



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

## Balancing Sovereignty and Innovation: The Impact of Google India Data Privacy Case on Cross-Border Data Management and Compliance

*Ajanta Tejaswini.*

### Abstract

Google India's data privacy case marks an inflection point in India's digital governance story. But also, it critically evaluates the legality of international data transfers and requires informed users' consent. The ruling has established the basis for a rights-based and sovereignty-aware framework for data. The case commentary crystallizes the broader implications of the decision into a narrow exploration of three areas of significance particular to the evolution of regulation, compliance by corporations, and international jurisprudence. Providing a comparative analysis with global examples (GDPR, PIPL, CCPA), the commentary demonstrates how India continues to develop a hybrid model that professes digital sovereignty while attempting to remain interoperable with the global data economy. For each of these three areas of significance, the commentary makes practical policy recommendations aimed at delivering enforceable, innovation-facilitating, internationally recognized data governance.

### Keywords

Data Privacy, Google India, Cross-Border Data Flows, Digital Sovereignty, (DPDPA) Digital Personal Data Protection Act 2023, Compliance, Jurisprudence, Localization, Data Protection Board of India. Other important key terms are as follows: -

1. **GDPR known as General Data Protection Regulation:** It is a European Union law focused upon protecting the personal data of individuals within the state of EU.
2. **PIPL known as Personal Information Protection Law:** This is the Chinese law that regulates the processing of personal information by organizations within China.
3. **CCPA known as California Consumer Privacy Act:** It is a US state law, that provides residents of California rights regarding their personal information.

## **Introduction**

The historic ruling in the case of ‘Google India data privacy’ signifies India's shift from an aspirational to an actionable privacy regime. The judgment reaffirmed that user consent must be explicit, informed and limited to the purpose, particularly in context of cross-border data transfers. Moreover, the following commentary examines, that how the ruling would impact corporate compliance, regulatory design, and India’s international data diplomacy.

### **I. Background and Legal Context**

Rooted in the constitutional right to privacy affirmed in Justice K.S. Puttaswamy v. Union of India (2017), the Google case arose amid heightened scrutiny of Big Tech’s handling of Indian user data. The case prompted judicial review of how data was collected, consent obtained, and personal information transferred overseas. The ruling underscored the importance of purpose limitation and user autonomy, reinforcing the principles enshrined in the Digital Personal Data Protection Act, 2023 (DPDPA).

### **II. Impact on Cross-Border Data Management**

Restrictions on what data can leave the country (India) have been put in place because of the ruling. The court explicitly stated that moving data to countries with less protection is inconsistent with Indian constitutional rights, following the rationale in the EU's Schrems II case. Due to this ruling "India data rings", operational separation of Indian data, and contractual protections like Standard Contractual Clauses (SCCs) have increased.

### **III. Compliance Landscape Post-Ruling**

Indian firms have appointed Data Protection Officer roles, updated their privacy policies, and have adopted purpose based consent frameworks, especially in the fintech, edtech, and health verticals. For example, international companies like Google and Meta have begun to deploy Indian specific storage infrastructure and applications. The companies are using data mapping tools widely, and vendor contracts are being amended to include enhanced data protection terms & conditions. Whereas companies' internal governance controls include data audits and breach responses.

### **IV. Role of the Data Protection Board of India (DPBI)**

The new corrected decision handed down related to Google will work with DPBI as a central enforcement agency. It will likely discard the sectoral implementation of the DPDPA, collaborate with other regulators like the RBI and the IRDAI, experiment with a strategic enforcement path designed for high-risk data custodians, and of course, mandates notice and provision of due process, rule-based guidance, and transparency in enforcement.

## **V. Comparative Jurisprudence**

India's pathway is consistent with Southeast Asian models, like Singapore's PDPA, Brazil's LGPD, or the EU's GDPR. The Google decision recalls the demands of the Schrems II decision relating to redress, consent and proportionality for cross-border data transfers. India also achieves some balance between digital openness and national interest - and does not impose localization, as was mandated in China's PIPL. Therefore, this advances India's normative and legal influence in the Global South.

## **VI. Forward Looking Implications**

1. **Data Sovereignty and Diplomacy:** By asserting mutual privacy protection. India can leverage this ruling to impact its' future international agreements and digital trade arrangements.
2. **Innovation and Privacy Tech:** With the rise of AI audit tools, privacy engineering, and ethical data stewardship and compliance will become more reliant on these resources.
3. **Global Interoperability:** A third approach between China's authoritarian practices and the US sectoral model would be India's personalized yet rights-centered approach.
4. **Regulatory Risks:** For the government to ensure that there is no lag in innovation or compliance fatigue from organizations, it must guarantee proportional enforcement.

## **VII. Policy Recommendations**

1. Provide a clear public set of adequacy lists and protocols for cross border transfers.
2. Grant DPBI powers to make rules, enforce rules and handle grievances.
3. Provide SME's sandbox groups, tax breaks and already developed privacy templates.
4. Focus on professional development and data privacy literacy.
5. Consolidate and coordinate India's standing in global settings of digital diplomacy.

## **Conclusion**

Hence the following Google India case embodies the judiciary's commitment to enforceable privacy rights in a fast-growing economy. It pushes India toward a future where our personal data is protected not just by various policies, but through institutional integrity, industry

collaboration, and the international trust. As India refines its data governance, our real challenge lies in maintaining a delicate balance of upholding autonomy without sacrificing ambition.

## **References**

- a. India and the global battle for data. Carnegie endowment 2021.  
Link:<https://carnegieendowment.org>
- b. Privacy engineering/designed in the cloud era. Cloud Security Alliance 2024.  
Link:<https://cloudsecurityalliance.org>
- c. Privacy by design in Indian enterprises post, DPDPA. Deloitte 2024.  
Link:<https://deloitte.com/in>
- d. Digital Personal Data Protection Act (Also known as DPDPA), (2023-India).
- e. Economic and political weekly, 59(7), 28–34. Ghosh, A-2024. Data localization, costs and consequences.
- f. India DPDPA Compliance Playbook link:<https://iapp.org>
- g. International Association of Privacy Professionals (IAPP-2024).
- h. Storage of Payment System Data. Link:<https://rbi.org.in> Reserve Bank of India. (2018). Schrems II, CJEU Case C-311/18, 2020.
- i. Startups wary of rising compliance costs post google data ruling. Link:  
<https://economictimes.indiatimes.com> ET Tech 2025.