



INTERNATIONAL LAW  
JOURNAL

---

**WHITE BLACK  
LEGAL LAW  
JOURNAL**  
**ISSN: 2581-  
8503**

**Peer - Reviewed & Refereed Journal**

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

[WWW.WHITEBLACKLEGAL.CO.IN](http://WWW.WHITEBLACKLEGAL.CO.IN)

### **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK  
LEGAL

## **EDITORIAL** **TEAM**

### **Raju Narayana Swamy (IAS ) Indian Administrative Service** **officer**



a professional  
Procurement from the World Bank.

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public

### **Dr. R. K. Upadhyay**

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.





## **Senior Editor**

### **Dr. Neha Mishra**



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

### **Ms. Sumiti Ahuja**

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



### **Dr. Navtika Singh Nautiyal**

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



### **Dr. Rinu Saraswat**

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

### **Dr. Nitesh Saraswat**

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



### **Subhrajit Chanda**

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

## ***ABOUT US***

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provided dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

# **CROSS BORDER DATA TRANSACTION ANALYSIS**

AUTHORED BY - PRUTHVI KEDILAYA

## **ABSTRACT**

The Digital Personal Data Protection Rules (Draft) serve as a regulatory framework for cross-border data transfers under India's Digital Personal Data Protection Act (hereinafter DPDPA). The Act applies to all entities processing digital personal data of individuals in India, classifying them as data fiduciaries or significant data fiduciaries (hereinafter SDFs) based on data volume and sensitivity. A key feature of the DPDPA is its "negative list" approach, which restricts data transfers only to jurisdictions explicitly blacklisted by the Indian government, in contrast to the adequacy-based approach followed by the EU and UK. The paper outlines the evolution of India's cross-border data transfer laws, comparing them with international frameworks such as the General Data Protection Regulation (hereinafter GDPR), the Global Cross-Border Privacy Rules (hereinafter CBPR) system, and sectoral regulations in the United States. Recommendations include the introduction of Standard Contractual Clauses (hereinafter SCCs), Binding Corporate Rules (hereinafter BCRs), sector-specific transfer rules, and greater participation in global privacy frameworks.

A comparative analysis of DPDPA vs. GDPR highlights key differences in legal basis for processing, the role of Data Protection Officers (hereinafter DPOs), and data breach notification requirements. The GDPR enforces granular compliance measures for sensitive data and mandates a 72-hour breach notification, whereas DPDPA maintains uniform compliance standards and lacks a specified timeframe. To align with global standards, the DPDPA must incorporate nuanced classifications of personal data, periodic regulatory reviews, and enhanced legal mechanisms for secure international data flows. These reforms would enhance business efficiency while ensuring robust data protection and regulatory compliance.

## **INTRODUCTION**

The DPDP Act serves as India's cornerstone legislation for regulating the processing of personal data, safeguarding the rights of data principals (data subjects). It applies to all entities, domestic or international, that process the personal data of individuals residing in India. The



Act classifies entities handling personal data into two categories: *data fiduciaries and significant data fiduciaries (SDFs)*. While data fiduciaries manage personal data in general, SDFs are subject to more stringent compliance requirements due to their handling of larger volumes of sensitive data or engagement in high-risk activities.

Under the DPDP Act, the government holds the power to regulate cross-border data transfers by implementing a "negative list" of restricted countries. The concept of the rules has been introduced to govern cross-border data transfers from and to other countries that have not been banned under section 16 of the DPDP Act. This paper provides a comprehensive guide for organizations to navigate and comply with the DPDPA's cross-border data transfer regulations. Drawing insights from the Data Security Council of India (DSCI)'s Privacy Across Borders whitepaper, it outlines best practices and recommendations to ensure effective compliance with the Act.<sup>1</sup>

## **CROSS BORDER DATA TRANSFER**

### **Initial Laws on Cross-border data transfer**

The initial drafts of the DPDP Bill proposed strict and complex rules for cross-border data transfers, with specific restrictions for different categories of personal data.

- **Local Storage of Sensitive Personal Data:** A requirement to store sensitive personal data locally, even if transferred abroad, would have significantly increased operational costs for businesses, particularly multinational companies.
- **Compliance for Cross-Border Transfers:** The draft mandated explicit consent from data principals, approval of transfer contracts or intra-group schemes by the Data Protection Authority (DPA) and the government, and an adequacy determination to ensure data was not shared with foreign governments without approval.
- **Restrictions on Critical Personal Data Transfers:** Critical personal data transfers were prohibited, except in emergencies (e.g., health crises) or to entities approved under government adequacy decisions to protect national security.<sup>2</sup>

The finalized DPDP rules should be able to simplify these requirements, delegating cross-border transfer rules to sectoral regulators and government-issued guidelines.

---

<sup>1</sup> Securiti.ai, Cross-Border Data Transfer Requirements Under India DPDPA, <https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa> (last visited Jan. 29, 2025).

<sup>2</sup> Leegality, Cross-Border Data Transfer, <https://www.leegality.com/consent-blog/cross-border-data-transfer> (last visited Jan. 29, 2025).



## **GUIDANCE TOWARDS CROSS-BORDER DATA TRANSACTIONS**

To ensure a robust framework for cross-border data transfers under the DPDP Act, 2023, India must implement clear and structured guidelines that balance data protection with global trade facilitation. The current provision allowing the government to notify restricted countries through a "negative list" lacks transparency and predictability for businesses. Instead, India should adopt an adequacy or safeguard-based approach, similar to the EU's GDPR, where data transfers are permitted based on a country's data protection standards or contractual safeguards like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). This will provide businesses with a structured and reliable mechanism for international data flows while ensuring compliance with global privacy norms.

Additionally, the DPDP Act must establish sector-specific requirements for high-risk data categories, such as financial and health data, mandating additional technical and organizational security controls before transfer. This is crucial since industries like banking and healthcare deal with highly sensitive information that, if mishandled, could result in significant harm. Implementing clear audit mechanisms, breach notification requirements, and transparency obligations for data fiduciaries will further strengthen accountability. Aligning with best practices from frameworks like the GDPR and Australia's Privacy Act will help India foster trust in its data governance model while promoting cross-border collaboration and digital trade.<sup>3</sup>

## **COMPARISON BETWEEN OTHER COUNTRY LAWS**

1. The EU and UK assess whether a foreign country provides an "adequate" level of data protection before allowing free data transfers. This involves evaluating the recipient country's legal framework, enforcement mechanisms, and commitment to international privacy norms.
2. **Standard Contractual Clauses (SCCs)** are a widely accepted mechanism under **General Data Protection Regulation (GDPR)** for ensuring data protection when transferring to non-adequate jurisdictions. The Indian Legal System could create pre-approved SCC templates, offering businesses a legal framework to govern international transfers. These clauses should specify obligations for both the data exporter and the foreign recipient, covering aspects like data security, access controls, and limitations

---

<sup>3</sup> Ramakant Mohapatra et al., Privacy Across Borders: Guidance on Cross-Border Data Transfers for Indian Organisations, Data Security Council of India (2024).

on further transfers, fostering business efficiency while ensuring accountability in cross-border data handling.

3. Multinational Corporations hold an advantage by often transferring data securely across various jurisdictions internally. The EU's Binding Corporate Rules (BCRs) allows such transfers while maintaining uniform data protection standards within the organization.
4. France's GDPR enforcement emphasizes obtaining explicit and informed consent from individuals for cross-border data transfers, especially to countries with limited data protection. Individuals must consent completely and explicitly with respect to the transfer of data. Transparency obligations should include notifying individuals about the recipient's jurisdiction, intended purpose of processing, and data retention policies.
5. The US adopts a sectoral approach to privacy, with laws like HIPAA for healthcare and GLBA for financial services. A system of sector-specific data transfer rules can be created for critical industries like health, finance, and national security in order to ensure level of safety while transfer is defined.
6. International collaboration is key to fostering trust and interoperability in data transfers. India could participate in frameworks like the Global Cross-Border Privacy Rules (CBPR) system or negotiate bilateral agreements with key trading partners. These agreements would ensure reciprocal commitments to data protection, simplifying compliance for businesses while safeguarding individual privacy.<sup>4</sup>
7. The CBPR System is designed to enable cross-border data transfers among participating economies, regardless of differences in domestic laws, provided minimum global standards are met. On the other hand, the DPDP restricts transfers to jurisdictions deemed "trusted" by the Indian government. By adopting CBPR principles, India could expand its list of eligible jurisdictions for data transfers, provided they align with internationally recognized privacy frameworks, thus promoting greater global data connectivity.
8. The UK ensures that its data protection policies evolve with time by conducting regular reviews and consulting stakeholders, including businesses, civil society, and technology experts. A similar practice can be established by a regulatory review committee to periodically assess cross-border data transfer rules. Engaging

---

<sup>4</sup> U.S. Department of Commerce, Global Cross-Border Privacy Rules Declaration, Commerce.gov, <https://www.commerce.gov/global-cross-border-privacy-rules-declaration> (last visited Jan. 13, 2025).

stakeholders would ensure that policies remain practical, business-friendly, and in line with global standards.

9. The GDPR classifies personal data into distinct categories, including sensitive data, with tailored compliance requirements for each. In contrast, the DPDP Act applies uniform standards to all personal data, lacking differentiation between sensitive or critical data. To improve, the DPDP Act should introduce nuanced classifications and corresponding compliance measures to enhance protection for sensitive data, aligning with global standards and addressing specific risks associated with high-risk data types.<sup>5</sup>

### **COMPARISON AMONG GDPR AND DPDP**

The DPDP Act and GDPR share foundational principles of data protection but differ in scope and enforcement. The DPDP Act applies to digital personal data processed in India and has extraterritorial applicability for data processing related to offering goods or services to individuals in India, akin to GDPR's extraterritorial reach. Both frameworks establish rules for data controllers (fiduciaries) and processors and provide rights to data subjects (principals). However, while GDPR enforces tailored obligations for sensitive data categories, the DPDP Act maintains uniform standards for all personal data. Here are a few more differences between the 2 and how the DPDP can adapt from the GDPR-

#### **A. Legal Basis for Processing**

Under the DPDPA, processing personal data is primarily based on obtaining consent from data principals or under specified "legitimate uses," such as compliance with legal obligations, employment purposes, or emergency responses. The GDPR offers a broader range of lawful bases for processing, including the performance of a contract, legitimate interests pursued by the controller, and vital interests of the data subject. *Hence, introducing a broader classification of personal data and lawful processing bases can strengthen the regulatory structure.*

#### **B. Data Protection Officer (DPO) Requirement**

The GDPR mandates the appointment of a Data Protection Officer for certain organizations, particularly those engaged in large-scale processing of sensitive data or monitoring individuals systematically. The DPDPA does not explicitly require the designation of a DPO, potentially leading to differences in accountability and oversight

---

<sup>5</sup> Leegality, GDPR vs. DPDP, <https://www.leegality.com/consent-blog/gdpr-vs-dpdp> (last visited Jan. 29, 2025).



structures between the two regulations. *Implementing mandatory Data Protection Officers for significant data fiduciaries would improve accountability.*

### **C. Data Breach notification**

Both regulations require notification in the event of a personal data breach. The GDPR specifies a 72-hour timeframe for reporting breaches to supervisory authorities. *The DPDPA also mandates breach notifications but does not stipulate a specific timeframe. Hence, it must be left to be defined by subsequent rules.*<sup>6</sup>

## **CONCLUSION**

The Digital Personal Data Protection Act (DPDPA), 2023, represents a significant step toward regulating data privacy in India, yet it requires further refinements to align with global best practices. The analysis highlights key differences between the DPDPA and international frameworks such as the GDPR, particularly in areas like cross-border data transfers, data classification, and compliance mechanisms. The GDPR employs an adequacy-based approach, stringent breach notification timelines, and differentiated data protection obligations, whereas the DPDPA currently relies on a "negative list" mechanism, uniform compliance standards, and undefined breach notification requirements. To strengthen its framework, India should adopt structured mechanisms like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), introduce sector-specific rules, and create a regulatory review committee for periodic assessments.

Furthermore, comparisons with countries such as France, the UK, and the US highlight the need for India to enhance its legal framework for cross-border transactions while ensuring business efficiency. Transparency, accountability, and adaptability are critical to maintaining trust in India's data governance model. By incorporating lessons from the GDPR, CBPR, and other global frameworks, the DPDPA can facilitate seamless international data flows while ensuring the highest standards of privacy and compliance.

## **THANK YOU!!**

---

<sup>6</sup> Latham & Watkins LLP, India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, LATHAM & WATKINS, <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf> (last visited Jan. 29, 2025).