Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Data Protection Compliance under the Digital Personal Data Protection Act 2023: Challenges for Indian Startups

Shubham Balasaheb Aute[a]

[a]Symbiosis Law School, Pune, India

Received 23 March 2026; *Accepted* 24 April 2026; *Published* 28 April 2026

This article examines compliance challenges for Indian startups under the new Digital Personal Data Protection Act, 2023[1] (DPDP Act). We explain the Act's scope, key definitions (such as Data Fiduciary, Data Processor, Data Principal, 'digital personal data', and consent requirements) and special provisions for startups. We summarise compliance obligations; notably consent management, notice requirements, data minimisation, security safeguards, which also include breach notification, data localisation, record-keeping, grievance redressal, data-processor contracts, and the duties of Significant Data Fiduciaries (including Data Protection Officers, audits and data protection impact assessments). We outline enforcement (the new Data Protection Board, penalties up to ₹250 crore[2], appeals to the Telecom Disputes Settlement & Appellate Tribunal) and observe that voluntary undertakings and digital-first grievance mechanisms are included. Next, we analyse practical burdens for startups: the cost of compliance (including higher cloud/ storage needs), limited technical/legal capacity, product design trade-offs (granular consents vs user experience), investor expectations (due diligence for privacy), cross-border data-transfer restrictions, third-party vendor risks, handling legacy data, and risks of consent fatigue. We illustrate these points with hypothetical startup scenarios (e.g. an e-commerce marketplace, a fintech app, a children's edtech platform). To help startups, we propose a detailed 12-month compliance roadmap and checklists, emphasizing low - cost measures (template policies, open-source consent managers, encryption, basic audits, etc.). We include tables summarising obligations, timelines and indicative cost/effort estimates. Our analysis is grounded in official sources (the DPDP Act text, Government press releases, and

[1] Digital Personal Data Protection Act 2023

[2] Digital Personal Data Protection Act 2023, s 27

DPDP Rules, 2025) and expert commentary. We conclude that while DPDP compliance is demanding, a structured, staged approach can enable startups to protect user privacy, build trust, and avoid penalties.

Keywords: *compliance challenges, startups, DPDP Act, data protection.*

INTRODUCTION

India's Digital Personal Data Protection Act, 2023 (DPDP Act), was introduced in August 2023 and is being brought into force in phases. It replaces earlier rules under the Information Technology Act 2000 and creates a comprehensive legal framework for personal data. The Act's goals are to protect individuals' personal data rights while permitting lawful data processing for innovation. The DPDP Act emphasises consent, purpose limitation, data minimisation, storage limitation, security safeguards, accuracy and accountability[3]. Key features include enforceable rights (access, correction, erasure, nomination), new obligations for data controllers (Data Fiduciaries) and processors, a new Data Protection Board of India (DPB) to enforce the law, and hefty penalties for non-compliance. Compared to previous drafts and GDPR, the DPDP Act focuses on a 'SARAL' (simple, actionable) approach, but still imposes wide requirements on all entities processing digital personal data.

For Indian startups – defined generally as small tech-driven companies – DPDP compliance can be especially challenging. Startups often lack the legal, financial and technical resources of large firms, yet many handle sensitive user data to build products. They face obligations from day one if they collect or process any personal data of Indian residents (even if physically outside India). This article explores the legal framework of the DPDP Act with a focus on startups. We first outline the Act's scope and definitions (Data Fiduciary, Data Processor, Data Principal, etc.) and how these apply to new ventures. We then detail core compliance obligations – from consent notices and data protection principles to breach reporting and grievance redress. The enforcement regime (Data Protection Board, penalties, appeals to TDSAT) is reviewed. Next, we analyse practical challenges faced by startups in meeting these rules, such as costs (e.g. audit fees, increased cloud storage), technical capacity

[3] 'Salient Features of the Digital Personal Data Protection Bill, 2023' (*Press Information Bureau,* 09 August 2023) <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264&reg=3&lang=2> accessed 19 March 2026

(secure architecture, consent management), product design trade-offs (granular consents vs friction), investor expectations, cross-border data flows, and legacy data issues.

LEGAL FRAMEWORK AND SCOPE

The DPDP Act is India's first cross-sectoral data protection law, enacted on 11 August 2023. It applies broadly to the 'processing of digital personal data' in India. Specifically, Section 3 provides that the Act applies to: (a) processing of digital personal data within India where such data is collected in digital form or digitised; and (b) processing outside India if it is connected with offering goods or services to individuals in India[4]. Thus, even foreign startups targeting Indian users or markets fall under its jurisdiction. The Act clarifies that it does not apply to (i) personal data processed by an individual for purely personal or domestic purposes; or (ii) personal data already public (made public by the individual or by someone legally obliged to publish it). There are also exemptions for state agencies in certain areas (e.g. national security, public order), and the government may notify of other exemptions.

The Act is guided by core principles. The Press Information Bureau summary highlights seven core principles: consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards and accountability. These mirror global privacy norms. In practice, this means Data Fiduciaries must collect data only for specified lawful purposes, minimise unnecessary data collection, keep data accurate and as short-lived as possible, and protect it with appropriate technical/organisational measures. Consent and notice are central: startups must give clear, standalone notices explaining the specific purpose of data collection and obtain the user's free, specific, informed consent. This approach has been described as a 'stringent consent-based regime'. Unlike GDPR (which has multiple lawful bases), DPDP requires consent for most processing, meaning startups must design their products around explicit user permissions.

The Act allows phased implementation. The Data Protection Rules 2025 formalise a staged rollout. For example, the Data Protection Board was constituted first (effective 13 Nov 2025), and major compliance obligations take effect by the end of May 2027. This 18-month timeline (from November 2025 to May 2027) gives organisations time to adjust. Specifically, the Board and its platform were set up in Nov 2025. By Nov 2026 (12 months), the regime for registering

[4] Digital Personal Data Protection 2023, s 3

'Consent Managers' was to be in place. By May 13, 2027 (18 months), all general obligations take full effect (notice requirements, security, breach notification, Significant Data Fiduciary obligations, and rights of data principals). In practice, startups should begin compliance planning immediately, even during the grace period, to avoid last-minute scrambling.

KEY DEFINITIONS AND APPLICABILITY OF STARTUPS

The DPDP Act defines key terms in Section 2(1)(i), a Data Fiduciary is 'any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data'[5]. In common language, this is the entity (company) deciding why and how data is processed (e.g. to provide a service). A Data Processor is 'any person who processes personal data on behalf of a Data Fiduciary'; typically, this means vendors or subcontractors (cloud providers, analytics firms, etc.) who handle data per the fiduciary's instructions. The Data Principal is the individual to whom the personal data relates (with special rules if the principal is a child or a legally incapacitated person). The Act covers only 'digital personal data,' meaning 'personal data in digital form', and 'personal data' is any data about an identifiable individual. Unlike earlier Bills, the DPDP Act does not create 'special categories' like 'sensitive personal data' – it applies uniformly to all personal data (with some extra rules for children).

For startups, these definitions mean that virtually any company that collects or processes user data will be a Data Fiduciary (or uses one). Even small firms are within scope. Importantly, the Act is extraterritorial: an Indian startup's foreign affiliates or SaaS providers processing data outside India must comply if the processing relates to Indian users. Conversely, a U.S. or European startup serving Indian customers is equally bound. There are no de minimis exemptions based on company size. The Carnegie Endowment analysis notes that, unlike some laws, DPDP 'applies regardless of organisation size'. However, the government may grant limited exemptions for startups. Section 17(3)[6] of the Act authorises the government to notify certain classes of Data Fiduciaries (including startups) to exempt them from specific obligations in sections 5, 8(3,7), 10 and 11[7]. These relate to notice, accuracy/consistency, and some rights obligations. The intent is presumably to give nascent firms breathing room. In practice, no startup-specific notification has yet been issued.

[5] Digital Personal Data Protection Act 2023, s 2(1)(i)
[6] Digital Personal Data Protection Act 2023, s 17(3)
[7] Digital Personal Data Protection Act 2023, ss 5, 8, 10 and 11

Startups should not assume any blanket exemption – they should plan to comply with core duties from the outset.

The Act also defines a Significant Data Fiduciary (SDF) (Section 2(1)(z)) as any Data Fiduciary or class thereof that the Central Government notifies under Section 10. In practice, 'Significant' will mean data-heavy or sensitive businesses (e.g. large social media, fintech, telecom, health data platforms) with high volumes or sensitive categories. Identifying SDF status will largely be in the Rules or notifications. Startups unlikely to be SDF at first, but fast-growing firms should monitor announcements. SDFs have extra obligations (see below).

Section 3 of the Act lists exclusions. The Act does not apply to data processing for personal or household use, or to data already public. It also excludes certain government uses (security, law enforcement). Notably, there are no sector-specific carve-outs for most commercial industries. All online services and digital businesses must comply once they process Indian individuals' data. Even if a startup merely uses analytics or cloud storage, it falls under the rules (as either a fiduciary or at least a processor).

COMPLIANCE OBLIGATIONS

Once in scope, a startup (as a Data Fiduciary, and possibly as a Data Processor) faces multiple obligations under the DPDP Act and its Rules. These can be grouped as follows:

Consent and Notice (Sections 5–6): Consent is the primary legal basis for processing under DPDP. A fiduciary must not process personal data without consent, except as allowed by law. Consent must be 'free, specific, informed, unconditional and unambiguous, with a clear affirmative action'[8]. Practically, this means consent requests must use plain, simple language (including major Indian languages) and detail exactly what data will be used and for what purpose. Startups must provide standalone consent notices preceding data collection, explaining the data elements and purposes clearly (e.g. 'email address for order updates' or 'contact list for friend suggestions'). Bundled or vague consents are invalid. Consent forms cannot waive rights; any clause attempting to waive the user's rights (e.g. the right to complaint) is void. Once given, consent can be withdrawn at any time by the user. If a user withdraws consent, the fiduciary must stop processing their data 'within a reasonable time' and erase it (unless legally required to retain).

[8] Digital Personal Data Protection Act 2023, ss 5 and 6

Purpose Limitation, and Data Minimisation (Sections 4–6): The data collected must be limited to the specified purpose, and only necessary data elements must be used. The fiduciary must not ask for or process extra data beyond such personal data as is necessary for the specified purpose. For example, if a startup's service only needs name and email, asking for social media data or biometric data would violate minimisation. The published DPDP principles explicitly include purpose limitation and data minimisation[9].

Notice of Processing (Section 5): Before seeking consent, the fiduciary must give the Data Principal a notice detailing the data to be processed and the purpose. If consent was given before DPDP's commencement, the fiduciary must retrospectively provide notice[10]. In practice, this means privacy policies or consent screens must enumerate data categories (e.g. 'your profile photo', 'device location'), how they will be used, and how to complain to the DPB. Startups should ensure their privacy notices align with Section 5's requirements and are easily accessible.

Accuracy and Security (Sections 8 and Rules): Data Fiduciaries must implement 'appropriate technical and organisational measures' to protect personal data. This includes encryption, access controls, logging, monitoring, backups, and other safeguards. For any processing by a Data Processor, the Data Fiduciary remains fully responsible; all vendor contracts must include clauses mandating 'all reasonable security safeguards'[11]. In a breach, the fiduciary must notify the DPB and affected individuals 'promptly' (the Board has prescribed a 72-hour timeline). Unlike some laws, DPDP has no de minimis threshold for breach reporting; any breach must be reported. The press release emphasises notifying in 'plain language' and assisting victims.

Records and Data Management: While the Act does not explicitly require a central data inventory, good practice under DPDP involves maintaining records of processing and consents. Each Data Fiduciary should log what data was collected, when and how consent was obtained (with timestamps), where data is stored, and with which processors it was shared. These records help fulfil the DPB's potential inquiries and demonstrate compliance. Section 8(2) mandates that any Data Processor relationship be under a written contract, so

[9] Digital Personal Data Protection Act 2023, ss 4, 5, 6, 7 and 8
[10] Digital Personal Data Protection Act 2023, s 5
[11] Digital Personal Data Protection Act 2023, s 8

startups must review and update vendor agreements to include DPDP clauses (security commitments, audit rights, etc.).

Data Principal Rights (Sections 11–14): The Act grants several rights to individuals. Primarily, a Data Principal can request from any fiduciary 'to whom she has given consent' a summary of her personal data being processed and the processing activities. She also has the right to correction or erasure of inaccurate or excessive data[12]. The fiduciary must comply 'within such period as may be prescribed' (DPDP Rules specify a 30-day timeline) and at no cost. In practice, startups must design user interfaces or support processes to allow users to access or delete their data easily. Section 13 requires a readily accessible grievance redressal mechanism: every fiduciary must designate a contact (often called a Data Protection Officer or other point-person) and respond to user complaints within a prescribed time. The Rules set specific timelines (e.g. 30 days, 90 days for SDFs). Startups should include a 'Contact Us' or 'Privacy' link on their website/app describing how users can complain or query about their data. The user must exhaust this mechanism before approaching the DPB. Sections 14 and 15 also allow users to nominate another person in case of death/incapacity and impose duties on data principals (to provide true data, not mislead).

Significant Data Fiduciary Obligations (Section 10): If notified as an SDF, a startup must comply with extra measures. These include appointing a Data Protection Officer (DPO) based in India, who answers to the board or executives and is the contact for the DPB. The SDF must also appoint an independent auditor to conduct regular compliance audits[13]. Crucially, SDFs must carry out periodic Data Protection Impact Assessments (DPIA) for processing that poses a high risk to individual rights. DPIAs involve mapping the data flow, identifying risks, and detailing mitigations. For example, a fintech startup using AI to score loans may need a DPIA on its credit scoring algorithms. The SDF provisions also allow the government to impose additional safeguards (e.g. enhanced due diligence) as prescribed by rules. Most startups will not immediately be classified as SDFs, but fast-growing or data-intensive ones should anticipate these tasks.

Data Localisation and Cross-border Transfers (Section 16): The Act empowers the Central Government to notify which countries/territories can receive personal data from India. Until

[12] Digital Personal Data Protection Act 2023, ss 11-14
[13] Digital Personal Data Protection Act 2023, s 10

rules are specified, all cross-border transfers may face restrictions. The PI¬B press release indicates that some categories of data (e.g. government-mandated) may require localisation. Startups with international customers or teams should design data flows flexibly – for instance, storing a copy in India if required by later notification. The transfer restrictions under DPDP parallel global adequacy regimes: where countries with adequate data protection may be exempt, others may need explicit approval.

PRACTICAL CHALLENGES FOR INDIAN STARTUPS

In theory, DPDP compliance is straightforward 'privacy-by-design'. In reality, startups face a host of practical obstacles:

Cost: Compliance requires investment in technology, security, and legal resources. For instance, encryption, secure backups and logging can push up cloud storage and compute costs. Industry observers predict that implementing DPDP-compliant architectures could raise cloud and storage bills by 25–40% for data-heavy services. (One LinkedIn discussion even quipped that DPDP is a 'cloud architecture reset') Building or buying consent management tools, audit services, DPIA consulting, and possibly hiring a DPO (even on contract) all incur fees. For early-stage startups on tight budgets, prioritising spending is hard: delaying compliance risks fines, but rushing could derail growth.

Technical Capacity: Startups often lack seasoned security engineers or data experts. Implementing robust security safeguards (encryption at rest/in transit, intrusion detection, secure development practices) is non-trivial. Small teams may also not be familiar with GDPR-like principles (even if they serve global markets). The DPB requires logs of unauthorised access to be kept for a year – startups will need new logging infrastructure. Managing data deletion on consent withdrawal or data retention timelines also requires writing or acquiring new software modules. Without strong DevOps or security teams, these tasks can be overwhelming.

Product and UX Design: The Act's granular consent and notice requirements affect product design. Startups built for rapid sign-up or 'frictionless' onboarding must now insert additional screens and checkboxes. Each distinct purpose (e.g. marketing emails, personalised ads, new service features) ideally needs a separate consent. This can lead to multi-page sign-up flows. Industry analysts warn of a risk of consent fatigue: when every app and website in India pops up detailed consent forms, users may simply click 'Accept'

without reading or become frustrated. Designing a user-friendly, legally compliant consent UI is a challenge. Some startups may experiment with layered notices or privacy-friendly defaults to balance compliance and UX. Another example: a SaaS B2B startup might rely on Google Analytics or Mixpanel for usage tracking – under DPDP, it must disclose each piece of tracked data and allow opt-out. Such retrofitting may require rearchitecting analytics pipelines or switching to privacy-centric alternatives.

Investor and Market Expectations: Investors now expect data privacy diligence. As one due diligence expert notes, startups with poor privacy practices can be 'deal killers': missing privacy policies, no consent logs, or inadequate breach plans can scuttle investments. In 2025 and beyond, venture capital firms increasingly view DPDP compliance like financial audits or IP checks – red flags during fundraising. For example, global VC firms often ask for the startup's privacy policy, consent records, and any history of breaches during term sheets. The Corrida Legal blog echoes this: startups are now assessed on their compliance stance 'before they invest'. Thus, even if legally a startup could delay full compliance, market pressure may force early adoption. Conversely, good privacy practice can be a competitive advantage: a public privacy policy and visible DPO contact may reassure customers and partners.

Cross-border Data Transfers: Startups with international elements face uncertainty. The Act allows the government to ban transfers to countries with 'inadequate' protection. If (for instance) a South Asian startup outsources analytics to a US firm, it might later need to restrict such transfers. No 'adequacy list' has been issued yet (this will come via rules), so the safe assumption is to minimise transfers or use secure alternatives (e.g. maintain Indian servers)[14]. This can increase costs (dual infrastructure) or limit the choice of global tools.

Third-party Services and Vendors: Startups typically rely on many third-party services (cloud, payment gateway, marketing tools). Under DPDP, each Data Processor engagement must be by written contract, with the processor bound to DPDP's standards. Many startups have off-the-shelf or SaaS contracts that lack these clauses. Reviewing and amending each agreement (with dozens of vendors) can be onerous. Moreover, third-party risk is high: if a vendor suffers a breach, the startup must report it and faces liability. For example, if a

[14] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Organisation for Economic Co-operation and Development, 2002)

startup's email vendor leaks customer emails, the startup is legally responsible for not safeguarding that data. This may lead startups to restrict or carefully vet vendors (e.g. using only DPDP-compliant consent managers or EU-standard processors).

Legacy Data: Startups often have user data collected before DPDP took effect (e.g. leads, account info). The Act does not automatically legalise old consents. In many cases, consent obtained under mere IT Act-era privacy terms is not DPDP-compliant. Startups need to audit legacy datasets: can they continue using them? In some cases, they may need to 're-consent' users (sending a notice and opt-in request) or purge certain data[15]. This is a major headache – reaching out to possibly unresponsive users, and losing data if they do not opt in. There is no grace period exception for pre-Act data; the Act requires fiduciaries to notify users about past processing and provide rights immediately. Many startups might not have recorded how they collected data historically, which complicates this process. User Experience and Consent Fatigue: As noted, Indian users vary widely in digital literacy. Complex legal language or lengthy forms can alienate customers. The DPDP Rules emphasise 'plain-language' notices, but startups must balance legal precision with clarity. Over-notification might scare users away; under-notification risks non-compliance. For example, an e-commerce app might decide to implement a single consent that combines multiple purposes (a practice not allowed under DPDP). Instead, it must break down each purpose, which might deter some users from signing up. Tech founders will need creativity: perhaps progressive consent flows (small consents upfront, additional ones later), or finely segmented consents. This redesign effort can slow product development.

Data Principal Rights: Fulfilling user requests (access, correction, deletion) requires process planning. A startup must allocate someone (often the DPO or a team) to receive and act on such requests. This consumes time and documentation. For small teams, maintaining an audit trail that you responded to in the required time might be new.

RECOMMENDED COMPLIANCE ROADMAP AND LOW-COST MEASURES

Based on the requirements and challenges above, startups can follow a phased roadmap to DPDP compliance, minimising cost:

[15] 'DPDPA IN 2026 WHAT EVERY RESEARCH LEADER AND BRAND MUST KNOW BEFORE IT IS TOO LATE' (*Question Pro*) <https://www.questionpro.com/dpdpa/> accessed 19 March 2026

Phase 1 (0–6 months): Assessment & Planning –

Conduct A Data Mapping Exercise: Use simple spreadsheets or low-cost tools (even manual interviews) to list all sources of personal data. This uncovers hidden processing (e.g. marketing emails, survey data).

Gap Analysis: Compare current practices to DPDP standards. Identify missing policies, outdated consent notices, or unsecured storage. Protiviti's survey suggests creating a checklist (e.g. appointing a DPO, drafting notices, breach processes).

Draft or Update: The privacy notice and consent text so that it meets DPDP language and contains the required disclosures. Use plain-language templates (many are freely available).

Assign Responsibility: Formally designate who (or which team) will handle data protection issues.

Phase 2 (6–12 months): Core Implementation –

Consent Mechanisms: Build or integrate a user consent interface that logs each user's choices. For small apps, even storing an 'opt-in' flag in the database with a timestamp can suffice initially.

Data Protection Measures: Implement basic technical controls. For example, enable encryption at rest on databases (many cloud providers allow toggling this on per-database). Turn on HTTPS everywhere. Use the built-in identity management features of frameworks to limit internal access[16]. These steps are usually low-cost.

Document Policies and Procedures: Write down the company's privacy policy, data retention policy, and breach response plan. Use existing open-source guides (e.g. templates from industry associations). Ensure every employee knows how to follow them.

Vendor Contracts: Use model contract addenda (similar to GDPR standard clauses) for new vendors. For key partners, negotiate DPDP compliance clauses (many vendors will accept this with little pushback, as global companies already have privacy language).

[16] *STATE OF DATA PRIVACY IN INDIA* (Protiviti India, 2024)

Breach Readiness: Create an incident-response runbook. Identify who will do what when a breach is suspected. Prepare notification templates (email or app alerts) that include all required information.

Phase 3 (12–18 months): Advanced Controls and Testing –

Data Protection Impact Assessments (DPIAs): If the startup is or may become an SDF, conduct an initial DPIA on any high-risk processing (e.g. profiling, new product launch). Use free DPIA tools or checklists from regulators; these can be outsourced or done in-house via guided templates.

Independent Audit: Engage an external cybersecurity auditor or certified chartered accountant to review compliance. This can often be negotiated at reduced rates for startups, and some government grants or incubators may subsidise it.

Privacy-Enhancing Tech: Consider open-source privacy technologies (e.g. selective encryption libraries, privacy libraries for user data) to minimise personal data exposure.

Staff Training and Awareness: Provide online privacy training to new and existing employees. Focus especially on engineers and customer-service staff, who handle data directly.

Ongoing Review: Set up periodic (e.g. annual) reviews of data practices and policies. Automate reminders to refresh consents if needed. Monitor regulatory updates and adapt (for example, if new rules change how cross-border data is handled, or if the Board issues guidelines).

Low-Cost and Scalable Solutions –

Cloud Compliance Offerings: Most cloud providers (AWS, Azure, GCP) offer built-in security tools and compliance reports, which can be used to demonstrate safeguards.

Template Documents: Many law firms and government bodies have sample privacy notices, DPIA forms, and breach templates. These can be adapted rather than drafted from scratch.

Shared Services: For DPO and auditing roles, startups can share consultants or use part-time officers through incubator programs.

Privacy-Enhancing Frameworks: Use privacy-friendly defaults. For example, require explicit opt-in for cookies, anonymise logs, and purge logs older than necessary.

Community Resources: Industry associations (NASSCOM, IAMAI) and government initiatives (Startup India) may offer hackathons, webinars, and guidance on DPDP. Staying engaged can reduce trial-and-error costs.

EMPIRICAL EVIDENCE AND CASE LAWS

Empirical and legal analysis of DPDP compliance is still emerging, but several sources provide insight:

Government and Authority Guidance: The Ministry of Electronics & IT (MeitY) has published the Act and Rules, and through FAQs/press releases, it stresses strong user rights and accountability. For example, the official press note for the DPDP Rules emphasises *verifiable* consent for children and swift breach reporting. The government has also clarified (in press) that only digital personal data is covered and that DPDP repealed the earlier Privacy Rules.

Supreme Court Jurisprudence: DPDP was framed in the backdrop of *Justice K.S. Puttaswamy v Union of India* (2017)[17], where India's Supreme Court held privacy to be a fundamental right under the constitution. This landmark case gave constitutional backing to any privacy legislation, and the DPDP Act echoes its emphasis on personal autonomy. While not a compliance tool, citing *Puttaswamy* underlines the importance of data protection in India's legal landscape.

Industry Surveys: Surveys indicate growing awareness, but also a lack of readiness. For instance, a 2024 *State of Data Privacy in India* report (by CII–Tata Communications/Protiviti) found that only 24% of Indian companies feel prepared to handle privacy for emerging tech. Significantly, it warned that most startups and SMEs lack dedicated privacy budgets. The survey also offered a compliance roadmap (see Table 40 of that report), breaking tasks into categories for ordinary fiduciaries, SDFs, and startups – our checklist incorporates many of these steps.

[17] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

CONCLUSION

India's DPDP Act, 2023, ushers in a new era of data protection accountability. For startups, this means adapting to a law that was designed with simplicity in mind, but imposes substantial obligations. We have shown that the DPDP Act applies to virtually all startups processing Indian users' personal data, with key definitions (data fiduciary, consent, significant fiduciary) shaping who must do what. Compliance obligations span from transparent notices and consent mechanisms, to robust security, breach reporting, and user rights facilitation, to organisational measures like appointing Data Protection Officers (for large players) and conducting impact assessments. The enforcement framework is stringent: a new Data Protection Board with powers to fine up to ₹250 crore for serious violations. Appeals go to TDSAT, emphasising that data protection is now as enforceable as telecom regulations.

Startups face real challenges – costs can rise, technical and legal gaps must be closed, and product design may need an overhaul to accommodate DPDP norms. Investor scrutiny is also a driving force, making compliance both a risk and an opportunity for trust-building. Yet with a methodical approach (as outlined in our roadmap and tables), startups can integrate DPDP requirements into their fabric. Practical measures – using templates, leveraging low-cost tools, and documenting diligently – can mitigate burdens. In the end, robust data practices can become a competitive differentiator: users and investors increasingly value privacy-minded companies.