

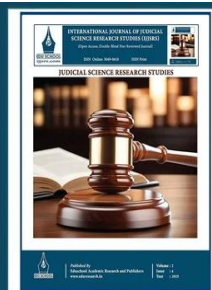


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Cross-Border Data Protection: Comparative Analysis of GDPR and India's DPDP Act

Sharmila

Indian Institute of Management, Rohtak, India.

Article information

Received: 5th June 2026

Received in revised form: 20th June 2026

Accepted: 12th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0049>

Abstract

The General Data Protection Regulation 2016 and India's Digital Personal Data Protection Act 2023 represent two of the most consequential data-protection instruments globally. They share structural commitments to individual rights, principles-based processing, and accountability-based compliance, while differing in material respects on cross-border transfer mechanisms, sensitive-data classification, public-authority exemptions, regulator independence, and enforcement architecture. This paper offers a comparative doctrinal analysis of the two regimes with particular attention to cross-border data transfers, a site of sustained regulatory innovation since the 2020 Schrems II decision invalidated the EU-US Privacy Shield. It examines the GDPR's Chapter V mechanisms adequacy decisions, standard contractual clauses, binding corporate rules, and derogations—and the DPDP Act's section 16 notified-jurisdictions framework. The paper argues that India's post-2023 position is converging with European practice but retains structural differences in the public-authority and government-access domains that complicate the prospect of a reciprocal adequacy arrangement. It proposes calibrated reforms to support interoperability.

Keywords:- Data protection, GDPR, DPDP Act, cross-border transfers, adequacy, Schrems II, Puttaswamy, digital rights

I. INTRODUCTION

Data protection has become a defining field of twenty-first-century law. The European Union's General Data Protection Regulation (GDPR), in force since May 2018, established a horizontal framework with global influence. India's Digital Personal Data Protection Act 2023 (DPDP Act), enacted in August 2023 and commencing through staged notification, represents the culmination of more than a decade of legislative effort following the Supreme Court's recognition of privacy as a fundamental right in Puttaswamy (2017). The two frameworks jointly govern the personal data of more than 1.8 billion individuals and influence data-protection practice across numerous jurisdictions.

Cross-border data transfers are central to the digital economy and constitute a particular site of regulatory innovation. Cloud services, software-as-a-service, global payment processing, cross-border healthcare, and multinational employee management all depend on the routine movement of personal data across jurisdictional boundaries. Regulatory regimes must reconcile this reality with protective standards that may differ substantially between origin and destination jurisdictions.

This paper offers a comparative doctrinal analysis of the GDPR and the DPDP Act, with particular attention to cross-border transfer mechanisms. It proceeds in six steps: foundational context (Puttaswamy and the GDPR adoption); GDPR core architecture; DPDP Act structure and scope; cross-border transfer mechanisms under each regime; gaps, convergences, and interoperability prospects; and recommendations. The paper argues that Indian law is broadly converging with European practice, with residual differences concentrated in public-authority exemptions and government-access frameworks that may complicate the prospect of reciprocal adequacy.

II. PRIVACY AS A FUNDAMENTAL RIGHT: PUTTASWAMY'S LEGACY

The Indian Supreme Court's unanimous Nine-Judge Bench decision in *K. S. Puttaswamy v. Union of India* (2017) held that the right to privacy is a fundamental right under Part III of the Constitution, protected under articles 14, 19, and 21. The judgment articulated a tripartite test for legitimate interference:

- legality, requiring a basis in validly enacted law;
- necessity, meaning a legitimate state aim; and
- proportionality, requiring that the measure be the least restrictive means to achieve the aim.

The decision grounded subsequent privacy jurisprudence, including *Puttaswamy II* (2018) on Aadhaar and subsequent data-protection developments.

The *Puttaswamy* framework mirrors the Charter of Fundamental Rights of the European Union's Article 8 on personal data protection and the European Court of Human Rights' Article 8 jurisprudence on private life. The GDPR gives effect to Charter Article 8 and ECHR Article 8 through comprehensive statutory implementation, including the appointment of independent supervisory authorities, codification of data-subject rights, and robust enforcement mechanisms with administrative fines up to EUR 20 million or 4 percent of global annual turnover.

The trajectory from *Puttaswamy* to the DPDP Act was lengthy. The Srikrishna Committee's 2018 draft, the Personal Data Protection Bill 2019, and iterative revisions preceded the DPDP Bill 2022 and the enacted DPDP Act 2023. The final text diverges in material respects from the Srikrishna draft, including on data-localization, public-authority exemptions, and regulator appointment mechanisms.

III. GDPR: CORE ARCHITECTURE

The GDPR applies to the processing of personal data by controllers and processors either established in the European Union or targeting data subjects in the European Union (Articles 2 and 3). It articulates six processing principles in Article 5: lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality, with accountability as an overarching principle.

Lawful bases for processing (Article 6) include consent, contractual necessity, legal obligation, vital interests, public task, and legitimate interests. Special categories of data (Article 9) racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometric data, health, and sexual orientation are subject to heightened protection with an additional set of narrow permissions.

Data-subject rights (Articles 12–22) include the rights to information, access, rectification, erasure, restriction, data portability, objection, and protection against solely automated decision-making with legal or similarly significant effects. These rights are individually actionable and supported by the supervisory authorities' investigatory and enforcement powers under Chapter VI and VII.

Cross-border transfers are governed by Chapter V. A transfer to a third country or international organization requires either:

- an adequacy decision by the Commission;
- appropriate safeguards such as standard contractual clauses, binding corporate rules, approved codes of conduct, or certification schemes; or
- derogation for specific situations under Article 49. \

The Court of Justice's *Schrems II* decision (2020) invalidated the EU-US Privacy Shield adequacy decision and conditioned SCC use on case-by-case assessment of third-country law, with supplementary measures as needed. The EU-US Data Privacy Framework adopted in July 2023 restored an adequacy decision for certified US organizations, subject to ongoing legal challenge.

IV. DPDP ACT 2023: STRUCTURE AND SCOPE

The DPDP Act applies to the processing of digital personal data within India and to processing outside India in connection with offering goods or services to data principals in India (section 3). The Act is notably concise relative to the GDPR twenty-five numbered sections plus definitions and schedules reflecting a principles-based design with significant implementation to be specified in subordinate rules.

Core provisions include consent as the default lawful basis (section 6), with 'legitimate uses' serving as a limited additional basis (section 7) covering specified situations such as government services, medical emergencies, and employment contexts. Data fiduciaries (equivalent to GDPR controllers) owe duties of accurate processing, data minimization, security safeguards, breach notification to the Data Protection Board and affected data principals, and limited retention (section 8).

Data-principal rights (Chapter III) include rights to information, correction and erasure, grievance redress, and nomination. The Act does not include a right to data portability or a specific right analogous to GDPR Article 22 on automated decision-making, gaps that have attracted scholarly criticism.

The enforcement architecture centers on the Data Protection Board of India (sections 18–27). The Board may impose penalties up to INR 2.5 billion (approximately EUR 25 million) per violation. Critics note that the Board's appointment by the Central Government, absence of judicial-power recognition, and limited procedural safeguards create concerns about regulator independence. The Act provides substantial exemptions for government processing, including where the Central Government notifies an instrumentality as exempted under section 17(2).

Significantly, the DPDP Act's treatment of cross-border transfers (section 16) shifts away from the localization models of earlier drafts. The Central Government may restrict transfers to specified jurisdictions by notification; in the absence of

such restriction, transfers are permitted. This 'blacklist' approach contrasts with the GDPR's 'whitelist' adequacy model and with the localization requirements of some other jurisdictions.

V. CROSS-BORDER TRANSFER MECHANISMS AND ADEQUACY PROSPECTS

The GDPR and DPDP Act adopt structurally different approaches to cross-border transfers. The GDPR restricts transfers to third countries absent adequacy, appropriate safeguards, or derogations, reflecting a precautionary logic that places the burden of protection on the exporter. The DPDP Act permits transfers except to notified restricted jurisdictions, reflecting a permissive default with discretionary governmental restriction.

The practical implications differ. Under the GDPR, an Indian data importer handling EU personal data must rely on the EU-Indian adequacy decision (not currently in place), SCCs supplemented by case-by-case assessment under Schrems II, binding corporate rules, or Article 49 derogations. The EU has not issued an adequacy decision for India; the Schrems II assessment burden is non-trivial, particularly in view of Indian government-access frameworks such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 and the Telecommunications (Temporary Suspension of Services) Rules 2017.

Under the DPDP Act, an EU data importer handling Indian personal data need only comply with the Act's general obligations, subject to restriction notifications under section 16. This asymmetry—stricter EU restrictions on outbound transfers to India, combined with more permissive Indian restrictions on outbound transfers to the EU creates a de facto imbalance in cross-border flows.

The prospects for an EU-India adequacy decision depend on three factors. First, the extent to which the DPDP Act's rule-specified operational details provide protections comparable to the GDPR, particularly on data-principal rights, regulator independence, and enforcement. Second, the treatment of government-access requests under Indian law, including the interaction with the Information Technology Act 2000's section 69 and recent decisions on surveillance-law constitutionality. Third, institutional trust between the Commission and the Indian authorities. Recent negotiations on EU-India trade and digital-economy cooperation have created some momentum, but the adequacy-specific dialogue remains at an early stage.

Bilateral corporate mechanisms offer a more immediate path. SCCs may be adapted for EU-India transfers; emerging Indian SCCs, if promulgated under DPDP Act rules, could be reciprocally recognized. The ASEAN Model Contractual Clauses and APEC Cross-Border Privacy Rules provide potential templates for regional harmonization.

VI. CONVERGENCES, DIVERGENCES, AND GAPS

Four convergences are notable. First, both regimes enshrine consent as the presumptive lawful basis for processing. Second, both regulate data-controller/fiduciary accountability through obligations of purpose limitation, minimization, security, and breach notification. Third, both provide individual rights of access, correction, and erasure. Fourth, both adopt an extraterritorial scope that captures processing outside the regulating jurisdiction where directed at data subjects within.

Four divergences are significant. First, the DPDP Act lacks an Article 22 equivalent on solely automated decision-making, leaving Indian individuals without an explicit right to contest algorithmic decisions. Second, the DPDP Act does not classify data categories with the GDPR's specificity; all personal data is subject to uniform protection, though sensitive-data designation may emerge through rules. Third, the DPDP Act's public-authority exemptions are broader than the GDPR's, particularly under section 17(2). Fourth, regulator independence and procedural safeguards in enforcement differ, with the Data Protection Board more closely tied to executive appointment than the typical GDPR supervisory authority.

Beyond these structural differences, implementation gaps are significant. The DPDP Act's commencement is staged through rule notification; at the time of writing, key rules on data-fiduciary classifications, cross-border restrictions, children's data, and grievance mechanisms are at varying stages of consultation. Effective protection depends heavily on rule-level specification and on the eventual operational capacity of the Data Protection Board.

VII. RECOMMENDATIONS AND CONCLUSION

Five reforms would strengthen interoperability between the GDPR and DPDP Act frameworks. First, the DPDP Act rules should specify categories of sensitive data subject to heightened protection, drawing on the GDPR Article 9 taxonomy adapted for Indian context. Second, provisions analogous to GDPR Article 22 on automated decision-making should be introduced, either in the DPDP Act or through a successor Digital India Act. Third, regulator independence should be strengthened through staggered appointments, judicial involvement in selection, and enhanced procedural protections.

Fourth, cross-border transfer mechanisms should be specified with clarity. The DPDP Act's section 16 notification framework should be complemented by Indian standard contractual clauses and a pathway for EU-India adequacy dialogue. Reciprocal recognition of binding corporate rules, building on EU practice, would support multinational compliance.

Fifth, government-access frameworks should be reformed to meet the proportionality and accountability standards implied by Puttaswamy. Modernization of surveillance laws, judicial authorization requirements, and transparency reporting would align Indian practice with international standards and support adequacy dialogues.

This paper has argued that the GDPR and DPDP Act represent convergent but distinct approaches to data protection. Convergence is substantial on principles and individual rights; divergence persists on public-authority exemption, regulator independence, and government-access architecture. Closing these gaps would strengthen both frameworks, support cross-border data flows, and ensure that the Puttaswamy promise of privacy as a fundamental right is operationalized in the digital economy. Data protection is no longer a technical specialism; it is a foundational layer of twenty-first-century law.

REFERENCES

- Asia-Pacific Economic Cooperation. (2011). *APEC cross-border privacy rules system*.
- Association of Southeast Asian Nations. (2021). *ASEAN model contractual clauses for cross-border data flows*.
- Charter of Fundamental Rights of the European Union. (2012). *Official Journal of the European Union*, C 326, 391.
- Court of Justice of the European Union. (2020). *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II)*, Case C-311/18, EU:C:2020:559.
- Court of Justice of the European Union. (2023). *SCHUFA Holding AG v. OQ*, Case C-634/21, EU:C:2023:957.
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India.
- European Commission. (2023). *Commission implementing decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final.
- European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. (2016). *Official Journal of the European Union*, L 119, 1.
- Greenleaf, G. (2023). India's data protection act 2023: Rules await to fill in many gaps. *Privacy Laws & Business International Report*, 183, 1–9.
- Information Technology Act, No. 21 of 2000, Acts of Parliament, India.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. (2021). India.
- Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.
- Puttaswamy v. Union of India (Puttaswamy I), (2017) 10 SCC 1 (India).
- Puttaswamy v. Union of India (Puttaswamy II – Aadhaar), (2019) 1 SCC 1 (India).
- Srikrishna, B. N. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna.