Submitted February 18, 2025

Comments on India's Proposed Digital Personal Data Protection Rule

Introduction and Summary

Below please find the submission of the Computer & Communications Industry Association (CCIA) regarding India's Ministry of Electronics and Information Technology (MeitY) proposed Digital Personal Data Protection Rule. CCIA is an international, not for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks.[1]

CCIA appreciates the opportunity to provide input on this Rule. Specific comments are as follows.

Article 12 - Additional Duties for Significant Data Fiduciaries

Article 12 establishes additional duties for "significant data fiduciaries," including ensuring that certain types of personal data and traffic data related to its flow remain within India and adhere to any subsequent government restrictions on cross-border data transfers. The central government would be granted nearly absolute discretion in designating "significant information fiduciaries,"[2] which leaves companies uncertain whether they will have to comply or not. Compounding this problem, the law targets specific entities rather than specific categories of digital personal data.

This would impose substantial compliance burdens on significant data fiduciaries, as restrictions on cross-border data flows would impose operational and administrative costs for data processors currently managing data outside of India. Moreover, the potential to require that significant data fiduciaries store certain personal and traffic data domestically creates friction for businesses that rely on global infrastructure for data storage, especially companies with overseas servers. The rule could undermine privacy protections by centralizing control over data localization without clear safeguards,[3] while also risking disruption of cross-border data flows vital for global business operations.

To address these concerns, CCIA recommends that any future government restrictions on cross-border data transfers should be subject to a reasonable notice-and-comment period for relevant stakeholders, allowing for a careful analysis of any potential implications for cross-border commerce or India's obligations under trade rules. Additionally, restrictions on

[1] For more, visit www.ccianet.org.
[2] *See* Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India , pt. II sec. 1 (Aug. 11, 2023), at 9-10, *available at* https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
[3] *See* Peter Swire & DeBrae Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity – Organizational Effects*, Ga. Tech. Scheller Coll. of Bus. Res. Paper No. 4030905 (June 16, 2023), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905.

data transfers should be based on particular risks the transfers could pose, not on whether data will be carried across national borders or who performs the transfer. Article 12 should specify that future such restrictions are specific to types of personal data flows presenting a specified risk, rather than select entities.

Article 14 - Processing of Personal Data Outside India

Rule 14 would allow personal data to be transferred outside India only if it meets requirements set by the government. It grants the government authority to impose conditions on international data transfers, including restrictions on disclosing personal data to foreign government agencies or entities controlled by foreign states. It does not specify which countries will be restricted, as these will be determined by the government through general or special orders.

This rule raises several concerns. First, it would significantly complicate operations for businesses providing cross-border services, such as social media platforms or e-commerce companies that rely on multiple data processors across various jurisdictions. These businesses would need to ensure that their data processors are not located in restricted countries, creating significant operational overhead. Additionally, the government's authority to determine the categories of data that cannot be stored outside India affects businesses that rely on global cloud infrastructure. This uncertainty could create substantial administrative burdens, as companies would need to continually monitor and manage their data storage practices to comply with evolving government directives.

Second, this restriction on foreign data transfers could conflict with foreign laws requiringcompanies to disclose data to foreign government agencies for routine regulatory purposes or comply with international regulatory investigations. Such a situation could lead to serious conflicts of law and force businesses to navigate complex legal challenges, potentially risking penalties in both India and abroad.

Third, this requirement diverges from global norms. For example, Europe's GDPR allows cross-border data transfers with safeguards,[4] but the DPDP Rules lack any mechanism for businesses to guarantee their ability to transfer data abroad. The DPDP imposes stricter controls on cross-border data transfers without providing similar protections for data stored outside India. Additionally, the Draft Rules lack clear breach notification procedures and compliance monitoring, unlike the GDPR, which provides detailed and consistent guidelines.[5] This ambiguity could lead to inconsistent enforcement, creating confusion and placing undue compliance burdens on businesses.

Fourth, the presumption against cross-border data transfers would likely conflict with India's international trade obligations, particularly under the World Trade Organization's General Agreement on Trade in Services (GATS). India has committed under GATS to allow firms to offer cross-border supply of services, many of which involve personal data. Restricting cross-border data flows, especially without a clear 'whitelist' of approved countries, could

[4] *See* General Data Protection Regulation, 2016 O.J. (L119) 679, art. 45, § 1, *available at* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[5] *Id.*, art. 33-34.

disrupt these services and place foreign companies at a competitive disadvantage, violating India's commitments to national treatment and Most Favored Nation (MFN) treatment. For example, India has committed to allow foreign firms to supply, on a cross-border basis, online information and data processing services,[6] categories that encompass many commonly traded services. Applying data localization requirements to such services would make this commitment meaningless, as discriminating against cross-border supply would violate the national treatment commitments India promised to uphold– i.e., treating cross-border suppliers no less favorably than domestic suppliers.

To address these concerns, India could establish an certification framework that designates certain countries (or companies) as having sufficient data protection safeguards for cross-border transfers, comparable to what would be required within India, thus providing clarity for businesses. Such a regime (e.g., modeled on the APEC Cross-Border Privacy Rules system) would allow companies to transfer data if they meet specific safeguards.[7] These safe harbor rules should have clear, non-arbitrary guidelines that ensure transparency and reduce compliance uncertainty.

Conclusion

CCIA appreciates the opportunity to provide input on this draft Rule. To ensure the Rule's success while limiting its potential impacts on privacy and trade, CCIA strongly recommends revising Articles 12 and 14. As written, they lack clarity for designating "significant data fiduciaries," grant the government broad discretion to restrict data flows, and may conflict with India's international trade obligations.

To mitigate these concerns, CCIA recommends that any future restrictions on cross-border data transfers be clearly defined, based on specific risks, and subject to a reasonable notice-and-comment period. Additionally, a framework for certifying that certain countries or companies have sufficient data protection safeguards would provide much-needed clarity, facilitate global business, and ensure privacy protections. By addressing these issues, India can both protect its citizens' data and promote cross-border trade and innovation. CCIA appreciates the opportunity to provide this feedback and looks forward to continuing engagement on this issue.

[6] *See India: Schedule of Specific Comments*, WTO (Apr. 15, 1994), *available at* (https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/SCHD/GATS-SC/SC42.pdf&Open=True.

[7] *See APEC Cross-Border Privacy Rules System Program Requirements*, Asia-Pac. Econ. Cooperation, *available at* https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-ProgramRequirements.pdf.