INTERNATIONAL JOURNAL OF JURIDICAL SCIENCE AND POLICY (IJJSP)

VOL. 1 · ISSUE 1 · 2026

EDITOR IN CHIEF

Mr. Ashish Kaushik

CENTRE FOR JURIDICAL SCIENCE AND POLICY RESEARCH

VOL. 1 — ISSUE 1

The Digital Personal Data Protection Act, 2023: India's Emerging Paradigm for Data Privacy

Tripti Sharma, LL.B.2nd Year, Institute of Legal Studies, Ch. Charan Singh university, Merut, U.P., India.[1]

ABSTRACT

In the contemporary digital ecosystem, the exponential growth of data-driven technologies, digital identity systems, and online platforms has intensified concerns surrounding data privacy, protection frameworks, and responsible surveillance. India, as one of the world's largest digital societies, has witnessed unprecedented expansion in digital governance, financial technologies, healthcare digitisation, and social media usage, all of which involve large-scale collection, processing, and storage of personal data. policy challenge. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in India's data protection journey, seeking to establish a comprehensive framework governing the processing of digital personal data. The Act introduces key principles such as consent-based data processing, purpose limitation, data minimisation, and accountability of data fiduciaries, while also recognising the rights and duties of data principals. At the same time, it creates institutional mechanisms such as the Data Protection Board of India to oversee compliance and adjudicate disputes. While the DPDP Act represents a progressive step towards aligning India's data protection regime with global standards, it also raises important questions regarding implementation, enforcement capacity, exemptions granted to the State, and the adequacy of safeguards against excessive surveillance.

This article critically examines India's evolving data privacy and protection frameworks within the broader cyber security landscape, with particular emphasis on digital identity systems and responsible surveillance. It analyses how large-scale digital identity

[1] Tripti Sharma, LL.B.2nd Year, Institute of Legal Studies, Ch. Charan Singh university,Meerut.

Initiatives and data-intensive governance models, while enhancing efficiency and service delivery, also amplify risks of data breaches, profiling, function creep, and misuse of personal information. The study evaluates whether the DPDP Act, 2023 sufficiently addresses these risks, especially in relation to government access to data, cross-border data transfers, and proportionality in surveillance practices.

Further, the article situates India's data protection framework in a comparative perspective, drawing insights from international data protection regimes such as the EU's General Data Protection Regulation (GDPR), to assess the strengths and limitations of the Indian approach. Special attention is paid to the concept of responsible surveillance, examining the constitutional principles of privacy, necessity, and proportionality as articulated by Indian courts, and their practical application in the digital era. The research also highlights challenges faced by enforcement agencies, private entities, and individuals in navigating compliance obligations under the DPDP Act amid rapid technological advancements and increasing cyber security threats.

Keywords: Data Privacy, Digital Personal Data Protection Act, 2023, Data Protection Board of India, General Data Protection Regulation (GDPR)

Introduction

The unprecedented growth of digital technologies has fundamentally transformed the manner in which personal information is generated, collected, processed, and utilized across various sectors of society[1]. In an increasingly interconnected world, data has become a valuable economic and strategic resource that supports innovation, facilitates public administration, and drives digital commerce. However, the extensive use of personal information by governments, corporations, and digital platforms has simultaneously intensified concerns relating to privacy violations, unauthorized surveillance, data breaches, and the misuse of sensitive information. [2] These developments have underscored the necessity of establishing a comprehensive legal

[1] World Econ. Forum, Personal Data: The Emergence of a New Asset Class (2011).
[2] Daniel J. Solove, Understanding Privacy (2008).

framework capable of balancing technological advancement with the protection of individual rights.

The evolution of data protection law in India is closely linked to the constitutional recognition of privacy as a fundamental right[3]. A significant turning point occurred with the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, wherein a nine-judge bench affirmed that the right to privacy forms an integral part of the right to life and personal liberty guaranteed under Article 21 of the Constitution[4].The judgment emphasized the importance of informational privacy in the digital era and highlighted the State's obligation to create an effective legal regime for safeguarding personal data[5]. In the aftermath of this decision, the Government of India constituted the Justice B.N. Srikrishna Committee to formulate recommendations for a dedicated data protection framework, thereby initiating a new phase in India's privacy jurisprudence and regulatory development[6].

India's legislative efforts toward data protection have undergone considerable evolution over the past decade. The Personal Data Protection Bill, 2019 represented the first major attempt to establish a comprehensive statutory regime governing the processing of personal data. Nevertheless, the proposed legislation attracted substantial criticism from legal scholars, industry stakeholders, and civil society organizations due to concerns regarding extensive governmental exemptions, stringent data localisation requirements, and the perceived inadequacy of safeguards against potential infringements of privacy rights[7]. Following prolonged consultations and deliberations, the Bill was withdrawn, paving the way for a revised legislative approach that ultimately resulted in the enactment of the Digital Personal Data Protection Act, 2023[8].

[3] Kharak Singh v. State of U.P., AIR 1963 SC 1295 (India); Gobind v. State of M.P., (1975) 2 SCC 148 (India).
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[5] R. Rajagopal v. State of T.N., (1994) 6 SCC 632 (India).
[6] Comm. of Experts Under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
[7] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
[8] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

The Digital Personal Data Protection Act, 2023 constitutes India's first comprehensive legislation exclusively dedicated to the protection of digital personal data. The Act seeks to establish a regulatory framework that reconciles the protection of individual privacy with the legitimate demands of a rapidly expanding digital economy [9] .It introduces obligations for data fiduciaries, recognises a range of rights available to data principals, and adopts a consent-oriented model for the processing of personal information. Additionally, the legislation provides for the establishment of the Data Protection Board of India, which is entrusted with the responsibility of ensuring compliance and addressing violations under the statutory framework. Through these mechanisms, the Act aims to promote transparency, accountability, and trust in the digital ecosystem.

Despite being regarded as a significant step in India's data governance landscape, the DPDP Act has generated extensive debate concerning its scope and effectiveness. Critics have questioned whether the legislation provides sufficient safeguards against excessive governmental access to personal information, adequately regulates cross-border data transfers, and effectively protects individuals in the absence of a distinct category for sensitive personal data [10] . Furthermore, concerns have been expressed regarding the independence of enforcement mechanisms and the broader implications of the Act for informational privacy in a data-driven society. Against this backdrop, the present study undertakes a critical examination of the DPDP Act, 2023, evaluates its alignment with international standards such as the GDPR, and explores the reforms necessary to strengthen India's evolving data protection regime while supporting innovation and economic development[11].

Core Framework of the DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act of 2023 marks a revolutionary shift in India's legislative landscape, establishing seven core pillars that dictate how digital

[9] Id.
[10] Graham Greenleaf, *India's Digital Personal Data Protection Act 2023: A Critical Assessment*, 179 Privacy Laws & Bus. Int'l Rep. 1 (2023).
[11] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

information must be governed. The overarching objective of this statutory framework is to strike a delicate, sustainable equilibrium: it guarantees the fundamental right of citizens to secure their personal information while simultaneously providing a structured, legal pathway for corporate enterprises and state agencies to process data to foster economic development and technological innovation.[12]

Essential Principles of Data Governance

Consent, Legality, and Openness: Under this principle, data fiduciaries are strictly prohibited from gathering, storing, or processing any information without obtaining the explicit, unambiguous, and informed permission of the user. Organizations must abandon vague, complex legal jargon and instead communicate their intent in a highly clear, transparent, and accessible manner, ensuring that the individual is fully aware of how their information will be utilized[13]. Purpose Specification: This tenet mandates that any personal metrics collected by an organization can only be utilized for the precise, explicit reason for which it was initially acquired. Should an entity wish to repurpose this information for secondary commercial ventures, marketing campaigns, or algorithmic training, they are legally bound to re-engage the user and secure a fresh round of authorization[14]. Data Minimization (Parsimony): To mitigate the severe societal risks associated with corporate data hoarding, this principle dictates that enterprises must limit their collection activities to the bare minimum amount of information required to execute a specific service. By preventing companies from aggregating superfluous user statistics, the law inherently reduces the scale and impact of potential security failures[15]. Precision and Maintenance: It is the affirmative duty of data fiduciaries to ensure that all user profiles in their custody are kept accurate, comprehensive, and up-to-date. This requirement is particularly critical in high-stakes environments such as banking,

[12] The Digital Personal Data Protection Act, 2023, Preamble, No. 22, Acts of Parliament, 2023 (India).
[13] *Id.* § 6.
[14] *Id.* § 7(1).
[15] *Id.* §§ 4(1), 6(1).

consumer finance, and healthcare, where a single clerical error or outdated record could result in catastrophic financial losses or flawed medical treatments for the individual[16].

Temporal Storage Constraints: This principle establishes that data fiduciaries do not have a perpetual right to hold onto consumer records. Once the underlying objective or contractual obligation that justified the initial data collection has been fully satisfied, the organization must systematically and permanently purge that data from its servers, thereby reducing the digital attack surface available to malicious actors[17]. The legislation obligates data processors to implement institutional defenses and cutting-edge cyber security protocols. This includes deploying advanced encryption standards, multi-factor authentication, and rigorous access controls to fortify internal infrastructure against sophisticated cyber-attacks and unauthorized corporate espionage [18] . Enforcement, Oversight, and Liability: To ensure these rules are not merely performative, the Act establishes a rigorous system of corporate liability. Entities must maintain verifiable records of compliance and are held legally answerable for any operational oversights. The Data Protection Board of India (DPBI) operates as the central regulatory watchdog, armed with the statutory power to investigate compliance failures, adjudicate grievances, and hand down substantial financial penalties to violators.[19]

Legal Scope and Jurisdiction

The DPDP Act delineates an extensive, highly modern regulatory boundary designed to address the realities of a borderless digital economy. It explicitly outlines who is bound by these laws and how far India's regulatory arm extends in protecting its citizenry[20]. The jurisdiction of the legislation covers all forms of personal data that are either natively

[16] *Id.* § 8(3).
[17] *Id.* § 8(7).
[18] *Id.* § 8(5).
[19] *Id.* § 19.
[20] *Id.* § 3.

generated in a digital format within Indian borders or initially collected via traditional physical methods and subsequently migrated into digital databases[21].

Crucially, the lawmakers incorporated a robust clause regarding extra-territorial applicability. This means that even if an enterprise operates entirely outside the geographic boundaries of India and processes data on foreign servers, it remains fully subject to the strictures of the DPDP Act if it deals with the personal information of individuals residing in India in connection with offering them commercial products, digital applications, or localized services.

This cross-border enforcement mechanism mirrors international gold standards, most notably the European Union's General Data Protection Regulation (GDPR), preventing foreign tech conglomerates from bypassing domestic privacy laws.[22]

At the heart of this legislation is the Data Principal the individual citizen whose personal attributes and behaviors are being tracked. The Act introduces a suite of enforceable statutory rights designed to return digital autonomy to the consumer.Right to Complete Transparency: Individuals possess the legal authority to demand comprehensive summaries from fiduciaries[23] detailing exactly what elements of their personal data are being retained, how those data points are being manipulated, and which third-party entities have been granted access to them[24]. Right to Correction, Updating, and Erasure: If a consumer identifies errors, omissions, or outdated facts within their corporate profile, they have the right to compel the data fiduciary to rectify the records immediately[25]. Furthermore, users can demand the complete deletion of their digital footprint if the initial operational necessity for retaining that information has elapsed. [26]Right to Legal Representation and Continuity: Recognizing the vulnerabilities associated with unexpected life events, the Act allows individuals to formally designate a trusted

[21] *Id.* § 3(a).
[22] *Id.* § 3(b); *see also* GDPR, *supra* note 11, pmbl.
[23] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 297 (India).
[24] The Digital Personal Data Protection Act, 2023, § 11, No. 22, Acts of Parliament, 2023 (India).
[25] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317; X v. Registrar General, High Court of Karnataka, 2021 SCC OnLine Kar 424 (India).
[26] The Digital Personal Data Protection Act, 2023, § 12, No. 22, Acts of Parliament, 2023 (India).

nominee. In the event of the data principal's death, mental incapacity, or physical limitation, this chosen representative can step in to exercise, manage, and defend their privacy rights, ensuring continuous data protection[27].Right to Grievance Redressal and Escalation: If a user suspects that their personal records have been mismanaged, leaked, or processed in defiance of the law, they are entitled to launch an official complaint directly through the fiduciary's internal resolution channels. If the corporation fails to provide a satisfactory remedy within a reasonable timeframe, the citizen can escalate the dispute to the DPBI for formal regulatory arbitration.[28]

Mandates for Data Fiduciaries

Conversely, any corporate, governmental, or non-profit entity that determines the purpose and means of data processing defined under the law as a Data Fiduciary is bound by a stringent set of operational obligations[29].

Systemic Integrity and Safeguards: Fiduciaries must actively design their data pipelines with privacy in mind. They are required to construct durable technical and organizational firewalls to eliminate the possibilities of accidental exposure, rogue insider access, or external data harvesting[30].

Mandatory Security Breach Notification: In the unfortunate event of a system compromise or data leak, fiduciaries no longer have the luxury of concealing the incident to protect their brand reputation. They are legally mandated to immediately report the precise nature of the security failure to both the DPBI and the specific individuals, whose privacy has been compromised, allowing victims to take swift countermeasures[31].

Automated Data Deletion Routines: To remain compliant with storage limitations, companies must establish automated system protocols to expunge consumer records the

[27] *Id.* § 14.
[28] *Id.* § 13.
[29] *Id.* ch. II.
[30] *Id.* § 8(1).
[31] *Id.* § 8(6).

moment the specific transactional or service-oriented purpose of that data has concluded, neutralizing the threat of long-term data exploitation. [32]

Role of the Data Protection Board of India (DPBI)

The statutory enforcement mechanism of the DPDP framework centers heavily upon the Data Protection Board of India (DPBI), which operates as the principal supervisory authority responsible for compelling administrative compliance among information custodians[33].This regulatory body is legally empowered to oversee operational standards, resolve institutional conflicts, and levy financial penalties against any entity found acting in defiance of the established data privacy rules[34].To achieve this, the Board possesses wide-ranging administrative powers to launch inquiries into reported infractions, compel disclosure from non-compliant organizations, and issue legally binding executive mandates[35].

A definitive characteristic of this oversight body is its quasi-judicial status, which legally equips it to arbitrate formal disputes arising between private citizens and processing corporations over alleged privacy violations[36].Furthermore, the legislative architecture incorporates a robust system of administrative checks and balances: if an affected individual or a penalized data fiduciary seeks to challenge an adverse ruling or decree handed down by the DPBI, they have the statutory right to appeal the decision before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) [37] . This specialized appellate tier guarantees judicial oversight, ensures procedural fairness, and reinforces institutional liability across the entire regulatory landscape[38].

Statutory Protections Safeguarding Juvenile Privacy

Acknowledging the acute vulnerabilities associated with the processing of minors' digital

[32] *Id.* § 8(7)(b).
[33] *Id.* § 18.
[34] *Id.* §§ 27–28.
[35] *Id.* § 28.
[36] *Id.* § 27(1).
[37] *Id.* § 29(1).
[38] *Id.* § 29.

footprints, the Indian legislative framework institutes stringent safeguards specifically designed to protect underage users [39] .Under these mandates, data fiduciaries face an absolute statutory prohibition against executing behavioral tracking, targeted profile monitoring, or consumer-directed advertisement tailored toward individuals below eighteen years of age[40].This uncompromising regulatory threshold represents a sharp divergence from dominant transnational paradigms, most notably the European Union's GDPR, which delegates autonomy to its member states to lower the operational age of digital consent to anywhere between thirteen and sixteen years[41].

While the enforcement of an absolute eighteen-year age ceiling reflects a highly paternalistic and rigorous approach to shielding youth from digital exploitation, it simultaneously introduces systemic compliance frictions for digital enterprises. Corporate entities catering to younger cohorts face extensive operational overheads in implementing robust age-verification mechanisms.[42] Furthermore, this comprehensive prohibition on customized content delivery presents a dual-edged reality: while it successfully insulates minors from predatory tracking practices, it inherently restricts their access to specialized, age-appropriate educational tools, localized applications, and digital services meticulously calibrated to their developmental requirements.

Regulatory Approach to Cross-Border Data Mobility

The jurisdictional parameters governing the outbound transmission of personal information represent one of the most heavily litigated features of the DPDP framework [43] . The final text of the statute establishes a permissive negative-list or blacklisting mechanism, allowing the unrestricted flow of digital personal assets overseas to all jurisdictions, except those explicitly restricted by Central Government notifications. This reflects a substantial shift away from the rigid local data storage (data localization) mandates championed in prior legislative iterations.

[39] *Id.* § 9.
[40] *Id.*; *id.* § 9(2).
[41] GDPR, *supra* note 11, art. 8(1).
[42] The Digital Personal Data Protection Act, 2023, § 9(1), No. 22, Acts of Parliament, 2023 (India).
[43] *Id.* § 16.

While this architectural choice accommodates the functional realities of multinational enterprises, it has drawn sharp academic criticism for omitting structural data protection guarantees [44] . Unlike the European Union's framework which mandates institutional adequacy determinations, standard contractual clauses, or binding corporate rules before data can leave the continent the Indian model relies purely on executive decrees[45]. This approach leaves a distinct legal vacuum regarding the precise criteria the state will deploy to gauge whether an overseas territory provides a reciprocal level of data security.

Categorical Exemptions and State Surveillance Power

The statutory framework carves out extensive legislative immunities for specific classes of information processing, generating intense constitutional debate regarding the erosion of the fundamental right to privacy[46].Chief among these are the expansive powers granted to state instruments and sovereign agencies under the banners of national security, maintenance of public order, and criminal investigation [47] . When invoked, these provisions allow the state apparatus to completely bypass key data privacy compliance duties, effectively immunizing government surveillance programs and administrative data aggregation from the requirement of individual consent[48]

Beyond sovereign exceptions, the statute provides specialized carve-outs for academic research, historical archival preservation, and active judicial or legal proceedings, ensuring that the strictures of data parsimony do not paralyze essential public interest or legal functions[49].Nevertheless, the lack of robust external check-and-balance protocols within these exemption clauses raises serious administrative law concerns, creating an environment susceptible to unmonitored state profiling and a structural deficit in institutional accountability[50].

[44] Lok Sabha Secretariat, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (2021).
[45] GDPR, *supra* note 11, arts. 45–47.
[46] The Digital Personal Data Protection Act, 2023, § 17, No. 22, Acts of Parliament, 2023 (India).
[47] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India).
[48] *Id.* § 17(2).
[49] *Id.* § 17(2).
[50] *Id.* §§ 17(1)(b)–(c); Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

Recent concerns regarding the deployment of sophisticated surveillance technologies have further intensified the debate on the need for judicial oversight and transparency in State surveillance practices. In *Manohar Lal Sharma v. Union of India* (Pegasus case), the Supreme Court underscored that national security cannot be invoked as a blanket justification to avoid judicial scrutiny and constituted an independent technical committee to investigate allegations of unlawful surveillance.

The decision reaffirmed the importance of balancing legitimate security interests with the constitutional protection of privacy and civil liberties[51].

[51] Manohar Lal Sharma v. Union of India, 2021 SCC OnLine SC 985 (India).

Comparison of the Digital Personal Data Protection (DPDP) Act, 2023, with the General Data Protection Regulation (GDPR)

The structural architecture of India's Digital Personal Data Protection (DPDP) Act of 2023 and the European Union's General Data Protection Regulation (GDPR) share a unified conceptual core: both statutory regimes are engineered to govern the systemic lifecycle of personal data, fortify individual privacy protocols, and institutionalize rigorous liability structures for corporate fiduciaries and information processors[52].

Nonetheless, despite their shared teleological objectives, these two landmark legal instruments exhibit profound doctrinal divergences across multiple critical vectors. Specifically, they split significantly regarding their absolute jurisdictional reach, statutory taxonomies and definitions, the spectrum of entitlements vested in individual data owners, corporate compliance thresholds, emergency security leak reporting windows, cross-border data mobility paradigms, and administrative penalty enforcement mechanisms [53] . The subsequent analysis delineates a highly detailed, systematic evaluation of these core structural friction points and operational symmetries.

1) Cross-Border Data Transfers and Territorial Jurisdiction

The material application of the European Union's framework encompasses the systemic management of personal datasets irrespective of the physical medium utilized; it explicitly blankets any operation executed via automated mechanisms or arranged within a systematic manual indexing structure[54]. Consequently, conventional physical documents and paper filing registries are fully bound by the GDPR, provided they are structured logically[55].

---

[52] The Digital Personal Data Protection Act, 2023, Preamble, No. 22, Acts of Parliament, 2023 (India); *see also* GDPR, *supra* note 11, pmbl.
[53] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); *comparing* GDPR, *supra* note 11.
[54] GDPR, *supra* note 11.
[55] *Id.* art. 2(1); Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650; Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559.

Conversely, the DPDP Act institutes a much narrower material scope, confining its sovereign authority exclusively to digital information assets[56]. The Indian statute governs only two specific vectors: data born digitally at the phase of collection, or offline information that is subsequently converted into a digital format [57] . As a direct consequence of this deliberate legislative limitation, purely legacy paper records that avoid digitalization remain entirely immune to the obligations of the DPDP framework.

Furthermore, their extra-territorial matrices reflect a distinct imbalance in global enforcement. The GDPR asserts an expansive territorial web, binding any corporate processor worldwide if their tracking activities or processing workflows target data subjects located inside the European Union[58]. While the DPDP Act similarly projects its authority beyond domestic borders, it activates this extra-territorial arm under a more restrictive condition: the foreign processing operations must be explicitly linked to the marketplace distribution of products or localized commercial services to consumers inside Indian Territory[59].

2) Comparative Age Thresholds for Digital Autonomy

The two statutory models diverge sharply on the precise developmental milestone at which a young citizen can independently navigate the digital economy. The GDPR institutes a baseline ceiling of sixteen years as the default age of digital capacity, while simultaneously delegating sovereign flexibility to individual European member states to lower this operational boundary down to a minimum of thirteen years via domestic legislation[60]. This decentralization enables European jurisdictions to calibrate digital consent barriers to their distinct cultural and educational realities.

In stark contrast, the DPDP Act rejects any variable scale or regional flexibility, codifying a rigid, uniform standard that designates all individuals under eighteen years of

[56] The Digital Personal Data Protection Act, 2023, § 3, No. 22, Acts of Parliament, 2023 (India).
[57] *Id.* § 3(a).
[58] GDPR, *supra* note 11, art. 3(2).
[59] The Digital Personal Data Protection Act, 2023, § 3(b), No. 22, Acts of Parliament, 2023 (India).
[60] GDPR, *supra* note 11, art. 8(1).

age as minors [61] . Under this rule, processing and data belonging to an adolescent necessitates the mandatory prior authorization of a parent or legal guardian[62]. While this protective stance harmonizes with India's domestic juvenile justice and child safety laws, it presents acute operational friction in practice, effectively paralyzing the ability of teenagers to independently utilize vital digital spaces, educational networks, and modern online applications that mandate basic profile creation[63].

3) **Crisis Notification Mandates**

Under the European framework, data controllers must report any security leak to the designated supervisory authority within a strict seventy-two-hour window upon detection [64].Furthermore, if the compromise introduces a severe threat to individual liberties, the affected consumers must be notified immediately [65] .In contrast, the Indian statute lacks a specified, mathematically fixed timeframe for fiduciaries to report a breach to the Data Protection Board of India (DPBI), creating structural ambiguities that could delay mitigation efforts[66].

4) **Spectrum of Enforceable Rights**

While both regimes empower individuals, their statutory entitlements differ. The GDPR grants data subjects the rights of access, rectification, erasure (the Right to be forgotten), processing restriction, and data portability [67] .The DPDP Act provides similar guarantees to data principals including transparency, modification, deletion, and dispute resolution but entirely omits the right to data portability, meaning users cannot compel a company to transfer their profile to a competitor[68].

However, the DPDP Act introduces a unique right to designate a nominee to manage digital assets in the event of user death or mental incapacity a feature missing from the

[61] The Digital Personal Data Protection Act, 2023, § 9, No. 22, Acts of Parliament, 2023 (India).
[62] *Id.* § 9(1).
[63] *Id.* § 9.
[64] GDPR, *supra* note 11, art. 33(1).
[65] *Id.* art. 34(1).
[66] The Digital Personal Data Protection Act, 2023, § 8(6), No. 22, Acts of Parliament, 2023 (India).
[67] GDPR, *supra* note 11, arts. 15–20.
[68] The Digital Personal Data Protection Act, 2023, ch. III, No. 22, Acts of Parliament, 2023 (India).

European law[69]. Lastly, while the GDPR forces corporate entities to fulfill user requests within a strict thirty-day window, the DPDP Act leaves response timelines unquantified, creating risks of administrative delay[70].

5) Comparative Mechanisms for Global Data Transfers

The European Union's framework mandates a highly structured, legalistic protocol for the outbound migration of personal data to external nations, guaranteeing that exported profiles maintain an equivalent baseline of security [71] . This objective is accomplished through three distinct statutory instruments: formal adequacy determinations issued by the European Commission, standard contractual clauses embedded within commercial agreements, and binding corporate rules adopted internally by multinational enterprises[72].

Conversely, the DPDP Act rejects this multi-tiered, compliance-heavy matrix[73]. Instead, it implements a permissive model that allows outbound data mobility by default to all international territories, except those explicitly restricted via a government-notified negative list[74]. Consequently, rather than compelling corporate entities to independently integrate rigorous contractual or structural safeguards, the Indian framework shifts the regulatory burden entirely onto state-level executive decrees. This shift creates a more volatile cross-border data environment, where operational permissions are susceptible to geopolitical shifts and strategic bilateral considerations[75]

6) Rules for Appointing a Data Protection Officer (DPO)

The GDPR institutes an expansive enforcement model, requiring both data controllers and data processors to formally designate a Data Protection Officer (DPO) under specific conditions[76].These triggers include the systematic, large-scale monitoring of individual

[69] *Id.* § 14.
[70] GDPR, *supra* note 11, art. 12(3).
[71] *Id.* ch. V.
[72] *Id.* arts. 45–47.
[73] The Digital Personal Data Protection Act, 2023, § 16, No. 22, Acts of Parliament, 2023 (India).
[74] *Id.* § 16(1).
[75] Srikrishna Committee Report, *supra* note 6.
[76] GDPR, *supra* note 11, art. 4.

behaviors or the intensive processing of special categories of sensitive information[77]. Within this European paradigm, the DPO serves as an independent statutory anchor, acting as the primary liaison for supervisory authorities and ensuring baseline compliance across all internal operational workflows.

In absolute contrast, the DPDP Act introduces a highly selective, tiered approach, restricting the mandatory appointment of a Data Protection Officer exclusively to entities categorized as Significant Data Fiduciaries (SDFs)[78].This special status is determined by executive discretion based on factors like data volume, potential risks to state sovereignty, and societal impact [79] . Consequently, ordinary data fiduciaries face no statutory obligation to establish a dedicated DPO position[80]. This legislative carve-out draws scrutiny for potentially weakening internal oversight mechanisms and compliance accountability across a vast majority of mid-sized commercial organizations.

7) Statutory Mandates for Documenting Data Activities

The GDPR establishes a rigorous administrative standard by mandating that both data controllers and data processors maintain comprehensive documentation of their information-handling activities[81]. These systemic logs serve as an essential auditing tool, allowing supervisory authorities to evaluate institutional compliance, trace operational workflows, and investigate potential data protection infractions [82] . By forcing companies to log their internal data movements, the European framework creates a high baseline of structural transparency.

In sharp contrast, the DPDP Act does not impose any equivalent legal obligation on regular data fiduciaries to maintain continuous records of their processing operations[83]. While this legislative omission significantly lowers the daily regulatory overhead and administrative costs for commercial enterprises, it simultaneously creates a distinct

[77] *Id.* art. 37(1).
[78] The Digital Personal Data Protection Act, 2023, § 10, No. 22, Acts of Parliament, 2023 (India).
[79] *Id.* § 10(1).
[80] *Id.* § 10(2)(a).
[81] GDPR, *supra* note 11, art. 1.
[82] *Id.* art. 30.
[83] The Digital Personal Data Protection Act, 2023, § 8, No. 22, Acts of Parliament, 2023 (India).

information barrier[84]. Legal analysts note that without a statutory mandate for data logging, it becomes considerably harder for external oversight bodies or individual users to verify how information is being managed internally.

Enhancing Privacy Protection under the DPDP Act: Recommendations for Reform

The enactment of the Digital Personal Data Protection Act, 2023 represents an important milestone in India's evolving data governance framework; however, several structural and regulatory concerns continue to limit its effectiveness. As the volume of personal data generated and processed within digital ecosystems continues to expand, the legal framework must evolve to address emerging privacy risks while maintaining public confidence in digital governance. Achieving this objective requires targeted reforms that enhance accountability, strengthen individual rights, and ensure greater institutional independence[85].

One of the most significant areas requiring legislative refinement relates to the regulation of cross-border data transfers. The current framework permits the transfer of personal data outside India unless specifically restricted by the Central Government. While this approach offers flexibility, it provides limited clarity regarding the safeguards that must accompany such transfers[86]. In the absence of clearly articulated standards, concerns may arise regarding the level of protection afforded to personal data once it leaves Indian jurisdiction. Incorporating internationally recognised mechanisms such as adequacy assessments, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs) would contribute towards greater legal certainty and ensure that privacy protections remain consistent irrespective of geographical boundaries[87].

[84] *Id.* § 10(2)(b).
[85] The Digital Personal Data Protection Act, 2023, Gazette of India, Extraordinary, part II, section 1 (Aug. 11, 2023).
[86] *Id.* § 16.
[87] GDPR, *supra* note 11, arts. 45–47.

Equally important is the need to reinforce the rights available to data principals. Although the Act recognises several important rights, it does not expressly provide individuals with certain protections that have become central to modern data protection regimes. The inclusion of rights such as data portability and the right to erasure would significantly enhance individual autonomy by enabling greater control over personal information and reducing long-term privacy risks[88]. Furthermore, the absence of clearly defined retention obligations creates the possibility of prolonged storage of personal data beyond what is reasonably necessary. Establishing mandatory retention limits and requiring periodic deletion of unnecessary data would reduce the likelihood of misuse, unauthorised access, and secondary exploitation of personal information[89].

Another area that merits careful reconsideration concerns the broad exemptions available to public authorities. While the protection of national security and maintenance of public order remain legitimate governmental objectives, exemptions from data protection obligations should not operate without adequate safeguards. Excessively broad discretionary powers may undermine the constitutional commitment to informational privacy recognised by the Supreme Court and create the perception of unchecked State surveillance[90]. To preserve the balance between collective security and individual liberty, exemptions should be narrowly construed and accompanied by meaningful judicial or independent oversight mechanisms capable of reviewing the necessity and proportionality of governmental actions[91].

The effectiveness of any data protection legislation ultimately depends upon the strength and credibility of its enforcement architecture. In this regard, enhancing the institutional autonomy of the Data Protection Board of India remains a critical priority. Safeguards relating to appointment procedures, tenure security, financial independence, and operational transparency would strengthen the Board's ability to function as an impartial

[88] *Id.* arts. 17, 20.
[89] Greenleaf, *supra* note 10.
[90] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India); Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
[91] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

regulatory authority[92]. A regulatory body perceived as independent is more likely to command public trust and ensure effective enforcement of privacy obligations.

Greater transparency in governmental data practices is equally essential for fostering accountability within a democratic society. Public authorities should be required to disclose the categories of personal data collected, the legal basis for such collection, the purposes for which the data is utilised, and the duration of its retention[93]. Increased transparency would not only promote informed public scrutiny but would also reinforce confidence in the legitimacy of data-driven governance initiatives.

In conclusion, the long-term success of the DPDP Act will depend upon the extent to which it evolves in response to technological developments, constitutional values, and emerging global standards. By addressing existing regulatory gaps, strengthening oversight mechanisms, and expanding privacy protections, India can move towards a more resilient and rights-oriented data protection framework that effectively balances innovation, economic growth, and the protection of individual freedoms in the digital age[94].

Conclusion

The enactment of the Digital Personal Data Protection Act, 2023 represents a pivotal development in India's evolving approach to data governance and privacy regulation. By establishing a legal framework for the processing of digital personal data, the Act seeks to address the growing challenges associated with the digital economy and the increasing reliance on data-driven technologies. Although the legislation reflects several principles commonly found in international data protection regimes, particularly the GDPR, notable differences remain in relation to the scope of protection, the range of rights available to

[92] The Digital Personal Data Protection Act, 2023, §§ 18–28, No. 22, Acts of Parliament, 2023 (India).
[93] Org. for Econ. Co-operation & Dev. [OECD], *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).
[94] GDPR, *supra* note 11, pmbl.; The Digital Personal Data Protection Act, 2023, Preamble, No. 22, Acts of Parliament, 2023 (India).

individuals, the regulation of cross-border data transfers, and the structure of enforcement mechanisms.

While the DPDP Act provides an important foundation for protecting personal data, certain aspects of the framework continue to raise concerns regarding the adequacy of privacy safeguards. The absence of explicit rights such as data portability and the right to be forgotten, the limited recognition of enhanced protections for sensitive personal information, and the broad exemptions available to governmental authorities have generated debate regarding the extent to which the Act effectively balances individual privacy with competing regulatory and security interests. These issues assume greater significance in light of the constitutional recognition of privacy as a fundamental right and the increasing volume of personal data processed within India's digital ecosystem.

Strengthening the effectiveness of the Act will require a combination of legislative refinement and institutional reform. The adoption of structured safeguards governing cross-border data transfers, including mechanisms comparable to adequacy determinations and Standard Contractual Clauses, would promote greater legal certainty and facilitate secure international data flows. Similarly, expanding the rights available to data principals through the inclusion of data portability and the right to be forgotten would enhance individual autonomy and control over personal information. Furthermore, ensuring meaningful oversight of governmental exemptions and reinforcing the independence, transparency, and accountability of the Data Protection Board of India would contribute significantly to the credibility and effectiveness of the regulatory framework.

Ultimately, the long-term success of India's data protection regime will depend upon its ability to adapt to technological developments while remaining firmly grounded in constitutional values and international best practices. A balanced, transparent, and rights-oriented framework is therefore indispensable for safeguarding informational privacy, strengthening public trust in digital governance, and ensuring that India's digital transformation remains consistent with constitutional principles and evolving global data protection standards.