# The DPDP Compliance Clock: What Company Secretaries Need to Know and Do Now?

This Article is a practical walkthrough of India's Digital Personal Data Protection Act, 2023, and the DPDP Rules, 2025 — with a governance lens for Company Secretary Professionals.

**Narasimhan Elangovan**
Data Privacy professional
Bangalore, Karnataka
*narasimhan.e@incorpadvisory.in*

## INTRODUCTION

On 13 November 2025, the Ministry of Electronics and Information Technology published three gazette notifications in quick succession. The first brought several sections of the Digital Personal Data Protection Act, 2023 into force immediately. The second notified the Digital Personal Data Protection Rules, 2025. The third formally established the Data Protection Board of India, with its headquarters in the National Capital Region.

For Company Secretaries, this date matters more than it might first appear. The DPDP Act, 2023 is not a niche technology regulation. It cuts across board governance, compliance reporting, vendor contracts, employee data handling, and customer-facing operations. Every company that collects personal data in digital form — which, in 2026, is practically every company — falls within its scope.

The timeline is staggered. Some provisions took effect immediately in November 2025. Consent Manager registration provisions shall come into force by November 2026. The remaining bulk of the Act — covering notice, consent, data principal rights, security safeguards, breach notification, and Significant Data Fiduciary obligations — kicks in by May 2027, eighteen months from the date of notification.

That gives organisations roughly twelve months from the date of this publication to get their house in order. For the CS, this window is when the real work begins.

## THE DPDP FRAMEWORK: ACT AND RULES (HEREINAFTER THE ACT)

The DPDP Act, 2023 (No. 22 of 2023), received Presidential assent on 11 August 2023. It is a principles-based statute — deliberately concise, with much of the operational detail left to subordinate rules. The Act defines the key roles (Data Fiduciary, Data Processor, Data Principal, Significant Data Fiduciary, Consent Manager), sets out obligations, and establishes the enforcement mechanism through the Data Protection Board.

The DPDP Rules, 2025, notified on 13 November 2025, fill in those operational gaps. They prescribe the contents of a privacy notice, the form of breach intimation, the requirements for verifiable parental consent when processing children's data, the retention timelines for specific classes of Data Fiduciaries, and the additional obligations of Significant Data Fiduciaries including periodic Data Protection Impact Assessments and audits.

One cannot read the Act without the Rules, and the Rules make little sense without the Act. For compliance planning, both must be read as one consolidated framework.

## APPLICABILITY

Section 3 of the Act makes the applicability broad. The Act applies to any processing of digital personal data within India, whether the data was collected digitally or was collected in non-digital form and later digitised. It also reaches processing outside India if it relates to offering goods or services to individuals in India.

The only carve-outs are narrow: personal data processed by an individual for personal or domestic purposes, and personal data that the Data Principal (or someone under a legal obligation) has made publicly available.

For Company Secretary professionals advising listed companies, unlisted public companies, or private companies of any size, the question is not whether the Act applies. It does. The question is what needs to change in your current governance and compliance setup to meet these obligations.

## GOVERNANCE OBLIGATIONS THAT REACH THE BOARD

The Act places obligations squarely on the Data Fiduciary — defined under Section 2(i) as any person who alone or in conjunction with others determines the purpose and means of processing personal data. The company acts

through its board and officers, and these obligations become board-level governance matters.

Here are the specific obligations that a Company Secretary should track:

## ACCOUNTABILITY REGARDLESS OF OUTSOURCING

Section 8(1) clear that the Data Fiduciary is responsible for complying with the Act and Rules in respect of any processing done by it or on its behalf by a Data Processor, irrespective of any agreement to the contrary. Accountability cannot be outsourced. If your vendor mishandles personal data, the liability sits with you as the Data Fiduciary. This has direct implications for vendor due diligence, contract terms, and board-level risk oversight.

## SECURITY SAFEGUARDS ARE NOW A LEGAL MINIMUM

Section 8(5) requires the Data Fiduciary to take reasonable security safeguards to prevent personal data breach. Rule 6 expands this with specific technical requirements: encryption, obfuscation, masking or virtual tokens for securing personal data; access controls on computer resources; monitoring logs for detecting unauthorised access; data backups for business continuity; and a one-year minimum retention of logs. Rule 6 also mandates that contracts with Data Processors include appropriate security safeguard provisions.

> The DPDP Act is not a technology law dressed in legal language. It is a governance statute. It asks organisations to be accountable for the personal data they collect, to be transparent about why they collect it, and to give individuals meaningful control over their own information.

For the Company Secretary, this means the company's information security posture is no longer just an IT matter. It is a compliance obligation with statutory backing and penalty exposure of up to two hundred and fifty crore rupees under the Schedule to the Act.

## BREACH NOTIFICATION WITHIN SEVENTY-TWO HOURS

Section 8(6) requires the Data Fiduciary to intimate the Board and each affected Data Principal in the event of a personal data breach. Rule 7 adds teeth to this: the Data Fiduciary must notify each affected Data Principal without delay, describing the breach, its consequences, the mitigation measures taken, and the safety measures the individual can take. The intimation to the Board must include an initial description without delay, followed by a detailed report within seventy-two hours covering the events leading to the breach, findings regarding the person who caused it, remedial measures, and a report on intimations given to affected Data Principals.

This is a tight timeline. Organisations that lack an incident response playbook, a pre-drafted notification template, and a tested escalation chain will struggle when an incident occurs. The CS should ensure these are in place, tested through tabletop exercises, and reviewed by the board or a designated committee at least annually.

## NOTICE AND CONSENT ARE SUBSTANTIVE, NOT CEREMONIAL

Section 5 and Rule 3 together define what a proper privacy notice looks like under the DPDP framework. The notice must be presented independently — not buried in a terms-of-service document. It must give, in clear and plain language, an itemised description of the personal data being collected and the specific purpose for which it will be processed. It must also provide the communication link for withdrawing consent, exercising rights, and making a complaint to the Board.

Section 6(1) defines consent as free, specific, informed, unconditional, and unambiguous, with a clear affirmative action. Any consent obtained through bundling, dark patterns, or pre-ticked boxes will not meet this standard. Section 6(3) requires that consent requests be presented in English or any language listed in the Eighth Schedule to the Constitution. Section 6(10) places the burden of proof on the Data Fiduciary: if a question arises in proceedings, the Data Fiduciary must prove that proper notice was given and valid consent was obtained.

For organisations that have been collecting consent through generic privacy policies or blanket terms, this is a significant recalibration. The CS should work with legal and IT teams to audit existing consent mechanisms and redesign them where they fall short.

## CHILDREN'S DATA: VERIFIABLE PARENTAL CONSENT

Section 9 imposes additional safeguards for processing personal data of children (defined as individuals below eighteen years) and persons with disability who have a lawful guardian. The Data Fiduciary must obtain verifiable consent from the parent or lawful guardian before processing. Section 9(2) prohibits processing that is likely to cause any detrimental effect on the well-being of a child. Section 9(3) bans tracking, behavioural monitoring, and targeted advertising directed at children.

Rule 10 specifies how verifiable parental consent works: the Data Fiduciary must adopt appropriate technical and organisational measures and exercise due diligence to confirm that the person identifying herself as the parent is an identifiable adult — either through reliable identity and age details already held by the Data Fiduciary, or through details voluntarily provided by the individual or through a virtual token issued by an authorised entity.

Rule 12 and the Fourth Schedule list specific exemptions — for instance, healthcare establishments processing a child's data for health services, educational institutions for educational activities and child safety, and certain purposes like creating email accounts or determining a child's real-time location for safety. But these exemptions are narrow and conditional.

Companies operating in edtech, gaming, social media, or any consumer-facing digital service should map their data flows against these requirements immediately.

## DATA PRINCIPAL RIGHTS AND THE NINETY-DAY RESPONSE WINDOW

The Act grants Data Principals four rights: the right to access information about their personal data and its processing (Section 11); the right to correction, completion, updating, and erasure (Section 12); the right to grievance redressal (Section 13); and the right to nominate another individual to exercise these rights in case of death or incapacity (Section 14).

Rule 14(1) requires the Data Fiduciary and Consent Manager to prominently publish on their website or app the means through which a Data Principal can exercise these rights. Rule 14(3) sets the grievance response timeline at a reasonable period not exceeding ninety days, and requires appropriate technical and organisational measures to ensure the system works within that period.

Ninety days may sound generous, but in practice, if an organisation receives a correction or erasure request and the data sits across multiple systems, processors, and backups, fulfilling it within ninety days takes planning and tested workflows. The Company Secretary should ensure that a documented Standard Operating Procedure exists for handling these requests.

## RETENTION, DELETION AND THE ONE-YEAR LOG RETENTION RULE

Section 8(7) requires the Data Fiduciary to erase personal data when the Data Principal withdraws consent or when the specified purpose is no longer being served, whichever is earlier — unless retention is needed for compliance with another law. Section 8(8) deems the purpose as no longer served if the Data Principal neither approaches the Data Fiduciary nor exercises her rights for a prescribed period.

Rule 8 and the Third Schedule specify these periods for certain large Data Fiduciaries: e-commerce entities with at least two crore registered users, online gaming intermediaries with at least fifty lakh users, and social media intermediaries with at least two crore users must erase personal data of three years after the Data Principal last approached them, unless the data is needed for enabling access to the user account or stored virtual tokens.

Rule 8(3) introduces a separate obligation: Every Data Fiduciary must retain personal data, associated traffic data, and processing logs for a minimum of one year from the date of processing, for purposes specified in the Seventh Schedule (which covers State use for sovereignty, security, and law enforcement functions). After that one-year minimum, the data must be erased unless another law requires longer retention.

This creates a balancing act. You cannot delete too soon (the one-year floor applies), and you cannot retain too long (the purpose-based ceiling applies). Getting this right requires a retention schedule that maps each category of personal data to its lawful purpose, the applicable retention floor, and the trigger for deletion.

## IF YOU ARE (OR MAY BECOME) A SIGNIFICANT DATA FIDUCIARY

Section 10 empowers the Central Government to notify any Data Fiduciary or class of Data Fiduciaries as a Significant Data Fiduciary based on factors such as volume and sensitivity of data processed, risk to Data Principals' rights, and impact on sovereignty, electoral democracy, security, and public order.

Once notified, the obligations escalate. Section 10(2) requires the Significant Data Fiduciary to appoint a Data Protection Officer who is based in India, is responsible to the board of directors or equivalent governing body, and is the point of contact for grievance redressal. The Significant Data Fiduciary must also appoint an independent data auditor and undertake periodic Data Protection Impact Assessments and audits.

Rule 13 adds specifics: The DPIA and audit must happen at least once every twelve months, and the person conducting them must furnish a report of significant observations to the Board. Rule 13(3) requires the Significant Data Fiduciary to verify that its algorithmic software and technical measures are not likely to pose a risk to Data Principals' rights. Rule 13(4) requires measures to ensure that personal data specified by the Central Government is not transferred outside India.

Even if your organisation is not yet notified as a Significant Data Fiduciary, it is worth building toward these standards. The notification criteria are broad, and the Central Government retains discretion. Being prepared beats scrambling after a notification.

## CROSS-BORDER DATA TRANSFER

Section 16 allows the Central Government to restrict transfer of personal data to specific countries or territories by notification. Rule 15 clarifies that personal data may be transferred outside India subject to requirements the Central Government may specify regarding making such data available to any foreign State or any person or entity under the control of or any agency of such a State.

As of the date of writing, no country-specific restriction notifications have been issued. But organisations with global operations or offshore data processing arrangements should build contractual safeguards and monitor government notifications closely. The CS should ensure that data transfer clauses in vendor contracts are reviewed and updated to reflect this evolving position.

## CONSENT MANAGER: A NEW INTERMEDIARY

Section 6(7) allows the Data Principal to give, manage, review, or withdraw consent through a Consent Manager. Rule 4 and the First Schedule set out the registration conditions and obligations. A Consent Manager must be a company incorporated in India with a minimum net worth of two crore rupees, must operate an interoperable platform, must maintain consent records for at least seven years, and must avoid conflicts of interest with Data Fiduciaries.

For the Company Secretary, this is relevant in two ways. First, if your organisation is considering registration as a Consent Manager, the compliance burden is substantial — including periodic audits reported to the Board, conflict-of-interest controls, and restrictions on transfer of control without Board approval. Second, if your organisation will use a registered Consent Manager, you need to assess whether that manager meets the conditions in the First Schedule before onboarding them.

## PENALTIES

The Schedule to the Act prescribes penalties that are significant by any measure. Failure to take reasonable security safeguards: up to two hundred and fifty crore rupees. Failure to notify the Board or affected Data Principals of a breach: up to two hundred crore rupees. Breach of children's data obligations: up to two hundred crore rupees. Breach of Significant Data Fiduciary obligations: up to one hundred and fifty crore rupees. Breach of any other provision: up to fifty crore rupees.

Section 33(2) lists the factors the Board will consider while determining penalty amounts: the nature, gravity, and duration of the breach; the type of personal data affected; whether the breach was repetitive; whether the Data Fiduciary gained or avoided loss from the breach; the mitigating actions taken and their timeliness; proportionality; and the likely impact of the penalty on the person.

These are not academic numbers. They are designed to get Board attention. The Company Secretary should ensure that the board or audit committee is briefed on the penalty framework, the company's current compliance gaps, and the remediation roadmap.

## CHECKLIST FOR COMPANY SECRETARIES

Here is a practical checklist — not exhaustive, but a reasonable starting point:

1. **Map your data:** Identify what personal data the company collects, where it is stored, who processes it, for what purpose, and for how long. This is essential inventory to comply with Act.
2. **Audit your notices and consent mechanisms:** Compare them against Section 5, Section 6, and Rule 3. Are notices itemised and specific? Is consent free, informed, and unambiguous? Is it available in regional languages? Fix what falls short.
3. **Review vendor contracts:** Ensure every Data Processor engagement is backed by a valid contract with security safeguard provisions as required under Section 8(2) and Rule 6(1)(f). Add breach notification obligations and audit rights.
4. **Build a breach response playbook:** Pre-draft notifications for the Board and Data Principals. Define escalation chains. Run a tabletop drill. Document everything.
5. **Establish a grievance redressal mechanism:** Publish contact details of the Data Protection Officer (if applicable) or a designated person on the company's website and app. Set up workflows to handle and respond to requests within ninety days, as required under Rule 14(3).
6. **Prepare a retention schedule:** Map each category of personal data to its lawful purpose and applicable retention period. Build automated deletion triggers where possible. Remember the one-year log retention floor under Rule 8(3).
7. **Brief the Board:** Present the DPDP compliance status, the gap analysis, the remediation plan, and the penalty exposure. Ensure this is a standing agenda item for the audit committee or risk committee.
8. **Check children's data processing:** If the company operates any consumer-facing digital service — apps, websites, platforms — assess whether children's personal data is being collected and whether the verifiable consent requirements under Section 9 and Rule 10 are met.
9. **Monitor Significant Data Fiduciary notifications:** If the company processes large volumes of personal data or operates in a sensitive sector, anticipate the possibility of being notified as a Significant Data Fiduciary and start building toward DPO appointment, DPIA, and audit readiness.
10. **Train your people:** Compliance policies are only as good as the people who follow them. Conduct role-specific training — different content for the IT team, HR, marketing, customer support, and the legal function.

## CONCLUSION

The DPDP Act, 2023 is not a technology law dressed in legal language. It is a governance statute. It asks organisations to be accountable for the personal data they collect, to be transparent about why they collect it, and to give individuals meaningful control over their own information. For the Company Secretary, these are familiar themes — accountability, transparency, and stakeholder protection are what the profession has always been about.

The compliance deadline of May 2027 feels distant, but the ground to cover is considerable. Data mapping, consent redesign, vendor contract overhaul, breach readiness, retention engineering, and board-level reporting — none of these happen overnight. The organisations that start now will have a working compliance programme by the time enforcement begins. Those that wait will find themselves retrofitting under pressure.

The CS professionals are well positioned to lead this effort. They understand governance frameworks, regulatory compliance cycles, and the language of board reporting. The DPDP framework is one more layer — but a layer that touches every function, every system, and every customer relationship the company has. The earlier, the Company Secretary engage, the better the outcome for the organisation and its stakeholders.

## REFERENCES:

i. *Gazette Notification G.S.R. 843(E), dated 13 November 2025 (Commencement dates for various provisions of the Act).*

ii. *Gazette Notification G.S.R. 844(E), dated 13 November 2025 (Establishment of the Data Protection Board of India).*

iii. *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), dated 11 August 2023.*

iv. *The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated 13 November 2025.*