

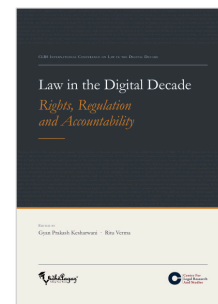
CHAPTER 18

From Privacy to Practice: Evaluating the Implementation of India's Digital Personal Data Protection Act

Maliya and Santosh Kumar

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 217–225

DOI <https://doi.org/10.63108/VAB.LDD.1.18>



CITATIONS

BLUEBOOK (21ST ED.)

Maliya & Santosh Kumar, *From Privacy to Practice: Evaluating the Implementation of India's Digital Personal Data Protection Act*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 217 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Maliya and Santosh Kumar, 'From Privacy to Practice: Evaluating the Implementation of India's Digital Personal Data Protection Act' in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 217.

CHICAGO (17TH ED.)

Maliya, and Santosh Kumar. "From Privacy to Practice: Evaluating the Implementation of India's Digital Personal Data Protection Act." In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 217–225. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.18>.

APA (7TH ED.)

Maliya, & Kumar, S. (2026). From privacy to practice: Evaluating the implementation of India's digital personal data protection act. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 217–225). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.18>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.18>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 18

From Privacy to Practice: Evaluating the Implementation of India's Digital Personal Data Protection Act

DR. MALIYA* AND SANTOSH KUMAR**

India's Digital Personal Data Protection Act 2023 (DPDP Act) is the country's first comprehensive cross-sectoral framework for digital personal data. Its significance lies in whether it can translate the constitutional right to privacy recognised in Justice K.S. Puttaswamy v. Union of India into effective institutional and organisational safeguards. This paper evaluates that translation at a critical transitional moment. The final DPDP Rules were notified and the Data Protection Board of India was legally established in November 2025, but most substantive duties and enforcement powers follow an eighteen-month commencement period. Using doctrinal and institutional analysis, the paper assesses the Act's consent architecture, rights, duties of data fiduciaries, children's-data regime, breach response, state exemptions, regulatory design and organisational implementation.

It argues that the Act provides a usable compliance framework but only partially embodies the constitutional conception of informational privacy. Its strengths include plain-language notice, purpose limitation, security safeguards, breach notification and potentially substantial penalties. Its weaknesses include broad state-processing grounds, limited rights, reliance on executive rulemaking, the absence of a general special-category framework and questions concerning the independence and capacity of the Data Protection Board. Effective implementation will depend on moving beyond formal consent toward demonstrable accountability: data inventories, purpose governance, privacy engineering, processor oversight, risk assessment, accessible rights channels and transparent enforcement. The paper proposes a phased implementation model and concludes that the success of the DPDP regime should be measured not by the number of consent notices or penalties, but by whether it reduces informational power asymmetries and makes lawful, fair and secure data practices routine across the Indian digital economy and the State.

Keywords: DPDP Act; privacy; data protection; India; Data Protection Board; compliance; digital governance

1 INTRODUCTION

India's digital transformation has created extensive public and private data infrastructure. Everyday life now depends on Aadhaar-enabled services, digital payments, e-commerce, telecommunications, health platforms, educational technology and data-driven welfare systems. This expansion has economic and administrative value, but it also concentrates informational power. Personal data can be reused, aggregated, inferred and stored in ways that individuals may neither understand nor control. Data breaches, manipulative consent interfaces, behavioural profiling and function creep show why confidentiality alone cannot protect privacy. Effective protection requires rules for the entire data lifecycle and institutions capable of enforcing them.

* Assistant Professor at School of Law, NIILM University, Kaithal, Haryana, India.

** Research Scholar at School of Law, NIILM University, Kaithal, Haryana, India.

The constitutional starting point is Justice K.S. Puttaswamy (Retd.) v Union of India, in which a nine-judge bench unanimously held that privacy is a fundamental right grounded in dignity, liberty and autonomy. The judgment did not enact a complete privacy code. It required intrusions on privacy to have a legal basis, pursue a legitimate aim, use proportionate means and include safeguards against abuse. It also recognised informational privacy as essential to individual freedom in a networked society and anticipated a data-protection framework that balances individual interests with legitimate uses of data.¹ The Digital Personal Data Protection Act 2023 (DPDP Act) is Parliament's principal response to that constitutional requirement.²

This paper asks whether the Act translates constitutional privacy into meaningful institutional and organisational protection. The question is practical. Enacting a statute does not by itself change how a retailer collects phone numbers, an employer monitors staff, a platform profiles children, a processor secures databases or a public authority combines welfare records. Implementation depends on regulatory capacity, organisational routines, accessible rights and remedies and credible enforcement incentives. The paper argues that the DPDP Act provides a credible minimum architecture but remains an incomplete constitutional translation. Its effectiveness will depend on whether the implementation phase creates demonstrable accountability or produces little more than notices and consent records.

2 METHOD AND EVALUATIVE FRAMEWORK

This study uses doctrinal and institutional analysis. It interprets the DPDP Act, the final Digital Personal Data Protection Rules 2025 (DPDP Rules), the commencement and institutional notifications, Puttaswamy and the Aadhaar judgment. It then considers how the resulting obligations would operate within data-processing organisations. The EU General Data Protection Regulation (GDPR) and the OECD privacy principles are used as comparators, not as models that India must reproduce, but as sources of established implementation tools such as independent supervision, privacy-management programmes and risk assessment.³

The analysis uses four criteria. Constitutional fidelity asks whether the regime reflects legality, necessity, proportionality, dignity and protection against arbitrary informational power. Institutional effectiveness concerns the independence, competence, accessibility and remedial capacity of the Data Protection Board. Organisational operationality asks whether the statutory duties can be translated into governance, engineering, contracting and incident-response practices. Distributive fairness considers whether safeguards work for children, people with limited literacy, workers, people who depend on essential services and those dealing with the State. Together, these criteria distinguish formal compliance from substantive privacy protection.

This is necessarily an early implementation study. On 13 November 2025, the Government notified the final Rules, commenced specified institutional provisions, legally established the Board and set a

¹ Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

² Digital Personal Data Protection Act 2023 (Act No 22 of 2023).

³ Regulation (EU) 2016/679 (General Data Protection Regulation), especially arts 5, 12-22, 25, 32-35 and 51-52; OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013 revision).

phased commencement schedule.⁴ The principal provisions on lawful processing, consent, fiduciary obligations, individual rights, penalties and Board procedure are due to commence after an eighteen-month transition, in May 2027. MeitY began recruiting the Chairperson and members in May 2026, but no appointment notification was found in the public record by the end of August 2026.⁵ The analysis therefore addresses readiness, institutional design and foreseeable implementation problems rather than mature enforcement outcomes.

3 CONSTITUTIONAL PRIVACY AND STATUTORY DATA PROTECTION

Puttaswamy treated privacy as more than secrecy. It protects decisional autonomy, bodily integrity and control over the disclosure of personal information. Its proportionality framework requires a valid law, a legitimate state purpose and proportionate means, supported by safeguards against abuse.⁶ The Aadhaar litigation likewise shows that constitutional assessment must examine the architecture of a data system, including data minimisation, retention, authentication records, security and oversight. A formally lawful system may still become constitutionally excessive.⁷

The DPDPA Act uses distinct terminology. The person to whom personal data relates is the ‘Data Principal’; the person who determines the purpose and means of processing is the ‘Data Fiduciary’; and an entity that processes data on a fiduciary’s behalf is a ‘Data Processor’. The Act applies to digital personal data processed in India and to processing outside India connected with offering goods or services to Data Principals in India. It covers data collected digitally and data collected offline that is later digitised. Personal or domestic processing falls outside the Act and publicly available data is excluded in specified circumstances.⁸ This broad, technology-neutral scope is practical, but the exclusion for publicly available data may leave individuals unprotected when such data is aggregated or used for profiling.

Processing must serve a lawful purpose and rest on consent or one of the statutory ‘certain legitimate uses’. Consent must be free, specific, informed, unconditional and unambiguous, expressed through clear affirmative action and limited to the personal data necessary for the specified purpose. Withdrawing consent must be as easy as giving it.⁹ The final Rules require a standalone, comprehensible notice that identifies the data and purpose, explains the relevant goods or services and describes withdrawal, rights and grievance procedures.¹⁰ These requirements can discipline opaque privacy policies. They do not, however, eliminate consent fatigue, take-it-or-leave-it services or manipulative interfaces. Constitutional autonomy requires more than clicking ‘agree’ when a person lacks bargaining power or understanding.

⁴ Digital Personal Data Protection Rules 2025, G.S.R. 846(E), 13 November 2025, as corrected; Commencement Notification, G.S.R. 843(E), 13 November 2025; Notification Establishing the Data Protection Board of India, G.S.R. 844(E), 13 November 2025; Notification on the Size of the Data Protection Board of India, G.S.R. 845(E), 13 November 2025.

⁵ Ministry of Electronics and Information Technology, Appointment to the Post of Chairperson and Other Members in the Data Protection Board of India, F No 2(1)/2026-Pers.I, 6 May 2026.

⁶ Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; see also Anuradha Bhasin v Union of India (2020) 3 SCC 637 and Internet and Mobile Association of India v Reserve Bank of India (2020) 10 SCC 274 on proportionality.

⁷ K.S. Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1.

⁸ Digital Personal Data Protection Act 2023, ss 2-3.

⁹ Digital Personal Data Protection Act 2023, ss 4, 6-7.

¹⁰ Digital Personal Data Protection Rules 2025, r 3.

4 RIGHTS, DUTIES AND THE ACCOUNTABILITY GAP

The Act gives Data Principals rights to obtain information about processing, seek correction and erasure, pursue grievances and nominate another person to exercise rights after death or incapacity. These rights include access to a summary of the personal data being processed and the identities of other fiduciaries and processors with which the data has been shared. The Act also imposes duties on Data Principals, including duties not to impersonate another person, suppress specified material information or submit false or frivolous grievances. Breach of those duties may attract a penalty.¹¹

The catalogue is narrower than that found in many comprehensive data-protection regimes. The Act creates no freestanding rights to data portability, objection to processing or restriction of processing and no general protection against decisions based solely on automated processing. It also creates no general category of sensitive personal data subject to enhanced safeguards.¹² Health, biometric, financial, sexual-orientation and political-affiliation data therefore receive the Act's general protection unless sectoral law or the duties of a Significant Data Fiduciary add further safeguards. A technology-neutral framework is simpler, but it can treat materially different risks alike. A leaked restaurant preference and a leaked genomic record are both personal data, but their consequences differ sharply.

A Data Fiduciary remains responsible for processing carried out on its behalf. Its core duties include ensuring accuracy when data is used for a decision or disclosed, applying reasonable security safeguards, notifying personal-data breaches, erasing data when consent is withdrawn or the purpose is exhausted, publishing contact information and providing an effective grievance mechanism.¹³ The final Rules translate the security duty into more concrete controls, including contractual safeguards for processors, access controls, encryption or comparable protection, backups, monitoring and retention of relevant logs.¹⁴ These minimum controls are useful, but 'reasonable' security must remain contextual. A checklist can establish a floor; the level of protection above that floor should reflect risk, scale, sensitivity and likely harm.

5 BREACH RESPONSE AND ORGANISATIONAL PREPAREDNESS

Breach notification will test how the regime performs under pressure. The final Rules require a fiduciary to notify each affected Data Principal promptly and in clear language, describing the breach, its likely consequences, mitigation and protective measures and a contact point. The fiduciary must also notify the Board promptly and provide a fuller report within seventy-two hours unless the Board permits more time.¹⁵ This approach is broader than the GDPR's risk-based rule for notifying affected individuals.¹⁶ Universal notice may improve transparency, but without guidance that distinguishes material communications from routine technical events, it may also produce over-notification and notification fatigue.

An organisation cannot meet this duty by drafting a template after an incident. It needs asset inventories, data classification, detection capabilities, escalation thresholds, decision logs, forensic-preservation

¹¹ Digital Personal Data Protection Act 2023, ss 11-15 and Schedule.

¹² Compare Regulation (EU) 2016/679 (General Data Protection Regulation), arts 9 and 15-22, with the rights and obligations in the Digital Personal Data Protection Act 2023.

¹³ Digital Personal Data Protection Act 2023, s 8.

¹⁴ Digital Personal Data Protection Rules 2025, r 6.

¹⁵ Digital Personal Data Protection Act 2023, s 8(6); Digital Personal Data Protection Rules 2025, r 7.

¹⁶ Regulation (EU) 2016/679 (General Data Protection Regulation), arts 33-34.

procedures, communication workflows and rehearsed coordination among security, privacy, legal, communications and senior management teams. Processor contracts should specify notification times, access to evidence, cooperation duties and responsibility for response. Outsourcing infrastructure does not out-source accountability: the Data Fiduciary remains responsible for processing carried out on its behalf.¹⁷

These operational demands are especially difficult for micro, small and medium enterprises, start-ups, public bodies and organisations with legacy systems. Risk-based implementation support can include model notices, standard contractual clauses, sectoral codes, breach exercises, shared security services and plain-language guidance from the Board. Enforcement should distinguish organisations that acted in good faith and maintained demonstrable governance from those that ignored known risks or shifted responsibility to others. Penalties matter, but predictable standards and technical assistance are also necessary to build capacity.

6 CHILDREN, CONSENT MANAGERS AND SIGNIFICANT DATA FIDUCIARIES

Processing a child's data generally requires verifiable parental consent. The Act also restricts processing likely to harm a child's well-being, behavioural monitoring or tracking of children and targeted advertising directed at them, subject to prescribed exceptions.¹⁸ Treating everyone under eighteen as a child is protective but operationally difficult. Age assurance may itself require intrusive data collection and parental control may conflict with adolescents' growing autonomy, particularly in health, counselling and educational services. Implementation should use proportionate age-assurance methods, collect only the minimum evidence, avoid persistent identity databases and account for differences in risk across services.

Consent Managers are intended to provide interoperable means to give, manage, review and withdraw consent. If trusted, they could reduce fragmented consent interfaces and make withdrawal effective. The Rules prescribe eligibility, financial, technical, governance and fiduciary requirements.¹⁹ Yet an intermediary that manages consent may itself become a concentrated source of behavioural data and cyber risk. Consent Managers will either strengthen individual control or add another layer to the data economy, depending on registration standards, conflict-of-interest controls, auditability, interoperability and limits on secondary use.

The Government may designate Significant Data Fiduciaries by considering factors such as the volume and sensitivity of data processed, risks to Data Principals' rights, sovereignty, electoral democracy, security and public order. A designated entity must appoint a Data Protection Officer in India, engage an independent data auditor, conduct periodic data-protection impact assessments and audits and comply with additional prescribed measures.²⁰ This risk-tiered model sensibly links additional duties to systemic influence. Its legitimacy will depend on clear criteria, reasoned designation and a fair opportunity to challenge arbitrary selection. Impact assessments should inform actual decisions to deploy, redesign or stop high-risk processing and meaningful summaries should show affected people and the Board that necessity, alternatives and risks were genuinely considered.

¹⁷ Digital Personal Data Protection Act 2023, s 8(1)-(2).

¹⁸ Digital Personal Data Protection Act 2023, s 9; Digital Personal Data Protection Rules 2025, rr 10 and 12, and Fourth Schedule.

¹⁹ Digital Personal Data Protection Act 2023, ss 2(g) and 6(7)-(9); Digital Personal Data Protection Rules 2025, r 4 and First Schedule.

²⁰ Digital Personal Data Protection Act 2023, s 10.

7 STATE PROCESSING EXEMPTIONS AND CONSTITUTIONAL PROPORTIONALITY

State processing is the most important test of constitutional fidelity. Section 7 permits specified uses without consent, including the provision of subsidies, benefits, services, certificates, licences or permits in defined circumstances; the performance of state functions under law or pursuant to judgments; and responses to medical emergencies and disasters. The Act also permits exemptions by Central Government notification and contains exemptions connected with sovereignty, integrity, security, public order, investigation and related grounds.²¹

Some flexibility is necessary because government cannot obtain bespoke consent for every legitimate public function. The constitutional question is whether the legal basis, purpose, scope, retention, sharing and safeguards are necessary and proportionate. Broad statutory language can allow welfare databases to migrate into policing, profiling or exclusion. The Rules' standards for state service delivery, including lawful processing, purpose limitation, necessity, accuracy, retention controls, security, notice and accountability, are useful.²² They should be supported by published data inventories and purpose statements, access logs and independent audits.

The relationship between privacy and transparency also requires attention. The DPDP Act amended section 8(1)(j) of the Right to Information Act 2005, which governs the exemption for personal information.²³ Privacy law should prevent disclosure that causes unjustified harm without becoming a shield against accountability for public officials, public spending or regulatory action. Public-interest balancing, proportionality and severability remain important. The central constitutional danger is asymmetry: demanding the narrowest consent and compliance from the private sector while allowing the broadest discretion to the State. Puttaswamy is especially important where state databases affect access to essential services and rights.

8 DATA PROTECTION BOARD: INDEPENDENCE, CAPACITY AND REMEDY

The Data Protection Board connects rights on paper with enforcement in practice. It is a statutory body corporate, designed to operate digitally, with powers to inquire into non-compliance and breaches, order urgent mitigation, accept voluntary undertakings and impose monetary penalties. Decisions may be appealed to the Appellate Tribunal.²⁴ The Government legally established the Board in the National Capital Region and fixed its size in November 2025. Recruitment documents issued in 2026 contemplated a Chairperson and four members, but no completed appointments were identified in the public record by the end of August 2026.²⁵ In addition, the provisions conferring the Board's principal functions and procedures are subject to the later commencement schedule. Legal existence must therefore be distinguished from operational capacity.

The Board's independence is a central design concern. The Central Government appoints members through the statutory selection process; members serve two-year terms and may be reappointed; and the

²¹ Digital Personal Data Protection Act 2023, ss 7 and 17.

²² Digital Personal Data Protection Rules 2025, r 5 and Second Schedule.

²³ Digital Personal Data Protection Act 2023, s 44(3), amending Right to Information Act 2005, s 8(1)(j).

²⁴ Digital Personal Data Protection Act 2023, ss 18, 27-29 and 32-33.

²⁵ Notification Establishing the Data Protection Board of India, G.S.R. 844(E), 13 November 2025; Notification on the Size of the Data Protection Board of India, G.S.R. 845(E), 13 November 2025; Ministry of Electronics and Information Technology, Appointment to the Post of Chairperson and Other Members in the Data Protection Board of India, F No 2(1)/2026-Pers.I, 6 May 2026.

executive retains substantial rulemaking and administrative influence.²⁶ By comparison, GDPR Articles 51 and 52 require supervisory authorities to act with complete independence and to receive adequate human, technical and financial resources.²⁷ India need not copy the European model for its Board to be constitutionally valid. Even so, perceived dependence may weaken trust when the Board hears complaints about government data systems. Longer and staggered terms, published selection criteria and recusals, an independent secretariat and a separately disclosed budget would strengthen credibility.

Capacity is equally important. A Chairperson and four members may face complaints and violations across one of the world's largest digital populations. A digital-by-design process can widen access, but it can also exclude people with poor connectivity, limited language options, disabilities or limited legal literacy. The Board should provide multilingual and accessible interfaces, assisted filing, reasoned and searchable decisions, predictable timelines and procedures for consolidating systemic cases. Effective remedies should include mitigation and corrective directions rather than treating monetary penalties as the only outcome. Annual statistics on complaints, sectors, disposal times, breaches, penalties, undertakings and compliance would allow Parliament and the public to assess performance.

9 FROM LEGAL TEXT TO ORGANISATIONAL PRACTICE

A sound implementation programme begins with governance, not a privacy notice. Boards and senior managers should establish ownership, risk appetite and the evidence required to demonstrate compliance. Every organisation should maintain records of processing that identify data types, sources, purposes, systems, locations, recipients, processors, retention periods and legal bases. Without such a map, an organisation cannot reliably answer access requests, delete data or assess breaches and unlawful use. Product approval and change-management procedures should enforce purpose limitation so that a new analytical use does not bypass the original notice.

Consent must be designed into and enforced through the interface. Organisations should separate purposes, eliminate pre-ticked boxes, retain notice versions, record affirmative action and propagate withdrawal to processors and downstream systems. Erasure should extend through production systems, archives and derived datasets, subject to documented legal-retention exceptions. Rights portals should use proportionate authentication and provide human escalation. Privacy by design should incorporate access control, data minimisation, encryption, tokenisation, safe testing data, logging and secure deletion throughout the development lifecycle.²⁸ For AI systems, organisations should document training-data provenance, inference risks, purpose compatibility and human review even though the Act creates no express right concerning automated decisions.

Supply chains are another channel through which accountability operates. Vendor due diligence should examine security, sub-processing, data location, breach history, deletion and audit rights. Contracts should reflect operational reality and be tested against evidence rather than questionnaires alone. Significant Data Fiduciaries should connect impact assessments and audits to decisions to deploy, redesign, restrict or abandon high-risk processing. The OECD privacy-management approach is useful because it treats accountability as a programme proportionate to an organisation's structure, scale, volume

²⁶ Digital Personal Data Protection Act 2023, ss 19-20.

²⁷ Regulation (EU) 2016/679 (General Data Protection Regulation), arts 51-52.

²⁸ European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (final version 2020).

and sensitivity, supported by risk assessment and incident planning.²⁹ Substantive compliance requires an organisation to explain why it processes data, how it minimises risk and what it did when controls failed.

10 COMPARATIVE LESSONS WITHOUT REGULATORY COPYING

Comparison is useful, but India's framework is deliberately more minimalist than the GDPR. The GDPR provides multiple lawful bases, special-category protections, extensive processor duties, rights to portability and objection, safeguards for automated decision-making, impact assessments for high-risk processing and independent supervisory authorities.³⁰ The DPDP Act relies more heavily on consent and specified legitimate uses, delegated rulemaking and additional duties for notified Significant Data Fiduciaries. Simplicity may reduce compliance complexity, but it can also leave protection dependent on future designation and interpretation.

Three comparative lessons are especially relevant. First, regulatory independence and resources are functional requirements, not institutional decoration. Second, consent should be supplemented by risk-based accountability because people cannot negotiate their way out of surveillance or insecure infrastructure. Third, guidance and enforcement should be transparent. European experience also shows that broad rights may accomplish little without an empowered, well-resourced and efficient regulator. India should not assume that a shorter statute is easier to enforce or that a high maximum penalty necessarily produces deterrence.

India can develop a model suited to its scale, linguistic diversity and digital public infrastructure. Consent Managers could become distinctive rights-enabling institutions; digital Board proceedings could reduce geographic barriers; and interoperable technical standards could improve withdrawal and grievance procedures. These benefits depend on privacy-enhancing, auditable systems that are accessible beyond smartphone-centred, English-language services. Regulation that supports innovation must still make rights effective and difficult to evade.

11 RECOMMENDATIONS FOR THE IMPLEMENTATION PHASE

The phased commencement period should be treated as a regulatory build-out period. MeitY and the Board should publish a common implementation calendar, model notices, breach-reporting formats, standards for rights requests and sector-specific guidance. The Government should also publish transparent risk criteria for designating Significant Data Fiduciaries. Before the substantive duties commence, the Board should have trained legal, technical and investigative staff and tested digital and assisted-filing channels. Appointment and budget information should be public and decisions should be searchable and available in major Indian languages.

Organisations should prioritise demonstrable controls: executive accountability, processing inventories, lawful-purpose review, consent records, retention schedules, rights workflows, processor governance, incident exercises and performance metrics. Organisations engaged in high-risk processing should conduct impact assessments even before formal designation. Public entities should publish data-purpose registers and audit access to population-scale datasets. Children's services should use proportionate age

²⁹ OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013 revision); OECD, Going Digital Guide to Data Governance Policy Making (2022).

³⁰ Regulation (EU) 2016/679 (General Data Protection Regulation), especially arts 5, 9, 12-22, 25, 28, 32-35 and 51-52.

assurance and prevent behavioural advertising by design. Exemptions should be limited, reasoned and time-bound, while model documents and technical support should help MSMEs comply.

Implementation should be assessed by outcomes. Useful indicators include the time taken to fulfil rights requests, the proportion of withdrawn consents propagated across systems, deletion after a purpose expires, breach-detection and notification times, recurrence of control failures, accessibility of complaint mechanisms, remedial orders and sectoral patterns of harm. Civil-society organisations, researchers and consumer groups should have access to anonymised enforcement data. After the first enforcement cycle, parliamentary review should consider whether the exemptions, Board structure and catalogue of rights remain adequate.

12 CONCLUSION

The Digital Personal Data Protection Act 2023 creates India's first general law for digital personal data and gives statutory form to the fundamental right to privacy recognised in *Puttaswamy*.³¹ It requires Data Fiduciaries to process personal data for lawful purposes on the basis of valid consent or another authorised ground, adopt reasonable security safeguards and notify affected individuals and the Data Protection Board of personal-data breaches.³² A food-delivery application that requests a user's name, address and telephone number should explain why those details are needed and should not seek access to photographs, contacts or location history unless they are necessary for a stated purpose. The DPDP Rules 2025 add operational detail, while phased commencement gives organisations time to adjust systems and internal processes.³³

Consent alone cannot ensure privacy where people have unequal power. An employee may accept workplace surveillance for fear of losing a job, while a student may accept an educational application's privacy policy because no realistic alternative exists. The absence of a general category for sensitive personal data is also significant: disclosure of medical, biometric or financial information can cause far greater harm than disclosure of an ordinary shopping preference. Similarly, the Act's limited protections concerning profiling and automated decision-making may leave people without a clear statutory remedy when an algorithm rejects an application for credit, employment or insurance without an adequate explanation or human review.

The Act should therefore be understood as a foundation for India's privacy system rather than a complete achievement. Effective protection will require an independent, adequately staffed and accessible Data Protection Board, responsible organisational conduct and constitutional limits on state processing. Collecting identity data to administer welfare benefits may serve a legitimate public function; indefinitely linking it with medical, travel and communications data may be disproportionate. The regime's success should be measured not by the number of consent notices or penalties, but by whether people can exercise their rights easily and whether organisations and public authorities routinely collect only necessary data, protect it and erase it when it is no longer required.

* * *

³¹ Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Digital Personal Data Protection Act 2023.

³² Digital Personal Data Protection Act 2023, ss 4, 6-8.

³³ Digital Personal Data Protection Rules 2025, G.S.R. 846(E), 13 November 2025, as corrected; Commencement Notification, G.S.R. 843(E), 13 November 2025.