Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Cross-Border Data Transfers and Privacy Law

Article History:

Name of Author:
Steven Mendoza[1], Robert Young[2], Mr. Justin Walton[3], Daniel Ruiz[4] and Michael Raymond[5]

Affiliation: [1]Research Associate, Department of Corporate Governance, Pacific Coast University, Chile
[2]Research Associate, School of Retail Management, Balkan University of Technology, Serbia
[3]Adjunct Faculty, Department of Banking and Insurance, Arctic Circle University, Norway
[4]Professor, Department of Commerce, Central Eurasia University, Kazakhstan
[5]Senior Research Fellow, Department of Corporate Governance, Central Eurasia University, Kazakhstan
Corresponding Author: Steven Mendoza

How to cite this article: Steven Mendoza, *et, al.* Cross-Border Data Transfers and Privacy Law. *J Community Med* 2024;5(1);39-42.

Abstract: In today's interconnected digital economy, cross-border data transfers are essential for international operations, cloud services, and AI-driven applications. However, the legal frameworks governing these transfers are increasingly complex, fragmented, and evolving. This article examines the key regulatory regimes shaping international data movement—including the EU's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act (DPDPA), and U.S. state and federal rules—highlighting their divergent mechanisms such as adequacy decisions, standard contractual clauses, and localization requirements. The analysis addresses core legal risks, enforcement trends, and compliance challenges, particularly following landmark developments like Schrems II and the introduction of the EU-U.S. Data Privacy Framework. Through comparative charts and workflow diagrams, the article outlines a practical compliance strategy that includes data mapping, risk assessments, contractual safeguards, and privacy-enhancing technologies (PETs). As global scrutiny intensifies and AI systems further complicate data flows, cross-border compliance will require proactive governance, technical innovation, and continuous regulatory alignment to ensure legal integrity and consumer trust.

Keywords: Cross-border data transfers, GDPR, DPDPA, SCCs, BCRs, data localization, international privacy law, EU-U.S. Data Privacy Framework.

INTRODUCTION

In the age of data-driven global commerce, cross-border data transfers—movement of personal data between jurisdictions—are foundational to international collaboration, digital services, and cloud-based ecosystems. This logistical necessity, however, is paralleled by a patchwork of privacy laws whose complexity and enforcement have grown exponentially. Organizations now face legal, operational, and reputational risks in navigating these frameworks, particularly as regulatory scrutiny intensifies and penalties escalate.

DEFINING CROSS-BORDER DATA TRANSFERS

A cross-border data transfer occurs whenever personal data is sent, accessed, or processed outside the originating country. This may include:

- Sharing customer data from a European company to a cloud provider in the U.S.

- Outsourcing HR processing from India to a server in Singapore.
- Using SaaS platforms with globally distributed data centers[1][2].

These activities trigger a host of requirements under leading privacy regimes, including the EU's General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act (DPDPA), U.S. state laws (CPRA, CCPA), and Brazil's LGPD.

LEGAL RISKS AND COMPLIANCE CHALLENGES

Regulatory Patchwork

Cross-border data movement is governed by a variety of domestic and extraterritorial laws. Notably:

- **GDPR** imposes some of the strictest rules, restricting outbound transfers unless conditions like Adequacy Decisions, Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs) are satisfied[3][4][5][6].
- **India's DPDPA (2023)** permits personal data transfers unless a destination country is explicitly "blacklisted" by the government, lacking mechanisms like adequacy or SCCs and creating regulatory unpredictability[7][8][9][10].
- **U.S. and others**: Laws such as the California Consumer Privacy Act (CCPA) and new federal proposals add further layers of compliance, with national security rules restricting transfers to certain countries[11].

Core Legal Requirements

Mechanism	Jurisdictional Example	Requirement
Adequacy Decision	EU (GDPR)	EU Commission certifies "adequate" data protection, no extra safeguards needed.
Standard Contractual Clauses	EU, Brazil	Boilerplate legal commitments between sender/receiver to enforce GDPR-like standards.
Binding Corporate Rules	EU, Global	Corporate group-wide rules, approved by regulators, for multinational intra-group transfers.
Explicit User Consent	Various	Informed consent may permit transfer in absence of other mechanisms.
Data Localization	India (sectoral), Russia	Certain sensitive data must remain in-country or backed up locally.
National Security Restrictions	U.S., India	Bans or restricts data transfer to "countries of concern."

Caption: Key Mechanisms for Lawful Cross-Border Data Transfers

Major Frameworks: A Comparative Analysis

1. The EU's GDPR

GDPR prohibits transfers of personal data to non-EU/EEA countries unless:

- An **Adequacy Decision** is issued, certifying the recipient country's protections[5][3].
- The parties use **SCCs** that contractually bind the recipient to GDPR-level protections. After the "Schrems II" ruling invalidated Privacy Shield (for US–EU transfers), the Commission updated SCCs with more robust requirements like Transfer Impact Assessments (TIAs)[6].
- **BCRs**: Internal multinational policies pre-approved by data regulators.
- **Derogations** exist for narrow, exceptional circumstances such as explicit user consent.

Key obligations include risk assessments, data mapping, and continuous monitoring of legal changes[4][2][6].

2. India's Digital Personal Data Protection Act (DPDPA)

India's DPDPA adopts a **"blacklist approach"**: transfers to any country except those specifically restricted by the government are allowed. There's no "adequacy" process nor a legal basis for SCCs or BCRs. Broad discretion remains, creating uncertainties and requiring vigilant tracking of government notifications[7][10].

Sectoral rules (e.g., RBI for banking, SEBI for securities) may further require data localization, especially for financial or biometric data[10].

3. The United States and Other Jurisdictions

- **EU-U.S. Data Privacy Framework (2023+)**: A new framework post-Privacy Shield, aiming to address adequacy needs for transatlantic transfers[12][13].
- **CCPA/CPRA (California):** Mandates transparency, consent management, and consumer redress for international data movement of Californian residents.
- Jurisdictions like Russia, China, and some Middle Eastern states require stricter data localization[2][5].

RISKS AND ENFORCEMENT TRENDS

- **Regulatory fines**: Recent GDPR fines include €290m for Uber and €30.5m for Clearview AI due to unlawful cross-border transfers[11].
- **Operational delays**: Unclear legal mechanisms or localization rules can halt business operations or slow data access.
- **Reputational and strategic risk**: Data breaches or illegal transfers erode consumer trust and can trigger multi-jurisdictional lawsuits[2][11].

Building a Compliance Framework

1. **Data Mapping & Classification**: Identify and document all personal data types, storage locations, and transfer destinations[14].
2. **Legal Mechanism Selection**: Choose the most appropriate mechanism (adequacy, SCCs, BCRs, or consent) based on transfer context and destination[5][6].
3. **Transfer Impact Assessments**: Carry out risk assessments for each cross-border transfer scenario, with board-level oversight[4][6].
4. **Contract Management**: Ensure contracts include appropriate clauses and audit rights; update regularly as laws evolve.
5. **Technical Safeguards**: Deploy encryption, pseudonymization, and multi-layered access controls, as well as privacy-enhancing technologies (PETs)[15].
6. **Ongoing Monitoring**: Stay alert to regulatory updates, blacklists, and enforcement actions in all relevant jurisdictions.

[image:2]

Caption: Sample Compliance Workflow for Cross-Border Data Transfers—data mapping, mechanism selection, risk assessment, and ongoing monitoring.

VISUALIZING THE REGULATORY LANDSCAPE

International Data Transfer Mechanisms (2025)

[image:3]

Caption: Comparative view of data transfer mechanisms in the EU, India, U.S., and selected APAC/LatAm jurisdictions.

Emerging Threats and Opportunities

- AI/ML models and generative tools often ingest international datasets, triggering GDPR and extraterritorial compliance concerns[11][4].
- Use of privacy-enhancing technologies (PETs) such as federated learning, secure enclaves, and fully homomorphic encryption is increasingly critical for secure global collaboration[15].
- By 2027, Gartner predicts over 40% of AI-driven privacy breaches will involve cross-border data mishandling by emerging GenAI tools[11].

CONCLUSION

Cross-border data transfers are now at the intersection of legal complexity, technology innovation, and operational risk. Success demands not just compliance "by design," but proactive governance, robust technical controls, and continuous legal vigilance. The future will see the fusion of evolving privacy-enhancing technologies and a global push for harmonized protocols amid enduring geopolitical and commercial tensions.

REFERENCES

1. https://www.privacyengine.io/resources/glossary/cross-border-data-transfer/
2. https://atlan.com/know/data-governance/cross-border-data-transfers/
3. https://gdpr-info.eu/chapter-5/
4. https://techgdpr.com/blog/gdpr-compliance-for-ai-managing-cross-border-data-transfers/
5. https://mandatly.com/gdpr-compliance/international-data-transfers-understanding-legal-frameworks
6. https://www.gdpr-advisor.com/gdpr-and-international-data-transfers-key-regulations-and-frameworks/
7. https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/
8. https://nliulawreview.nliu.ac.in/blog/guarding-the-data-frontier-navigating-cross-border-data-transfer-under-digital-personal-data-protection-act/

9. https://www.leegality.com/consent-blog/cross-border-data-transfer
10. https://www.dataguidance.com/sites/default/files/dcsi_privacy_across_borders-_guidance_on_cross-border_data_transfers_for_indian_organizations.pdf
11. https://trustarc.com/resource/webinar-cross-border-data-transfers-in-2025-regulatory-changes-ai-risks-and-operationalization/
12. https://www.dataprivacyframework.gov/Program-Overview
13. https://policies.google.com/privacy/frameworks?hl=en-US
14. https://www.clutchevents.co/resources/building-a-compliance-framework-for-cross-border-data-transfers
15. https://dualitytech.com/blog/cross-border-data-transfer/