and separate leads for the privacy, business, contractual and security workstreams.

2 What Rules 6 and 8 really require you to show

Rule 6 names seven minimum safeguard categories for personal data in the organisation's possession or under its control, including processing on its behalf. It does not require a particular brand or product category. A review should test both **control design**—was the safeguard appropriately designed?—and **operating effectiveness**—did it work during the period examined? [2]

Rule 6 safeguard	Evidence an assessor may reasonably ask for
Protect the data: encryption, masking or tokenisation	Covered systems, relevant configuration, exceptions and control tests
Control access to computing resources	Permissions, access reviews, separation of duties, privileged approvals and expiry
Log, monitor and review access	Source logs, collection health, investigated alerts, findings and remediation
Support continuity after compromise	Backup records, a dated restore test and recovery arrangements
Retain specified logs and personal data for one year	Source-specific settings, integrity protection and a successful retrieval test
Require processor security safeguards in contracts	Signed provisions, escalation contacts and evidence of oversight
Ensure safeguards remain effective	Control owners, vulnerability and patch evidence, tests, exceptions and re-verification

Rule 8 is related, not the same requirement. It includes specific erasure triggers and an additional one-year retention obligation for personal data, associated traffic data and processing logs for the purposes described in the Seventh Schedule. The 48-hour advance notice concerns particular Rule 8(1) cases—not all deletion. Retention schedules must reconcile these duties with erasure, other laws and processor arrangements. [2]

CERT-In separately requires specified ICT-system logs to be kept for a rolling 180 days in India, relevant clock synchronisation and reporting of specified cyber incidents within six hours of noticing them, where applicable. These are distinct duties and clocks. [5]

Existing ISO 27001 controls or relevant SOC 2 assurance can provide useful evidence. Reuse them—but identify gaps in personal-data scope, statutory retention, breach reporting and processor commitments. No certification automatically establishes DPDP compliance. **You cannot demonstrate that a control operated throughout a quarter if the underlying evidence was not retained.**



THE DECISION

Build one seven-safeguard evidence register: control owner, systems covered, method, last verification, exceptions, historical record and retrieval path.

3 Protect information across the digital estate

Consider a plausible incident: a user account is compromised, the attacker changes a cloud-sharing setting, uses an over-privileged application account and exports customer information. Relevant endpoint, identity, cloud and application records may sit in separate systems—or may be missing if logging was not enabled. Reconstructing the sequence can take too long, or prove impossible after the fact.

Six capabilities need to work together. They may be native to a platform, supplied by specialist tools or provided by existing enterprise systems:

- **Discover what exists:** assets, personal-data repositories, cloud and SaaS services, data owners and what has not been examined.
- **Prevent avoidable exposure:** endpoint and server protection, vulnerability and patch management, configuration and cloud/SaaS posture checks.
- **Govern access:** identity lifecycle, MFA, in-application permissions, access reviews and privileged or temporary access.
- **Protect the data:** encryption, key management, appropriate data-loss controls, safe external-file intake, monitoring of extracts and data lifecycle workflows.
- **Investigate and act:** connected endpoint, identity, network, cloud and application evidence feeding detection, case management and an operated or managed SOC.
- **Recover and prove:** tested backup and restoration, synchronised timelines, source-specific retention, exception tracking and exportable evidence.



Two important blind spots

Incoming files. Customers, candidates and suppliers send identity documents, invoices and spreadsheets through portals. Inspect them for threats **before downstream use or storage.** Where content classification is supported, identify sensitive personal data and route it to a governed repository. A file can be safe from malware yet contain personal data the business had not planned to collect. Threat screening does not by itself establish a lawful processing purpose. [7]

ERP, CRM, HR and other core applications. These systems hold concentrated personal data but may have separate role models, audit settings and export paths. Verify application access, monitor bulk extracts, use appropriate masking in non-production copies and connect available native audit events to a shared investigation. **An endpoint agent cannot recreate record-level access evidence that the application never collected.**

For DPDP readiness, the operating requirement is not to replace every specialist tool. It is to ensure that observations, owners, decisions and evidence survive the handoffs—from data intake through processing, sharing, retention and disposal.

THE DECISION

Trace one personal-data process end to end. Identify the protection, the evidence sources and the gaps that no product currently sees.

4 Make security posture current and verifiable

Suppose a dashboard says “96% compliant.” When were the underlying configurations checked? If an administrator removed a safeguard at 10:42, would the dashboard change now, after an overnight log batch, after the next scan—or not at all?

An SIEM is valuable for events, correlation and investigations. But a log stream alone is not a reliable current inventory of configuration or enforcement state. A well-integrated SIEM can support current posture if it receives actual control-state data, identifies source silence and records the age of every input.

Different controls need different verification methods. Endpoint policy may be evaluated by a local agent; cloud access through an API; an ERP permission through application records; and a supplier recovery obligation through a scheduled test. Continuous does not mean every second. It means risk-appropriate check frequency, timely alerts on drift and visible stale or missing evidence. This reflects NIST continuous-monitoring guidance. [6]



THE USEFUL QUESTION

What was checked, on which systems, when, with what result—and who owns what remains unresolved? An honest “last checked at 10:42” beats an unexplained green score.

THE DECISION

Trace one personal-data process end to end. Identify the protection, the evidence sources and the gaps that no product currently sees.

5 Make audit readiness a daily capability

An external auditor may sample an application and a period, not merely read today's policy. A credible evidence pack shows coverage, owners, settings, access and logging records, reviews, exceptions, actions taken and proof that corrections remained effective. "Not assessed" is a legitimate status; silently treating it as "passed" is not.

One evidence base should serve several reviews: internal audit, ISO 27001/SOC 2 assessments where relevant, customer questionnaires, DPDP readiness reviews and incident investigations. This can reduce repeated screenshot collection and reconstructing the same history for different reviewers. Independent assurance remains a separate professional judgement—not a vendor dashboard.

What management should report to the audit committee

Report to the audit committee	Report alongside it
Important personal-data processes mapped	Systems, copies and processors still unmapped
Access and security control coverage	Assets or applications not tested
Controls verified as effective	Checks that are stale, partial or failed
Log collection availability	Missing sources and interruptions
Breach report readiness	Corrections or unanswered questions in rehearsal
Remediation actions closed	Fixes independently rechecked

For financial context, IBM's 3 August 2026 India release reported ₹25.5 crore as the average organisational cost of a data breach in its 2026 study. This is a study average, not a prediction for an individual company. The more immediate CFO question is how many person-weeks the business spent recreating evidence during last year's reviews. [8]

THE DECISION

Commission a sample evidence pack for one critical process before the external readiness assessment, and reuse the results in the board discussion.

6 Respond to a breach with facts and speed

Rule 7 reporting is triggered **when the Data Fiduciary becomes aware of a personal data breach.** A cyber alert is not necessarily a breach. But once the legal definition is met, Rule 7 adds no separate small-incident or likely-harm threshold. Affected individuals and the Data Protection Board must be informed without delay; an updated detailed report to the Board follows within 72 hours of awareness unless an extension is permitted on written request. [1–2]

Breach means more than information leaving the company. The Act includes a qualifying **loss of access,** so ransomware can be a personal data breach even without demonstrated theft. CERT-In's existing six-hour clock concerns specified cyber incidents and has a different trigger; neither reporting process replaces the other. [1–2, 5]

The 72 hours are measured from **your organisation's awareness,** not automatically from a processor's awareness. Require suppliers to raise suspected incidents promptly so that you can investigate and meet your own obligations. High-quality initial communication distinguishes established facts from open questions and names the actions already taken.

Illustrative scenario—not a legal timetable. A supplier-linked cloud folder holding identity records becomes public at 21:40; the change is detected at 23:12.

Example time	What a prepared organisation can demonstrate
23:12	On-call investigation begins; folder is linked to data category and business owner.
23:21	Public access withdrawn; action and authorization recorded.
23:40	Cloud, identity and access evidence preserved; absent logs marked as unknown.
00:15	Preliminary affected population assessed; Legal and Privacy review reporting.
Following hours	Required initial communications and any separately applicable CERT-In report; investigation continues.
Rule 7 period	Updated detailed Board submission with actions, findings, limitations and notification record.

Agentic SOC: automate the routine, retain accountability

An Agentic SOC uses AI agents for bounded work: gather supporting events, correlate timelines, check stale control records, run approved response playbooks, document low-risk case closure and escalate decisions that need a person. It can help teams evaluate more potential incidents consistently without treating every raw alert as reportable.

Security telemetry may itself contain personal data. Ask where AI analysis takes place, what data goes to external models, under whose contract, and whether a task can run inside a controlled or isolated environment. Task-focused smaller models may reduce latency and per-use costs for suitable high-volume tasks; their accuracy and economics must be demonstrated, not assumed. Human owners keep control of legal classification, regulatory communications and disruptive containment. Designated Significant Data Fiduciaries must also consider their specific due-diligence obligations for algorithmic processing of personal data.



THE DECISION

Rehearse both a data-exposure incident and a loss-of-access incident, including after-hours escalation, evidence gaps and human approval points.

7 Nine demonstrations to demand from security providers

Do not judge security capabilities from a feature slide. Ask existing providers and prospective partners to demonstrate these on authorised representative systems. Accept an honest “requires integration” or “not visible” rather than a misleading claim of universal coverage.

Ask the supplier to demonstrate	What you are testing
1. Show the estate and its unknowns. Include cloud, applications, endpoints, processors and unmanaged sources.	Coverage with a denominator, not an invented completeness score.
2. Show today and last quarter. Provide last verification, drift, missing source intervals and prior control state.	Current posture and historical operating evidence.
3. Connect an incident. Correlate identity, privilege, endpoint, cloud and application activity.	Whether context survives across tools and teams.
4. Follow an inbound file. Show pre-storage screening, optional data classification and its governed destination.	Secure intake without confusing threat inspection with lawful processing.
5. Trace ERP/CRM access. Show who had access, what reads or exports were logged and what is unknown.	Actual application-level evidence rather than server telemetry.
6. Correct and verify. Fix a privilege or unsafe cloud setting and show the correction held.	Remediation effectiveness, not just a closed ticket.
7. Retrieve historical logs. Show retention, clock alignment, integrity, gaps and export.	Ability to answer an auditor and investigate an incident.
8. Rehearse both breach clocks. Include a processor, affected individuals and unfinished facts.	Operational ability to act and communicate accurately.
9. Inspect an AI-assisted case. Show evidence, approved actions, data flows, model location, cost and latency.	Bounded, explainable and economically sustainable automation.

THE DECISION

Run the demonstrations on one critical service. Keep tools that work; improve the connections and the evidence they produce.

8 A practical route to May 2027

For most organisations, preparation is no longer a blank-sheet exercise. Prioritise what can materially reduce risk and produce evidence before the core May 2027 commencement.

IF YOU CAN ONLY DO THREE THINGS

1	Map your highest-risk data process, owner and processor dependencies
2	Verify access, patch, cloud, logging, backup and retention evidence; own the gaps
3	Rehearse a breach with Security, Legal, Operations and suppliers—including an after-hours event. These are triage priorities, not a substitute for privacy and contractual duties.



When	Work that matters	Evidence for management
First 30 days	Assign owners; map priority processes; open the seven-safeguard evidence and gap register.	An agreed picture of scope, ownership and unknowns.
Next 60 days	Fix high-risk access, vulnerabilities, exposed sharing, logging and recovery gaps; pursue processor terms.	Verified improvements and open dependencies.
Following 60 days	Run risk-based posture checks; test erasure handoffs; rehearse both reporting clocks and evidence export.	Test records, draft communications and owned exceptions.
Before 13 May 2027	Obtain independent challenge; close material failures; report residual risks to leadership.	A candid status: proven, partial, missing or unassessed.

Start small, but make it real. For one well-defined high-risk process, a small cross-functional team may use about ten working days for a focused diagnostic if relevant owners and records are accessible. That is a scoping illustration, not an estimate for complete DPDP implementation. Product changes and supplier contract remediation may take months.

After 13 May 2027, organisations should not assume a general grace period. Once the relevant enforcement provisions commence, the Data Protection Board may initiate inquiries under the statutory process. Continuous protection and demonstrable evidence remain essential beyond the commencement milestone.

THE DECISION

Approve one process-level diagnostic now, and make readiness reporting about evidence and decisions—not an unexplained percentage.

9 Conclusion | Protection, assurance and response belong together

DPDP asks the business to protect personal data, keep safeguards effective and explain promptly what happened when something fails. These are difficult when access policies, cloud settings, application records, incident tickets and audit evidence sit in disconnected silos.

Connected endpoint-to-SOC operations bring prevention, current control state, investigation, authorised response and evidence into a more reliable workflow. Weaknesses can surface while action is still possible. Audits become more about retrieving existing records and less about reconstructing them. During a breach, investigators can start from the facts available—and identify what is still unknown.

No platform supplies lawful purpose, valid consent, rights handling or independent assurance. Those remain business responsibilities. The value of integrated security is making the protective part of those responsibilities easier to operate—and easier to demonstrate. The question for leadership is simple: Can we show, today, that our important personal data is protected, our safeguards are working, and the evidence is ready?



About K7 CyberSecurity | A practical next step

K7 CyberSecurity helps enterprises connect protection, security operations and actionable evidence. If the questions in this briefing are difficult to answer, begin with **one critical business process,** not an enterprise-wide product replacement.

Use the seven-row Rule 6 table as a **self-check before independent assessment.** For a focused **DPDP Security Evidence Review**, ask K7 to examine the process with your team: scope, existing safeguards, evidence freshness, missing sources and a customer-owned action list. Authorised agentless discovery may assist with reconciling source-recorded asset inventory; it is not a verification of installed protection or a DPDP certification.

References and scope notes

[1] Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023.pdf

[2] DPDP Rules, 2025, G.S.R. 846(E), 13 November 2025.
https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

[3] DPDP Act commencement, G.S.R. 843(E), 13 November 2025.
https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf

[4] Corrigendum, G.S.R. 892(E), 10 December 2025 (Gazette dated 11 December): corrects “of this Gazette” to “in the Official Gazette” without changing the specified periods.
https://www.meity.gov.in/static/uploads/2025/12/3c7ebbae0e5456f493f486e6845df86b.pdf

[5] CERT-In Directions under section 70B(6), 28 April 2022, and FAQs.
https://www.cert-in.org.in/Directions70B.jsp

[6] NIST SP 800-137, Information Security Continuous Monitoring.
https://csrc.nist.gov/pubs/sp/800/137/final

[7] OWASP File Upload Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

[8] IBM India, Cost of a Data Breach Report 2026, India news release, 3 August 2026.
https://in.newsroom.ibm.com/India-Records-its-Highest-Average-Cost-of-a-Data-Breach-2026

Scope and assurance. This is educational guidance on security safeguards and operating evidence within a wider DPDP programme, not legal advice. Applicability, exemptions, sectoral duties, data retention, notification and transitional issues need an organisation-specific legal review. The capabilities discussed are buyer evaluation criteria, not claims of current product availability or certification. Independent assurance remains appropriate.

K7 CYBER SECURITY

Security That Answers To You

REQUEST A DPDP SECURITY EVIDENCE REVIEW

marketing@k7cybersecurity.com | www.k7cybersecurity.com



© 2026 K7 Enterprise Security Private Limited. All Rights Reserved.

202611113