ARTICLE

DPDP Rules 2025 and the Company Secretary as Data Governance Officer: Navigating India's New Data Protection Landscape

The Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, mark the operationalisation of India's landmark DPDP Act, 2023 transforming high-level privacy principles into concrete, enforceable obligations for every organisation that processes personal data of individuals in India. With penalties reaching ₹250 crore per violation and a compliance deadline of 13 May 2027, this new framework has profound implications for corporate governance and the role of the Company Secretary. This article, authored from the perspective of a Practising Company Secretary at a technology-focused legal practice, critically examines the DPDP Rules through the lens of corporate compliance, board accountability, and the CS's unique position at the intersection of governance, law, and regulatory disclosure. It argues that the Company Secretary is and must position itself as the primary architect of DPDP compliance governance within the Indian corporate boardroom, bridging the gap between legal obligation, technology infrastructure, and stakeholder accountability.

CS Sahiba Khan, ACS
Associate — Secretarial and Corporate Law
Fullstack Lawyer LLP, Delhi
khansahiba470@gmail.com

INTRODUCTION

Privacy, for most of the history of Indian corporate law, was a peripheral concern — a matter for technology teams, not boardrooms. That era has decisively ended. On 13 November 2025, the Ministry of Electronics and Information Technology (MeitY) notified the Digital Personal Data Protection Rules, 2025 (DPDP Rules), operationalising the Digital Personal Data Protection Act, 2023 (DPDP Act) — India's most comprehensive data protection legislation since the enactment of the Information Technology Act, 2000. The full compliance deadline is 13 May 2027, and the Data Protection Board of India (DPBI) is already operational.

For Company Secretaries, this development is not merely a new compliance checklist. It represents a structural expansion of the governance function. The DPDP framework — with its consent architecture, breach notification obligations, board-level accountability requirements, and penalty regime that can reach ₹250 crore per violation — places data protection squarely within the domain of corporate governance. And corporate governance is, by training, profession, and statute, the domain of the Company Secretary.

This article provides a comprehensive analysis of the DPDP Rules, 2025 from a CS practitioner's perspective. It examines the key obligations imposed on companies as Data Fiduciaries, the enhanced duties of Significant Data Fiduciaries (SDFs), the penalty framework, the interface between DPDP and existing corporate law obligations, and the practical steps that CS professionals must take to ensure their organisations achieve timely compliance. It also addresses the specific challenges faced by technology companies and startups — entities at the frontier of the data economy — where the intersection of digital business models and data governance is most acute.

₹250 Cr *Maximum penalty per violation under the DPDP Act, 2023 — for failure to implement reasonable security safeguards. The Data Protection Board of India (DPBI) is already operational.*

THE DPDP FRAMEWORK: ARCHITECTURE AND KEY CONCEPTS

1. The Act and the Rules: A Two-Tier Framework

The DPDP Act, 2023 establishes the foundational principles: the rights of Data Principals (individuals whose data is processed), the obligations of Data Fiduciaries (organisations that determine the purpose and means of processing), the constitution of the Data Protection Board of India (DPBI) as the regulatory and adjudicatory authority, and the penalty framework. The Act is deliberately principle-based — it establishes what must be achieved without prescribing in exhaustive detail how to achieve it.

The DPDP Rules, 2025 provide the operational precision that the Act left to subordinate legislation. They specify: the form and content of consent notices; the mechanics of data erasure and the right to be forgotten; the registration and obligations of Consent Managers; the breach notification procedure and timelines; the enhanced obligations of Significant Data Fiduciaries; and the procedures for cross-border data transfers. For compliance professionals, the Rules are where the rubber meets the road.

2. Who is a Data Fiduciary? Applicability to Indian Companies

Every company incorporated under the Companies Act, 2013 that processes digital personal data of individuals in India — whether as an employer processing employee data, a consumer-facing business processing customer data, or a B2B service provider processing vendor data — is a Data Fiduciary under the DPDP Act. The obligations imposed on Data Fiduciaries are comprehensive: lawful processing on the basis of consent or legitimate use, purpose limitation, data minimisation, accuracy maintenance, storage limitation, security safeguards, and accountability.

The Act also creates a sub-category of Significant Data Fiduciaries (SDFs) — entities designated by the Central Government on the basis of the volume and sensitivity of data processed, the risk to the rights of Data Principals, and national security considerations. SDFs are subject to enhanced obligations, including mandatory appointment of a Data Protection Officer (DPO), periodic Data Protection Impact Assessments (DPIAs), and annual audits by independent data auditors.

Every company that processes digital personal data of individuals in India is a Data Fiduciary under the DPDP Act — and every Data Fiduciary needs a Company Secretary who understands what that means.

KEY OBLIGATIONS UNDER DPDP RULES, 2025: A GOVERNANCE MAP

The following table maps the principal obligations under the DPDP Rules, 2025 against the corresponding governance role of the Company Secretary, providing a structured reference for CS practitioners designing their organisation's DPDP compliance programme.

Table 1: DPDP Rules 2025 — Key Obligations and the Role of the Company Secretary

Stakeholder	Key Obligation under DPDP Rules, 2025	Role of Company Secretary
Data Fiduciary (All Companies)	Obtain free, specific, informed consent before processing personal data; issue plain-language notice in all 22 scheduled languages	Draft consent frameworks; advise board on data governance policy; review vendor contracts for DPDP clauses
Significant Data Fiduciary (SDF)	Appoint Data Protection Officer (DPO); conduct periodic Data Protection Impact Assessments (DPIAs); mandatory annual audits by independent auditors	Facilitate DPO appointment; co-ordinate DPIA disclosures; ensure board oversight of audit outcomes
All Entities	Report personal data breaches to Data Protection Board of India (DPBI) within prescribed timelines; notify affected data principals	Maintain breach register; draft board-level breach response protocols; file regulatory notifications
Companies with Child Data	Verifiable parental consent before processing data of minors; prohibition on tracking/ behavioural monitoring of children	Review product/service data flows; advise on age-gating mechanisms and consent verification systems
Cross-Border Transfers	Transfer personal data only to countries notified by Central Government; maintain transfer impact records	Monitor approved country list; update data processing agreements; advise on cross-border M&A due diligence

Source: *DPDP Act, 2023; DPDP Rules, 2025 (notified 13 November 2025). Author's analysis.*

1. Consent Architecture: The Governance Dimension

The DPDP Rules require that consent be obtained through a clear, standalone notice — separate from other terms and conditions — that itemises the personal data to be processed, the purpose of processing, and the manner in which Data Principals can withdraw consent. For companies operating consumer-facing digital platforms, this requires a fundamental redesign of existing consent mechanisms, privacy policies, and terms of service.

From a governance perspective, the consent architecture is not merely a technology problem — it is a board accountability issue. The DPDP framework makes the company (as Data Fiduciary) responsible for the accuracy and completeness of consent notices. This means the board must approve the organisation's consent framework and ensure it is reviewed periodically. The Company Secretary, as the primary advisor to the board on compliance matters, is the natural owner of this governance process.

2. The Data Protection Officer: Appointment, Role, and Independence

For companies designated as Significant Data Fiduciaries, the appointment of a Data Protection Officer (DPO) is mandatory under Section 10(2) of the Digital Personal Data Protection Act (DPDPA), 2023. The DPO must be a person based in India and must report directly to the Board of Directors — not to the Chief Executive Officer or the Chief Technology Officer. This structural requirement — board-level reporting for the DPO — mirrors the independence requirements that apply to the Compliance Officer under SEBI's LODR Regulations and the Company Secretary under the Companies Act, 2013.

The parallel is instructive. Just as the Company Secretary derives the authority to advise the board independently of management, the DPO's effectiveness depends on their independence from operational management. In many organisations, particularly mid-sized companies that are not yet large enough to justify a standalone DPO, the Company Secretary's governance expertise makes his/her the most suitable candidate to either serve as DPO or to closely support the DPO function.

> India's digital economy is the fastest-growing in the world. The companies that will lead this economy are data companies. And the governance of those companies will increasingly be defined by how well they protect the personal data entrusted to them.

THE PENALTY FRAMEWORK: BOARD ACCOUNTABILITY AND PERSONAL LIABILITY

The DPDP Act's penalty framework is designed to ensure that data protection failures attract consequences commensurate with the risk they pose to individual rights and national interests. The penalty quantum — reaching ₹250 crore for the most serious violations — is not merely symbolic. It is calibrated to be significant even for large enterprises, and potentially existential for mid-sized and smaller companies.

Table 2: DPDP Penalty Framework — Compliance Stakes for Indian Companies

Violation	Maximum Penalty (₹ Crore)	Practical Implication for Governance
Failure to implement reasonable security safeguards (Section 8(5))	**₹250 Crore**	Board must approve and oversee a documented Information Security Policy aligned with DPDP standards
Failure to notify DPBI or Data Principals of a breach (Section 8(6))	**₹200 Crore**	CS must design and maintain a Board-approved breach notification SOP with defined escalation timelines
Non-compliance with special provisions for processing children's data (Section 9)	**₹200 Crore**	Review all products/services collecting user data; age-gate where necessary; obtain verifiable consent
Failure to fulfil additional Significant Data Fiduciary obligations (Section 10)	**₹150 Crore**	SDFs must appoint a DPO, conduct DPIAs, and submit to annual independent audits — CS to monitor compliance
Failure of Consent Manager to comply with DPDP Rules	**₹50 Crorex**	Applicable to platforms acting as Consent Managers — CS to review contracts and ensure DPDP compliance

Source: *Schedule to the DPDP Act, 2023. INR figures are per instance of non-compliance.*

1. Board-Level Accountability: The CS's Role in Risk Governance

The scale of potential penalties under the DPDP framework requires that data protection risk be treated as a material corporate risk — alongside credit risk, market risk, and operational risk — and be subject to the same board-level governance disciplines. This means: regular reporting of DPDP compliance status to the Board and Audit Committee; inclusion of DPDP risk in the company's risk register and Enterprise Risk Management (ERM) framework; and appropriate disclosure in the Board's Report under Section 134 of the Companies Act, 2013.

The Company Secretary is uniquely positioned to drive this integration. His/her existing mandate under the Companies Act includes responsibility for board-level compliance reporting, coordination of Audit Committee meetings, and oversight of the Annual Report. Extending this mandate to encompass DPDP compliance reporting requires no structural change — only a conceptual expansion of the CS's existing role.

2. Interface Between DPDP and Companies Act Obligations

The DPDP framework does not operate in isolation from existing corporate law obligations. Several important intersections must be navigated by the CS practitioner. First, the Board's Report under Section 134 of the Companies Act should, going forward, include a disclosure on the company's DPDP compliance posture — the status of consent frameworks, the outcomes of any DPDP audits, and any breach notifications made to the DPBI during the year. Second, the Secretarial Audit under Section 204 should be extended to cover DPDP compliance, given that the Secretarial Auditor is required to report on compliance with 'all applicable laws' — and the DPDP Act is unambiguously an applicable law for virtually every company.

Third, and perhaps most importantly, the DPDP framework has direct implications for the M&A due diligence process. A resolution applicant or acquirer who fails to identify and price the target company's DPDP compliance gaps — including outstanding consent deficiencies, unaddressed breach notifications, or pending DPBI investigations — may find themselves inheriting liabilities that were not reflected in the purchase price. CS professionals advising on M&A transactions must integrate DPDP due diligence into their standard checklist.

May 2027	*Deadline for full DPDP Rules compliance — including consent frameworks, breach notification SOPs, DPIA processes, and (for SDFs) DPO appointment and independent annual audits.*

SPECIAL CHALLENGES: TECHNOLOGY COMPANIES, STARTUPS & FINTECH

1. The Data-Rich Business Model and DPDP Exposure

For technology companies, consumer internet platforms, fintech firms, and SaaS businesses — entities whose entire value proposition is built on the collection and analysis of user data — the DPDP framework is not merely a compliance requirement. It is a fundamental

business model constraint. A fintech company that uses customer transaction data to offer personalised financial products must now ensure that its consent architecture is granular enough to support each specific use of data. A consumer platform that monetises user behaviour data through targeted advertising must ensure that its advertising partners are contractually bound to DPDP-compliant data processing standards.

The Company Secretary at a technology company must, therefore, develop a working understanding of the company's data architecture — the systems in which personal data is collected, stored, and processed — in order to provide meaningful governance advice. This does not require technical expertise in database management or software engineering. It requires the ability to ask the right questions: What data do we collect? Why do we collect it? Who has access to it? How long do we retain it? What is our legal basis for each processing activity?

2. Cross-Border Data Transfers and Global Business Operations

For companies with global operations — including foreign subsidiaries, offshore development centres, and cloud computing arrangements with foreign service providers — the DPDP Rules' cross-border transfer framework introduces a new compliance variable. Personal data of Indian individuals may be transferred to foreign jurisdictions only where the Central Government has specifically permitted such transfer. The list of approved countries has not yet been published in its final form; companies currently operating cross-border data flows must monitor MeitY's notifications closely.

The Company Secretary advising multinationals or companies with cross-border data flows must ensure that: all data processing agreements with foreign vendors are reviewed for DPDP compliance; the company maintains a current record of cross-border data transfers and the legal basis for each; and any changes to the approved country list are reflected promptly in the company's vendor management and data governance frameworks.

3. Startups and the DPDP Compliance Paradox

For early-stage startups — companies that are data-intensive by design but resource-constrained by necessity — the DPDP framework presents a genuine compliance paradox. The Act applies to all Data Fiduciaries irrespective of size or stage of development; there is no explicit startup exemption analogous to the small company concession under the Companies Act. Yet the cost of building a full DPDP compliance infrastructure — data mapping, consent management systems, DPO functions, DPIA frameworks — can be prohibitive for a company operating on a Series A runway.

The ICSI and the MCA have an opportunity here to develop simplified DPDP compliance templates specifically designed for startups recognised under the DPIIT framework. The Company Secretary community — many of whose members advise startup boards through the ICSI's startup advisory initiatives — can play a meaningful role in developing and disseminating these templates.

THE DPDP COMPLIANCE ROADMAP: A CS PRACTITIONER'S ACTION PLAN

Given the May 2027 compliance deadline, companies — and their Company Secretaries — cannot afford a 'wait and watch' approach. The following action checklist, organised by priority level, provides a structured starting point for DPDP compliance governance.

Table 3: CS-Led DPDP Compliance Action Checklist (2025–2027)

Priority	Action Item	Timeline	Owner
High	Conduct enterprise-wide Data Audit — map all personal data collected, stored, processed	Immediate (0–3 months)	CS + DPO + IT
High	Identify if company qualifies as Significant Data Fiduciary (SDF); initiate DPO appointment if applicable	0–3 months	CS + Legal
High	Review and redraft consent notices for all digital touchpoints in plain language (22 languages for SDFs)	0–6 months	CS + Marketing
Medium	Update all third-party vendor and processor contracts with DPDP-compliant data processing clauses	3–9 months	CS + Procurement
Medium	Design Breach Notification SOP; obtain board approval; test via tabletop exercise	3–9 months	CS + Board
Medium	Assess cross-border data transfer flows; ensure destinations are on MeitY-approved country list	3–9 months	CS + DPO
Ongoing	Include DPDP compliance status as standing agenda item in Board/Audit Committee meetings	Quarterly	CS
Ongoing	Conduct annual DPDP compliance audit (mandatory for SDFs); present findings to Board	Annual (from 2026)	CS + Auditor

Source: *Author's framework based on DPDP Rules, 2025. Priority levels are indicative; organisations should calibrate based on their specific risk profile.*

1. Data Audit: The Foundation of DPDP Compliance

The starting point for any DPDP compliance programme is a comprehensive data audit — a systematic mapping of every category of personal data the organisation collects, stores, processes, and shares, together with the legal basis for each processing activity, the retention period, and the third parties with whom the data is shared. This is not a one-time exercise; it must be maintained as a living document and updated whenever a new product, service, or system processing personal data is introduced.

The Company Secretary should lead the governance process for the data audit — commissioning it, reviewing the outcomes, presenting findings to the Audit Committee, and ensuring that remediation actions are tracked and reported. The actual technical execution will involve IT and legal teams, but the governance framework

for the audit — the terms of reference, the reporting structure, and the follow-up mechanism — is squarely within the CS's domain.

2. **Board Training and Awareness: The Governance Imperative**

   Board members in India are personally accountable for their company's regulatory compliance posture. The DPDP Act, while it does not impose personal criminal liability on individual directors for data breaches, creates institutional accountability at the board level through its requirement that the DPO report directly to the Board. This means the Board must be sufficiently informed about DPDP obligations to exercise meaningful oversight.

   The Company Secretary should arrange for a structured DPDP awareness session for the Board of Directors — covering the key obligations, the penalty framework, the company's current compliance status, and the remediation roadmap. This is a governance investment that also serves a protective function: a board that has been informed of DPDP obligations, and has received and approved a compliance plan, is in a far stronger position if the DPBI ever investigates the company's data practices.

UPSKILLING IMPERATIVES: THE COMPANY SECRETARY AS A DIGITAL GOVERNANCE LEADER

The DPDP framework is one dimension of a broader transformation in the governance landscape — a transformation driven by the digitalisation of business, the proliferation of data, and the growing regulatory expectation that boards and their advisors will be technically literate as well as legally competent. For Company Secretaries, this transformation is both a challenge and an opportunity.

The challenge is real: DPDP compliance requires CS professionals to develop a working familiarity with concepts — data mapping, consent management, DPIAs, security safeguards — that have not historically been part of the CS skill set. The opportunity is equally real: the CS who masters these concepts occupies a uniquely valuable position, able to translate technical data governance requirements into the language of board reporting, regulatory disclosure, and institutional accountability that the boardroom understands.

The ICSI's existing Continuing Professional Development (CPD) framework, supplemented by targeted courses on data governance and DPDP compliance, can provide the institutional infrastructure for this upskilling. CS professionals practising in technology-intensive sectors — fintech, healthtech, e-commerce, SaaS — should treat DPDP literacy as a priority professional development investment for 2025–26.

The Company Secretary who masters data governance is not adding a new function — He/she is extending the oldest function in his/her profession: the governance of risk, disclosure, and accountability at the heart of the Indian boardroom.

CONCLUSION

The DPDP Rules, 2025 are not a technical regulation for IT departments. They are a governance framework for the Indian boardroom. By imposing board-level accountability for data protection, requiring direct reporting lines from the DPO to the Board, and calibrating penalties at a scale that demands senior management attention, the DPDP framework has made data governance a core component of corporate governance — and corporate governance is the Company Secretary's calling.

The Company Secretary who understands the DPDP framework — who can conduct a data audit, design a consent governance framework, advise on DPO appointment, manage breach notification obligations, and integrate DPDP risk into the Board's Report — is not merely a compliance officer. CS is a strategic governance advisor, providing a service that no other professional in the Indian corporate ecosystem is as well-positioned to provide.

India's digital economy is the fastest-growing in the world. The companies that will lead this economy are data companies. And the governance of those companies — their accountability to their customers, their regulators, and their stakeholders — will increasingly be defined by how well they protect the personal data entrusted to them. The Company Secretary who is ready for this world — technically literate, governance-oriented, and proactively engaged with the DPDP framework — is not just keeping pace with the profession. CS is shaping its future.

REFERENCES:

i. *Companies (Amendment) Acts 2019, 2020 — Decriminalisation provisions, Ministry of Corporate Affairs, Government of India.*

ii. *Companies Act, 2013 (No. 18 of 2013) — Sections 134, 204, 2(85); Ministry of Corporate Affairs, Government of India.*

iii. *Digital Personal Data Protection (Amendment) Bill, 2025 (Consultation Draft), Ministry of Electronics and Information Technology — comparative analysis.*

iv. *Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Ministry of Electronics and Information Technology, Government of India.*

v. *Digital Personal Data Protection Rules, 2025, notified vide G.S.R. 846(E) dated 13 November 2025, Ministry of Electronics and Information Technology, Government of India.*

vi. *GDPR Regulation (EU) 2016/679 — Articles 5, 6, 37, 83; European Parliament and Council, 2016 (comparative reference).*

vii. *IBBI Quarterly Newsletter, October–December 2025, Insolvency and Bankruptcy Board of India, available at www.ibbi.gov.in.*

viii. *ICSI Guidance Note on Secretarial Audit under Section 204 of the Companies Act, 2013, Institute of Company Secretaries of India, 2023.*

ix. *Information Technology (Amendment) Act, 2008 and IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics and Information Technology.*

x. *PwC India Survey on Consumer Awareness of DPDP Law (2025 Edition), PricewaterhouseCoopers India.*

xi. *Report of the Justice B.N. Srikrishna Committee on Data Protection (A Free and Fair Digital Economy), Ministry of Electronics and Information Technology, 2018.*

xii. *SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 — Regulation 6 (Compliance Officer), Securities and Exchange Board of India.*

xiii. *World Justice Project Rule of Law Index 2025 — Digital Rights Indicator, World Justice Project.*