



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

RECALIBRATING DATA PROTECTION IN INDIA: A COMPARATIVE ANALYSIS OF THE GDPR, THE DPDP ACT 2023 AND THE DPDP RULES 2025 — CORPORATE COMPLIANCE, RIGHTS AND REGULATORY ACCOUNTABILITY

AUTHORED BY - PARI KALLA

Abstract

The emergence of robust data protection legislation across the global digital economy has created complex, multi-jurisdictional compliance obligations for multinational corporations. This paper conducts a systematic comparative legal analysis of two pivotal regulatory frameworks: the European Union's General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, which entered into force in May 2018, and India's Digital Personal Data Protection Act, 2023 (DPDP Act), operationalised through the Digital Personal Data Protection Rules, 2025 (DPDP Rules). Drawing upon doctrinal legal methodology and primary statutory sources, this paper examines the structural and philosophical divergences between these two regimes across six critical dimensions: (i) material and territorial scope; (ii) lawful bases and consent architecture, including India's novel Consent Manager ecosystem; (iii) individual data rights and the omission of portability and automated decision-making protections under the DPDP Act; (iv) corporate governance obligations and the Significant Data Fiduciary classification; (v) enforcement mechanisms, penalty structures, and breach notification obligations; and (vi) constitutional dimensions, including the broad governmental exemptions under Section 17 of the DPDP Act and the consequential amendment of the Right to Information Act, 2005. The paper identifies several critical research gaps in the existing comparative legal scholarship, particularly the absence of analysis incorporating the DPDP Rules, 2025, and the corporate compliance implications of the 2025–2027 co-existence period during which both the legacy Sensitive Personal Data or Information (SPDI) Rules, 2011 and the DPDP Act remain simultaneously operative. The paper further contributes a structured, three-phase compliance roadmap for multinational enterprises navigating dual regulatory exposure, alongside a constitutional analysis of the ongoing Supreme Court challenge to Section 17 of the DPDP Act. The findings establish that while both regimes share foundational commitments to individual dignity and informational autonomy constitutionally anchored in

the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 and the EU Charter of Fundamental Rights they reflect materially divergent regulatory philosophies. The GDPR embodies a rights-heavy, comprehensive, and globally prescriptive model, whereas the DPDP Act establishes a digitally-centred, consent-centric, and government-steered framework tailored to India's rapidly expanding digital economy. This doctrinal divergence carries significant practical consequences for data adequacy under Article 45 of the GDPR, corporate penalty exposure, processor liability allocation, and the cross-border flow of personal data between the EU and India. The paper concludes that achieving transnational compliance requires multinational corporations to adopt a locally differentiated, multi-tiered data governance model that proactively reconciles the structural gaps between both frameworks.

Keywords: General Data Protection Regulation; Digital Personal Data Protection Act, 2023; DPDP Rules, 2025; Comparative Data Protection Law; Right to Privacy; Consent Architecture; Significant Data Fiduciary; Cross-Border Data Transfers; Corporate Compliance; Puttaswamy; India-EU Regulatory Divergence; Surveillance Exemptions; Right to Information Act.

I. Theoretical and Historical Foundations of Data Privacy Law

The normative foundations of modern data protection law are anchored in the philosophical conception of privacy as a fundamental human right, inseparable from individual autonomy, dignity, and liberty. The seminal theoretical contribution of Warren and Brandeis, who in 1890 articulated the "right to be let alone" in the *Harvard Law Review*, established the philosophical substrate upon which contemporary data protection regimes are constructed.¹ Building on this foundation, subsequent scholarship by Alan Westin reconceptualised privacy as the individual's capacity to control information about themselves a framework that directly informs the consent-centric architecture adopted by both the GDPR and the DPDP Act.²

At the supranational level, the right to privacy received formal legal recognition through Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966), both of which protect individuals against arbitrary interference with their privacy, family, home, or correspondence.³ The Council of

¹ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

² Alan F Westin, *Privacy and Freedom* (Atheneum 1967).

³ Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III), art 12; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March

Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, 1981) represented the first binding international instrument governing data protection, foreshadowing the comprehensive regulatory architecture later codified in the GDPR.⁴

II. Scholarship on the General Data Protection Regulation

The GDPR, which entered into force on 25 May 2018, has generated an extensive body of comparative legal scholarship. Paul Schwartz, in his widely cited article "Global Data Privacy: The EU Way" published in the NYU Law Review, characterises the GDPR as a transnational regulatory instrument whose extraterritorial reach has effectively exported European privacy norms to jurisdictions across the globe, a phenomenon widely described as the "Brussels Effect."⁵ Schwartz and Peifer, in their earlier comparative study "Transatlantic Data Privacy Law," examined the fundamental doctrinal divergences between the EU and US regulatory models, highlighting the EU's rights-based framework as distinct from the American sectoral and market-driven approach.⁶

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 introduced a unified, technology-neutral, and extraterritorially applicable framework premised upon six co-equal lawful bases for processing, a tiered taxonomy of sensitive data categories under Article 9, and graduated penalty structures under Article 83 capable of reaching four percent of an undertaking's total global annual turnover.⁷ Academic commentary has documented the GDPR's transformative influence on national regulatory development across Asia, Latin America, and Sub-Saharan Africa, establishing what Graham Greenleaf has described as a global wave of data protection legislation spanning more than 157 jurisdictions.⁸

1976) 999 UNTS 171, art 17.

⁴ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, opened for signature 28 January 1981, entered into force 1 October 1985).

⁵ Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYU Law Review 771.

⁶ Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115.

⁷ Regulation (EU) 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] OJ L119/1.

⁸ Graham Greenleaf, 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 Privacy Laws & Business International Report 1.

III. The Indian Constitutional and Legislative Background

India's journey toward comprehensive data protection legislation is constitutionally rooted in the landmark nine-judge bench judgment of the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1, which unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution of India.⁹ The Court established a three-part proportionality test requiring that any state interference with privacy satisfy the requirements of legality, legitimate aim, and necessity a constitutional standard which scholars have subsequently invoked to critically evaluate the adequacy of the DPDP Act's sweeping governmental exemption clauses under Section 17.¹⁰ Prior to the DPDP Act, India's data protection framework comprised Section 43A and Section 72A of the Information Technology Act, 2000, supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These provisions offered limited and sectoral protections and were widely criticised in legal scholarship for their inadequacy in addressing the complexities of India's rapidly expanding digital economy.¹¹ The Committee of Experts on a Data Protection Framework for India, chaired by Justice B.N. Srikrishna, submitted its report to the Ministry of Electronics and Information Technology in July 2018, recommending a rights-centred framework that drew significant inspiration from the GDPR while adapting core principles to India's socio-economic context.¹²

IV. Comparative Scholarship on the GDPR and DPDP Act

A growing body of comparative legal scholarship has examined the structural similarities and doctrinal divergences between the GDPR and the DPDP Act. Bhardwaj (2025), writing in the Indian Journal of Law, identifies key points of departure including the absence of a commercial "legitimate interests" balancing mechanism for private entities under the DPDP Act, the statutory omission of data portability and automated decision-making rights, and the structurally flat approach to data classification that treats all personal data uniformly regardless of sensitivity.¹³ The comparative analysis conducted by Latham and Watkins similarly

⁹ *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.* (2017) 10 SCC 1 (Supreme Court of India).

¹⁰ *ibid* [267]–[270] (DY Chandrachud J).

¹¹ Information Technology Act 2000 (India), ss 43A, 72A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, SI 2011/No G.S.R. 313(E).

¹² Committee of Experts on a Data Protection Framework for India (Chair: Justice B.N. Srikrishna), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, 2018).

¹³ A Bhardwaj, 'Data Protection and Privacy Laws: Comparison Between GDPR and India's Digital Personal

concludes that while the DPDP Act broadly converges with GDPR principles of purpose limitation, data minimisation, and individual access rights, it departs significantly in areas of processor liability, consent management architecture, and enforcement mechanisms.¹⁴

A Springer-published study examining India's DPDP Act in light of the GDPR employs doctrinal legal methodology to assess whether the DPDP Act meets the international gold standard for data protection. The study concludes that while the DPDP Act introduces foundational principles such as consent-based processing, individual rights, and a Data Protection Board, it lacks robust enforcement infrastructure, adequately independent regulatory oversight, and statutory protection against automated algorithmic decision-making, leaving India's rapidly expanding artificial intelligence and fintech sectors in a regulatory gap.¹⁵

From a jurisprudential standpoint, Motiwala (2025), drawing on legal positivism and critical legal theory, argues that the DPDP Act reflects a compliance-heavy rather than rights-driven philosophy, characterising India's regulatory stance as treating data primarily as a sovereign asset and instrument of digital economy governance, rather than as an extension of individual constitutional liberty.¹⁶ This theoretical framing directly informs the present paper's comparative analysis, which situates doctrinal divergences between the GDPR and the DPDP Act within their broader jurisprudential and constitutional contexts.

V. Cross-Border Data Transfers, Adequacy, and the Global Dimension

A critical dimension of the comparative legal literature concerns cross-border data transfers and the question of whether India's DPDP Act meets the GDPR's "essential equivalence" standard for an adequacy decision under Article 45 of the GDPR. As of the date of this research, no formal adequacy decision by the European Commission has been adopted in respect of India. In April 2025, the European Data Protection Supervisor declined a request by the European Investment Bank to transfer contact data to India, citing the absence of definitive evidence that India offers an essentially equivalent level of data protection.¹⁷ Scholarly analysis

Data Protection Act' (2025) 3(2) Indian Journal of Law 17.

¹⁴ Latham & Watkins LLP, India's Digital Personal Data Protection Act, 2023 vs. the GDPR: A Comparison (Client Alert, 2024) <<https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf>> accessed 1 June 2026.

¹⁵ Vibushan Sivapatham and Meghana Srinivasan, 'Bridging the Gap: Assessing India's Digital Personal Data Protection Act in Light of the EU GDPR' (2025) SN Computer Science (Springer) <<https://doi.org/10.1007/s42979-025-04269-7>> accessed 1 June 2026.

¹⁶ Abdullah Zubair Motiwala, 'A Jurisprudential Analysis of the DPDP Rules 2025 and the Evolution of Data Privacy Laws in India' (30 April 2025) SSRN Working Paper <<https://ssrn.com/abstract=5335388>> accessed 1 June 2026.

¹⁷ European Data Protection Supervisor, Annual Report 2024 (EDPS 2025); Observer Research Foundation, 'The

concludes that in the absence of an adequacy decision, data exporters from the European Economic Area must rely on Standard Contractual Clauses or Binding Corporate Rules to authorise transfers of personal data to Indian data fiduciaries, creating compliance complexity for multinational enterprises operating across both jurisdictions.¹⁸

VI. Research Gap and Contribution of the Present Study

The existing literature, while substantive in its foundational comparative analysis, presents several identifiable research gaps that the present paper seeks to address. First, the bulk of academic scholarship on the GDPR–DPDP Act comparison was produced prior to the notification of the Digital Personal Data Protection Rules, 2025 on 13 November 2025, which introduced significant operational specifications concerning Consent Manager interoperability, Significant Data Fiduciary designation thresholds, mandatory data retention periods, and children’s data verification mechanisms. This paper provides an analysis incorporating the DPDP Rules 2025 in their entirety, filling a temporal gap in the existing comparative literature. Second, while existing scholarship addresses the abstract doctrinal comparison, there is a relative paucity of corporate compliance-oriented legal analysis examining the practical transition challenges faced by multinational enterprises operating under both regulatory regimes simultaneously. The present paper addresses this gap by providing a structured phased compliance roadmap for the 2025–2027 transition period, during which the SPDI Rules, 2011 and the DPDP Act legally co-exist.

Third, the constitutional dimensions of the DPDP Act particularly the interaction between broad governmental exemptions under Section 17 and the right to information framework under the Right to Information Act, 2005, as amended by Section 44(3) of the DPDP Act remain insufficiently examined in the existing comparative legal scholarship. This paper contributes a focused constitutional analysis of this intersection, situating the emerging constitutional litigation, including the writ petition challenging Section 17 before the Supreme Court of India, within the broader comparative regulatory framework.

Adequacy Dilemma: India’s DPDPA and the GDPR’ (18 June 2025) <<https://www.orfonline.org/expert-speak/the-adequacy-dilemma-india-s-dpdpa-and-the-gdpr>> accessed 1 June 2026.

¹⁸ Indian Journal of Law and Technology, ‘Jurisdictional Challenges to Personal Data Transfers into India: Does the Digital Personal Data Protection Act, 2023 Ensure an Adequate Level of Protection?’ (2024) <<https://www.ijlt.in/post/jurisdictional-challenges-to-personal-data-transfers-into-india-does-the-digital-personal-data-prot>> accessed 1 June 2026.

Structural and Scope-Based Divergences: The Technological and Jurisdictional Divide

The evolution of data privacy laws worldwide represents a continuous struggle to balance individual fundamental liberties with global digital commerce.¹⁹ The European Union's General Data Protection Regulation (GDPR), which came into force in May 2018, established a comprehensive, rights-heavy paradigm²⁰ that has served as the global regulatory benchmark. Conversely, India's Digital Personal Data Protection Act, 2023 (DPDP Act)²¹, enacted in August 2023 and operationalized through the Digital Personal Data Protection Rules, 2025 (DPDP Rules), reflects a newer, highly streamlined regulatory philosophy. Rather than copying the European model, India has designed a context-specific, digital-first framework²² tailored to its rapidly expanding digital market and complex socio-economic realities. This fundamental divergence begins with how both regimes define the physical, material, and territorial boundaries of personal data.

The material scope of the GDPR is technology-neutral and intentionally expansive²³, covering any information relating to an identified or identifiable natural person, regardless of the format, medium, or storage system. It applies to both automated digital processing and structured manual filing systems, ensuring that physical paper records, analog databases, and traditional filing cabinets remain subject to strict privacy controls. In contrast, the DPDP Act is strictly digital-centric.²⁴ Its statutory scope is confined exclusively to "digital personal data," defined as personal data collected in digital form or physical data collected offline that is subsequently digitized. Purely physical, offline paper records that are never converted into digital formats fall completely outside the scope of the Act, representing a significant structural limitation.

This digital-only boundary introduces operational complexity during customer onboarding and Know-Your-Customer (KYC) processes.²⁵ For example, when an organization collects a

¹⁹ A Comparative Legal Study of the GDPR and India's Digital Personal Data Protection Act, RJ Wave, <https://www.rjwave.org/jaaf/papers/JAAFR2601594.pdf>; Cross-Border Data Transfers: Reconciling Indian Law with Global Privacy Regimes, DPO India, <https://www.dpo-india.com/Blogs/cross-border-data-transfers/>

²⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1

²¹ Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Aug. 11, 2023.

²² India's Digital Personal Data Protection Act, 2023 (DPDP Act) vs GDPR, Securiti, <https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/>

²³ India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Latham & Watkins, <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf>

²⁴ Key Difference Between India's DPDP Act and EU's GDPR You Should Know, Complinty, <https://complinty.com/blog/compliance/key-difference-between-indias-dpd-act-and-eus-gdpr-you-should-know/>

²⁵ India's New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach, Fisher Phillips

physical, paper-based registration form, the data is initially exempt from the DPDP Act. However, the moment a corporate employee scans that document or manually inputs the data into an electronic customer relationship management (CRM) database, the data is digitized, instantly triggering the full compliance obligations of the DPDP Act and Rules.

Furthermore, the DPDP Act introduces a significant exclusion absent from the GDPR: it does not apply to personal data made publicly available by the data principal²⁶ themselves, or under a statutory legal obligation in India. Under the GDPR, the fact that personal data is public does not strip it of its protected status or exempt organizations from establishing a valid lawful basis for its processing. Under the DPDP Act, however, this broad exclusion creates a distinct regulatory gap. Offshore web-scraping engines, public directories, and third-party data aggregators can legally harvest and compile publicly available personal profiles without facing statutory penalties under the Indian framework.

The divergence in data classification further highlights their different regulatory approaches. The GDPR utilizes a tiered taxonomy, distinguishing standard personal data from “special categories of personal data” (such as genetic, biometric, health, racial, ethnic, political, and trade union data) under Article 9.²⁷ These special categories are subject to strict processing prohibitions unless explicit, narrow statutory exemptions are satisfied.

The DPDP Act rejects this tiered classification.²⁸ It treats all digital personal data under a single, flat framework with no differentiated statutory safeguards for sensitive data categories like health, financial, or biometric information. This lack of statutory differentiation creates compliance uncertainty for high-risk industries like healthcare and fintech. These sectors must navigate both the baseline obligations of the DPDP Act and the separate, preexisting data security mandates of sectoral regulators, such as the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI), which continue to enforce their own industry-specific data localization and encryption standards.

Regarding territorial reach, both laws project their authority extraterritorially, but through different mechanisms. The GDPR applies to non-EU entities under Article 3(2) if their processing activities relate to either the offering of goods or services to individuals in the EU, or the monitoring of their behavior (such as online profiling and tracking) within the Union. The DPDP Act also applies extraterritorially²⁹, but only if the processing of digital personal

²⁶ India’s Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Latham & Watkins

²⁷ GDPR, art. 9

²⁸ GDPR vs DPDP Act: Key Differences Explained, DPDP Consultants

²⁹ GDPR, art. 3; Cross-Border Data Transfers: Reconciling Indian Law with Global Privacy Regimes, DPO India

data outside India is directly in connection with the offering of goods or services to data principals located within India.

Crucially, the DPDP Act does not contain a behavioral monitoring or profiling trigger equivalent to the GDPR³⁰. Consequently, offshore artificial intelligence platforms, advertising networks, or analytics firms that track, profile, and monitor Indian citizens without actively marketing or offering goods and services within India may fall entirely outside the statutory reach of the DPDP Act.

Finally, the allocation of direct statutory duty differs. Under the GDPR, both data controllers and data processors are directly regulated, and processors face direct statutory liabilities and administrative fines under Article 28³¹. Under the DPDP Act, statutory obligations and liabilities fall exclusively on the “Data Fiduciary” (the equivalent of a controller). Data processors are not directly liable to the regulator; instead, they are bound indirectly through mandatory bilateral commercial contracts. The Data Fiduciary remains entirely accountable³² to the Data Protection Board of India (DPBI) for any data breaches or non-compliance caused by its third-party vendors and processors.

Regulatory Dimension	General Data Protection Regulation (GDPR)	Digital Personal Data Protection Act (DPDP Act)
Primary Statutory Focus	Comprehensive, media-neutral data protection and individual rights.	Streamlined protection of digital-only personal data and digital economy growth.
Material Scope of Data	All personal data, including digital, manual, paper, and analog formats.	Digital personal data only (including physical records subsequently digitized).
Exclusion of Public Data	No general exemption; public availability does not strip personal data status.	Broadly excludes personal data made publicly available by the data principal or by law.
Data Safeguard Taxonomy	Tiered: Standard vs. Special Categories (Biometric, Genetic, Health).	Flat: Uniform statutory standards applied to all digital personal data.
Extraterritorial	1. Offering of goods or services to	Offering of goods or services to

³⁰ DPDP Act’s Global Reach: Cross-Border Data, AI Impact, and International Alignment, TrustArc

³¹ GDPR, art. 28

³² DPDP Act Non-Compliance Penalties: What You Must Know, VISTA InfoSec

Triggers	EU residents. 2. Monitoring behavior of EU residents.	data principals located within the territory of India.
Direct Processor Liability	High: Processors face direct statutory obligations and liabilities under Art. 28.	None: Processors are bound solely via mandatory bilateral contracts with the Fiduciary.

Lawful Bases, Consent Architecture, and the Consent Manager Ecosystem

The legal foundation for processing personal data represents a major point of divergence between the European Union and Indian frameworks. The GDPR provides a highly flexible operational framework under Article 6(1), permitting data controllers to justify data processing across six co-equal lawful bases:³³ consent, contractual necessity, legal obligations, vital interests of the individual, public tasks, and the highly utilized “legitimate interests” of the data controller. This legitimate interests basis³⁴ allows private commercial organizations to process personal data without seeking explicit consent, provided they pass a structured three-part balancing test demonstrating that their business interests are not overridden by the fundamental rights of the individual.

The DPDP Act rejects this co-equal approach³⁵, establishing a much narrower, consent-centric framework. Under the Indian law, organizations are restricted to just two lawful grounds for processing: explicit consent, or specifically enumerated “legitimate uses”³⁶. Crucially, the DPDP Act does not recognize “contractual necessity” or a broad commercial “legitimate interest” balancing framework for private, commercial organizations. Instead, its statutory “legitimate uses” are strictly defined and limited to:

- Specified state and public functions.
- Compliance with judicial orders and legal obligations.
- Medical emergencies and public health crises.
- Disasters or breakdowns of public order.
- Employment-related purposes (such as preventing corporate espionage, maintaining IP confidentiality, and managing employee benefits).

For multinational businesses accustomed to relying on “legitimate interests” or “contractual

³³ GDPR, art. 6

³⁴ GDPR, art. 6(1)(f)

³⁵ Comparative Analysis of the Digital Personal Data Protection Act of India 2023 and GDPR, Pen Acclaims

³⁶ DPDP Act Exemptions Explained, Consentin

necessity” under the GDPR to justify processing activities like internal corporate reorganizations, direct marketing, product improvements, or fraud prevention, this represents a severe compliance challenge.³⁷ These entities must systematically conduct data mapping exercises and retroactively build robust, explicit consent mechanisms to validate processing operations that would otherwise be considered unlawful under the DPDP Act.

The consent standard under the DPDP Act is highly rigid. Valid consent must be free, specific, informed, unconditional, and unambiguous³⁸, requiring a clear affirmative action from the user. The statutory addition of “unconditional” strictly prohibits “bundled consent,”³⁹ meaning companies cannot condition the provision of a core service or contract on a user consenting to non-essential data processing activities (such as behavioral marketing).

To operationalize consent in India’s highly fragmented linguistic and socio-economic landscape, the DPDP framework introduces an innovative statutory intermediary known as the “Consent Manager”⁴⁰. Functioning similarly to the Unified Payments Interface (UPI) model⁴¹ but for digital privacy, Consent Managers are interoperable, registered platforms through which users can centrally give, manage, review, and withdraw consent across multiple digital services via unified dashboards. Consumer-facing platforms must integrate with Consent Manager application programming interfaces (APIs) by late 2026, shifting consent management from isolated corporate silos to a standardized national ecosystem.

Furthermore, privacy notices under the DPDP Act must be itemized and made available in English as well as any of the 22 scheduled official languages of India⁴², creating substantial localization requirements for corporate user interfaces.

Lawful Ground for Processing	GDPR (EU)	DPDP Act (India)
Explicit Consent	Yes (Article 6(1)(a)): Must be granular, specific, and easy to withdraw.	Yes (Section 6): Must be free, specific, informed, unconditional, and unambiguous.
Contractual	Yes (Article 6(1)(b)): Core ground	No equivalent basis:

³⁷ DPDP Act vs GDPR: Key Differences for Indian Companies, TCSA

³⁸ Digital Personal Data Protection Act, 2023, § 6; FAQs on the Digital Personal Data Protection Act and Rules, CMS INDUSLAW

³⁹ The Right to (Pry)-vacy: Understanding India’s Dystopian Data Protection Legislation, NYU Journal of International Law & Politics

⁴⁰ DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

⁴¹ DPDP Act vs GDPR: Key Differences for Indian Companies, TCSA.

⁴² India’s New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach, Fisher Phillips

Necessity	for executing and delivering consumer services.	Organizations must establish explicit consent for service delivery.
Legitimate Interests	Yes (Article 6(1)(f)): Subject to a balancing test; widely used by private entities.	No commercial equivalent: Limited to narrow statutory public and employment uses.
Employment Processing	Subject to national member state laws and collective bargaining agreements.	Yes: Broadly recognized as a “legitimate use” for internal employee data management.
Compliance with Law	Yes (Article 6(1)(c)): Necessary to comply with legal mandates.	Yes: Explicit “legitimate use” ground for court orders and statutory compliance.
Consent Management	Managed locally by each data controller’s individual consent registry.	Standardized: Consent Managers act as unified, interoperable national platforms.

Rights of the Individual: Discrepancies in Data Principal Empowerment

Both the GDPR and the DPDP Act prioritize individual empowerment⁴³, granting fundamental rights to control personal data. Under both regimes, individuals (termed “data subjects” under the GDPR and “data principals” under the DPDP Act) possess the right to seek confirmation of processing⁴⁴, access their processed personal data, obtain a summary of processing activities, and request correction of inaccurate data or complete erasure of their records once the processing purpose is fulfilled.

Despite these shared foundational rights, the DPDP framework is considerably narrower, omitting several advanced rights that are central to the GDPR’s comprehensive rights architecture. Specifically, the DPDP Act does not grant:

- 1. The Right to Data Portability⁴⁵:** Data principals cannot legally demand that a data fiduciary transfer their personal data directly to a competing service provider in a structured, machine-readable format, a gap that reduces interoperability and limits consumer mobility in digital markets.

⁴³ GDPR vs DPDP Act: Key Differences Explained, DPDP Consultants

⁴⁴ GDPR arts. 15–17; Digital Personal Data Protection Act, 2023, §§ 11–12

⁴⁵ GDPR art. 20

2. **The Right to Object to Processing**⁴⁶: Unlike GDPR Article 21, which provides individuals with a detailed right to object to specific processing activities (including direct marketing), the DPDP Act relies solely on the binary mechanism of consent withdrawal.
3. **Protection against Automated Decision-Making and Profiling**⁴⁷: Under GDPR Article 22, individuals have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects. The DPDP Act contains no equivalent provision. This is a highly notable regulatory omission given the rapid proliferation of artificial intelligence, algorithmic credit scoring, automated hiring, and digital lending platforms across India's booming fintech and digital sectors.

However, the DPDP Act introduces two progressive, culturally contextualized rights that are absent from the GDPR: the Right to Grievance Redressal⁴⁸ (obligating firms to resolve user complaints within a strict 90-day window before the user can escalate the matter to the regulator) and the Right to Nominate⁴⁹ (allowing individuals to designate a representative to manage and exercise their data privacy rights in the event of their death, physical incapacity, or mental incompetence).

Individual Right	GDPR (EU)	DPDP Act (India)
Right to Access & Information	Yes (Article 15): Comprehensive access to data, purposes, and recipients.	Yes (Section 11): Right to obtain a summary of data processed and identities of sharing partners.
Right to Correction & Erasure	Yes (Articles 16 & 17): Comprehensive correction and "right to be forgotten".	Yes (Section 12): Mandatory correction, completion, and erasure once purpose is served.
Right to Portability	Yes (Article 20): Direct transfer of data in structured, machine-readable format.	No: No statutory right to data portability exists under the primary legislation.
Right to Object to Processing	Yes (Article 21): Right to halt specific processing operations like	No: Individuals must withdraw consent entirely, halting all

⁴⁶ GDPR art. 21

⁴⁷ GDPR art. 22; Regulating Innovation: The IT Act 2000 and DPDP Act 2023 in the Age of AI and Data, JETIR

⁴⁸ Digital Personal Data Protection Act, 2023, § 13

⁴⁹ Digital Personal Data Protection Act, 2023, § 14

	direct marketing.	connected processing.
Automated Decision-Making	Yes (Article 22): Strict limits on profiling and automated legal outcomes.	No: No equivalent protection against algorithmic decision-making and profiling.
Right to Nominate Representative	No equivalent: Subject to national inheritance or probate laws.	Yes (Section 14): Right to designate a representative to manage rights post-death or incapacity.
Grievance Redressal	Yes: Right to lodge complaints directly with Supervisory Authorities.	Yes (Section 13): Mandatory internal resolution (90-day cap) before regulatory escalation.

Corporate Governance, Significant Data Fiduciaries, and Operational Safeguards

The DPDP Act establishes a tiered compliance framework, introducing a unique classification known as the Significant Data Fiduciary (SDF)⁵⁰. Unlike the GDPR, which scales obligations based on processing risk under a general accountability principle, the Indian government directly notifies specific organizations as SDFs based on structural criteria. These criteria include the volume and sensitivity of personal data processed⁵¹, risk of harm to data principals, impact on national sovereignty, and risks to public order or electoral democracy.

Under the notified DPDP Rules, an organization is likely to be designated as an SDF if it meets any of the following quantitative or qualitative criteria:

- 1) **User Base:** Processing the personal data of 5 million or more active Indian residents.
- 2) **Financials:** Having an annual Indian turnover exceeding INR 2.5 billion (approximately US\$26.24 million).
- 3) **Risk Profile:** Large-scale processing of highly sensitive financial or health data, or deployment of artificial intelligence systems for automated decision-making and profiling.

Designated SDFs are subject to a suite of advanced governance and compliance mandates that must be operationalized by Q1 2027. These include:

⁵⁰ Digital Personal Data Protection Rules, 2025; India's DPDP Timeline: Critical Compliance Deadlines for 2026–27, India Briefing

⁵¹ DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

1. **Appointing an India-Based Data Protection Officer (DPO)**⁵²: The DPO must reside in India, serve as the primary point of contact for the regulator, and report directly to the company's board of directors.
2. **Undergoing Annual Independent Audits**⁵³: SDFs must appoint an independent external data auditor to review and certify data governance, security controls, and statutory compliance.
3. **Conducting Formal Data Protection Impact Assessments (DPIAs)**⁵⁴: Detailed assessments must be documented for high-risk data processing activities.
4. **Performing Algorithmic Transparency and Fairness Assessments**⁵⁵: SDFs utilizing automated decision-making or AI-driven profiling must systematically evaluate and document their algorithms to ensure they do not exhibit bias or violate data principal rights.

The DPDP Rules 2025 introduce a strict, mandatory one-year data retention rule⁵⁶. Every business operating as a data fiduciary in India must store personal data, processing logs, and system traffic logs for a minimum of one year from the date of processing, even if a user explicitly deletes their account or withdraws consent. For large digital platforms, e-commerce entities with over 20 million users, social media intermediaries, and online gaming platforms categorized under Schedule 3 of the Rules, this retention mandate is extended to a minimum of three years from the date of the last user interaction.

This mandatory retention rule creates an intense regulatory paradox⁵⁷. On one hand, the DPDP Act promotes data minimization and requires fiduciaries to erase personal data as soon as the specified processing purpose is completed or consent is withdrawn. On the other hand, the DPDP Rules mandate long-term storage of logs and data for regulatory traceability. To resolve this operational conflict, corporate compliance programs must implement sophisticated deletion workflows. These workflows must ensure that data is completely purged from production systems after the retention period, while also providing a mandatory 48-hour pre-deletion notification to the affected user before permanent removal.

Furthermore, the DPDP Act establishes a unique standard for the protection of children's data. While the GDPR permits member states to set the age of consent for digital services between

⁵² Digital Personal Data Protection Rules, 2025

⁵³ DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

⁵⁴ The Practicalities of Implementing India's Digital Personal Data Protection Act, International Bar Association

⁵⁵ DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

⁵⁶ India's DPDP Rules 2025: Leading Digital Privacy Compliance, Deloitte

⁵⁷ Decrypting India's Data Protection Regime: Principles of Data Protection, Clyde & Co

13 and 16, the DPDP Act defines a “child” as any individual under the age of 18⁵⁸. For all users under 18, organizations must establish verifiable parental consent mechanisms.

The DPDP Rules 2025 clarify that minors may self-declare their parent or guardian’s contact details to initiate verification. Organizations must then verify this consent using either existing verified data on file, or government-authorized digital identity services, specifically DigiLocker⁵⁹. Additionally, fiduciaries are strictly prohibited from conducting targeted advertising, behavioral monitoring, or any processing activities detrimental to a child’s well-being. Certain exceptions are carved out for vital services like healthcare, education, and child transport, which are exempt from these parental consent requirements.

Jurisdictional Compliance Risks: Enforcement, Penalties, and Breach Management

The financial and operational risks associated with non-compliance differ fundamentally across both jurisdictions. The GDPR utilizes a percentage-of-turnover penalty model under Article 83. For severe violations (such as breaching core data processing principles or cross-border transfer rules), supervisory authorities can impose administrative fines of up to €20 million or 4% of the undertaking’s total global annual turnover of the preceding fiscal year⁶⁰, whichever is higher. By defining “undertaking” as the entire corporate group, the GDPR ensures that penalties are highly proportionate to corporate size, occasionally resulting in massive, multi-billion euro fines for technology conglomerates.

The DPDP Act rejects the turnover-based model, opting instead for fixed statutory caps⁶¹ categorized by the nature and severity of the specific infraction.⁶² While these caps are lower in absolute Euro terms than the GDPR’s 4% global turnover model, they are highly severe relative to the Indian market, presenting an existential threat to small-and-medium enterprises and startups.⁶³ Crucially, the DPDP Act specifies that penalties are applied per violation, meaning a single cybersecurity incident could trigger multiple separate penalties simultaneously.

Mathematically, the corporate financial exposure of an organization under these dual frameworks can be represented as follows. Under the GDPR, the maximum penalty is

⁵⁸ Digital Personal Data Protection Act, 2023, § 2(f)

⁵⁹ DPDP Rules 2025: The Complete Implementation Roadmap, TCSA

⁶⁰ GDPR art. 83; Fines/Penalties, GDPR Info

⁶¹ DPDP Act Non-Compliance Penalties: What You Must Know, VISTA InfoSec

⁶² Digital Personal Data Protection Act, 2023, § 33; DPDP Act Non-Compliance Penalties: What You Must Know, VISTA InfoSec

⁶³ DPDP Act’s Global Reach: Cross-Border Data, AI Impact, and International Alignment, TrustArc; DPDP Act Non-Compliance Penalties: What You Must Know, VISTA InfoSec

calculated as:⁶⁴

$$P_{GDPR} = \max(C, p \times T)$$

where C is the statutory fixed cap (€10 million or €20 million⁶⁵ depending on the tier), p represents the regulatory percentage multiplier, and T is the global annual turnover of the corporate group.

Under the DPDP Act, the maximum penalty is a cumulative function of discrete, categorized violations, represented as:

$$P_{DPDP} = \sum_{i=1}^n C_i$$

where C_i represents the statutory cap assigned to the i -th categorized violation (such as failure to notify or lack of parental consent), capped at a maximum of ₹2.5 billion (approx. US\$30 million) per individual violation.⁶⁶ This means a single security breach could theoretically trigger a penalty of ₹2.5 billion for failing to implement reasonable security safeguards under Section 8(5), and an additional ₹2 billion under Section 8(6) for failing to notify the regulator and affected data principals, resulting in a compounded fine of ₹4.5 billion.⁶⁷

Under Section 33(1), the DPBI must consider specific factors⁶⁸ before determining the final penalty: the nature, gravity, and duration of the breach, the type of data affected, and the financial capacity and size of the Data Fiduciary. All administrative penalties collected by the DPBI are deposited directly into the Consolidated Fund of India⁶⁹ and do not compensate the victims.

Furthermore, unlike the GDPR and the CCPA, the DPDP Act does not provide a private right of action⁷⁰ or statutory damages for affected individuals. Individuals seeking financial compensation must pursue separate, lengthy civil litigation, rendering the DPBI the sole public enforcement channel.⁷¹

Regulatory Requirement	GDPR (EU)	DPDP Act (India)
Maximum	Percentage-based: Up to €20M or	Category-specific: Compounded

⁶⁴ Regulation (EU) 2016/679, art. 83

⁶⁵ Regulation (EU) 2016/679, art. 83(4)–(5)

⁶⁶ Digital Personal Data Protection Act, 2023, § 33

⁶⁷ DPDP Act Non-Compliance Penalties: What You Must Know, VISTA InfoSec

⁶⁸ Digital Personal Data Protection Act, 2023, § 33(2)

⁶⁹ Digital Personal Data Protection Act, 2023, § 33

⁷⁰ DPDP Act's Global Reach: Cross-Border Data, AI Impact, and International Alignment, TrustArc

⁷¹ Digital Personal Data Protection Act, 2023, §§ 27–39

Penalty Model	4% of global annual group turnover. ⁷²	fixed caps of up to ₹2.5 billion per violation.
Cybersecurity Breach Cost	Average cost varies; scaled to market size and group revenue.	Indian average breach cost is ₹22 Crore, with statutory caps up to ₹250 Crore.
Breach Notification Trigger	Mandatory for supervisory authorities within 72 hours if a risk exists.	Mandatory for ALL breaches ⁷³ , reported to DPBI and data principals.
Notification Timeline	Within 72 hours ⁷⁴ of becoming aware of the breach.	Immediate “without delay” notification; formal detailed report within 72 hours.
Private Right of Action	Yes: Direct judicial remedies and statutory compensation for material harm.	No: All enforcement flows through the DPBI; no private damages.

Constitutional Dimensions: State Exemptions, Surveillance, and the Transparency Conflict

The intersection of national security, state surveillance, and data privacy represents a critical constitutional debate in India’s emerging data protection regime. While the GDPR limits processing exceptions for national security and public safety through member state laws subject to European Court of Justice (ECJ) oversight, the DPDP Act introduces broad executive exemptions⁷⁵.

Specifically, Section 17 of the DPDP Act carves out two tiers of exemptions:

- 1) **Complete Exemptions (Section 17(1))⁷⁶**: Waives the entire application of the Act for designated processing activities.
- 2) **Partial Exemptions (Section 17(2))⁷⁷**: Exempts data fiduciaries from core obligations such as Notice (Section 5), Consent (Section 6), and Deletion (Section 8) while preserving basic data principal rights.

Under Section 17(2)(a), the Central Government may exempt any “instrumentality of the

⁷² Regulation (EU) 2016/679, art. 83(5)

⁷³ Digital Personal Data Protection Rules, 2025; DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

⁷⁴ Regulation (EU) 2016/679, art. 33

⁷⁵ Digital Personal Data Protection Act, 2023, § 17

⁷⁶ Digital Personal Data Protection Act, 2023, § 17(1)

⁷⁷ Digital Personal Data Protection Act, 2023, § 17(2)

State”⁷⁸ from the entire Act in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign states, or public order. Under Section 17(1)(c), state law enforcement and intelligence agencies are exempt⁷⁹ from compliance when processing personal data for the prevention, detection, investigation, or prosecution of any offense in India⁸⁰.

Digital rights organizations and academic scholars argue that these sweeping exemptions, combined with Section 36 (which empowers the Central Government to compel any data fiduciary to furnish any information required by the executive without explicit statutory guidance), could enable a disproportionate state surveillance regime⁸¹.

This controversy culminated in February 2026, when activist Venkatesh Nayak filed a landmark writ petition under Article 32 of the Constitution (*Venkatesh Nayak v. Union of India*)⁸², challenging the constitutionality of Section 17. The Supreme Court of India referred the matter to a larger constitutional bench to evaluate whether these sweeping exemptions are manifestly arbitrary under Article 14⁸³ and fail the three-part constitutional test of proportionality (legality, legitimate aim, and necessity).

Section 44(3) of the DPDP Act immediately amended Section 8(1)(j) of the Right to Information (RTI) Act, 2005.⁸⁴ Under the original RTI Act, public authorities could exempt “personal information” from public disclosure only if it had no relationship to public activity, or if it caused an unwarranted invasion of privacy. Crucially, the original Section 8(1)(j) contained a vital balancing mechanism: public officials were required to disclose personal information if a larger public interest justified it⁸⁵, and information that could not be denied to Parliament could not be denied to an ordinary citizen.

Section 44(3)⁸⁶ of the DPDP Act completely removed this balancing mechanism and the public interest override.⁸⁷ It replaced it with a blanket, absolute ban on the disclosure of any “personal

⁷⁸ Digital Personal Data Protection Act, 2023, § 17(2)(a)

⁷⁹ Digital Personal Data Protection Act, 2023, § 17(1)(c)

⁸⁰ Digital Personal Data Protection Act, 2023, § 17(1)(c)

⁸¹ Constitutionality of the Digital Personal Data Protection Act, 2023, Supreme Court Observer; Regulating Innovation: The IT Act 2000 and DPDP Act 2023 in the Age of AI and Data, JETIR

⁸² Constitution of India art. 32; Constitutionality of the Digital Personal Data Protection Act, 2023, Supreme Court Observer

⁸³ Constitution of India art. 14; *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

⁸⁴ Right to Information Act, No. 22 of 2005, § 8(1)(j)

⁸⁵ Right to Information Act, 2005, § 8(1)(j) (prior to amendment)

⁸⁶ Digital Personal Data Protection Act, 2023, § 44(3)

⁸⁷ The Data Protection Act Is Critical for Privacy, but Sweeping Provisions Threaten Right to Information, Article 14

information” held by public authorities. Transparency advocates and information activists argue that this amendment subverts the twenty-year jurisprudence⁸⁸ of the RTI Act.

By using the “right to privacy” (originally intended to protect private citizens from corporate data extraction) as a shield to protect public officials from scrutiny, the government has enabled bureaucratic opacity.⁸⁹ Under the amended clause, public departments routinely deny crucial public accountability information such as the assets and liabilities of public servants, government procurement details, academic credentials of candidates, and public spending records by citing the “personal nature” of the data. This ongoing tension between transparency (the right to know) and privacy (the right to be let alone) remains a major constitutional challenge currently pending final adjudication before the Supreme Court of India.⁹⁰

Corporate Strategy during the 2025–2027 Transition: The Coexistence of SPDI and DPDP

As of 2026, corporate legal and compliance departments operating in India find themselves in a complex, dual-regulatory transition phase.⁹¹ While the DPDP Rules 2025 were notified on November 13, 2025, and are proceeding on schedule toward the full enforcement deadline of May 13, 2027, Section 43A of the IT Act, 2000⁹², and the SPDI Rules, 2011⁹³, have not yet been formally omitted. This omission will occur as a defined legal moment on the final May 2027 deadline.

Consequently, both regulatory regimes legally co-exist. During this 18-month window, businesses face a dual compliance burden :

- 1) They must maintain their legacy SPDI controls (including obtaining specific written consent for SPDI categories like passwords or financial data, publishing SPDI-compliant privacy policies, and maintaining ISO/IEC 27001 certifications⁹⁴ to avert liability before Adjudicating Officers under the IT Act).

⁸⁸ Data Protection Act vs the Right to Information Act, Shankar IAS Parliament

⁸⁹ Impact of the Digital Personal Data Protection Act, 2023 on Third-Party Information under the Right to Information Act, 2005, IJFMR

⁹⁰ Constitutionality of the Digital Personal Data Protection Act, 2023, Supreme Court Observer

⁹¹ India’s New Data Privacy Rules Are Here, Fisher Phillips; Are the SPDI Rules Still in Force After DPDP Act 2023, Opsio

⁹² Information Technology Act, 2000, § 43A

⁹³ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

⁹⁴ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 8

- 2) Simultaneously, they must actively build, test, and deploy the highly automated, digital-first architectures required for full DPDP compliance.

A common corporate pitfall is the premature removal of SPDI-compliant consent forms and ISO references in favor of DPDP-only language. Until the SPDI Rules are formally retired in May 2027, dropping these legacy artifacts can expose a business to significant regulatory liability under Section 43A of the IT Act. Organizations should maintain a dual-control matrix, mapping internal processing activities to both sets of statutory requirements until the transition is legally complete.

To bridge the remaining compliance gap, businesses must execute a phased compliance roadmap.

Operational Phases for Transitions (May 2026 – May 2027)

Phase 1: Months 0–6 (Immediate Planning and Legacy Revalidation)

- 1) **Conduct a Comprehensive Audit:** Inventory the HR lifecycle, IT systems, and databases. Map where data is processed (inside versus outside India), identify which entities act as Data Fiduciaries, and determine which vendors act as Data Processors.
- 2) **Legacy Data Revalidation Planning:** Prior to the November 13–14, 2026 milestone, systematically revalidate all historical databases collected before the DPDP Act. Ensure that notices and consent mechanisms are updated to comply with the new statutory requirements.
- 3) **Formulate a Dual Control Matrix:** Maintain legacy SPDI written consents and ISO/IEC 27001 certifications while mapping out future DPDP controls to ensure continuous compliance during the co-existence period.

Phase 2: Months 6–12 (Ecosystem Readiness and API Integration)

- 1) **Notice and Consent Re-engineering:** Update consumer-facing interfaces to replace bundled consent with plain-language, granular, itemized notices. Ensure these notices are available in English and any of the 22 scheduled Indian languages relevant to the user base.
- 2) **Consent Manager Integration:** Prepare backend data systems to interface with registered Consent Managers. Ensure internal registries can dynamically sync with Consent Manager APIs to handle user consent withdrawals instantly.
- 3) **Vendor Contract Remediation:** Review and update third-party vendor contracts with formal Data Processing Agreements (DPAs). Contractually bind processors to strict security standards and immediate breach-reporting protocols, as the Fiduciary remains fully liable to the regulator.

Phase 3: Months 12–18 (Operational Automation and Advanced Governance)

- 1) **Deploy Automated Retention and Deletion:** Configure data retention systems to satisfy the mandatory one-year log retention requirement while automating the permanent deletion of expired data. Implement the mandatory 48-hour pre-deletion warning to data principals.
- 2) **Build User Privacy Centers:** Launch self-service privacy portals on websites and mobile applications, allowing users to exercise their rights of access, correction, erasure, and nomination. Establish internal grievance mechanisms to resolve disputes within the 90-day statutory window.
- 3) **Perform Advanced Risk Assessments:** Conduct Data Protection Impact Assessments (DPIAs) for high-risk HR and customer technologies, specifically biometrics, AI-driven screening, psychometric profiling, geolocation tracking, continuous employee monitoring, and large-scale global data transfers.
- 4) **Deploy Age Verification Workflows:** For services targeting children, integrate age-gating and deploy integration paths with government-authorized digital identity services, such as DigiLocker, to verify parental identity.

To execute this roadmap, corporate financial planning must allocate dedicated budgets. Typical compliance retrofitting cost estimates for medium-to-large-scale digital enterprises in India include:

- 1) Comprehensive Data Mapping and Gap Analysis: INR 100,000 – 200,000.
- 2) Consent Flow Redesign and API Integration: INR 200,000 – 300,000.
- 3) Linguistic Translation of Notices (3-4 languages): INR 50,000 – 100,000.
- 4) DPA Contract Remediation and Vendor Risk Assessment: INR 100,000 – 150,000.
- 5) Children's Verification & DigiLocker Integration: INR 150,000 – 200,000.

Furthermore, given that a single major security incident can attract a penalty of up to INR 2.5 billion, businesses must view Cyber Insurance as an indispensable financial risk mitigation layer. While commercial cyber insurance does not eliminate statutory liability or serve as a substitute for a comprehensive compliance program, a robust policy covering first-party forensics, business interruption, customer notification expenses, and third-party legal defense costs is highly recommended for entities in high-risk sectors like EdTech, Fintech, Healthcare, and E-commerce.

Conclusions

The parallel navigation of the European Union's GDPR and India's DPDP Act represents a critical operational reality for modern multinational corporations. While both regimes are structurally anchored in the constitutional protection of individual dignity and the right to privacy, they embody distinct regulatory philosophies, scope-based architectures, and enforcement mechanisms. The GDPR remains a highly mature, rights-heavy, and globally prescriptive model, whereas India's DPDP Act establishes a highly digitized, streamlined, and government-driven framework tailored to the socioeconomic dynamics of India's rapid digital expansion.

For businesses, achieving transnational compliance requires transitioning away from a singular, unified global privacy policy toward a highly localized, multi-tiered data governance model. Organizations must carefully reconcile the structural gaps between the two frameworks such as the absence of commercial "legitimate interests" in India, the strict one-year logging and data retention paradox, and the highly localized 22-language consent notice and Consent Manager API⁹⁵ requirements while simultaneously maintaining legacy SPDI controls during the ongoing 2025–2027 transitional phase. Ultimately, corporations that proactively embrace these dual-compliance mandates will not only shield themselves from severe financial penalties but will establish a significant competitive advantage, unlocking trust, operational resilience, and seamless market access across two of the largest consumer demographics on earth.

References and Sources

1. A COMPARATIVE LEGAL STUDY OF THE GDPR AND INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT - RJ Wave, <https://www.rjwave.org/jaafr/papers/JAAFR2601594.pdf>
2. Cross-Border Data Transfers: Reconciling Indian Law with Global Privacy Regimes, <https://www.dpo-india.com/Blogs/cross-border-data-transfers/>
3. Key difference between India's DPDP Act and EU's GDPR you should know - Complinty, <https://complinty.com/blog/compliance/key-difference-between-indias-dpdp-act-and-eus-gdpr-you-should-know/>
4. India's Digital Personal Data Protection Act, 2023 (DPDP Act) vs GDPR - Securiti, <https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/>

⁹⁵ DPDP Rules 2025 Notified by MeitY: Complete Guide, EY India

5. India's DPDP Rules 2025: Leading digital privacy compliance - Deloitte, <https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html>
6. REGULATING INNOVATION: THE IT ACT 2000 AND DPDP ACT 2023 IN THE AGE OF AI AND DATA - JETIR.org, <https://www.jetir.org/papers/JETIR2508143.pdf>
7. India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison - Latham & Watkins, <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf>
8. GDPR vs DPDP Act: Key Differences Explained - DPDP Consultants, <https://www.dpdpc consultants.com/blog.php?id=70&title=comprehensive-comparative-analysis-of-gdpr-and-dpdp>
9. FAQs on the Digital Personal Data Protection Act and Rules. - CMS INDUSLAW, <https://cms-induslaw.com/en/ind/publication/faqs-on-the-digital-personal-data-protection-act-and-rules>
10. India's New Data Privacy Rules Are Here: 8 Steps for Businesses as Key Compliance Deadlines Approach, <https://www.fisherphillips.com/en/insights/insights/indias-new-data-privacy-rules-are-here>
11. India's DPDP Timeline: Critical Compliance Deadlines for 2026-27, <https://www.indiabriefing.com/news/india-dpdp-compliance-timeline-enforcement-2026-27-44740.html/>
12. DPDPA's Global Reach: Cross-Border Data, AI Impact, and International Alignment, <https://trustarc.com/resource/dpdpas-global-reach-cross-border-data-ai/>
13. The practicalities of implementing India's Digital Personal Data Protection Act, <https://www.ibanet.org/The-practicalities-of-implimenting-India-digital-personal-data-protection-act>
14. How the DPDP Rules Impact the Insurance Sector Introduction India's current data - Tuli & Co, <https://www.tuli.co.in/pdf/2025/251210TCArticle2.pdf>
15. DPDP Act Non-Compliance Penalties: What You Must Know - VISTA InfoSec, <https://vistainfosec.com/blog/dpdp-act-non-compliance-penalties/>
16. "Comparative Analysis of the Digital Personal Data Protection Act of India 2023 and GDPR" - Pen Acclaims, <https://penacclaims.com/wp-content/uploads/2024/05/MehreenImtiaz.pdf>

17. DPDP Act Exemptions explained - changes in DPDP Rules - Consentin, <https://www.consent.in/blog/dpdp-exemptions>
18. DPDP Act vs GDPR: Key Differences for Indian Companies (2026 ..., <https://www.tcsa.in/resources/dpdp-vs-gdpr-comparison-guide>
19. The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation, <https://nyujilp.org/the-right-to-pry-vacy-understanding-indias-dystopian-data-protection-legislation/>
20. DPDP Rules 2025 Notified by MeitY: Complete guide | EY - India, https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025
21. DPDP Rules 2025: The Complete Implementation Roadmap for ..., <https://www.tcsa.in/resources/dpdp-rules-2025-implementation-roadmap>
22. Decrypting India's Data Protection Regime: Principles of Data Protection - Clyde & Co, <https://www.clydeco.com/en/insights/2025/12/decrypting-india-s-data-protection-regime-principi>
23. A Comparative Analysis of DPDP Act, GDPR, and CCPA: Understanding Global Data Privacy Regulations | Neostra, <https://www.neostra.io/blog/a-comparative-analysis-of-dpdp-act-gdpr-and-ccpa-understanding-global-data-privacy-regulations>
24. Fines / Penalties - General Data Protection Regulation (GDPR), <https://gdprinfo.eu/issues/fines-penalties/>
25. Digital Personal Data Protection Act notified after two years, RTI Act amended, <https://www.aslindia.net/public/newsletters/digital-personal-data-protection-act-notified-after-two-years-rti-act-amended>
26. Digital Personal Data Protection Act, 2023 - DPDPA SECTION 17 ..., <https://www.dpdpa.com/dpdpa2023/chapter-4/section17.html>
27. Constitutionality of the Digital Personal Data Protection Act, 2023 - Supreme Court Observer, <https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/>
28. The Data Protection Act Is Critical For Privacy, But Sweeping Provisions Threaten Right To Information, Undermine Governance & Enable A Surveillance Regime | Article14, <https://article-14.com/post/the-data-protection-act-is-critical-for-privacy-but-sweeping-provisions-threaten-right-to-information-undermine-governance-enable-a-surveillance-regime-699fbc690f3e4>

29. Data Protection Act vs the Right to Information Act - Shankar IAS Parliament, <https://www.shankariasparliament.com/blogs/pdf/data-protection-act-vs-the-right-to-information-act>
30. Impact of the Digital Personal Data Protection Act, 2023 on Third-Party Information under the Right to Information Act, 2005: A - IJFMR, <https://www.ijfmr.com/papers/2025/4/53436.pdf>
31. Are the SPDI Rules Still in Force After DPDP Act 2023? - Opsio, <https://opsiocloud.com/in/knowledge-base/are-spdi-rules-still-in-force/>
32. Does the DPDP Act 2023 Override the IT Act 2000? (India) | ConsentOS Learn, <https://consentos.in/learn/dpdp-vs-it-act/>

