Manuscript ID:
TIJCMBLIR-2025-020629

Volume: 2

Issue: 6

Month: December

Year: 2025

E-ISSN: 3065-9191

Submitted: 17 Nov. 2025

Revised: 28 Nov. 2025

Accepted: 16 Dec. 2025

Published: 31 Dec. 2025

Address for correspondence:
G Shiv Kumar Shriniwas Rao
Assistant Professor, MES Night College of Arts & Commerce, Savitribai Phule Pune University
Email: shiv90367@gmail.com

DOI: 10.5281/zenodo.19061963

DOI Link:
https://doi.org/10.5281/zenodo.19061963

Navigating The Digital Frontier: An Overview of India's DPDP Act and the UK's Data Privacy and Protection Laws

G Shiv Kumar Shriniwas Rao
Assistant Professor, MES Night College of Arts & Commerce,
Savitribai Phule Pune University

Abstract

In a vast interconnected world, the data protection which are especially personal data, has developed a foremost topic for individual persons, corporations, & the state. Rapid advancements in digital technologies have made robust legal frameworks essential for safeguarding privacy and regulating the handling of personal data. This study undertakes a detailed comparative analysis of India's Digital Personal Data Protection Act, 2023 (DPDP Act), and the United Kingdom's data protection regime, with particular emphasis on the UK General Data Protection Regulation (UK GDPR). Hence, this study compares India's DPDP Act, 2023, with the UK GDPR to assess how both legal systems address privacy and personal data protection in the digital age. This research thus examines the core principles, reach, personal rights, responsibilities of data fiduciaries/controllers, enforcement strategies, and impacts on international data transfers, underscoring the shared goals and differing methods of these two important jurisdictions. Utilising a wide range of secondary sources such as legislative documents, academic papers, legal analyses, and regulatory standards, the paper seeks to offer a detailed insight into these frameworks, highlighted by pertinent case examples from India and the UK. The goal is not just to outline their similarities and differences but also to highlight the changing landscape of global data governance and the necessity for businesses to maintain compliance across various regulatory contexts.

Keywords: *Data Privacy, Data Protection, DPDP Act, UK GDPR, India, United Kingdom, Personal Data, Data Fiduciary, Data Controller, Cross-border Data Transfer, Consent, Accountability, Enforcement.*

Introduction

The digital era, though providing unmatched chances for innovation and connection, also brings intricate challenges to personal privacy. With personal data emerging as the new oil, its acquisition, handling, and commercialisation by companies have triggered a worldwide push for more robust data protection laws. Countries around the globe are struggling to maintain the fragile equilibrium between promoting a dynamic digital economy and safeguarding essential privacy rights. India, featuring its growing digital populace and swiftly advancing tech industry, alongside the United Kingdom, a developed digital economy with an adept legal framework, embodies intriguing examples in this worldwide initiative. India's path to a holistic data protection law has been lengthy, resulting in the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act). This law signifies a critical point in India's legal environment, aiming to establish a contemporary and efficient system for protecting personal data in the online space. Following Brexit, the United Kingdom adapted the European Union's GDPR into its own framework, now known as the UK GDPR. While both India's DPDP Act and the UK GDPR share the common goal of protecting personal data, they diverge in design, reflecting distinct legal traditions, socio-economic contexts, and policy priorities. This research seeks to deliver a comprehensive summary and comparative study of India's DPDP Act and the UK's data privacy and protection regulations, particularly emphasising the UK GDPR. Through an analysis of their scope, fundamental principles, individual rights, responsibilities of data-handling entities, enforcement methods, and regulations for cross-border data exchanges, the paper will underscore the similarities and differences that both businesses and individuals must manage. The research will solely depend on secondary data, extracting insights from legislative texts, governmental directives, scholarly evaluations, and news articles to guarantee a thorough and unbiased evaluation. Incorporating Indian cases and examples will offer a localised viewpoint, enhancing the comparative dialogues and interactions.

How to Cite this Article:
Rao, G. S. K. S. (2025). Navigating The Digital Frontier: An Overview of India's DPDP Act and the UK's Data Privacy and Protection Laws. The International Journal of Commerce Management and Business Law in International Research, 2(6), 139–143. https://doi.org/10.5281/zenodo.19061963

Literature Review:

Data privacy and protection have become central themes in academic and legal debates, particularly since the adoption of the European Union's General Data Protection Regulation (GDPR). The literature shows a worldwide movement toward implementing extensive privacy regulations, frequently shaped by the GDPR's rigorous criteria. Research comparing worldwide data protection systems often regards the GDPR as a standard. For example, studies frequently underscore the GDPR's focus on accountability, data protection inherently and as a standard, along with extensive individual rights, juxtaposing these with previous, more disjointed national regulations. The idea of adequacy decisions in the GDPR, which enables cross-border data transfers to nations considered to have similar protection levels, has also been a key topic of conversation concerning global data governance. In the Indian setting, academic research examines the progression of data protection from the restricted clauses of the Information Technology Act, 2000, along with its related regulations, to the constitutional acknowledgement of privacy as a fundamental right in the Justice K.S. Puttaswamy (Retd.) decision. The later formulation and implementation of the DPDP Act, 2023, has produced significant discourse emphasising its distinct characteristics, including the idea of Significant Data Fiduciaries, a consent-centred method, and the authority of the government to designate allowable jurisdictions for transnational data transfers. Commentaries often compare the DPDP Act's stipulations with the GDPR, pointing out similarities in principles while also emphasising differences in scope, enforcement methods, and specific responsibilities. Some analysts suggest that although both seek strong protection, the DPDP Act may be viewed as offering more exceptions for government processing and a less detailed strategy for special data categories in comparison to the UK GDPR.

Literature examines the real-world effects of these regulations on companies. Recurring themes include challenges in compliance, like establishing strong consent management systems, performing data protection impact assessments, and handling data breach notifications. The financial effects of adherence, especially on small and medium enterprises (SMEs), are an area of continuing study. Additionally, the extraterritorial scope of both the UK GDPR and the DPDP Act establishes a complicated compliance landscape for multinational companies, requiring a unified strategy for data management. The continuous discussion about finding a balance between innovation and privacy, particularly in new technologies such as Artificial Intelligence, is a crucial element in the existing literature, shaping conversations on upcoming changes and interpretations of these laws and regulations.

Research Methodology:

This research paper employs a qualitative research method centred on secondary data analysis to explore the similarities and differences between India's DPDP Act, 2023, and the data privacy and protection regulations in the UK, primarily the UK GDPR. The research framework employs a comparative legal analysis approach, deconstructing each law into its fundamental components, including principles, rights, duties, and enforcement mechanisms. Secondary data sources encompass legislative documents, governmental and regulatory frameworks, scholarly articles, legal analyses, and news reports. Data gathering was carried out via focused searches employing keywords associated with the DPDP Act, UK GDPR, data privacy, data protection, India, and the UK. The gathered data underwent analysis through a thematic analysis method, highlighting essential themes and categories for both the DPDP Act and the UK GDPR. An implicit comparative matrix was utilised to outline the similarities and differences among these themes. Concrete examples and case studies from India and the UK were included in the analysis to demonstrate the real-world effects of the legal provisions. A critical assessment was conducted to evaluate the strengths, weaknesses, and possible effects of each legal framework.

Research Objectives:

This paper seeks to accomplish the following objectives:

1. **To analyse India's Digital Personal Data Protection Act, 2023 (DPDP Act):** Present a structured overview of its key provisions, definitions, and guiding principles to establish a clear understanding of its scope and intent.
2. **To examine the United Kingdom's data protection framework, with emphasis on the UK GDPR:** Outline its foundational principles, rights, and obligations, trace its evolution from the EU GDPR, and highlight the distinctive adaptations made for the UK context.
3. **To undertake a comparative study of the DPDP Act and the UK GDPR:** Identify and evaluate convergences and divergences across dimensions such as scope, principles, individual rights, obligations of data fiduciaries/controllers, and rules governing cross-border data transfers.
4. **To assess enforcement mechanisms and penalty regimes under both legislations:** Investigate the role of regulatory authorities (the Data Protection Board of India and the UK Information Commissioner's Office), and analyze the nature and severity of sanctions for non-compliance, supported by illustrative cases.
5. **To explore compliance challenges and business implications in India and the UK:** Highlight practical difficulties and strategic considerations for organizations handling personal data across these jurisdictions, with a focus on ensuring adherence to both regulatory regimes.

Data Collection:

This study relies exclusively on **secondary sources**, with no primary data generated through surveys, interviews, or experiments. Information was gathered

through systematic searches of credible, publicly available materials relevant to India's *Digital Personal Data Protection Act, 2023 (DPDP Act)*, the *UK General Data Protection Regulation (UK GDPR)*, and related UK data privacy laws.

The key categories of sources include:

- **Government and Legislative Portals:** Official texts of the DPDP Act (Government of India), the UK GDPR, and the Data Protection Act 2018 accessed via governmental and parliamentary websites.
- **Regulatory Authority Websites:** Guidance documents, codes of practice, enforcement reports, and advisories from the UK Information Commissioner's Office (ICO). For India, materials from the Ministry of Electronics and Information Technology (MeitY) and emerging documentation from the Data Protection Board were reviewed.
- **Academic Databases and Journals:** Peer-reviewed articles and legal analyses sourced from JSTOR, Scopus, Google Scholar, and university libraries, using targeted queries such as *"DPDP Act," "UK GDPR," "cross-border data transfers,"* and *"consent management."*
- **Legal News and Analysis Portals:** Reputable law publications and firm blogs (e.g., Legal 500, SFLC.in, ClearTax, Spice Route Legal) offering insights into compliance practices, enforcement trends, and interpretive debates.
- **Industry Reports and Whitepapers:** Publications from cybersecurity firms, privacy consultancies, and industry associations highlighting business challenges and compliance strategies.

Data collection followed an iterative process, beginning with broad searches and narrowing to focused inquiries as key themes and comparative dimensions emerged. Reliability and timeliness were prioritized, with emphasis on official records and peer-reviewed scholarship. This approach ensured a robust evidentiary base for the comparative analysis of India's DPDP Act and the UK GDPR.

Data Analysis and Findings:

An analysis of secondary sources shows that India's DPDP Act, 2023, and the UK's GDPR share the common goal of protecting personal data and safeguarding privacy rights, yet they diverge in how these objectives are carried out. These differences arise from each nation's distinct historical context, legal traditions, and socio-economic priorities, which shape the specific provisions and enforcement approaches within their frameworks.

a. **Foundational Principles and Scope**

India's DPDP Act, 2023, and the UK GDPR both rest on widely accepted principles of data protection—such as lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, storage limitation, and integrity—and emphasize accountability by requiring organisations to prove compliance. Yet, their scope and treatment of sensitive data differ. The DPDP Act applies to digital personal data within India and extraterritorially, while exempting personal or domestic use and publicly available data, and it does not define "special categories." In contrast, the UK GDPR distinguishes between general personal data and "special categories of personal data," imposing stricter safeguards in line with EU standards to address the heightened risks of sensitive information.

b. **Rights of Data Principals/Data Subjects**

Both legislations empower individuals with rights over their data. The **DPDP Act** grants rights such as the right to access information, correction and erasure, grievance redressal, and the crucial right to nominate someone in case of death or incapacity. Critically, it emphasizes a **consent-centric model**, requiring clear and explicit consent for processing. The "right to withdraw consent" is also a highlighting salient provision.'

The UK's GDPR provides a more extensive set of "data subject rights," such as:

Data protection frameworks grant individuals a set of fundamental rights designed to safeguard their personal information. These include the right to be informed about how their data is used, the right of access to obtain copies of their data, and the right to rectification to correct inaccuracies. Individuals may also exercise the right to erasure (or be forgotten) under certain conditions, restrict how their data is processed, and transfer their data across services through portability. Additionally, they hold the right to object—particularly against direct marketing—and the right to challenge decisions made solely through automated processing or profiling.

The UK GDPR's expanded set of rights, particularly data portability and specific rights concerning automated decision-making, suggests a more developed framework that expects sophisticated data processing methods.

For Instance, in India, the enforcement of the consent requirement under the DPDP Act is crucial. As major e-commerce platforms, Flipkart and Amazon India must explicitly acquire consent for the collection of user data, such as transaction records and behavioural information (Corrida Legal, n.d.). Users must have simple choices to revoke consent for marketing or ask for their data to be deleted. A significant telecom provider such as Reliance Jio or Bharti Airtel is mandated by the DPDP Act to implement transparent consent processes for gathering call records, internet activity, and location information, along with systems that allow users to request data access or deletion (Financial Express, 2025).

c. **Obligations on Data Fiduciaries/Controllers and Data Processors**

Both laws impose strict obligations on entities handling data.

Under the DPDP Act, Data Fiduciaries must:

- Obtain verifiable consent, especially for children's data (requiring parental consent).
- Implement reasonable security safeguards against data breaches.

- Notify the Data Protection Board of India and affected Data Principals of a personal data breach.
- Ensure accuracy and completeness of data.
- Cease retention of data when the purpose is no longer served.
- Establish a grievance redressal mechanism.
- **Significant Data Fiduciaries** may have additional duties, including appointing a Data Protection Officer (DPO) and conducting Data Protection Impact Assessments (DPIAs) (JISA Softech Pvt Ltd, 2025). The Act also explicitly prohibits tracking, behavioural monitoring, or targeted advertising to children (DPDP Consultants, n.d.).

Under the UK GDPR, Data Controllers and Processors have some obligations such as:

Obligation	Meaning / Application
Lawful Basis for Processing	Every data activity must have a valid legal ground, beyond just relying on consent.
Data Protection by Design & Default	Privacy safeguards must be built into systems and processes from the outset.
Security Measures	Organisations must apply appropriate technical and organisational protections to secure personal data.
Data Protection Impact Assessments (DPIAs)	Required for high-risk processing to evaluate and mitigate potential privacy risks.
Breach Notification	The ICO must be informed within 72 hours of a data breach, and individuals notified if risk is high.
Data Protection Officer (DPO)	Must be appointed in certain cases, such as large-scale or sensitive data processing.
Records of Processing Activities (RoPA)	Organisations must maintain detailed documentation of how personal data is processed.

Table 1: Obligations of Data Controllers and Processors

The DPDP Act mandates robust cybersecurity for financial data, clear consent for services like credit cards, and prompt reporting of data breaches. Indian EdTech platforms must implement age verification, obtain verifiable parental consent for children's data, and prohibit targeted advertising to minors. Hospitals like Apollo Hospitals must ensure explicit patient consent for health data, implement strong security, and have clear mechanisms for patients to access or correct their records. The UK GDPR has been actively enforced, with fines for data leaks and breaches. In 2024, the Police Service of Northern Ireland was fined £750,000 for an accidental data leak, while the Ministry of Defence received a £350,000 fine for exposing Afghan citizens' identities. TikTok was fined £12.7 million in 2023 for failing to protect children's data, including allowing underage access and not being transparent about data usage.

d. **Cross-Border Data Transfers**

The DPDP Act in India adopts a government‑controlled "whitelisting" model for cross‑border data transfers, permitting flows only to countries or territories explicitly approved by the Central Government. This approach centralises authority over international data movement and may create uncertainty for global businesses awaiting clarity on which jurisdictions will be deemed permissible. By contrast, the UK GDPR relies on an adequacy decision framework, allowing transfers to nations that demonstrate sufficient data protection standards, such as EU member states. Where no adequacy decision exists, organizations must establish appropriate safeguards to ensure compliance and protect personal information.

e. **Enforcement and Penalties**

The DPDP Act establishes the Data Protection Board of India (DPBI) as the enforcement authority for the GDPR, with fines up to INR 250 crore for serious violations. In contrast, the UK GDPR is enforced by the Information Commissioner's Office (ICO), which can issue warnings, enforcement notices, and substantial monetary penalties. The ICO's approach has shifted towards fewer financial penalties and lower sums against the public sector, favouring reprimands and enforcement notices.

Conclusion:

The Digital Personal Data Protection Act, 2023 (DPDP Act) in India and the UK's General Data Protection Regulation (GDPR) are comprehensive frameworks designed to safeguard personal privacy, reflecting global consensus on principles such as legality, fairness, purpose limitation, and accountability. While both share these foundations, the DPDP Act distinguishes itself through a consent-centric model, uniform application across all personal data without special categories, and a government-controlled "whitelisting" approach to cross-border transfers that reinforces India's digital sovereignty goals. In contrast, the UK GDPR—rooted in EU standards—provides a more nuanced structure, explicitly defining "special categories of personal data," offering multiple lawful bases for processing beyond consent, and relying on adequacy decisions and contractual safeguards like Standard Contractual Clauses (SCCs) for international transfers. For global businesses, navigating these frameworks requires robust data governance, adaptable consent management, strong cybersecurity, and close

monitoring of evolving regulations. Together, the DPDP Act and UK GDPR are pivotal in shaping the trajectory of international data governance toward greater security, transparency, and respect for privacy.

Suggestions and Recommendations:

Drawing from the comparative analysis, the subsequent proposals and advice are presented for companies, policymakers, and prospective researchers: Companies functioning in both regions should implement a "highest standard" strategy to guarantee adherence to the Data Protection and Data Sharing Act (DPDP Act) and UK GDPR. This involves following stricter criteria, investing in strong consent management systems, enhancing data governance and accountability structures, focusing on data protection and breach readiness, closely tracking regulatory changes, and creating clear complaint resolution processes. The Indian government must fast-track the announcement of comprehensive regulations under the DPDP Act, especially about verifiable consent details, the standards for "Significant Data Fiduciaries," and the "notified" list of authorised nations for cross-border data transfers. Investigating ways to enhance the alignment and interoperability of data protection standards between India and the UK might enable easier international data transfers and lessen compliance challenges for companies.

The Indian government and the Data Protection Board of India should focus on public awareness campaigns and capacity-building initiatives to promote broad comprehension and acceptance of the DPDP Act's stipulations. Future studies might examine empirical investigations regarding compliance with the DPDP Act, the lasting effects of the DPDP Act and UK GDPR on innovation, digital transformation, and cross-border trade between India and the UK, as well as how both legal frameworks evolve in response to emerging technologies such as AI, IoT, and quantum computing.

In summary, companies functioning in both areas should implement a high-standard strategy, invest in reliable consent management systems, enhance data governance and accountability structures, emphasise data security and breach readiness, and focus on public education campaigns and capacity-building programs.

Acknowledgment

In the era of rapid technological advancements and data-driven economies, ensuring the protection and privacy of personal data has become a critical concern globally. Different nations have introduced legislation to regulate how personal data is collected, stored, processed, and shared. In this context, the Digital Personal Data Protection (DPDP) Act of India and the Data Protection Act 2018 (which incorporates the General Data Protection Regulation (GDPR) in the UK) are pivotal. Below is an acknowledgment of their significance and the role they play in shaping global data privacy standards.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References:

1. Corrida Legal. (n.d.). *E-Commerce and Data Privacy: A Comprehensive Guide for Businesses*. https://corridalegal.com/e-commerce-and-data-privacy/
2. Dalberg. (n.d.). *Navigating the DPDP Act: What It Means for EdTech and the Future of Digital Learning*.https://dalberg.com/our-ideas/navigating-the-dpdp-act-what-it-means-for-edtech-and-the-future-of-digital-learning/
3. DPO India. (2025, March 5). *Impact of the Digital Personal Data Protection (DPDP) Act on Cross-Border Data Transfers*. https://www.dpo-india.com/Blogs/impact-dpdpa-cross-border/
4. DPDP Consultants. (n.d.). *Children's Data Protection Under DPDP Act: Guidelines for Businesses*.https://www.dpdpconsultants.com/blog.php?id=4&title=Children's%20Data%20Protection%20Under%20DPDP%20Act:%20Guidelines%20for%20Businesses
5. Facit Data Systems. (n.d.). *Right to be Forgotten UK |YourGuide*.https://facit.ai/insights/right-to-be-forgotten-uk
6. Financial Express. (2025, February 7). *DPDP consultations: Telcos call for single digital platform for data breach reporting*. https://www.financialexpress.com/life/technology-dpdp-consultations-telcos-call-for-single-digital-platform-for-data-breach-reporting-3740197/
7. Infosecurity Magazine. (2025, February 7). *Most UK GDPR Enforcement Actions Targeted Public Sector in 2024*. https://www.infosecurity-magazine.com/news/uk-gdpr-enforcement-public-sector/
8. JISA Softech Pvt Ltd. (2025, March 29). *The Digital Personal Data Protection (DPDP) Act 2023: Key Challenges and Compliance Framework*. https://www.jisasoftech.com/the-digital-personal-data-protection-dpdp-act-2023-key-challenges-and-compliance-framework/
9. LegalVision UK. (n.d.). *How Does GDPR Affect My Business?* https://legalvision.co.uk/data-privacy-it/how-does-gdpr-affect-my-business/
10. Monaco Solicitors. (n.d.). *Subject access request made by employee: Example 1*. https://www.monacosolicitors.co.uk/evidence/templates/subject-access-request-example-1
11. Seqrite. (2025, April 25). *The DPDP Act 2023 Guide for Healthcare Leaders*.https://www.seqrite.com/blog/the-dpdp-act-2023-guide-for-healthcare-leaders/
12. Skillcast. (2025, April 22). *20 Biggest GDPR Fines 2018 - 2024 | Breaches of GDPR*. https://www.skillcast.com/blog/20-biggest-gdpr-fines
13. URM Consulting. (2025, February 5). *Analysis of Fines Imposed by the ICO in 2024*. https://www.urmconsulting.com/blog/analysis-of-fines-imposed-by-the-information-commissioners-office-in-2024