**Indian Journal of Law**
ISSN: 3048-4936 | Vol. 3 Issue 2 | Mar– Apr 2025 | Peer Reviewed & Refereed

# Data Protection and Privacy Laws: Comparison Between GDPR and India's Digital Personal Data Protection Act

**Aashish Bhardwaj**
Research Scholar
Department of Law
Uttar Pradesh.

Published: 18/04/2025 * Corresponding author

**How to Cite this Article:**
Bhardwaj, A. (2025). Data Protection and Privacy Laws: Comparison Between GDPR and India's Digital Personal Data Protection Act. *Indian Journal of Law*, 3(2), 17-22.
DOI: https://doi.org/10.36676/ijl.v3.i2.85

## Abstract
In the digital age, data is a vital resource, fueling economies and governance alike. However, with growing data dependency, issues of privacy and protection have gained unprecedented significance. The European Union's General Data Protection Regulation (GDPR) is often hailed as the gold standard for data privacy globally. In contrast, India, after years of deliberation, enacted the Digital Personal Data Protection Act (DPDPA), 2023, to secure personal data and ensure privacy in alignment with the landmark Puttaswamy judgment. This paper provides an in-depth comparative analysis of GDPR and DPDPA, exploring similarities and divergences in their scope, consent mechanisms, data subject rights, regulatory structures, cross-border data transfers, and enforcement frameworks. The research critically examines how India's model reflects indigenous policy priorities and evaluates the adequacy of protections it offers in light of global standards.
**Keywords:** GDPR, Digital Personal Data Protection Act, DPDPA, Data Privacy, Comparative Analysis, Consent, Data Protection Authority, Right to Privacy, India, EU.

## 1. Introduction
The digital revolution has led to a massive surge in data creation and collection. As personal data becomes central to digital economies, concerns over its misuse, breach, and exploitation have intensified. In this context, legal frameworks governing data protection are indispensable. The European Union's General Data Protection Regulation (GDPR), enacted in 2016 and effective since May 2018, is a benchmark legislation. Meanwhile, India, after the Supreme Court's 2017 judgment recognizing privacy as a fundamental right (Justice K.S. Puttaswamy v. Union of India), embarked on drafting its own data protection regime, culminating in the Digital Personal Data Protection Act, 2023 (DPDPA).

This research seeks to compare GDPR and DPDPA in a detailed and structured manner, highlighting their convergences, divergences, and implications for individual rights, corporate compliance, and state surveillance.

## 2. Historical and Legal Context

### 2.1. Evolution of GDPR

The GDPR replaced the outdated 1995 Data Protection Directive. It was designed to harmonize data protection laws across the EU and assert individuals' rights amid rising digitalization. GDPR's adoption was influenced by increased data breaches, misuse by tech giants, and transborder data flows.

### 2.2. India's Legislative Trajectory

India lacked a standalone data protection law until 2023. Prior frameworks like the Information Technology Act, 2000 (Sections 43A and 72A) provided only skeletal protections. Post-Puttaswamy (2017), various draft bills were tabled—culminating in the enactment of DPDPA in August 2023. The Act reflects a blend of global best practices and India's strategic interests, especially regarding data localization and state access.

## 3. Scope and Definitions

**Aspect GDPR DPDPA, 2023**

Personal Data Any information relating to an identified or identifiable natural person. Any data about an individual who is identifiable by or in relation to such data.

Sensitive Data Special categories: racial/ethnic origin, health, biometrics, sexual orientation, etc. No special category defined. Applies uniformly to "digital personal data."

Jurisdiction Extra-territorial; applies to data processors/controllers outside the EU if offering goods/services to EU residents. Applies to processing within India and outside India if offering goods/services to Indian data principals.

While GDPR classifies data based on sensitivity, India's DPDPA uses a simplified definition based on digital format without subclassifications.

## 4. Principles of Data Processing

| Principle | GDPR | DPDPA |
|---|---|---|
| Lawfulness, Fairness, Transparency | Yes | Implicit in purpose limitation and lawful use |
| Purpose Limitation | Explicit | Yes |
| Data Minimization | Yes | Not clearly emphasized |
| Accuracy | Required | Required |
| Storage Limitation | Yes | Limited to purpose fulfillment |

Accountability Explicitly mandated Data Fiduciary is accountable, but limited elaboration

GDPR elaborates on these principles extensively. The DPDPA acknowledges them but in a less prescriptive manner.

## 5. Legal Basis and Consent

### 5.1. Consent Mechanisms

GDPR mandates informed, unambiguous, and freely given consent for data processing. Explicit consent is required for special category data.

DPDPA requires free, specific, informed, unconditional, and unambiguous consent, with an obligation to inform the data principal of processing purposes, rights, and grievance mechanisms. However, it allows deemed consent under broad categories like employment, state functions, and emergencies, raising concerns over vagueness.

### 5.2. Legitimate Grounds

GDPR offers multiple legal bases besides consent—legitimate interest, public interest, contract necessity, etc.

DPDPA is largely consent-driven, with limited alternative grounds. "Deemed consent" is used in contexts such as legal obligations, employment, and state provision of services.

## 6. Rights of Data Subjects

| Right | GDPR | DPDPA |
|---|---|---|
| Right to Access | Yes | Yes |
| Right to Rectification | Yes | Yes |
| Right to Erasure | Yes (Right to be Forgotten) | Present, subject to adjudication |
| Right to Restriction | Yes | No equivalent |
| Right to Data Portability | Yes | No explicit provision |
| Right to Object | Yes | No equivalent |
| Right to Nominate (in death/incapacity) | Not explicitly stated | Explicitly provided in Section 13 |

DPDPA covers key rights but omits several nuanced rights under GDPR. Grievance redressal, however, is emphasized with timelines and accountability for data fiduciaries.

## 7. Regulatory Architecture

### 7.1. GDPR: Supervisory Authorities

Each EU country designates a Data Protection Authority (DPA). The European Data Protection Board (EDPB) ensures consistency across the EU. Authorities can impose administrative fines of up to €20 million or 4% of global turnover.

### 7.2. DPDPA: Data Protection Board of India (DPBI)

India's DPBI, under Section 18, is the central body for enforcement. It can inquire into breaches, impose penalties, and issue directions. However, concerns exist about:

Its lack of independence (appointed by the executive).

No power to impose criminal liability.
Limited judicial oversight mechanisms.

**8. Cross-Border Data Transfers**

GDPR allows transfers to countries with adequate protection or via standard contractual clauses, binding corporate rules, or explicit consent.

DPDPA, in contrast, permits cross-border transfer except to restricted countries notified by the Central Government. This reverse model raises transparency and trade law concerns as it vests excessive discretion in the executive.

**9. Enforcement and Penalties**

| Parameter | GDPR | DPDPA |
|---|---|---|
| Administrative Fines per breach | Up to 4% of global turnover or €20 million | Up to ₹250 crore (~€28 million) |
| Criminal Sanctions | Yes, under national laws | No criminal penalties |
| Private Right to Action | Yes | No explicit private right; grievance redressal through DPBI |

GDPR provides stronger deterrence due to private action, higher penalties, and autonomous regulators.

**10. Special Provisions: Children and State Access**

**10.1. Children's Data**

GDPR defines a child as under 16 (or lower depending on national law). Parental consent is required.

DPDPA sets the age at 18 and prohibits processing that causes "detrimental effect." However, it lacks clarity on verification mechanisms, and critics argue this could hinder innovation in EdTech and social platforms.

**10.2. Exemptions for Government**

GDPR allows exemptions for national security under strict legal safeguards.

DPDPA grants broad exemptions under Section 17 to the government for sovereignty, public order, or prevention of offences—without the requirement for judicial review or necessity-proportionality tests, raising fears of mass surveillance.

**11. Critical Evaluation**

**11.1. Strengths of GDPR**

Strong rights-based approach
Independent regulators
Accountability and transparency emphasis
High compliance standards

**11.2. Strengths of DPDPA**

Contextualized for Indian digital landscape
Simpler structure for implementation
Includes digital nominator provision
Allows sector-specific regulation

**11.3. Key Concerns in DPDPA**

Vague "deemed consent" clauses
Broad executive exemptions
Lack of DPA independence
No strong redressal mechanism for data principals
Poor protection against government surveillance

## 12. Future Directions and Policy Recommendations

Enhance Regulatory Independence: The Data Protection Board must be made constitutionally and functionally autonomous.

Limit Governmental Exemptions: Safeguards must align with international standards of necessity and proportionality.

Clarify Consent and Deemed Consent: Clear definitions and limited use of deemed consent will ensure data principal autonomy.

Enable Private Action: Introduce civil remedies for affected individuals to approach courts directly.

Cross-Border Flow Policy: Promote transparent frameworks for international data transfers compliant with trade agreements.

Capacity Building: Investments in cybersecurity, compliance infrastructure, and training are essential for effective implementation.

## 13. Conclusion

While GDPR and India's DPDPA share a commitment to data privacy, their underlying philosophies differ. GDPR is rooted in rights-based jurisprudence and transparency, whereas DPDPA reflects a balance between privacy, economic development, and state control. India's approach, while practical and simplified, lacks the robust checks and balances seen in the GDPR. For India to emerge as a global data economy and gain trust from international partners, it must ensure that individual rights are not subordinated to executive convenience. A nuanced, transparent, and accountable data protection regime is essential to realizing the constitutional promise of privacy and the economic potential of the digital ecosystem.

## References

Ashwinee Kumar, The Right to be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR, 2, Shimla Law Review, 75-104 (2020).

ersheds (2017). EU GDPR – Cross-Border Data Transfers. Retrieved from https://www.evershedssutherland.com/global/en/what/articles/index.page

Michael Douglas, Questioning the Right to be Forgotten, 40(2), Alternative Law Journal, 109 112 (2015)

Organization for Economic Cooperation and Development (2018). APEC Cross-Border Privacy Rules. Retrieved from https://www.oecd.org/sti/ieconomy/cross-border-privacy-rules.htm

Prashant Mali, Privacy Law: Right to Be Forgotten in India, 7 NLIU L. REV. 1 (2018).

Piyush Jha, Right to Be Forgotten and Its Conflict with Freedom of Speech and Expression in India, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

Shabnam Ahmed Zaman, Saptarishi Prasad Sharma & Modhu Chanda Dey, Right to Be Forgotten: SocioLegal Study, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).