DATA PRIVACY GAP ASSESSMENT: THE GROUND REALITY

INTRODUCTION

The compliance window under India's new data protection law is narrowing. The Digital Personal Data Protection Act, 2023 (**"DPDP Act"**) and the Digital Personal Data Protection Rules, 2025 (**"DPDP Rules"**) are being implemented in phases.

Recent developments show that preparation can no longer be delayed. In August 2026, the Cabinet Secretary asked Union ministries, State Governments and Union Territory administrations to set out how they would implement the law, assign responsibility and work to clear timelines. Separately, Secretary at Ministry of Electronics and Information Technology stated that the notified timelines would remain unchanged. He urged organisations to start preparing without delay.

The message is clear: organisations should not wait until the deadline. DPDP compliance may require changes to systems, contracts, policies and daily operations. These changes cannot be made overnight.

The first step is to understand how the organisation currently processes personal data. This is where a Data Privacy Gap Assessment becomes important. Although the term is not defined under the DPDP Act, it refers to a structured review of an organisation's existing practices against the DPDP Act and DPDP Rules. It helps identify gaps, assess risks and set priorities for remediation.

Most importantly, a gap assessment tests whether documented processes match actual practices. This article examines why the exercise is crucial and highlights the practical insights that commonly emerge from it.

WHY IT MATTERS

In practice, a gap assessment typically combines structured interviews with business units, review of policies and contracts, examination of technical controls, and identification of Personal Data (**"PD"**) flowing across the organization. The DPDP Act prescribes no methodology for this exercise. Organizations must design an assessment approach that is rigorous and suited to their specific operating context as the stakes are significant.

Section 33 of the DPDP Act[1] prescribes substantial financial penalties for non-compliance, including failures in consent management, data security, and breach notification. Beyond regulatory penalties, a privacy failure can cause lasting reputational damage that is far harder to repair than to prevent.

A well-conducted gap assessment functions as an early warning system. It identifies vulnerabilities before they attract regulatory scrutiny and enables organisations to demonstrate accountability through timely remediation.

PRACTICAL INSIGHTS

Personal Data is Broader than Organisations realise

The first challenge is often the most fundamental: identifying what constitutes PD.

[1] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf , accessed on May 03, 2026

FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400072
T. +91 98338 62234 E. rashmi@fountainheadlegal.com
www.FountainheadLegal.com

The DPDP Act defines 'data' under Section 2(h)[2] as a "representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means." Whereas, 'Personal data' under Section 2(t)[3] means "any data about an individual who is identifiable by or in relation to such data." Read together, these provisions have a consequence that organizations routinely underestimate: PD is not confined to conventional identifiers such as names or financial account numbers. Because 'data' expressly includes opinions and facts, any such representation, when linked to an identifiable individual, constitutes PD.

Correct identification is the threshold question on which the entire gap assessment rests. Under Section 8(5)[4] of the DPDP Act, data fiduciaries must implement reasonable security safeguards, a standard that cannot be calibrated for data that has not been identified. The point sharpens in breach proceedings. The DPDP Act does not formally categorize PD by sensitivity but when the Data Protection Board of India ("**Board**") determines penalties under Section 33 and the Schedule to the DPDP Act, it considers the type and nature of PD affected. An organization that has not correctly identified its PD cannot respond to a breach effectively, notify the Board accurately, or defend its compliance posture when scrutinized.

The blind spots are consistent across industries. Consider a market research organization for which the obvious identifiers include respondent names, or the banking details of sole-proprietor vendor that are typically captured. What is missed is that survey answers are opinions. As mentioned above, DPDP Act expressly includes opinions within the definition of 'data'. Where those answers can be linked back to an identifiable respondent, such answers may fall within the ambit of PD. For this reason, gap assessments should not assume a common understanding of PD across the organisation. Before collecting information through questionnaires or interviews, organisations should ensure that stakeholders have a practical understanding of what constitutes PD in the context of their specific functions.

Retention Policies Rarely Match Retention Practices

Most organizations have documented data retention schedules. Fewer adhere to them in practice. PD accumulates in archived email inboxes, backup tapes, decommissioned servers, and project folders that receive no attention once a matter concludes. During a gap assessment, it is common to discover that 'deletion' means different things to different teams such as logical deletion, anonymization, archival, or migration to cold storage, and only some methods may necessarily constitute erasure in the legal sense.

Section 8(7)[5] of the DPDP Act requires data fiduciaries to erase PD once the purpose for processing no longer exists, unless retention is required by law. Assessing compliance with this obligation requires more than reviewing policies, it demands validation of actual system-level practices.

A financial services organisation may have a documented policy requiring customer data to be deleted three years after a relationship ends. Yet archived mailboxes and legacy systems may continue storing that data for a decade. The policy says 3 years but the reality is indefinite. Organizations should test deletion practices through system walkthroughs and technical validation, not document reviews alone.

[2] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf , accessed on May 03, 2026
[3] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf , accessed on May 03, 2026
[4] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf , accessed on May 03, 2026
[5] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf , accessed on May 03, 2026

FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400072
T. +91 98338 62234 E. rashmi@fountainheadlegal.com
www.FountainheadLegal.com

Personal Data often moves Outside Formal Systems

One of the difficult parts of a gap assessment is identifying PD processed outside official systems. It may be shared through messaging applications or personal email accounts, saved on local drives, or maintained in standalone spreadsheets. These copies rarely appear in system inventories, retention schedules or documented workflows.

Such practices are rarely intended to bypass internal controls. They usually arise from operational convenience. Sales teams may download customer data from the CRM into Excel trackers. HR teams may store employee documents in local folders. Operations teams may maintain separate spreadsheets or messaging groups to track customer requests.

Once PD moves outside official systems, it may also fall outside access controls, retention periods, deletion processes and monitoring mechanisms. A gap assessment must therefore go beyond policies and questionnaires. It should include process walkthroughs and discussions with employees who handle PD regularly. The aim is to understand how work is actually performed, not simply how it is expected to be performed.

Vendor Documentation maybe Overlooked

This gap is particularly common in smaller organisations, where vendor engagements may be governed only by purchase orders, proposals, emails, Non-Disclosure Agreements or standard commercial agreements. These documents may cover the services and confidentiality but often do not address the personal data accessed, security safeguards, breach reporting, sub-processors, retention or deletion. A confidentiality clause alone may not be sufficient.

As Data Fiduciary remains responsible for processing undertaken on its behalf, vendors are a crucial part of a gap assessment. Organisations should identify vendors with access to personal data and review both their actual processing practices and contractual obligations. Organisations may begin by prioritising high-risk vendors, such as cloud, payroll, CRM, background-verification, marketing and payment service providers.

CONCLUSION

The challenges discussed above are not unique to any particular industry or organisation size. They arise wherever PD is collected and processed which, under the DPDP Act, encompasses a far wider range of activities than many organisations initially appreciate. Misidentifying PD, relying on retention policies that differ from actual practices, overlooking informal data repositories, and failing to account for business changes during the assessment process all point to the same underlying reality: organisations often have an incomplete understanding of how PD actually moves through their operations.

A Data Privacy Gap Assessment is therefore not merely a compliance exercise or a documentation project. Its value lies in challenging assumptions, validating whether documented processes reflect operational realities, and uncovering risks that may otherwise remain invisible. Organisations that approach the exercise with rigour, cross-functional collaboration, and continuous engagement will be better positioned not only to meet their obligations under the DPDP Act, but also to build a sustainable and accountable data governance framework.

FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400072
T. +91 98338 62234 E. rashmi@fountainheadlegal.com
www.FountainheadLegal.com