INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 1 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 1 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-1-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RIGHTS-FIRST VS. ECONOMY-FIRST: A COMPARATIVE ANALYSIS OF THE GDPR AND INDIA'S DPDP ACT

AUTHOR - NIHARIKA JAISWAL* & DR. KAVYA CHANDEL**

* LLM (CYBER LAW AND CYBER SECURITY), AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

** AMITY LAW SCHOOL, AMITY UNIVERSITY UTTAR PRADESH, LUCKNOW CAMPUS

BEST CITATION - NIHARIKA JAISWAL & DR. KAVYA CHANDEL, RIGHTS-FIRST VS. ECONOMY-FIRST: A COMPARATIVE ANALYSIS OF THE GDPR AND INDIA'S DPDP ACT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (1) OF 2026, PG. 641-646, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The global architecture of data privacy governance stands at a turning point. For nearly a decade, it has been shaped by the "Brussels Effect" of the European Union's GDPR. However, India's Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a distinct, development-oriented paradigm that prioritizes economic growth and digital innovation over a strict rights-based framework. This paper comparatively analyses these two models, arguing that while the GDPR operates as a robust "shield" safeguarding individual dignity and autonomy, the DPDP Act functions as a flexible "umbrella" framework designed to facilitate ease of business and technological expansion.

The study highlights key structural divergences. Unlike the GDPR's technology-neutral scope, the DPDP Act applies only to digital personal data, excluding physical records. It also reflects a dilution of certain core data subject rights, such as data portability, the right to object to processing, and safeguards against automated decision-making. Furthermore, while the GDPR imposes turnover-based penalties, India adopts fixed penalty caps, offering regulatory predictability. Ultimately, India's economy-first approach promotes growth but raises concerns about long-term citizen protection.

Keywords: GDPR, DPDP Act, Data Privacy, Digital Economy, Cross-Border Data Flows, Brussels Effect, Privacy Rights.

1.1 Introduction: The Divergent Paths of Global Privacy Governance

The global architecture of data privacy governance has arrived at a critical juncture. For nearly a decade, the European Union's General Data Protection Regulation (GDPR) has served as the normative hegemon, a "gold standard" that has influenced legislative drafting from Brazil to Japan, propagating what scholar Anu Bradford terms the "Brussels Effect." The GDPR is rooted in the post-war European constitutional order, treating privacy as a fundamental human right essential to dignity and autonomy, and as a safeguard against both corporate surveillance and state overreach.[1474] However, the enactment of India's Digital Personal Data Protection Act (DPDP Act) on August 11, 2023, signals the emergence of a distinct competing paradigm: a "developmental" privacy framework that seeks to balance individual rights with the sovereign necessity of data utilisation for economic growth and public administration.[1475]

[1474] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[1475] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The genesis of the DPDP Act lies in the landmark Supreme Court judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), which recognised a fundamental right to privacy under Article 21 of the Constitution of India.[1476] Yet, the resulting legislation, after traversing the abandoned 2019 Bill and the 2022 draft, has crystallised into a form that prioritises "simplicity" and "innovation" over the granular, rights-heavy approach of the GDPR.[1477] This analysis dissects these frameworks across structural, functional, and enforcement dimensions, illustrated by case studies of the CoWIN data-breach allegations and Meta's €1.2 billion GDPR fine, to forecast the operational realities of India's new digital regime.

1.2 Structural and Philosophical Divergences

The most immediate distinction between the GDPR and the DPDP Act lies in their volume and texture. The GDPR is a sprawling document of 99 Articles and 173 Recitals, offering dense, prescriptive guidance. The DPDP Act, in contrast, is "umbrella legislation" comprising only 44 Sections, leaving substantial procedural detail to be defined in subsequent rules.[1478] This brevity is a deliberate design choice aimed at a flexible, principle-based law, but it introduces significant ambiguity relative to the codified certainty of the EU model.

1.2.1 Material Scope: The Analogue-Digital Divide

A foundational divergence exists in the material scope of applicability. The GDPR adopts a technology-neutral stance. As per Article 2, it applies to the processing of personal data wholly or partly by automated means, and importantly, to "non-automated processing of personal data which forms part of a filing system or is intended to form part of a filing system".[1479] This ensures that physical records, such as paper files in a doctor's cabinet or a filing room, are subject to the same privacy standards as a cloud database.

The implications of this "digital-only" scope are profound for a country such as India, where digitising legacy records remains an ongoing project. Furthermore, the DPDP Act explicitly exempts "personal data that is made or caused to be made publicly available" by the Data Principal or by legal obligation.[1480] This creates a massive exception for data scraped from social media or public records, a resource heavily exploited by AI developers, which remains strictly regulated under the GDPR.[1481]

1.2.2 Territorial Reach and Extraterritoriality

Both frameworks exhibit strong extraterritorial ambitions, yet their jurisdictional triggers differ in nuance.

- **GDPR (Article 3):** The regulation applies to processing by controllers established in the EU, regardless of where the processing takes place. Crucially, it extends to non-EU entities if they either (a) offer goods or services to data subjects in the Union, or (b) *monitor the behaviour of data subjects as their behaviour* takes place within the Union.[1482]
- **DPDP Act (Section 3):** The Indian law applies to processing within India and extends to processing outside India if it is "in connection with any activity related to offering of goods or services to Data Principals within the territory of India".[1483]

The critical divergence here is the absence of "monitoring" or "profiling" as independent jurisdictional triggers under the DPDP Act.[1484] A foreign analytics firm that tracks Indian users for research or surveillance purposes, without offering them any goods or services, arguably falls outside the DPDP Act's territorial scope.

[1476] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[1477] Carnegie Endowment for International Peace, "Understanding India's New Data Protection Law" (Oct. 3, 2023).
[1478] DPDP Act, 2023, Section 40; *see also* Linklaters, "Data Protected - India" (Feb. 2024).
[1479] GDPR, art. 2(1).
[1480] DPDP Act, 2023, Section 3(c)(ii).
[1481] Bridge Counsels, "Text and Data Mining vs India's Digital Personal Data Protection Act 2023", *Bridge Counsels* (2023).
[1482] GDPR, art. 3(2).
[1483] DPDP Act, 2023, Section 3(b).
[1484] Khaitan & Co, "Comparison of the DPDP Act 2023 with GDPR and Global Privacy Laws", *KCO* (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

1.2.3 Categorisation of Data: The Vanishing "Sensitive" Category

One of the most radical structural shifts in the DPDP Act is the flattening of data taxonomies. The GDPR, under Article 9, establishes a rigid distinction between "Personal Data" and "Special Categories of Personal Data" (often referred to as sensitive data). This special category includes data revealing racial or ethnic origin, political opinions, religious beliefs, biometric data, and health data.[1485] Processing such data is prohibited unless a specific exception applies.

The DPDP Act abolishes this tiered classification entirely.[1486] It treats all personal data with a uniform baseline of protection. Financial data, biometric scans, health records, and caste information are treated with the same legal weight as a name or an email address.[1487] While this simplification reduces compliance friction for fintech and health-tech sectors, it represents a regression from a rights perspective, particularly given the ubiquity of Aadhaar (India's biometric ID) in daily life.[1488]

1.2.4 Lawful Bases: Consent and "Legitimate Uses"

The GDPR provides six lawful bases for processing (Article 6): Consent, Contract, Legal Obligation, Vital Interests, Public Task, and Legitimate Interests. The DPDP Act narrows this spectrum primarily to two: **Consent** and **Certain Legitimate Uses**.[1489]

The concept of "Legitimate Uses" in Section 7 of the DPDP Act is conceptually distinct from the GDPR's "Legitimate Interests."

- **GDPR Legitimate Interest:** A flexible, open-ended basis where the controller must conduct a balancing test.
- **DPDP Act Legitimate Use:** A closed, statutorily defined list.[1490] It includes situations in which the Data Principal has voluntarily provided data, data processing for State subsidies or benefits, medical emergencies, and employment purposes.[1491]

Critically, the DPDP Act effectively removes "Contractual Necessity" and "Legitimate Interest" (in the business sense) as independent bases, thereby imposing heavy reliance on Consent for private-sector operations.

1.3 Divergences in Rights: The Silence on Profiling and Exemptions

The suite of rights granted to individuals termed "Data Principals" in India and "Data Subjects" in the EU reveals the differing priorities of the two regimes.

1.3.1 The Missing Rights: Portability and Objection

Right to Data Portability (Article 20 GDPR):

The GDPR allows users to receive their personal data in a structured, commonly used, and machine-readable format.

- **Indian Context:** The DPDP Act does not include a Right to Data Portability.[1492] This omission is likely intended to reduce the technical compliance burden on startups and SMEs, but it significantly disempowers consumers by reinforcing the "walled gardens" of large tech platforms.[1493]

Right to Object (Article 21 GDPR):

Under GDPR, individuals can object to processing based on "public task" or "legitimate interests."

- **Indian Context:** The DPDP Act confers no general right to object to processing. A Data Principal can withdraw consent, but this only stops *future* processing and does not apply to processing based on

[1485] GDPR, art. 9.
[1486] Securiti.ai, "India Digital Personal Data Protection Act vs. GDPR", *Securiti.ai Blog*.
[1487] Record of Law, *supra* note 4.
[1488] *Id.*
[1489] DPDP Act, 2023, Section 4.
[1490] DPDP Act, 2023, Section 7.
[1491] Baker Botts, "India Notifies Final Rules for Digital Data Protection Act", *Baker Botts* (Nov. 2025).
[1492] Baker Botts, "India Notifies Final Rules for Digital Data Protection Act", *Baker Botts* (Nov. 2025).
[1493] *Id.*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

"Legitimate Uses" (e.g., employment or state benefits).[1494]

1.3.2 Automated Decision-Making and Profiling (Article 22)

The most glaring techno-legal divergence concerns Article 22 of the GDPR, which grants the data subject the right *not* to be subject to a decision based solely on automated processing, including profiling.

- **The Indian Void:** The DPDP Act is notably silent on "profiling," "automated decision making," and "behavioural monitoring" for adults.[1495] There is no statutory right to demand human intervention in an algorithmic decision.
- **Implications:** As India rapidly integrates AI into credit scoring and hiring, the absence of an Article 22 equivalent means a loan applicant rejected by an AI algorithm may have no legal basis under privacy law to demand an explanation or a human review.[1496]

1.3.3 The Introduction of Duties

A unique feature of the DPDP Act is the imposition of **Duties** on the Data Principal (Section 15). Users are legally obligated not to register false grievances or furnish false information.[1497] Breach of these duties can result in penalties of up to ₹10,000.[1498] This marks a philosophical shift from the GDPR, which views the individual primarily as a vulnerable entity needing protection.

1.3.4 Right to Erasure and its Exceptions

- **GDPR (Article 17):** Erasure can be denied for public health, archiving, scientific research, or legal claims.[1499]
- **DPDP Act (Section 12):** A Data Principal can request erasure, and the Data Fiduciary must erase data unless retention is "necessary for the specified purpose" or for compliance with any law.[1500]
- **The "Outsourcing" Loophole:** Section 17 of the DPDP Act exempts processing by Indian entities of foreign data (pursuant to a contract) from the Right to Erasure.[1501] This ensures that Indian processors handling EU/US data are not directly liable for erasure requests under Indian law.

1.4 Cross-Border Data Flows: Geopolitics and Sovereignty

1.4.1 Adequacy (GDPR) vs. The "Negative List" (DPDP)

- **GDPR Model:** The EU operates on a **"Prohibited unless Permitted"** basis (Adequacy, SCCs, BCRs).[1502]
- **DPDP Act Model:** India has adopted a **"Permitted unless Prohibited"** basis. Section 16 allows the transfer of personal data to any country *except* those notified by the Central Government.[1503] This "Negative List" approach removes bureaucratic hurdles for the vast majority of global commerce while retaining government control on geopolitical grounds.[1504]

1.4.2 The *Schrems II* Conundrum

The compatibility of these two regimes is cast into doubt by the CJEU's *Schrems II* judgment.[1505] The DPDP Act provides broad exemptions for the Indian State to access data in the interests of "sovereignty and integrity of India" and "security of the state" (Section 17), without the independent judicial oversight required by EU

[1494] Future of Privacy Forum, "The Digital Personal Data Protection Act of India Explained", *FPF* (Aug. 2023).
[1495] *Id.*; *see also* Record of Law, *supra* note 4.
[1496] IISPP, "AI and Data Protection Challenges in Automated Decision Making", *IISPP* (2023).
[1497] DPDP Act, 2023, Section 15.
[1498] DPDP Act, 2023, Schedule.
[1499] GDPR, art. 17(3).
[1500] DPDP Act, 2023, Section 12.
[1501] DPDP Act, 2023, Section 17(1); *see also* Future of Privacy Forum, *supra* note 25.
[1502] GDPR, Chapter V.
[1503] DPDP Act, 2023, Section 16.
[1504] DPO India, "Impact of DPDPA on Cross-Border Transfers", *DPO India* (2024).
[1505] *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, C-311/18 (CJEU).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

standards.[1506] Consequently, it is unlikely that the EU will grant India "Adequacy" status, forcing EU companies to rely on Standard Contractual Clauses (SCCs) and Transfer Impact Assessments (TIAs) when sending data to India.[1507]

1.5 Techno-Legal Frontiers: Innovation vs. Regulation

1.5.1 Breach Notification: The "Zero Threshold"

- **GDPR (Article 33):** Mandates notification within **72 hours**. Notification is *not* required if the breach is "unlikely to result in a risk" to rights and freedoms.[1508]
- **DPDP Act (Section 8):** Mandates notification to the Data Protection Board *and* the Data Principal for **every** personal data breach, regardless of risk or magnitude.[1509] While the Act says "without undue delay," parallel CERT-In directions mandate reporting within **6 hours**.[1510] This lack of a risk threshold creates a potential "notification storm."[1511]

1.5.2 Data Protection Impact Assessments (DPIA)

- **GDPR (Article 35):** Mandates a DPIA for any processing likely to result in high risk.[1512]
- **DPDP Act (Section 10):** DPIAs are mandatory only for **Significant Data Fiduciaries (SDFs)** notified by the government.[1513] A small startup deploying a high-risk AI algorithm might not qualify as an SDF and thus would be exempt from the DPIA requirement, unlike in the EU, where the *nature* of processing triggers the obligation.[1514]

1.6 Enforcement and Economics: The Cost of Compliance

1.6.1 The Regulator: Board vs. Authority

- **GDPR:** Supervisory Authorities (DPAs) are statutorily required to be completely independent (Article 52).
- **DPDP Act:** The Data Protection Board of India (DPBI) is appointed by the Central Government, raising concerns about impartial enforcement against state entities.[1515]

1.7 Case Studies: Divergence in Action

1.7.1 Case Study: Meta's €1.2 Billion Fine (GDPR)

In May 2023, the Irish Data Protection Commission imposed a record €1.2 billion fine on Meta for transferring EU user data to the US.[1516] This enforcement was grounded in the *Schrems II* ruling regarding US surveillance laws. Under India's DPDP Act, unless the US is on the "Negative List," such transfers would be lawful under Section 16, and the Board would not independently assess foreign surveillance laws.[1517]

1.7.2 Case Study: The CoWIN Data Breach Allegations (India)

In June 2023, reports alleged that a Telegram bot was leaking personal data from India's CoWIN vaccination portal.[1518] The government denied a direct breach, attributing it to previously stolen data.[1519] Under Section 17(2) of the DPDP Act, the government can exempt state instrumentalities from the Act in the interests of "sovereignty" or "public order."[1520] This creates a

[1506] DPDP Act, 2023, Section 17(2); see also Observer Research Foundation, "The Adequacy Dilemma: India's DPDPA and the GDPR", ORF (2024).
[1507] Pinsent Masons, "How Schrems II ruling impacts EU data transfers to India", *Pinsent Masons* (2020).
[1508] GDPR, art. 33.
[1509] DPDP Act, 2023, Section 8(6).
[1510] CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000", No. 20(3)/2022-CERT-In (April 28, 2022).
[1511] IDFY, "DPDP Breach Notification Mandates: Roadmap to Prepare for 72-Hour Rule", *IDFY* (2024).
[1512] GDPR, art. 35.
[1513] DPDP Act, 2023, Section 10.
[1514] Khaitan & Co, "DPIAs under DPDP Act: Managing High Risk Data Processing", *KCO* (2023).
[1515] ComplyDog, "GDPR vs India DPDPA", *ComplyDog Blog*.
[1516] IAPP, "Meta fined GDPR-record 1.2 billion euros in data transfer case", *IAPP News* (May 22, 2023).
[1517] LexNova Consulting, "Data Protection Act India vs GDPR US", *LexNova* (2024).
[1518] Tsaaro Research Team, "Understanding the developments in CoWIN portal Data leak Saga", *Tsaaro* (June 14, 2023).
[1519] Press Information Bureau, "CoWIN Data Breach: Co-WIN portal of Health Ministry is Completely Safe", *Ministry of Health and Family Welfare* (June 12, 2023).
[1520] DPDP Act, 2023, Section 17(2).

structural immunity that might prevent the rigorous scrutiny seen in the EU, where public health authorities are routinely fined for GDPR breaches.[1521]

1.8 Conclusion

The comparative analysis reveals two distinct visions. The GDPR is a **Rights-First** framework that accepts market friction to protect the individual. India's DPDP Act is an **Economy-First** framework that prioritises the unlocking of data for public welfare and economic growth.[1522] While the DPDP Act simplifies compliance and liberalises cross-border flows, it dilutes individual control (portability and objection) and retains broad state-level exemptions. Whether this "third way" can effectively protect the Indian citizen in an age of AI remains the defining question of the coming decade.

BIBLIOGRAPHY

I. Primary Sources: Statutes and Regulations

- **India**
  - The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
  - The Constitution of India, 1950 (Article 21).

II. Case Law

- **Supreme Court of India**
  - *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
  - (Relevant context: This judgment recognized the fundamental right to privacy under Article 21, serving as the genesis for the DPDP Act).
- **Court of Justice of the European Union (CJEU)**
  - Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (Schrems II), ECLI:EU:C:2020:559.

III. Secondary Sources: Books and Concepts

- **Bradford, Anu.** *The Brussels Effect: How the European Union Rules the World* (2020).

IV. Administrative Decisions and Reports

- **Data Protection Commission (Ireland)**
  - *Inquiry into Meta Platforms Ireland Limited* (Decision of 22 May 2023).
- **Media and Technical Reports**
  - Reports on CoWIN Data Breach Allegations (June 2023).

[1521] Reddy & Reddy Law Firm, "State vs Centre: Who Should Control Your Data?", *Reddy & Reddy* (2023).
[1522] IJRPR, "DPDP Act 2023 vs GDPR: A Comparative Analysis", 6 *International Journal of Research in Publication and Reviews* 54121 (2024)