INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DPDP ACT AND GDPR: CONCILIATION AND COMPARISON OF INTERNATIONAL DATA PROTECTION JURISPRUDENCE

AUTHORED BY - K. SAI KARTHIKEYAN
Damodaram Sanjivayya National Law University

ABSTRACT

This article examines India's Digital Personal Data Protection Act, 2023 (DPDP Act) through comparative analysis with the European Union's General Data Protection Regulation (GDPR). The DPDP Act was operationalized through Final Rules notified on November 13-14, 2025, establishing India's first comprehensive data protection framework, with phased implementation extending to May 2027. While the Act draws inspiration from the GDPR and has been influenced by the Brussels Effect, particularly following the Court of Justice of the European Union's landmark Schrems II decision invalidating the EU-US Privacy Shield, India's framework reveals significant divergences in rights enumeration, enforcement architecture, and cross-border transfer mechanisms.

The DPDP Act grants data principals limited rights: access, correction, erasure, grievance redressal, and nomination. Notably, it excludes data portability, objection rights, and protections against automated decision-making that characterize the GDPR's comprehensive rights catalogue. Institutional enforcement relies on a government-appointed Data Protection Board with adjudicatory powers but lacking investigative autonomy. This contrasts sharply with the EU's independent Data Protection Authorities and European Data Protection Board. Cross-border transfers under Section 16 permit permissive government notifications without adequacy assessments, diverging from the GDPR's strict adequacy determinations and standard contractual clauses refined through Schrems II jurisprudence and the 2025 Data Privacy Framework (upheld despite essential equivalence scrutiny). This analysis seeks to undertake a comparative analytical study of legislative scope and propose recommendations in light of the analysis done.

ISSN: 2582-6433

Introduction

On July 16, 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield framework in Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II), fundamentally reshaping international data transfer architecture and exemplifying the extraterritorial reach of EU data protection law. The decision demonstrated how judicial pronouncements from Luxembourg can dictate compliance obligations for entities operating beyond European borders. This underscores the Brussels Effect, whereby the European Union, through the GDPR and robust jurisprudential interpretation, establishes de facto global standards for data protection.[1] Schrems II[2] mandated that cross-border transfers to third countries must ensure essentially equivalent protection to that guaranteed within the EU, scrutinizing adequacy decisions, standard contractual clauses, and supplementary measures. Subsequently, the 2025 Data Privacy Framework (DPF), while upholding transatlantic data flows, continues to face essential equivalence scrutiny. Refinements have been proposed through the November 2025 Digital Omnibus Package, which clarifies legitimate interests, narrows personal data definitions for AI training, and reduces cookie consent requirements.

The DPDP Act represents India's first comprehensive legislative framework for digital personal data protection. While significantly influenced by the GDPR, it reflects distinct constitutional[3], developmental, and security priorities. The phased implementation timeline provides for immediate effect of Data Protection Board establishment and penalty provisions (November 2025), Consent Manager compliance by November 2026, and full obligations regarding notices, safeguards, individual rights, breach notifications, and children's protections by May 2027. This signals a gradualist approach to operationalization. This article critically analyzes the DPDP Act's scope, stakeholder categories, rights catalogue, fiduciary obligations, enforcement mechanisms, and cross-border transfer provisions in comparative perspective with the GDPR. The central research question addresses why substantial gaps persist between India's framework and global standards anchored in human dignity, despite EU influence, and what reforms are necessary to achieve substantive convergence while respecting contextual realities.

[1]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 O.J. (L 119) 1.
[2] Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ECLI:EU: C:2020:559 (CJEU, 16 July 2020).
[3] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

India's Digital Personal Data Protection Act, 2023: Scope, Stakeholders, and Implementation Framework

The DPDP Act applies to digital personal data processed within India, including processing in relation to goods or services offered to individuals in India, establishing territorial and extraterritorial jurisdiction analogous to the GDPR's Article 3. However, significant exclusions narrow its scope: personal data processed for personal or domestic purposes remains exempt, and Section 17 grants broad exemptions to governmental agencies for national security, sovereignty, public order, and law enforcement, raising proportionality concerns vis-à-vis the Puttaswamy framework articulating privacy as a fundamental right under Article 21.

The Act establishes three primary stakeholder categories. Data Principals are natural persons whose digital personal data is processed. Data Fiduciaries are entities determining the purpose and means of processing, bearing primary accountability obligations. Significant Data Fiduciaries, designated based on data volume, sensitivity, potential harm, and cross-border transfers, face enhanced obligations including mandatory Data Protection Impact Assessments (DPIAs) and periodic audits as prescribed under Rules 9-10 of the November 2025 Final Rules. This tiered approach mirrors the GDPR's distinction between controllers and processors, though the DPDP Act's concept of Data Processors remains underdeveloped.

Data Principal rights under the DPDP Act[4] are circumscribed. Section 11 grants rights to access personal data summaries, seek correction and completion of inaccurate or misleading data, demand erasure subject to compliance obligations, seek grievance redressal through fiduciary mechanisms, and nominate successors for posthumous rights exercise. Critically, the Act omits data portability (GDPR Article 20), objection rights to processing (GDPR Article 21), and protections against automated decision-making including profiling (GDPR Article 22). These omissions substantially weaken individual autonomy and control, particularly in AI-driven ecosystems where automated processing increasingly determines access to services, credit, employment, and social opportunities.

Data Fiduciary obligations encompass lawful grounds for processing, purpose limitation, data minimization, accuracy maintenance, storage limitation, and reasonable security safeguards. Section 6 permits processing based on consent or specified legitimate uses enumerated under

[4] Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025), Gazette of India (India).

ISSN: 2582-6433

Section 7, including voluntary data provision, contract performance, state functions, medical emergencies, employment, and reasonable expectations. Consent must be free, specific, informed, and unconditional, with withdrawal mechanisms mandated under Rules 4-5. Breach notification obligations under Section 8 require fiduciaries to notify the Data Protection Board and affected data principals in prescribed form within specified timelines, operationalized through Rules 7-8. Children's data receives enhanced protection under Section 9, prohibiting processing for behavioral monitoring, targeted advertising, or tracking, with parental consent required through verifiable mechanisms under Rule 6.

Institutional enforcement vests exclusively in the Data Protection Board established under Section 18, comprising a chairperson and members appointed by the central government, serving staggered terms to ensure continuity. The Board's powers under Section 28 include adjudicating complaints, imposing penalties up to ₹250 crore for violations, and issuing directions for compliance. However, the Board lacks proactive investigative or audit powers absent complaints, limiting preventive enforcement. Penalties distinguish between individual contraventions (up to ₹200 crore) and breach of children's data protections (up to ₹250 crore), signaling prioritization of minors' privacy. Section 16 governs cross-border transfers, permitting transfers to countries or territories notified by the central government without adequacy assessments or safeguards akin to GDPR Chapter V mechanisms.

The Final Rules notified on November 13-14, 2025, operationalize these provisions through phased implementation. Immediate effectiveness attaches to Data Protection Board establishment, penalty provisions, and appellate mechanisms. Consent Managers (intermediaries facilitating consent grant, management, and withdrawal under Section 15) must achieve compliance by November 2026, operationalized through Rules 11-13. Full obligations regarding data principal notices, security.

Comparative Analysis: DPDP Act and GDPR Divergences

The EU GDPR, effective since May 25, 2018, establishes comprehensive data protection principles anchored in human dignity as articulated in the Charter of Fundamental Rights[5]. Article 7 (respect for private and family life) and Article 8 (protection of personal data)

[5]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 O.J. (L 119) 1 (EU).

ISSN: 2582-6433

constitute foundational guarantees, complemented by European Convention on Human Rights Article 8. The GDPR's rights catalogue under Chapter III is expansive: information rights (Articles 13-14), access (Article 15), rectification (Article 16), erasure/'right to be forgotten' (Article 17), restriction of processing (Article 18), data portability (Article 20), objection (Article 21), and protections against automated decision-making including profiling (Article 22). These rights empower individuals with meaningful control over their personal data, enabling them to challenge processing activities, demand portability to alternative service providers, and object to processing based on legitimate interests or direct marketing.

In stark contrast, the DPDP Act's rights enumeration under Section 11 is narrower, granting only access, correction, erasure, grievance redressal, and nomination rights. The absence of portability prevents data principals from seamlessly switching service providers, entrenching market dominance and reducing competition. The omission of objection rights deprives individuals of mechanisms to contest processing based on legitimate uses under Section 7, particularly problematic given broad governmental exemptions under Section 17. Most critically, the lack of protections against automated decision-making fails to address algorithmic accountability in credit scoring, employment screening, and social profiling, where opaque AI systems increasingly determine life opportunities without meaningful human oversight or explanation rights.

Enforcement architecture reveals profound institutional divergences. The GDPR establishes independent Data Protection Authorities (DPAs) in each Member State under Article 51, mandated to exercise powers independently without external influence. The European Data Protection Board (EDPB) ensures consistent application across the Union through binding decisions, guidelines, and the one-stop-shop mechanism for cross-border processing under Article 56. DPAs possess investigative powers (Article 58(1)), corrective powers including administrative fines up to €20 million or 4% of global annual turnover (Article 58(2)), and authorization/advisory powers (Article 58(3)). This tripartite authority enables proactive supervision, preventive audits, and binding enforcement absent individual complaints. The November 2025 Digital Omnibus Package proposes further streamlining through harmonized procedural rules and enhanced EDPB coordination, reinforcing the precautionary principle central to EU data governance.[6]

[6] Anupam Guha, *India's Digital Personal Data Protection Act 2023 vs the GDPR: A Comparison* (Latham & Watkins 2023).

ISSN: 2582-6433

Conversely, the DPDP Act's Data Protection Board under Section 18 comprises government-appointed members without statutory independence guarantees or fixed tenures insulating them from political influence. Section 28 confines the Board's mandate to adjudicating complaints and imposing penalties, lacking proactive investigative, audit, or supervisory powers characteristic of independent regulators. This reactive model renders enforcement contingent upon individual data principals initiating complaints, undermining systemic accountability for widespread or covert violations. The Board cannot conduct sua sponte investigations, mandate DPIAs, or audit Significant Data Fiduciaries' compliance practices absent specific complaints, creating enforcement gaps particularly acute for surveillance technologies, biometric processing, and governmental data practices exempted under Section 17.

Essential equivalence assessments, scrutinizing surveillance laws, redress mechanisms, and judicial oversight in recipient countries. Subsequently, the 2025 Data Privacy Framework introduced enhanced safeguards, including necessity and proportionality requirements, independent review by the Data Protection Review Court, and binding redress mechanisms, which the CJEU upheld in 2025 rulings, though continued monitoring ensures ongoing compliance with essential equivalence standards.

Section 16 of the DPDP Act permits cross-border transfers to countries or territories notified by the central government, without mandating adequacy assessments, standard contractual clauses, binding corporate rules, or supplementary measures. This permissive approach prioritizes developmental imperatives and trade facilitation over rights protection, enabling unrestricted data flows to jurisdictions lacking equivalent protections or effective remedies.[7] The absence of adequacy frameworks risks exposing Indian data subjects to surveillance, arbitrary access, and inadequate redress in recipient countries, particularly concerning given Section 17 exemptions permitting extensive governmental access domestically. Furthermore, the Rules do not operationalize alternative transfer mechanisms analogous to SCCs or BCRs, leaving fiduciaries without standardized tools to demonstrate adequate safeguards.

Philosophically, these divergences reflect contrasting regulatory paradigms. The GDPR embodies a rights-centric model grounded in human dignity, treating personal data as an extension of individual personality and autonomy per the Charter's precautionary orientation.

[7] Digital Personal Data Protection Act § 16 (India).

ISSN: 2582-6433

Restrictions on fundamental rights must satisfy strict necessity and proportionality tests, with independent judicial and regulatory oversight ensuring accountability. India's DPDP Act reflects a security-pragmatic model balancing individual privacy against developmental priorities, national security, and state sovereignty. Section 17 exemptions, governmental Board appointments, reactive enforcement, and permissive transfer mechanisms prioritize state prerogatives over individual autonomy, reflecting constitutional traditions where fundamental rights under Part III are subject to reasonable restrictions under Articles 19(2)-(6) and Article 21's positive obligations for state welfare functions. While the Supreme Court's Puttaswamy decision established privacy as intrinsic to life and liberty under Article 21, requiring state limitations to satisfy proportionality (legitimate aim, suitability, necessity, and balancing), the DPDP Act's exemptions and enforcement architecture do not consistently operationalize these constitutional requirements.[8]

Recommendations for Strengthening India's Data Protection Framework in light of comparative jurisprudence

To achieve substantive convergence with global standards while respecting India's constitutional and developmental context, legislative and regulatory reforms across five domains are essential.

First, expanding the rights catalogue is imperative. Parliament should amend the DPDP Act to incorporate data portability rights enabling data principals to obtain and reuse personal data across service providers in structured, commonly used, machine-readable formats. This facilitates competition, prevents vendor lock-in, and empowers individuals to exercise meaningful choice in digital markets dominated by platform monopolies.

Objection rights must permit data principals to contest processing based on legitimate uses under Section 7, subject to fiduciaries demonstrating compelling legitimate grounds overriding individual interests. Most critically, protections against automated decision-making should mandate human intervention, explanation rights, and contestation mechanisms for decisions producing legal or similarly significant effects, addressing algorithmic opacity in credit, employment, and welfare determinations. These amendments align with Puttaswamy principles recognizing informational privacy as enabling individual autonomy and dignity.

[8] ibid

ISSN: 2582-6433

Second, institutional independence requires statutory guarantees insulating the Data Protection Board from governmental influence. Amendments should establish transparent appointment processes involving multi-stakeholder selection committees, fixed tenures with removal only for specified misconduct, and financial autonomy through dedicated budgetary allocations. Section 28 should be expanded to vest the Board with proactive investigative powers, enabling sua sponte inquiries into systemic violations, mandatory audit authority over Significant Data Fiduciaries, and binding advisory powers to issue sectoral codes of practice. Independent regulatory capacity, modeled on successful autonomous bodies like the Competition Commission of India and Securities and Exchange Board of India, is essential to prevent regulatory capture and ensure even-handed enforcement against governmental and private actors alike.

Third, preventive safeguards should be mandated. Data Protection Impact Assessments (DPIAs) must be required for all high-risk processing activities, including biometric identification, large-scale profiling, sensitive data processing, and systematic monitoring, not merely Significant Data Fiduciaries' discretionary audits. DPIAs should assess necessity, proportionality, risks to rights and freedoms, and mitigation measures, with Board review authority for high-risk determinations. Mandatory appointment of Data Protection Officers (DPOs) with defined qualifications, organizational independence, and reporting obligations to the Board would embed accountability within fiduciary structures. Privacy by design and by default principles should be statutorily mandated, requiring technical and organizational measures to implement data protection principles from design inception and default settings minimizing processing. These preventive measures shift compliance culture from reactive remediation to proactive risk management, reducing harm incidence rather than merely penalizing violations ex post.

Fourth, governmental exemptions under Section 17 require substantial narrowing and procedural safeguards. Drawing from Puttaswamy's proportionality framework, exemptions should be limited to demonstrably necessary purposes with procedural safeguards including: legislative authorization specifying permissible purposes and retention periods; independent oversight by designated authorities with ex ante approval requirements for surveillance activities; judicially reviewable decisions with effective remedies for unlawful access; and periodic parliamentary review ensuring continued necessity. Blanket exemptions for national security, public order, and sovereignty undermine rule of law and constitutional accountability.

ISSN: 2582-6433

Proportionate exemptions, as recognized in GDPR Article 23 limiting rights only to the extent necessary for specified purposes with safeguards, balance legitimate state functions against fundamental rights protection.

Fifth, cross-border transfer mechanisms must incorporate adequacy assessments and standardized safeguards. Section 16 should be amended to require adequacy determinations by the Data Protection Board assessing recipient countries' legal frameworks, surveillance practices, enforcement capabilities, and redress mechanisms. Where adequacy is absent, standard contractual clauses and binding corporate rules should provide contractual safeguards ensuring enforceable rights and effective remedies. Drawing from Schrems II, adequacy assessments must evaluate essential equivalence, scrutinizing limitations on governmental access, independent oversight, and judicial remedies. This multilayered framework, incorporating supplementary measures where necessary, balances legitimate international data flows with effective protection, positioning India as a credible interlocutor in cross-border data governance negotiations and enhancing prospects for EU adequacy recognition.

Conclusion

India's Digital Personal Data Protection Act, 2023, represents a significant milestone in establishing a comprehensive data protection framework, influenced by the GDPR's Brussels Effect and operationalized through phased implementation extending to May 2027. However, this comparative analysis reveals substantial divergences in rights enumeration, enforcement architecture, and cross-border transfer mechanisms that position India's framework as significantly weaker than the GDPR's rights-centric model anchored in human dignity. The absence of data portability, objection rights, and automated decision-making protections; the lack of independent regulatory oversight with proactive investigative powers; broad governmental exemptions insufficiently constrained by proportionality safeguards; and permissive cross-border transfers without adequacy assessments collectively undermine the DPDP Act's capacity to protect individual autonomy and dignity in data-driven ecosystems.

These gaps are not merely technical deficiencies but reflect fundamental philosophical divergences between the EU's precautionary, rights-centric approach treating personal data as an extension of individual personality, and India's security-pragmatic model balancing privacy against developmental imperatives and state sovereignty. While contextual variations are inevitable and appropriate, the Puttaswamy decision's constitutional framework (recognizing

ISSN: 2582-6433

privacy as intrinsic to life and liberty under Article 21 and mandating proportionality tests for limitations) provides normative foundations for substantive reform. Implementing the recommended amendments, which include expanding rights, strengthening institutional independence, mandating preventive safeguards, narrowing exemptions, and establishing robust transfer mechanisms, would align India's framework with constitutional principles and global standards. This would position India as a credible leader in data governance rather than a regulatory outlier.

As digital technologies, artificial intelligence, biometric surveillance, and transnational data flows intensify, the trajectory of India's data protection regime will significantly influence global privacy governance. Whether India evolves toward rights-centric convergence through legislative reform and judicial interpretation expanding Puttaswamy principles, or entrenches state-centric pragmatism prioritizing developmental and security prerogatives over individual autonomy, will shape whether data protection emerges as a universally enforceable human right or fragments into competing regional paradigms reflecting divergent constitutional traditions. The choice confronting Indian policymakers is clear: substantive reform aligned with human dignity and rule of law, or continued divergence risking regulatory isolation and diminished protection for millions navigating increasingly datafied lives.

IJLRA