Page: 1591-1613 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.190

DATA PROTECTION IN CYBERSPACE: A COMPARATIVE LEGAL STUDY OF INDIA'S DPDP ACT, 2023 AND THE DPDP RULES, 2025 WITH THE EU GDPR

Mr. Aaditya Gautam Balaji[1]

I. ABSTRACT

The rapid expansion of digital technologies has intensified concerns surrounding the collection, processing and cross-border movement of personal data, prompting jurisdictions to adopt comprehensive data protection frameworks. This paper undertakes a comparative cyber law analysis of India's Digital Personal Data Protection regime, as operationalised through the DPDP Act, 2023 and DPDP Rules, 2025, with the European Union's General Data Protection Regulation (GDPR). Using a doctrinal and comparative methodology, the study examines key dimensions of both regimes, including definitions and scope, lawful bases and consent architecture, rights of individuals, obligations of data fiduciaries/controllers, enforcement mechanisms, and cross-border data transfer frameworks. The analysis reveals that while the DPDP framework incorporates several globally recognised data protection principles, it reflects a distinct regulatory philosophy shaped by administrative efficiency, developmental priorities and regulatory flexibility. In contrast, the GDPR adopts a more rights-centric and institutionally robust model with detailed procedural safeguards and a decentralised supervisory structure. The paper argues that these structural and doctrinal differences have significant implications for individual rights protection, regulatory interoperability and compliance practices in an increasingly global digital economy. It concludes by offering targeted recommendations aimed at strengthening India's data protection framework while maintaining contextual relevance and facilitating greater alignment with international standards.

[1] LL.M. (Cyber Law and Cyber Security) student at SRM School of Law, SRMIST (India). Email: aadityagautambalaji@gmail.com

 (ISSN: 2583-7753)

II. KEYWORDS

Digital Personal Data Protection Rules, 2025, Digital Personal Data Protection Act, 2023, General Data Protection Regulation (GDPR), Data Protection Law, Cross-Border Data Transfers.

III. INTRODUCTION

The rapid growth of digital technologies has made personal data a vital economic and regulatory resource. Online platforms, financial services, governance systems, and emerging AI applications increasingly depend on large-scale personal data processing, raising serious concerns about privacy, informational autonomy, and accountability. In response, jurisdictions worldwide have adopted comprehensive data protection frameworks. Among them, the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 along with the recently operationalised Digital Personal Data Protection Rules, 2025 represent two influential yet distinct regulatory models in contemporary cyber law. The DPDP Rules, 2025 were notified on November 14, 2025, marking the full operationalisation of the DPDP Act, 2023, with an 18-month phased implementation timeline.

The GDPR is widely considered as a benchmark for rights-based data protection regulation, emphasising strong individual rights, detailed compliance obligations and robust enforcement mechanisms. Its legislative concept is based on the protection of fundamental rights and has shaped data protection beyond Europe. India's data protection regime, lead up to the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, reflects a different path. It aims to balance individual privacy interests with developmental priorities, state functions, and the realities of a rapidly expanding digital economy. While the Indian framework adopts several internationally recognised data protection principles, it does so through a more flexible, rule-based, and institutionally streamlined structure.

A comparative examination of these two regimes is particularly significant at a moment when India's data protection law is entering its implementation phase. The DPDP Rules, 2025 translate statutory principles into operational obligations, making

this an opportune time to assess how India's approach aligns with or departs from established global standards. Such comparison is not intended to rank one regime as superior, but to understand how differing constitutional values, regulatory capacities and socio-economic contexts shape legal responses to similar technological challenges.

This study adopts a cyber law perspective to examine how key issues such as consent, individual rights, regulatory oversight, and cross-border data flows are addressed under the GDPR and the DPDP Rules, 2025. Focusing on doctrinal design and regulatory outcomes. It identifies strengths, gaps, and areas for reform in the Indian framework while drawing measured lessons from the European experience. In doing so, it contributes to the evolving discourse on data protection governance in an increasingly interconnected digital world.

A. Research Problem

1. Despite the notification of the DPDP Rules, 2025, there is limited clarity on how effectively India's data protection framework operationalises individual rights when compared to established regimes such as the EU GDPR.
2. The structural and doctrinal differences between the DPDP Rules, 2025 and the GDPR raise concerns regarding consistency in consent standards, enforcement mechanisms and regulatory accountability.
3. Divergences between the Indian and EU data protection regimes may create challenges for cross-border data flows, compliance interoperability and India's integration into the global digital economy.

B. Research Objectives

1. To examine the legal framework of the DPDP Rules, 2025 and identify their core principles governing personal data protection in India.
2. To comparatively analyse the DPDP Rules, 2025 and the EU GDPR with respect to consent, individual rights and regulatory enforcement mechanisms.

3. To assess the implications of doctrinal and structural differences between the two regimes for cross-border data flows and regulatory interoperability.
4. To suggest legal and policy measures for strengthening India's data protection framework considering comparative insights from the GDPR.

C. Research Questions

1. How do the DPDP Rules, 2025 operationalise key data protection principles, and how do these compare with the corresponding provisions under the EU GDPR?
2. To what extent do differences in consent standards, individual rights, and enforcement mechanisms affect the adequacy of data protection under the DPDP Rules, 2025 compared to the GDPR?
3. What are the implications of divergences between the DPDP Rules, 2025 and the GDPR for cross-border data flows and regulatory interoperability?

D. Research Hypotheses

1. The DPDP Rules, 2025 adopt core data protection principles similar to the EU GDPR but provide a comparatively narrower scope of individual rights and procedural safeguards.
2. Differences in enforcement architecture between the DPDP Rules, 2025 and the GDPR are likely to influence the effectiveness of compliance and remedies for data principals.
3. Divergences between the two regimes may pose challenges to seamless cross-border data transfers and regulatory interoperability.

E. Research Methodology

This research adopts a doctrinal and comparative legal methodology to examine and analyse the data protection frameworks established under India's DPDP Rules, 2025 and the European Union's General Data Protection Regulation. The study is primarily based on authoritative legal texts, including statutory provisions, delegated

legislation and officially notified regulatory instruments, which constitute the core primary sources for analysis.

A comparative approach is used to assess similarities and differences between the two regimes across key doctrinal areas, including scope, consent requirements, data subject rights, fiduciary/controller obligations, enforcement mechanisms, and cross-border data transfers. The comparison is functional rather than purely textual, focusing on how shared regulatory objectives are pursued through different legal designs and institutional structures.

Secondary sources, limited to select scholarly books and peer-reviewed research articles, are used in a restrained manner to support doctrinal interpretation, contextual understanding and analytical depth. These sources assist in clarifying underlying principles, regulatory philosophies and theoretical debates surrounding data protection and privacy law, without displacing the primacy of statutory analysis.

The methodology deliberately excludes empirical fieldwork or quantitative analysis, as the DPDP Rules, 2025 are in the early stages of implementation. Instead, the research relies on normative legal reasoning and comparative interpretation to assess potential regulatory outcomes, identify gaps and propose reform-oriented recommendations grounded in established data protection jurisprudence.

F. Literature Review

This review focuses on the four selected scholarly articles that address core doctrinal tensions relevant to the comparative study, automated decision-making and explainability, purpose limitation in the era of AI, human-rights impact assessment, and the practical viability of consent, while situating those debates against the primary legal instruments (GDPR and India's DPDP framework) where necessary.

Emre Bayamlıoğlu's work sharpens the debate on contesting automated decisions and the limits of a litigable "right to explanation." His analysis highlights how procedural remedies and substantive transparency obligations interact with algorithmic opacity, an issue central to comparing how GDPR and the DPDP Rules approach automated

processing and redress.[2] Bayamlıoğlu's arguments clarify why a doctrinal focus on mere disclosure obligations may be insufficient for meaningful contestability.

R.Mühlhoff's normative treatment of purpose limitation interrogates classical privacy doctrines when confronted with machine-learning practices that repurpose datasets for model training and emergent inferences. Mühlhoff argues for rethinking purpose limitation to accommodate (and constrain) AI workflows without eroding individual protection; this reframing is crucial for assessing whether the DPDP Rules' drafting preserves the protective force of purpose limitation or permits functional workarounds common in data-driven development contexts.[3]

Alessandro Mantelero advances a structured, evidence-based approach for evaluating the impact on human rights of data-driven systems. Mantelero's model provides a procedural scaffold (risk identification, proportionality assessment, mitigation measures) that is directly translatable into regulatory instruments such as DPIA-type obligations. His framework supplies evaluative criteria for comparing the robustness of supervisory practices and preventive obligations under GDPR and the DPDP Rules.[4]

Finally, D.Hallinan's discussion of "broad consent" under the GDPR offers a cautiously optimistic view of consent's adaptability in complex processing landscapes. Hallinan examines when consent retains normative and practical force and when alternative lawful bases or governance mechanisms are preferable. This analysis informs the comparative inquiry into the DPDP Rules' consent architecture and whether it can function effectively in high-volume or platform contexts without producing consent fatigue or hollow notice practices.[5]

Taken together, these four articles provide targeted conceptual tools for the paper's comparative sections: (a) they foreground why automated decision-making, purpose limitation and consent are not merely technical matters but doctrinal stress-tests for

[2] Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the So-Called "Right to Explanation"'.
[3] Rainer Mühlhoff, 'Updating Purpose Limitation for AI: A Normative Approach'.
[4] Alessandro Mantelero, 'An Evidence-Based Methodology for Human Rights Impact Assessment'.
[5] Dara Hallinan, 'Broad Consent under the GDPR: An Optimistic Perspective'.

any data protection regime; and (b) they offer concrete evaluative criteria (contestability, purpose fidelity, rights-impact assessment, and consent efficacy) that will be applied to the GDPR and the DPDP Rules in the subsequent analysis.

IV. DEFINITIONS & SCOPE

A. Personal data / digital personal data:

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person, a broad, technology neutral formulation that captures direct identifiers and information that can reasonably identify an individual.[6] India's framework uses the term "digital personal data" and treats certain categories (notably sensitive and critical personal data) as attracting stricter safeguards under the DPDP regime.[7]

B. Sensitive / special-category data:

Both regimes single out categories of data that require higher protection, the GDPR by naming "special categories" (e.g., health, biometric data)[8] and the DPDP framework by providing enhanced safeguards through differentiated obligations rather than through explicit data category labelling.

C. Data principal / data subject; data fiduciary / controller:

The GDPR centres protection on the "data subject" and allocates duties to "controllers" and "processors" who determine processing purposes and means.[9] The Indian law frames the relationship in terms of a "data principal" and a statutory "data fiduciary," the latter being the actor carrying primary stewardship duties under the DPDP Act.[10]

[6] Regulation (EU) 2016/679 (General Data Protection Regulation), art 4(1) (hereinafter "GDPR").
[7] Digital Personal Data Protection Act, 2023, (Act No. 22 of 2023) ss. 2(10), 10 (hereinafter "DPDP Act, 2023").
[8] GDPR, art. 9(1).
[9] GDPR, arts. 4(1), 4(7)-(8).
[10] DPDP Act, 2023, ss. 2(3), 2(5), 4-8.

D. Processing and territorial scope:

Both instruments adopt expansive definitions of "processing" (collection, storage, use, disclosure, erasure and related operations), thereby covering modern data practices.[11] The GDPR explicitly extends to certain processing activities outside the EU that target EU data subjects (for example offering goods or services or monitoring behaviour), giving it clear extraterritorial effect. The DPDP framework is principally concerned with protecting the digital personal data of persons in India and sets out conditions for certain cross-border transfers and restrictions on specified categories in recognition of domestic policy priorities.[12]

E. Cross-border implications:

Differences in territorial design and transfer mechanisms affect international compliance strategies and the ease of cross-border flows: regimes with broad extraterritorial reach can impose obligations on foreign actors, while a domestic category tiered approach creates targeted safeguards that may require additional mechanisms for international interoperability. For analysis of the practical consequences of differing territorial designs on transborder flows, see Kuner's work on transborder data flows.[13]

V. LAWFUL BASES & CONSENT ARCHITECTURE

The EU GDPR adopts a pluralistic approach to lawful processing by recognising multiple legal bases, including consent, contractual necessity, legal obligation, public interest functions and legitimate interests. This structure reduces over reliance on consent and allows controllers to select an appropriate legal basis depending on the nature and context of processing.[14]

India's DPDP framework, while not exclusively consent based, places comparatively greater operational emphasis on consent as a primary legitimising mechanism for the processing of digital personal data. The DPDP Rules reinforce this orientation by

[11] GDPR, art. 4(2); DPDP Act, 2023, s. 2(16).
[12] DPDP Act, 2023, ss. 3, 16.
[13] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press).
[14] GDPR, art. 6(1).

prescribing detailed requirements for notice, consent communication and withdrawal, particularly in digital environments.[15]

Under the GDPR, consent must be freely given, specific, informed and unambiguous, and it must be simple for people to revoke their consent as easily as it was given. These requirements are designed to prevent coercive or illusory consent and to preserve individual autonomy in data processing relationships.[16] The DPDP Rules similarly require clarity and accessibility in consent mechanisms, while their application operates within a tiered framework of differentiated obligations for certain classes of data fiduciaries.[17]

The viability of broad or open-ended consent has been the subject of sustained scholarly debate. Hallinan argues that broad consent may be legally sustainable in narrowly defined research contexts under the GDPR, provided it is accompanied by strong governance and oversight mechanisms. However, the use of broad consent outside such controlled settings risks undermining meaningful individual choice.[18]

Technological developments, particularly artificial-intelligence systems complicate the consent-purpose relationship. Mühlhoff demonstrates that data initially collected for specific purposes may later be repurposed for AI training or inference generation in ways that strain traditional consent and purpose limitation doctrines. This exposes the limits of consent as a sole protective mechanism in complex data ecosystems.[19]

Conceptually, the limits of consent as a protective mechanism stem from the multifaceted nature of privacy itself. Solove explains that privacy harms are not confined to secrecy breaches but include aggregation, secondary use and power imbalances created by large-scale data processing. This insight reinforces the view that

[15] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India), ss. 4, 5, 7-8; Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
[16] GDPR, arts. 4(11), 7(3).
[17] DPDP Act, 2023, ss. 5, 10; DPDP Rules, 2025.
[18] Hallinan, 'Broad Consent under the GDPR'.
[19] Mühlhoff, 'Purpose Limitation for AI'.

consent alone cannot bear the full burden of data protection and must be supplemented by structural and institutional safeguards.[20]

To address such limitations, Mantelero emphasises the role of procedural safeguards such as impact assessments, which require ex-ante identification and mitigation of rights-based risks. These mechanisms function as structural complements to consent, especially where individuals cannot realistically anticipate downstream data uses.[21]

Comparatively, the GDPR's diversified lawful basis model provides greater doctrinal flexibility, while imposing stringent standards where consent is relied upon. India's consent forward and category tiered approach places a heavier burden on notice quality, ease of withdrawal and regulatory oversight to ensure that consent remains substantive rather than formalistic. The effectiveness of either regime ultimately depends on enforcement practices and the practical capacity of individuals to exercise real control over their personal data.

VI. RIGHTS OF DATA SUBJECTS

Rights conferred on individuals constitute the normative core of modern data protection regimes. Both the GDPR and India's DPDP framework recognise that effective protection requires more than abstract principles; it requires enforceable rights that enable individuals to access, correct, control and where necessary challenge the processing of their personal data.

A. Right to access and transparency:

The GDPR grants data subjects a right to access personal data along with comprehensive information on its uses, categories, recipients, and retention periods, as well as to receive confirmation of whether it is being processed.[22] This right operationalises transparency and allows individuals to understand and scrutinise data practices. India's DPDP framework similarly recognises the right of data principals to obtain information about the processing of their digital personal data though the scope and procedural detail are more streamlined and are shaped by the

[20] Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008).
[21] Mantelero, 'Human Rights Impact Assessment'.
[22] GDPR, art. 15(1).

Rules' emphasis on digital notice mechanisms and administrative feasibility.[23] The contrast reflects differing regulatory priorities, i.e the GDPR foregrounds exhaustive disclosure as a rights guarantee, while the DPDP framework balances transparency with simplified compliance expectations.

B. Right to correction and erasure:

Both regimes recognise that inaccurate or outdated personal data can cause tangible harm. The GDPR provides rights to rectification and erasure, enabling individuals to require correction of inaccurate data and in specified circumstances, deletion of data no longer necessary or unlawfully processed.[24] The DPDP framework similarly allows data principals to seek correction and erasure of their personal data, reinforcing accuracy and storage limitation as operational duties for data fiduciaries.[25] While doctrinally aligned, the Indian framework places greater reliance on procedural rules and administrative oversight rather than expansive judicially developed standards.

C. Right to data portability:

The GDPR explicitly grants a right to data portability, allowing data subjects to receive personal data in a structured commonly used format and to transmit it to another controller.[26] This right is designed to promote user autonomy and competition in digital markets. The DPDP framework does not articulate portability with the same breadth, reflecting a more cautious approach that prioritises data protection and security concerns over market driven mobility. This divergence has implications for platform competition and user switching costs in digital ecosystems.

D. Right to object and limits on automated decision-making:

The GDPR recognises the right to object to certain processing activities and establishes safeguards against decisions based solely on automated processing that produce legal or similarly significant effects.[27] These safeguards are intended to preserve human agency and prevent unaccountable algorithmic governance. India's DPDP framework

[23] DPDP Act, 2023, ss. 5, 11; DPDP Rules, 2025.
[24] GDPR, arts. 16, 17(1).
[25] DPDP Act, 2023, ss. 8, 12.
[26] GDPR, art. 20(1).
[27] Ibid, arts. 21, 22(1).

adopts a more restrained posture addressing automated processing primarily through consent requirements and general obligations of fairness rather than through an explicit standalone right to contest automated decisions. This distinction is significant in an era of algorithmic decision-making, where opacity and scale can erode meaningful individual control.

Scholarly analysis underscores that rights relating to automated decisions are effective only when they enable genuine contestability rather than mere disclosure. Bayamlıoğlu argues that transparency alone is insufficient unless individuals can meaningfully challenge outcomes and trigger review mechanisms.[28] This insight highlights a potential gap in frameworks that lack explicit procedural rights tailored to automated processing.

Beyond procedural contestability, the articulation of individual data protection rights reflects deeper constitutional commitments. Lynskey observes that EU data protection law is rooted in the protection of individual autonomy and dignity, framing informational control as an extension of fundamental rights rather than mere consumer protection. This constitutional orientation explains the GDPR's detailed rights architecture and judicially enforceable remedies, particularly in areas where power asymmetries between individuals and data controllers are pronounced.[29]

E. Right to grievance redressal and remedies:

Rights are meaningful only when supported by accessible remedies. The GDPR provides layered mechanisms for complaint, investigation and judicial remedy through independent supervisory authorities.[30] The DPDP framework establishes grievance redressal mechanisms and regulatory oversight through the Data Protection Board, offering administrative avenues for enforcement and penalties.[31] The effectiveness of these rights will depend on institutional capacity, accessibility and consistency of enforcement rather than on textual guarantees alone.

[28] Bayamlıoğlu, 'Right to Contest Automated Decisions'.
[29] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
[30] GDPR, arts. 51, 57-58, 77-79.
[31] DPDP Act, 2023, ss. 13, 18-19, 33.

F. Comparative assessment:

Comparatively, the GDPR articulates a dense and highly specified catalogue of rights reflecting its rights centric and constitutional orientation. The DPDP framework recognises a core subset of these rights but adopts a more restrained and administratively calibrated model. This approach may enhance implementability in a large and diverse digital environment, but it also raises questions about whether reduced specificity could limit the practical enforceability of individual rights. The divergence illustrates a broader regulatory trade-off between expansive rights expression and realistic governance.

VII. OBLIGATIONS OF DATA FIDUCIARIES / CONTROLLERS

Obligations imposed on entities that determine the purposes and means of processing translate abstract data protection principles into concrete compliance duties. Both the GDPR and India's DPDP framework impose such obligations, but they differ in structure, intensity and enforcement orientation.

A. Accountability and governance duties:

The GDPR adopts accountability as a central organising principle, requiring controllers to ensure and demonstrate compliance with data protection obligations through internal governance measures, documentation and oversight mechanisms.[32] This includes maintaining records of processing activities and implementing organisational measures proportionate to the risks involved. India's DPDP framework similarly places responsibility on data fiduciaries to comply with statutory duties relating to lawful processing, transparency and security, though the Rules emphasise procedural compliance and digital governance mechanisms rather than extensive documentation requirements.[33]

Commentary on the GDPR highlights that accountability obligations are intended not merely as formal compliance tools but as mechanisms to internalise responsibility within organisations. Kuner, Bygrave and Docksey emphasise that documentation,

[32] GDPR, arts. 5(2), 24(1), 30.
[33] DPDP Act, 2023, ss. 4-5, 8; DPDP Rules, 2025.

demonstrability and proactive governance are designed to shift data protection from reactive enforcement to preventive compliance culture. This rationale is relevant when assessing whether streamlined accountability duties under the DPDP framework can achieve comparable preventive effects.[34]

B. Data protection by design and security safeguards:

Under the GDPR, controllers must put in place the necessary organisational and technical safeguards to guarantee data protection by default and by design, incorporating privacy concerns into systems and procedures from the beginning.[35] These obligations are closely linked to security safeguards against unauthorised access, disclosure or loss of personal data. The DPDP framework also mandates reasonable security safeguards and places a duty on data fiduciaries to prevent personal data breaches, reflecting convergence on the importance of preventive technical measures.[36] The Indian approach, however, leaves greater discretion to regulatory guidance and sectoral practices in determining what constitutes "reasonable" safeguards.

C. Breach notification obligations:

The GDPR requires controllers to notify supervisory authorities of personal data breaches within prescribed timelines and in certain cases to inform affected data subjects.[37] These timelines are designed to ensure rapid regulatory response and harm mitigation. The DPDP Rules likewise impose breach notification duties on data fiduciaries, reinforcing accountability and transparency in incident response though the procedural pathways and supervisory engagement are tailored to India's administrative framework.[38]

[34] Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2021).
[35] GDPR, art. 25.
[36] DPDP Act, 2023, s. 8(5)-(6).
[37] GDPR, arts. 33-34.
[38] DPDP Act, 2023, s. 8(6); DPDP Rules, 2025.

D. Impact assessments and risk-based compliance:

A distinctive feature of the GDPR is the requirement to conduct Data Protection Impact Assessments (DPIAs) for processing activities likely to result in high risk to individual's rights and freedom.[39] DPIAs operationalise a risk-based approach by requiring prior identification and mitigation of harms. The DPDP framework does not mandate DPIAs in identical terms, but it adopts a risk-sensitive orientation through differentiated obligations for significant data fiduciaries and through regulatory oversight mechanisms.[40] Mantelero's work supports the view that such ex-ante assessment mechanisms are crucial complements to consent and posthoc enforcement in complex data ecosystems.[41]

E. Processor relationships and delegation:

The GDPR draws a clear distinction between controllers and processors and regulates their relationship through contractual obligations that ensure processors act only on documented instructions and maintain appropriate safeguards.[42] The DPDP framework similarly recognises the need to regulate entities that process data on behalf of fiduciaries, though the doctrinal separation is less elaborated and relies more heavily on statutory duties imposed on the primary fiduciary.[43]

F. Comparative assessment:

Overall, the GDPR imposes a dense and highly specified set of controller obligations anchored in accountability, documentation and risk assessment. The DPDP framework reflects a more streamlined and adaptive model that focuses on core duties, digital governance and regulatory oversight. While this approach may reduce compliance burdens and enhance implementability, it also places greater weight on supervisory guidance and enforcement consistency to ensure that obligations translate into effective protection rather than formal compliance alone.

[39] GDPR, art. 35(1).
[40] DPDP Act, 2023, ss. 10, 18-19.
[41] Mantelero, 'Human Rights Impact Assessment'.
[42] GDPR, arts. 28(3), 29, 32.
[43] DPDP Act, 2023, ss. 2(9), 8-9.

VIII. ENFORCEMENT, REMEDIES & INSTITUTIONAL DESIGN

Enforcement architecture determines whether data protection rights and obligations operate effectively in practice. While both the GDPR and India's DPDP framework provide for regulatory oversight and remedies, their institutional designs reflect different legal traditions and governance priorities.

A. Supervisory authorities and institutional structure:

The GDPR creates a decentralised structure of independent oversight authorities in every Member State, managed by the European Data Protection Board. These authorities possess investigative, corrective and advisory powers enabling consistent enforcement while respecting national administrative autonomy.[44] Independence of regulators is treated as a foundational requirement, reinforcing the rights-based orientation of the GDPR.

India's DPDP framework adopts a more centralised institutional model through the Data Protection Board of India. The Board is entrusted with adjudicatory and enforcement functions, including the imposition of penalties and directions for compliance.[45] This design reflects an administrative law approach aimed at streamlined decision making and uniform enforcement, though it raises questions about institutional independence and capacity when compared to the EU's multi-authority model.

B. Complaints, adjudication and remedies:

Under the GDPR, data subjects may lodge complaints with supervisory authorities and seek judicial remedies against controllers or processors.[46] This layered remedial structure ensures both administrative and judicial avenues for redressal. The DPDP framework similarly provides grievance redressal mechanisms and enables data principals to approach the Data Protection Board for resolution of complaints.[47]

[44] GDPR, arts 51(1), 57(1), 58(1)-(2), 68(1).
[45] DPDP Act, 2023, ss. 18-19, 33.
[46] GDPR, arts. 77, 79.
[47] DPDP Act, 2023, ss. 13, 18-19.

However, the Indian regime places stronger emphasis on administrative adjudication, with judicial review operating primarily as a secondary safeguard.

C. Sanctions and deterrence:

The GDPR is notable for its stringent administrative fines calibrated according to the nature, gravity and duration of infringement and linked to global turnover.[48] These sanctions are designed to create strong deterrence, particularly for large multinational entities. India's DPDP framework also provides for significant monetary penalties, signalling regulatory seriousness; however, their deterrent effect will depend on consistent application, transparency in decision making and the Board's enforcement capacity.[49]

D. Procedural fairness and due process:

Effective enforcement requires procedural safeguards for both individuals and regulated entities. The GDPR embeds procedural guarantees through established administrative law principles and access to courts.[50] The DPDP framework similarly incorporates procedural rules governing inquiry, hearing and penalty imposition, though much depends on how these procedures are operationalised by the Board in practice.[51]

E. Comparative assessment:

Comparatively, the GDPR's enforcement model prioritises independence, decentralisation and judicial integration reflecting its constitutional grounding in fundamental rights protection. India's centralised, board-led model prioritises administrative efficiency and uniformity. While this may enhance regulatory responsiveness in a complex digital environment, it places significant responsibility on the Data Protection Board to ensure transparency, consistency and rights sensitive adjudication. The effectiveness of India's enforcement regime will therefore hinge less on textual penalties and more on institutional practice and regulatory credibility.

[48] GDPR, art. 83(2), (4)-(6).
[49] DPDP Act, 2023, s. 33.
[50] GDPR, arts. 58(4), 78-79.
[51] DPDP Act, 2023, ss. 19, 33.

IX. CROSS-BORDER DATA TRANSFERS & INTEROPERABILITY

Cross-border data transfers are a defining challenge for contemporary data protection law, as digital services routinely process personal data across jurisdictions. The GDPR and India's DPDP framework approach this challenge through different legal techniques, reflecting distinct priorities regarding sovereignty, rights protection and regulatory interoperability.

A. GDPR approach to international transfers:

The GDPR permits transfers of personal data outside the European Union only where an adequate level of protection is ensured. This is achieved primarily through adequacy decisions for jurisdictions deemed to provide equivalent protection or through appropriate safeguards such as standard contractual clauses and binding corporate rules.[52] These mechanisms aim to preserve continuity of protection when data leaves the EU, anchoring cross-border transfers in a rights equivalence logic rather than loose data mobility.

B. Indian approach under the DPDP framework:

India's DPDP framework adopts a more state-calibrated model for cross-border transfers. While it does not impose a blanket localisation mandate, it empowers the government to regulate transfers of certain categories of digital personal data and to prescribe conditions or restrictions based on policy considerations.[53] This approach reflects a balance between enabling participation in the global digital economy and retaining regulatory control over sensitive or strategically significant data flows.

C. Interoperability challenges:

Divergences between the two regimes create practical challenges for interoperability. The GDPR's adequacy-based model is premised on equivalence of rights, enforcement independence and remedies. India's framework, which prioritises administrative efficiency and category-based controls, may not neatly align with EU adequacy criteria. This misalignment can increase compliance complexity for multinational

[52] GDPR, arts. 44-46.
[53] DPDP Act, 2023, s. 16.

entities operating across both jurisdictions and may necessitate layered contractual and technical safeguards.

D. Regulatory sovereignty and trust:

Cross-border data governance is not purely technical; it is bound up with questions of regulatory trust and institutional credibility. Kuner's analysis of transborder data flows highlights that transfer regimes function effectively only where legal systems recognise and trust each other's enforcement capacities.[54] In this light, interoperability depends not merely on formal legal provisions but on demonstrable regulatory practice, transparency and rights protection outcomes.

E. Implications for global digital trade:

For India, the DPDP framework's flexible transfer architecture offers adaptability but also introduces uncertainty for foreign partners seeking stable compliance benchmarks. For the EU, strict transfer conditions reinforce rights protection but can be perceived as restrictive by emerging digital economies. Bridging these approaches requires dialogue, sector-specific arrangements and possibly incremental convergence in procedural safeguards rather than wholesale legal transplantation.

F. Comparative assessment:

The GDPR's transfer regime emphasises continuity of rights through equivalence and safeguards, whereas India's model emphasises calibrated control and policy discretion. Each reflects legitimate regulatory objectives. However, sustained interoperability will depend on whether India's enforcement institutions demonstrate consistent rights-sensitive application of the DPDP framework and whether transfer mechanisms evolve to provide predictability without compromising domestic priorities.

[54] Kuner, *Transborder Data Flows*.

X. SUGGESTIONS & RECOMMENDATIONS

Based on the comparative analysis of India's DPDP framework and the EU GDPR, the following suggestions are proposed to strengthen India's data protection regime while preserving regulatory flexibility and domestic policy priorities:

1. **Clarify rights through regulatory guidance:**

Issuing detailed guidelines on the scope and exercise of data principal rights, particularly access, erasure and grievance redressal would enhance legal certainty without requiring statutory amendment.

2. **Strengthen procedural safeguards for high-risk processing:**

Introducing structured, risk-based assessment mechanisms for high-impact data processing (especially involving automation and AI) would complement consent-based protections and reduce reliance on ex post enforcement.

3. **Enhance institutional transparency and independence:**

Clear rules on appointment, tenure and decision-making processes of the Data Protection Board would improve public trust and reinforce regulatory credibility.

4. **Improve interoperability for cross-border transfers:**

Developing standard contractual templates and sector-specific transfer guidelines could reduce compliance friction for multinational entities while maintaining sovereign control over sensitive data.

5. **Promote meaningful consent practices:**

Encouraging simplified, layered notices and user-friendly consent dashboards would help prevent consent fatigue and improve informed decision-making by data principals.

6. **Invest in enforcement capacity and digital literacy:**

Strengthening technical expertise within regulatory bodies and promoting public awareness initiatives would ensure that rights and obligations function effectively in practice.

These measures, taken together would help align India's data protection framework with global best practices while respecting its distinctive constitutional, economic and governance context.

XI. CONCLUSION

This study set out to examine India's Digital Personal Data Protection framework, as operationalised through the DPDP Act, 2023 and DPDP Rules, 2025 in comparison with the European Union's General Data Protection Regulation, from a cyber law perspective. The comparative analysis demonstrates that while both regimes are grounded in shared foundational principles, such as lawful processing, transparency, accountability and protection of individual autonomy, their doctrinal structures and institutional choices reflect markedly different regulatory philosophies.

The GDPR represents a mature, rights-centric model that emphasises detailed articulation of individual rights, plural lawful bases for processing, and a decentralised yet independent enforcement architecture. Its design prioritises continuity of protection, particularly in cross-border contexts, and relies on strong supervisory authorities and judicial integration to ensure compliance. India's DPDP framework by contrast, adopts a more streamlined and administratively calibrated approach. By foregrounding consent, employing category-based safeguards and centralising enforcement through a specialised regulatory board, it seeks to balance individual data protection with regulatory feasibility in a large, diverse and rapidly evolving digital ecosystem.

The analysis shows that these differences create both strengths and vulnerabilities. The GDPR's detailed rights and safeguards offer strong protection but bring significant compliance burdens and complexity. India's more flexible framework may improve implementability and responsiveness, yet it relies heavily on regulatory guidance, institutional practice, and consistent enforcement to prevent dilution of rights. In areas such as automated decision-making, impact assessments, and cross-border data transfers, the gaps highlight the need for governance mechanisms beyond textual guarantees.

Ultimately, the effectiveness of any data protection regime depends not solely on statutory design but on how law is operationalised through institutions, compliance cultures and public awareness. As India's DPDP framework enters its implementation phase, its success will depend on the capacity of regulators to enforce obligations transparently, the willingness of data fiduciaries to embed privacy into system design, and the ability of data principals to exercise their rights meaningfully. By drawing measured lessons from the GDPR without uncritical transplantation, India could develop a data protection regime that is both context-sensitive and globally credible.

XII. REFERENCES

A. Primary Sources

1. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).
2. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

B. Books

1. Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (Oxford University Press 2021).
2. Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
3. Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008).
4. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press).

C. Journal Articles / Research Papers

1. Emre Bayamlıoğlu, 'The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the So-Called "Right to Explanation"' (research article).

2. Rainer Mühlhoff, 'Updating Purpose Limitation for AI: A Normative Approach' (scholarly article).
3. Alessandro Mantelero, 'An Evidence-Based Methodology for Human Rights Impact Assessment' (scholarly article).
4. Dara Hallinan, 'Broad Consent under the GDPR: An Optimistic Perspective' (research article).