

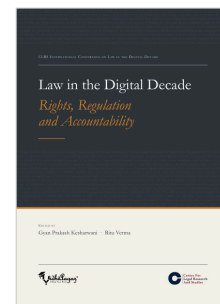
CHAPTER 17

The Data Protection Regime in India: Constitutional Privacy to Statutory Compliances

Enakshi Guha

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 203–215

DOI <https://doi.org/10.63108/VAB.LDD.1.17>



CITATIONS

BLUEBOOK (21ST ED.)

Enakshi Guha, *The Data Protection Regime in India: Constitutional Privacy to Statutory Compliances*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 203 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Enakshi Guha, “The Data Protection Regime in India: Constitutional Privacy to Statutory Compliances” in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 203.

CHICAGO (17TH ED.)

Guha, Enakshi. “The Data Protection Regime in India: Constitutional Privacy to Statutory Compliances.” In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 203–215. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.17>.

APA (7TH ED.)

Guha, E. (2026). The data protection regime in India: Constitutional privacy to statutory compliances. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 203–215). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.17>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.17>

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 17

The Data Protection Regime in India: Constitutional Privacy to Statutory Compliances

ENAKSHI GUHA *

In India, the data protection landscape has evolved from a constitutional principle into a comprehensive statutory and regulatory framework anchored in the recent Digital Personal Data Protection Act, 2023 (DPDP Act) and DPDP Rules, 2025, and parallel cybersecurity mandates under the Information Technology Act, 2000 and CERT-In Directions, 2022. Relying on the jurisprudential precedents of the data protection architecture, the recognition of right to privacy as a fundamental right intrinsic to Article 21 of the Indian Constitution, is analysed in the paper. The analysis details the four core rights conferred on data principals: the right to access, right to correction and erasure, right to grievance redressal, and right to nominate (Section 14), alongside the corresponding obligations of data fiduciaries, including notice, consent, legitimate uses, accuracy, security safeguards, personal data breach intimation (with a detailed report to the Board within 72 hours under rule 7 of the DPDP Rules, 2025), retention limits, and grievance redressal mechanisms provided in the Act.

The paper further examines cross-border data transfer provisions, noting that transfers are permitted except to countries or territories that the Central Government restricts by notification, and that no such notification has been issued as of July 2026. Until notified, organizations must rely on reasonable security safeguards and contractual protections, while monitoring for potential restrictions on sensitive categories (health, financial, biometric data). This paper provides a rigorous doctrinal and practical analysis of the emerging data protection, privacy, synthesising constitutional foundations, statutory obligations, enforcement mechanisms, and operational challenges facing organizations as the DPDP framework enters phased operational force. The paper further examines the core architecture and the ground level application of the Act, including definitions of Data Principal, Data Fiduciary, Data Processor, and the yet-to-be-notified category of Significant Data Fiduciary (SDF), which will trigger enhanced obligations such as data protection officer appointments, audits, and impact assessments.

Finally, the paper identifies five critical compliance challenges in practice: (1) consent fatigue from repeated user requests; (2) legacy data collected for broad or undefined purposes; (3) AI training on personal data without explicit statutory guidance; (4) SME and startup burden in meeting SDF-level obligations; and (5) CERT-In vs. DPDP reporting tension. Mitigation strategies, including layered notices, data mapping, shared compliance services, and integrated incident response frameworks, are proposed.

Keywords: Digital Personal Data Protection Act 2023, data privacy and CERT-In Directions, data fiduciary obligations, cross-border data transfers, proportionality test and constitutional foundations.

1 INTRODUCTION TO THE TOPIC

In India, the trajectory of data protection law represents a paradigmatic shift from constitutional recognition to statutory operationalisation. The Hon'ble Supreme Court of India in its landmark judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India,¹ established privacy as a fundamental right under Article 21, Constitution of India, laying the doctrinal foundation for comprehensive data protection

* Practicing Advocate.

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

legislation. Years later, the Digital Personal Data Protection Act, 2023 (DPDP Act) emerged as the nation's first dedicated data protection statute, received Presidential assent on 11th August, 2023, and entered phased commencement with the notification of DPDP Rules, 2025 on 13th November, 2025.²

The mentioned landmark judgment articulated a three-fold proportionality test for evaluating privacy intrusions: 1) legality, requiring valid statutory authorisation, 2) legitimate state aim of sovereignty, security and public order, and 3) proportionality, ensuring a rational nexus between the objects and the means adopted.³ This constitutional framework has governed subsequent privacy-related litigations, including Aadhaar challenges, surveillance disputes and data localisation debates. However, until the enactment of the Act, India lacked a comprehensive statutory regime governing personal data processing by private and public entities, relying instead on the Information Technology Act, 2000 and the SPDI Rules, 2011, which proved inadequate for addressing contemporary data processing practices. The DPDP Act operationalises this doctrine pronounced by the judgment by establishing rights-based obligations for data fiduciaries, enforcement mechanisms through the Data Protection Board of India, and penalties up to Rs. 250 crore for security failures. Later, the phased implementation reflects a calibrated approach to compliance, allowing organizations time to align data processing practices with statutory requirements.⁴

The paper pursues three primary objectives: 1) to examine the constitutional foundations of data protection in India, 2) to analyse how the core provisions of the DPDP Act – notice, consent, data principal rights, fiduciary obligations, breach notifications, and security safeguards – operate in practice for Indian organizations across sectors, and 3) to suggest a practical compliance framework integrating DPDP Act obligations with parallel cybersecurity mandates under CERT-In Directions addressing overlaps, tensions, and operational challenges. The scope of the paper is limited to the ground-level application of the Act within India focusing on data privacy and data protection obligations for domestic data fiduciaries, the judicial precedents interpreting privacy rights post-Puttaswamy judgment, existing research on compliance challenges, enforcement mechanisms, and sector-specific impacts, and the examination of cross-border data transfer restrictions (pending government notifications); it does not extend to technical cybersecurity standards beyond CERT-In's baseline requirements.

2 PATHWAY OF CONSTITUTIONAL FOUNDATIONS

The constitutional bedrock of the nation's data protection regime is the unanimous judgment pronounced by the Hon'ble Supreme Court of India in *Justice K. S. Puttaswamy (Retd.) vs. Union of India*.⁵ This decision recognized the right to privacy as a fundamental right intrinsic to Article 21 and protected under Article 14 and Article 19 of the Constitution.

The Privacy holding: The court rejected the earlier opinions given in *M.P. Sharma vs. Satish Chandra*⁶ and *Kharak Singh vs. State of Uttar Pradesh*⁷ that privacy was not a standalone fundamental right, and further held that privacy is an inalienable aspect of human dignity and a precondition for exercising other

² Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, Extraordinary, Part II, Section 1, 11 August 2023

³ The Law Academy, 'Puttaswamy Case Analysis: Right to Privacy' (20 August 2026) <https://thelawcademy.in/law_resources/puttaswamy-case-analysis-right-to-privacy/> accessed 5 September 2026

⁴ Vratex, 'The DPDP Act 2023 & DPDP Rules 2025, Explained' (28 May 2026) <<https://www.vratex.com/dpdp-act>> accessed 5 September 2026

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

⁶ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300

⁷ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295

fundamental freedoms. The judgment categorically identified multiple dimensions of privacy, including spatial privacy (protection of physical spaces), decisional privacy (autonomy over personal choices), and informational privacy (control over collection, use and disclosure of personal data). This informational privacy directly underpins the consent-based frameworks, data principal rights, privacy and fiduciary obligations as provided under the DPDP Act.

The three-fold proportionality test: The court established that any state action interfering with privacy must satisfy a three-fold proportionality test, which has become the governing standard for evaluating all privacy-related legislation and executive actions.

TABLE 1. *The three-fold proportionality test in Puttaswamy*

LIMB	REQUIREMENT	JUDICIAL STANDARD
Legality	Valid statutory authorisation	Executive action alone is insufficient; a clear, precise law enacted by Parliament or State Legislature must exist. The law must not be vague or overbroad.
Legitimate Aim	Proper state objective	The restriction must pursue a legitimate state interest: national security, crime prevention, welfare delivery, public order, or protection of other fundamental rights.
Proportionality	Rational nexus	There must be a rational nexus between the objects and the means adopted to achieve them; the Aadhaar judgment, (2019) 1 SCC 1, later added that the measure must be the least restrictive available and balanced.

In the case, Justice D.Y. Chandrachud held that an invasion of privacy must meet the three-fold requirement of legality, need (a legitimate state aim) and proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them.⁸

Application to data protection: The court had observed that “Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone.” In its interpretation, the famous Puttaswamy judgment explicitly recognized that informational privacy requires safeguards against unauthorized data collection, processing, and disclosure. Thus, the holding of the case directly structures the Act as follows:⁹

1. Consent requirements under section 6, DPDP Act: Data principals must exercise control over data processing through free, specific, informed, and unambiguous consent.
2. Purpose limitation under section 5, DPDP Act: Data fiduciaries must provide clear notice specifying the purposes for which data will be processed.
3. Retention limits under section 8(7), DPDP Act: Data must be deleted when the processing purpose is exhausted, preventing indefinite retention.
4. Security safeguards under section 8(5), DPDP Act: Fiduciaries must implement reasonable technical and organizational measures to protect data from breaches.

⁸ Record of Law, ‘JUSTICE K.S. PUTTASWAMY (RETD.) V. UNION OF INDIA (2017)’ (20 August 2026) <<https://recordof-law.in/justice-k-s-puttaswamy-retd-v-union-of-india-2017-6/>> accessed 5 September 2026

⁹ Right to Information Wiki, ‘Complete DPDP Act 2023 Guide — Citizen and Business Reference 2026’ (22 August 2026) <<https://righttoinformation.wiki/dpdp-act-2023-complete-guide>> accessed 5 September 2026

Post-Puttaswamy judgment: Subsequent to the Puttaswamy judgment, many other judgments have refined and applied the proportionality test to diverse contexts.¹⁰

1. Privacy challenges in regard to Aadhaar in 2018-2023: In the Aadhaar judgment,¹¹ the constitution bench upheld the constitutionality of Aadhaar for welfare delivery and its mandatory linking with PAN for income tax filing, but struck down mandatory linking with bank accounts as a disproportionate intrusion and held that Aadhaar could not be made mandatory for school admissions, education being an entitlement and not a subsidy, benefit or service. The court emphasized data minimisation, i.e., only necessary data shall be collected for specific purposes.
2. Surveillance and privacy: Many high courts have applied the same foundations to scrutinise mass surveillance programmes. In *Vinit Kumar vs. Central Bureau of Investigation*,¹² the Bombay High Court held that orders for the interception of telephone calls must observe the statutory safeguards and satisfy the proportionality test, and set aside orders that did not.
3. Compelled disclosure and biometric data: In *Ritesh Sinha vs. State of Uttar Pradesh*,¹³ the Hon'ble Supreme Court held that, until Parliament legislates on the point, a Judicial Magistrate may order a person to give a sample of his voice for the purpose of investigation, the right to privacy not being absolute and yielding to a compelling public interest.

Continuing legacy: The foundation established by the Puttaswamy judgment has transformed the constitutional law by elevating privacy from a common law right to a fundamental right enforceable against the state and, indirectly, the private entities through statutory frameworks like the DPDP Act; establishing proportionality as the analytical framework for evaluating privacy intrusions, influencing not only data protection but also surveillance laws, criminal procedure, and administrative law; and informing legislative design as the exemptions under the Act for government instrumentalities under section 17 and legitimate uses under section 7 are explicitly framed around the legitimate categories aimed at sovereignty, security and public order. However, the broad exemptions under section 17 risk undermining the proportionality requirement by allowing the executive to exempt itself from compliance without robust parliamentary oversight or judicial review. This stress between constitutional doctrine and statutory implementation remains a critical area for future judicial scrutiny.

3 STRUCTURIZATION OF THE DPDP ACT, 2023

The DPDP Act, 2023 represents one of the nation's first comprehensive statutory frameworks governing the processing of personal data by both public and private entities. The Act received Presidential assent on 11 August 2023 and was published in the Gazette of India, marking the culmination of a decade-long legislative journey that began with the Justice A.P. Shah Committee Report (2012) and included multiple draft bills (2018, 2019, 2022).

Phase Commencement: Following the parliamentary passage in August 2023, the Act entered a phased commencement schedule to allow organizations time to align their data processing practices with

¹⁰ Liberty Lexicon, 'Justice K.S. Puttaswamy v. Union of India' (25 April 2026) <<https://www.libertylexicon.in/blog/case-commentary-10/justice-k-s-puttaswamy-v-union-of-india-16>> accessed 5 September 2026

¹¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1.

¹² *Vinit Kumar v. Central Bureau of Investigation*, 2019 SCC OnLine Bom 3155

¹³ *Ritesh Sinha vs. State of Uttar Pradesh*, (2019) 8 SCC 1

statutory requirements. The DPDP Rules, 2025¹⁴ were notified on 13 November 2025, operationalising delegated provisions under section 40 of the Act. The MeitY Secretary has confirmed no extension to these deadlines, urging startups and enterprises to begin compliance preparations immediately. As of August 2026, organizations face a firm compliance deadline of May 2027 for core obligations.¹⁵

TABLE 2. *Phased commencement of the DPDP Act, 2023*

PHASE	COMMENCEMENT DATE	PROVISIONS IN FORCE
Phase 1	13 November 2025	Definitions (Section 2), Data Protection Board (Sections 18–26), rule-making powers (Section 40), Section 44(3) RTI amendment.
Phase 2	13 November 2026	Consent Manager registration (Sections 6(9) and 27(1)(d)).
Phase 3	13 May 2027	Full compliance with consent, notice, security and data rights obligations (Sections 3–17, except Section 6(9)), the Board's inquiry, appeal and penalty provisions (Sections 27–34, except Section 27(1)(d)), and Sections 36, 37 and 44(2).

Key concepts under the Act: The Act's operational framework rests on four foundational definitions provided under section 2.¹⁶

1. Data principal under section 2(j), DPDP Act: The individual to whom personal data relates, including the parents or lawful guardian of a child and the lawful guardian of a person with disability acting on her behalf.
2. Data fiduciary under section 2(i), DPDP Act: Any person (individual, company, organization, or government body) who, alone or in conjunction with others, determines the purpose and means of processing personal data. This definition mirrors the concept of 'data controller' under the General Data Protection Regulation, which is a comprehensive data privacy law passed by the European Union that sets strict rules for collecting and processing personal data. It imposes primary compliance responsibility on fiduciaries, irrespective of any agreement to the contrary.
3. Data processor under section 2(k), DPDP Act: A person who processes personal data on behalf of a data fiduciary under valid contractual arrangement. Processors are not directly liable under the Act, but fiduciaries remain responsible for ensuring processor compliance through contractual safeguards.
4. Significant data fiduciary (SDF) under section 2(z), DPDP Act: A category yet to be notified by the Central Government, expected to include entities that process large volumes of sensitive personal data or pose higher risks to data principals. Once it is notified, SDFs will face additional obligations of appointing a Data Protection Officer, based in India, appointing an independent data auditor, conducting periodic data protection impact assessments and additional compliance requirements as prescribed by DPDP Rules, 2025.

¹⁴ Ministry of Electronics and Information Technology, *Digital Personal Data Protection Rules, 2025* (Gazette of India, 13 November 2025)

¹⁵ Centre for Applied Data Protection, *DPDP Act Implementation Status 2026, Complete Tracker* (CADP, 9 March 2026)

<<https://cadp.in/resources/guides/dpdp-implementation-tracker/>> accessed 5 September 2026

¹⁶ Centre for Applied Data Protection, *DPDP Act Key Provisions Explained: A Detailed Analysis* (CADP, 30 January 2026)

<<https://cadp.in/resources/articles/dpdp-act-key-provisions-explained/>> accessed 5 September 2026

Territorial applicability: Section 3, DPDP Act establishes an extraterritorial reach so that processing outside India is covered where it is in connection with offering goods or services to data principals in India, as with foreign platforms such as Meta, Google and Amazon serving Indian users.

Personal data over sensitive private data: The Act defines personal data broadly as “any data about an individual who is identifiable by or in relation to such data” as provided under section 2(t). Unlike the General Data Protection Regulation, the DPDP Act does not create a separate category of ‘sensitive private data’ with enhanced protection. However, the SDF designation, once notified, may impose stricter obligations for processing certain data categories. Furthermore, the Act applies only to personal data collected in digital form or digitised afterwards (section 3(a)); section 3(c) excludes personal data processed by an individual for any personal or domestic purpose and personal data made publicly available by the data principal or under a legal obligation; and processing necessary for research, archiving or statistical purposes is exempted under section 17(2)(b), DPDP Act, where the personal data is not used to take any decision specific to a data principal and the processing follows the standards prescribed in the Second Schedule to the DPDP Rules, 2025.

The structurization of the Act reflects a rights-based approach balanced with enforcement mechanisms and flexibility for state interests. However, the definitional framework introduces several departures from international models like the following:

1. No explicit data minimisation principle: Unlike Article 5(1)(c) of the General Data Protection Regulation, the DPDP Act states no general data minimisation principle; section 6(1), however, expressly limits consent to such personal data as is necessary for the specified purpose.
2. Broad government exemptions: Section 17 of the Act allows the Central Government to exempt any instrumentality of the State from its provisions, raising serious proportionality concerns.

4 RIGHTS AND OBLIGATIONS UNDER THE ACT

The Act establishes a rights-based framework that confers enforceable entitlements on data principals while imposing corresponding obligations on data fiduciaries. The core provisions governing data principal rights under sections 11–14 and fiduciary obligations under sections 5–8, alongside government exemptions under section 17 and legitimate uses under section 7 are discussed below.¹⁷

Data principal rights: The Act confers several rights on data principals, enforceable against all data fiduciaries processing their personal data. The primary four rights are as follows:

1. Right to access under section 11, DPDP Act: Upon request, data principals may obtain a summary of personal data being processed, processing activities undertaken such as collection methods, usage patterns, disclosures, etc., and identities of all data fiduciaries and processors with whom data was shared, along with descriptions of data shared, from the data fiduciary. Organizations must maintain their data processing inventories and implement mechanisms to respond to access requests within a reasonable timeframe. Failure to comply may attract penalties up to Rs. 50 crores under section 33 read with the Schedule. However, legacy systems and fragmented data storage across departments may complicate comprehensive access responses, particularly for large organizations with decentralised data infrastructures.

¹⁷ Centre for Applied Data Protection, *DPDP Act Key Provisions Explained: A Detailed Analysis* (CADP, 30 January 2026) <<https://cadp.in/resources/articles/dpdp-act-key-provisions-explained/>> accessed 5 September 2026

2. Right to correction and erasure under section 12, DPDP Act: Data principals may demand correction of inaccurate or misleading data, completion of incomplete data, updating of outdated data and erasure of personal data when the processing purpose is exhausted, which is also subject to statutory retention obligations under other general laws of the nation. Fiduciaries must establish data quality assurance processes and verify the accuracy of data before using it for decision-making or disclosing it to any third parties. For erasure requests, organizations must balance DPDP obligations against retention requirements under sectoral laws. However, the Act does not specify any timeline for correction or erasure compliance, creating uncertainty for organizations managing high-volume requests.
3. Right to grievance redressal under section 13, DPDP Act: Every data fiduciary must publish their contact details for grievance communication, respond to grievances within a period not exceeding 90 days (rule 14(3), DPDP Rules, 2025); a data principal who remains dissatisfied may then complain to the Data Protection Board, having first exhausted this remedy (section 13(3)). Organizations must designate a grievance officer and implement ticketing systems to track response timelines. Non-compliance may attract penalties up to Rs. 50 crores.
4. Right to nominate under section 14, DPDP Act: Data principals may nominate another individual to exercise their rights in the event of death or incapacity. This provision addressed the post-mortem privacy gap in the existing law, allowing a nominee to exercise the deceased or incapacitated data principal's rights under the Act, such as access, correction and erasure. Platforms must implement nomination mechanisms and verify nominee credentials before granting access.

Data fiduciary obligations: Data fiduciaries bear primary responsibility for compliance, irrespective of any agreement to the contrary or failure of the data principal to carry out duties. The primary obligations are as follows:¹⁸

1. Notice under section 5, DPDP Act: Before collecting personal data, fiduciaries must provide a clear, concise, accessible notice containing an itemised description of the personal data, the specified purpose of processing with a description of the goods, services or uses it enables, the means by which the data principal may withdraw consent and exercise her rights, and the manner in which she may complain to the Board (section 5(1) and rule 3). Privacy policies must be layered, available in multiple languages, and presented before consent is obtained. Pop-up notices, just-in-time prompts, and granular preference centres are recommended for digital platforms. Organizations with legacy data collected before the commencement of the Act must give each data principal a notice under section 5(2) as soon as it is reasonably practicable, and may continue processing until she withdraws her consent; fresh consent is not required.
2. Consent under section 6, DPDP Act: Consent must be free, specific, informed, unambiguous, and capable of withdrawal. Consent management platforms (CMPs) must enable granular consent (for example, separate toggles for marketing, analytics, third-party sharing) and one-click withdrawal. Pre-ticked boxes, dark patterns, and consent fatigue (excessive pop-ups) are non-compliant. Consent fatigue, user exhaustion from repeated consent requests, may lead to 'click-through' behaviour,

¹⁸ 'Compliance with DPDP Act' (Economic Times, 10 August 2026) <<https://economictimes.indiatimes.com/topic/compliance-with-dpdp-act>> accessed 5 September 2026

undermining the informed consent requirement. Mitigation strategies include layered notices, contextual consent (just-in-time prompts), and consolidated preference dashboards.

3. Legitimate uses without consent under section 7, DPDP Act: Processing is permitted without consent for narrow, specified purposes like the specified purpose for which the data principal has voluntarily provided her data; State subsidies, benefits, services, certificates, licences and permits; State functions under law and the sovereignty, integrity and security of India; disasters and breakdown of public order; compliance with orders, judgments, statutory obligations, life-threatening situations where consent cannot be obtained, and processing necessary for employment-related activities. However, the broad phrasing of ‘state functions’ and ‘public order’ raises concerns about potential overreach, particularly given the section 17 exemptions for government instrumentalities.
4. Accuracy and completeness under section 8(3), DPDP Act: Where personal data is likely to be used to make a decision that affects the data principal, or to be disclosed to another data fiduciary, the fiduciary must ensure its completeness, accuracy and consistency. Organizations must implement data validation checks at collection points and periodic audits to identify and correct inaccuracies. Automated decision-making systems (AI/ML models) must be trained on accurate, representative datasets to avoid discriminatory outcomes.
5. Security safeguards under section 8(5), DPDP Act: Fiduciaries must implement reasonable security safeguards (technical and organizational measures) to prevent unauthorised access, acquisition, disclosure, use, loss, destruction, or damage. The term ‘reasonable’ is not defined in the Act, but rule 6 of the DPDP Rules, 2025 prescribes the minimum safeguards: encryption, obfuscation, masking or tokenisation; access controls; logging and monitoring; data backups; one-year retention of logs; and security clauses in processor contracts. Minimum safeguards may include encryption (in transit and at rest), access controls (role-based permissions, multi-factor authentication), regular vulnerability assessments and penetration testing, and incident response plans and breach notification procedures.
6. Breach notification under section 8(6), DPDP Act: Upon discovering a personal data breach, fiduciaries must intimate the breach, without delay, to each affected data principal and to the Data Protection Board, and must give the Board a detailed report within 72 hours of becoming aware of it. Organizations must establish incident response playbooks integrating 6-hour reporting obligation under CERT-In with the 72-hour detailed report to the Board under rule 7(2)(b) of the DPDP Rules, 2025. The intimation must describe the breach (its nature, extent, timing and location), its likely impact and consequences, the mitigation measures taken, and the safety steps data principals can take. The 72-hour deadline may be insufficient for organizations to identify all affected principals, particularly in complex breaches involving multiple systems.
7. Retention limitation under section 8(7), DPDP Act: Personal data must be deleted when the processing purpose is exhausted, unless retention is required by law. Organizations must implement data lifecycle management policies with automated deletion triggers in cases of account closure or statutory retention period expiry. This provision does not conflict with the 180-day log retention mandate under CERT-In, because section 8(7) does not apply where retention is necessary for compliance with any law; rule 6(1)(e) of the DPDP Rules, 2025 itself requires logs to be kept for one year.

Government exemptions under section 17, DPDP Act: The Central Government may exempt any instrumentality of the State from the provisions of the Act in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, and preventing incitement to cognizable offence relating to the abovementioned. These exemptions extend to processing by the Central Government of personal data furnished by such instrumentalities. However, the broad, undefined terms risk enabling mass surveillance and data collection without adequate safeguards, potentially violating the three-fold proportionality test.

Legitimate uses by the State under section 7, DPDP Act: Processing is permitted without consent for state functions under law, including welfare delivery such as subsidies, pensions and healthcare, tax collection, law enforcement and crime prevention and national security and intelligence operations. However, these require paramount judicial oversight and the presence of independent authorization mechanisms aligning to proportionality concerns.

5 INSTITUTIONAL INFRASTRUCTURE AND ENFORCEABILITY

The Act establishes a centralised enforcement mechanism through the Data Protection Board of India, supported by a tiered penalty structure and appellate review.¹⁹

Data Protection Board of India (DPB): The DPB was established in Phase 1 as the primary adjudicating body for complaints, disputes, and penalty determination under section 18 of the Act. The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify under section 19(1). The Board adjudicates complaints from data principals regarding violation of the above discussed rights, breach notification failures by fiduciaries, security safeguard deficiencies, consent and notice violations and references from the Central Government or a State Government or on the direction of a court. For proper adjudication, the Board is vested with the power to summon parties and examine witnesses under oath, impose penalties up to Rs. 250 crores, direct cessation of processing activities, and issue binding directions (section 27(2)) and interim orders (section 28(10)).

However, as of July 2026, no appointment of a chairperson or members had been notified, and the Board was not yet operational. This raises serious concerns regarding enforcement capacity and adjudicatory timelines once complaints begin flowing starting Phase 3 in May 2027.

Penalty structure under section 33 and the Schedule, DPDP Act: The Act prescribes tiered penalties considering which the DPB must determine the penalties. The Board must have regard to the nature, gravity and duration of the breach, the type and nature of the personal data affected, the repetitive nature of the breach, whether the person realised a gain or avoided a loss, any mitigating action and its timeliness and effectiveness, whether the penalty is proportionate and effective, and the likely impact of the penalty on the person (section 33(2)).

TABLE 3. *Maximum penalties under the DPDP Act, 2023*

Violation	Maximum Penalty
Failure to maintain reasonable security safeguards (Section 8(5))	₹250 crore

¹⁹ Centre for Applied Data Protection, *DPDP Act 2023 Full Text — Interactive Reference* (CADP, 6 March 2026) <<https://cadp.in/resources/official-texts/dpdp-act-2023/>> accessed 5 September 2026

Violation	Maximum Penalty
Failure to notify data breach to DPB/principals (Section 8(6))	₹200 crore
Breach of the additional obligations in relation to children (Section 9)	₹200 crore
Breach of the additional obligations of a Significant Data Fiduciary (Section 10)	₹150 crore
Breach of any other provision, including notice and consent (Sections 5–6), data principal rights (Sections 11–14) and grievance redressal within 90 days (Section 13)	₹50 crore

The enforcement process includes a complaint by a data principal, an intimation of a personal data breach by the data fiduciary, a reference by the Central Government or a State Government, or a direction of a court (section 27(1)); the Act gives the Board no suo motu power. This is followed by inquiry and summary proceedings by the DPB. Thereafter, the DPB passes an adjudication order of penalty imposition and/or compliance directives. The order is appealable to the Appellate Tribunal, the Telecom Disputes Settlement and Appellate Tribunal, within sixty days from the date of receipt of the order under section 29 of the Act, and a further appeal lies to the Supreme Court. However, there still persist enforcement gaps as the DPB remains unstaffed which creates uncertainty about operational readiness. Delays in appointments may result in a compliance backlog and undermine deterrence.

6 CYBERSECURITY COMPLIANCES UNDER CERT-IN DIRECTIONS, 2022

Parallel to the DPDP Act, the Indian Computer Emergency Response Team (CERT-In) issued directions under section 70B of the Information Technology Act, 2000 on 28th April 2022, effective from 28th June 2022, imposing stringent cybersecurity obligations on organizations operating in India. Non-compliance with the CERT-In directions is punishable under section 70B (7) of the IT Act, 2000, with imprisonment up to 1 year, or fine up to Rs. 1 crore, or both.²⁰

TABLE 4. *Principal obligations under the CERT-In Directions, 2022*

OBLIGATION	REQUIREMENT	APPLICABILITY
6-Hour Incident Reporting	Report specified cyber incidents to CERT-In within 6 hours of detection	Service providers, intermediaries, data centres, body corporates, government organizations.
180-Day Log Retention	Maintain logs of all ICT systems for a rolling 180-day period within India	All covered entities.
NTP Synchronisation	Synchronise clocks to NIC/NPL time sources (National Informatics Centre / National Physical Laboratory)	All covered entities.

²⁰ Indian Computer Emergency Response Team, *Directions under Section 70B(6) of the Information Technology Act, 2000* (Gazette of India, 28 April 2022)

OBLIGATION	REQUIREMENT	APPLICABILITY
5-Year Subscriber Data Retention	Data centres, VPS, cloud and VPN service providers must keep validated subscriber registration details for 5 years after the registration ends; virtual asset service providers, exchanges and custodian wallet providers must keep KYC records and financial transaction records for 5 years	Data centres, VPS, cloud and VPN providers; virtual asset service providers, exchanges and custodian wallet providers.

Annexure I provides for twenty categories of reportable incidents which include malware, ransomware, phishing attacks, unauthorized access, data breaches, DDoS attacks, website defacement, cryptojacking, IoT compromises, critical infrastructure incidents and so on.

The reporting mechanism undertakes a contact-based system where reports must be filed with CERT-In (<https://www.cert-in.org.in/> - contacts include their email: incident@cert-in.org.in).

7 OVERLAP AND TENSION: DPDP ACT VERSUS CERT-IN DIRECTIONS

Organizations operating in India face parallel compliance obligations under DPDP Act and CERT-In Directions, creating overlaps, tensions, and operational complexities.²¹

Dual breach notification duties: A practical compliance strategy is required. This may be presented as:

1. 0–6 hours: Immediate triage, assess incident scope, report to CERT-In;
2. 6–72 hours: Investigate breach, identify affected principals, intimate the DPB and each affected data principal without delay, and prepare the detailed report to the DPB;
3. Within 72 hours: Submit the detailed breach report to the DPB.

However, the 6-hour CERT-In deadline may precede full breach investigation, requiring organizations to report with incomplete information and submit supplementary updates later.

Log retention conflict: Organizations must retain logs for 180 days minimum under CERT-In Directions, even if the DPDP purpose is exhausted earlier, unless a specific DPDP exemption applies (for example, retention necessary for compliance with law under section 8(7)). This creates a statutory override scenario where sectoral mandate under CERT-In prevails over general retention limit under DPDP Act. Practical mitigation may include implementation of segregated log storage with access controls, ensuring logs are retained for 180 days but not used for unrelated processing purposes (for example, profiling, marketing, etc.).

NTP Synchronisation and Data Accuracy: NTP synchronisation requirement under CERT-In (clocks must align with NIC/NPL time sources) supports accuracy obligation under section 8(3), DPDP Act by ensuring timestamps on data processing activities are reliable and auditable. This alignment reduces compliance friction.

Subscriber Data Retention (VPN/Cloud Providers): 5-year subscriber data retention mandate under CERT-In for VPN providers and cloud services conflicts with purpose-based retention limit under section 8(7), DPDP Act. However, the same VPN/cloud providers must keep validated subscriber registration details for 5 years under CERT-In, and section 8(7), DPDP Act, permits retention necessary for

²¹ TCSA, *CERT-In Directions & ISO 27001: The 6-Hour Mapping* (11 July 2026) <<https://www.tcsa.in/frameworks/iso-27001/for-cert-in>> accessed 5 September 2026

compliance with any law for the time being in force, exempting such processing from the general retention limit.

Suggested integrated Compliance Framework: Organizations, thus, should adopt an integrated cybersecurity and data protection compliance framework which may include a unified incident response playbook addressing both CERT-In (6-hour) and DPDP (72-hour) reporting, data mapping inventory identifying which data categories trigger CERT-In vs. DPDP obligations, retention schedules reconciling 180-day/5-year mandates under CERT-In with purpose-based limits under DPDP Act, and vendor contracts ensuring processors comply with both regimes (for example, cloud providers keeping subscriber registration details for 5 years while implementing DPDP security safeguards).

8 CROSS-BORDER TRANSFER AND EMERGING CHALLENGES

Cross-Border data transfers: Under Section 16 of the DPDP Act, personal data may be transferred to any country or territory outside India except one that the Central Government restricts by notification; section 16(2) preserves any other law that provides a higher degree of protection or restriction, and rule 15 of the DPDP Rules, 2025 subjects transfers to such requirements as the Central Government may, by general or special order, specify for making personal data available to a foreign State or to any person or entity under the control of, or any agency of, such a State. As of July 2026, the Central Government has not notified any restricted country or territory. Until notifications are issued organizations may transfer data subject to reasonable security safeguards under section 8(5), DPDP Act and contractual protections (data processing agreements, standard contractual clauses), transfers should be purpose-specific and documented in privacy notices under section 5, DPDP Act, and sensitive data categories like health, financial, and biometric should be transferred with heightened caution until the Government's position on them is clear. Various industry expectations and speculations suggest the government will leave transfers to jurisdictions such as the European Union member states, the United Kingdom, Singapore and Japan unrestricted, while restricting transfers to countries with weak data protection regimes or mass surveillance laws. Multinational organizations are suggested to closely monitor MeitY notifications and prepare for potential data localisation requirements for critical sectors like healthcare, banking, telecom, and so on.

Emerging compliance challenges: Some of the legal impediments and implications concerning the compliances are discussed below:

1. **Consent fatigue:** Users face repeated consent requests from multiple platforms, leading to 'click-through' behaviour that undermines the informed consent requirement under section 6, DPDP Act. This may be mitigated by layered notices, just-in-time consent prompts, consolidated preference dashboards, and granular toggles like separate consent for marketing, analytics, third-party sharing.
2. **Legacy data and purpose limitation:** Organizations hold historical data collected for broad or undefined purposes, which may not meet the requirement that personal data be processed for a lawful purpose (section 4) stated in the notice as the specified purpose (sections 5 and 2(za)), DPDP Act. This may be mitigated by data mapping exercises, purpose re-justification documentation, deletion of obsolete records, re-consent campaigns for active users.
3. **Artificial Intelligence training and automated processing:** The DPDP Act does not explicitly address AI/ML model training on personal data. Processing for AI training may exceed original consent purposes, triggering fresh consent or legitimate use requirements. However, the risk includes

automated decision-making like credit scoring, hiring, insurance underwriting, which must comply with section 8(3), DPDP Act, (completeness, accuracy and consistency), requiring organizations to audit AI models for bias and ensure explainability.

4. SME and startup burden: Smaller entities lack resources for data protection officers, audits, impact assessments (once SDF rules are notified), and legal compliance teams. This may be mitigated by shared compliance services (third-party DPOs), regulatory sandboxes, government guidance documents, industry associations providing template policies and contracts.
5. Reporting tensions between CERT-In Directions and DPDP Act: The 6-hour CERT-In deadline conflicts with the need to identify affected principals for DPDP intimation without delay and for the detailed report to the DPB within 72 hours. The best practice is to maintain incident response playbooks with parallel reporting tracks, pre-drafted notification templates, and escalation matrices ensuring both deadlines are met.

9 CONCLUSION

The Digital Personal Data Protection Act, 2023, read with the DPDP Rules, 2025 and CERT-In Directions, 2022, establishes a comprehensive, risk-based, and enforceable data protection regime in India. The Act operationalises the three-fold proportionality test, established in the famous Justice K.S. Puttaswamy (Retd.) vs. Union of India, interpreting constitutional right to privacy into a statutory obligation for data fiduciaries and enforceable entitlements for data principals.

However, given the present scenario of the implementation, organizations might face a complex compliance landscape characterized by overlapping mandates like that of DPDP breach notification versus CERT-In incident reporting, conflicting retention requirements like 180-day logs versus purpose-based deletion, and evolving enforcement capacity like the non-functional Data Protection Board. The phased implementation schedule provides a calibrated timeline for alignment, but the firm deadlines and substantial penalties, up to ₹250 crore, demand immediate action.

Critical challenges still persist: consent fatigue undermining informed consent, legacy data requiring purpose re-justification, AI training on personal data without explicit statutory guidance, and SME resource constraints in meeting compliance obligations. Furthermore, the broad government exemptions under Section 17 risk violating the proportionality requirement unless accompanied by robust parliamentary oversight and judicial review.

However, the era of accountability for data fiduciaries has begun. As the Data Protection Board becomes fully operational and penalties take effect, organizations must prioritise data mapping, notice revision, consent mechanisms, security audits, and integrated incident response frameworks to achieve compliance. The established three-fold proportionality test remains the constitutional touchstone for balancing individual autonomy with legitimate state and commercial interests, ensuring that India's data protection framework evolves in harmony with technological innovation and fundamental rights.