GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

GLOBAL DATA ALLIANCE SUBMISSION ON PROPOSED REDUCTION OF DPDPA COMPLIANCE TIMELINES

February 2026

Office of the Secretary
Ministry of Electronics and Information Technology (**MeitY**) Government of India
New Delhi.
E-mail: secretary@meity.gov.in
Cc: Shri. Ajit Kumar, Joint Secretary, MeitY
Cc: Shri. Deepak Goel, Scientist 'G' and Group Coordinator, MeitY
Cc: Shri. Bharat Yadav, Scientist 'F' and Director, MeitY

The Global Data Alliance (GDA)[1] thanks the Ministry of Electronics and Information Technology for the opportunity to provide feedback on the proposal to reduce compliance timelines for specific provisions under the Digital Personal Data Protection Act (**DPDPA**)[2] and its Rules (**Rules**) [3].

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Global Data Alliance members share a deep and long-standing commitment to supporting economic development, building trust in the digital economy, and protecting personal data across regions, technologies, and business models. Alliance member companies rely on the ability to transfer data responsibly around the world to create jobs and make industries at home and abroad more competitive.

Cross-border data transfers power growth across the globe and all sectors of the economy — from farming, fisheries, and mining; to services of all types; to the manufacturing industries. Data transfers are critical for companies of all sizes, fostering innovation and economic development, creating jobs, and promoting productivity, safety, robust cybersecurity, and environmental responsibility. Cross-border data transfers are especially important for micro, small, and medium-sized enterprises (MSMEs).

The global economy faces an increasingly challenging environment characterized by rising geopolitical tensions and divisions. In this regard, undue restrictions on data transfers interrupt cross-border access to knowledge and digital tools and increase digital fragmentation. As UNCTAD has explained, such fragmentation "reduces market opportunities for domestic MSMEs to reach worldwide markets, [and] ... reduces opportunities for digital innovation,

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see https://www.globaldataalliance.org

[2] Digital Personal Data Protection Act, 2023,
https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[3] Digital Personal Data Rules, 2025,
https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation."

The GDA appreciates MeitY's commitment to operationalizing the DPDP Act, an important step in advancing privacy rights and strengthening India's data governance framework. However, the proposed reduction to compliance timelines for certain obligations will create significant difficulty for GDA members. The proposals fail to account for the scale of infrastructure upgrades, contractual alignments, and technical implementations required across enterprise operations.

Businesses have already begun sequencing compliance requirements around the original 18-month window; compressing this timeline will increase implementation risks and would disproportionately impact technology startups. It also departs from international norms: the General Data Protection Regulation (GDPR) provided a two-year compliance window, and Brazil's Lei Geral de Proteção de Dados (LGPD) deferred enforcement by nearly two years, among several other examples. Accordingly, we recommend that MeitY uphold the original compliance schedule published on November 14, 2025. Here are our specific suggestions:

1. Data retention: Rule 8(3)

The proposed 3-month timeline for implementing personal data and log retention requirements under Rule 8(3) is insufficient and creates significant practical concerns for companies working to implement the Act.

The Act's obligations to retain data may force organizations to adopt broad retention practices, which paradoxically expand data storage, amplifying security exposure and creating avoidable risks for individuals. As companies design compliance programs, they must assess their obligation to retain data under Rule 8(3), their obligation to honor requests for erasure of data under Section 12 of the Act, and the rights and obligations imposed in other global privacy laws.

Establishing compliant retention systems across distributed infrastructure may require systematic engineering changes, testing protocols, and deployment cycles that cannot be responsibly compressed into this timeframe. Organizations must design retention architectures that address regulatory compliance and operational efficiency while avoiding unnecessary data accumulation that increases security risks. Compressing this work into three months would not allow companies to fully address these issues.

In addition, Rule 8(3) also lacks clarity on which categories of data must be retained. Without specific guidance, organizations need adequate time to interpret requirements and design retention practices that are compliant and proportionate

Recommendation: MeitY should revert to the original 18-month implementation period and issue guidance clarifying the scope of data retention requirements under this Rule which help timely implementation.

2. Data localization and cross border data transfer restrictions: Rules 13(5) and 15

Both Rule 13(5) and 15 could benefit from further clarity to better support international data transfers, which underpin the modern global economy.

Rule 13 (5) supports the creation of a Committee that is to provide recommendations to the Central Government about restrictions on international data transfers by Significant Data Fiduciaries The specific details of the constitution of the committee under Rule 13 (5) are not yet available, and the criteria that will guide such classification are also unclear. We strongly recommend undertaking a consultative process about the establishment of this Committee and that industry be included in that process.

Rule 15 similarly provides that personal data may be transferred outside of India, subject to restrictions imposed by the Central Government when transfers are made to a person or entity under the control of a foreign State. Restrictions issued under this Rule could lead to a complex landscape for global businesses, where restrictions under India's laws may conflict with obligations under foreign laws, even for transfers to countries with strong data protection laws and close trade relationships with India.

This uncertainty makes compliance planning difficult. Architecting global data flows to accommodate localization or transfer restrictions is a technically complex undertaking. For instance, isolating a single data category – ensuring it is stored, processed, and accessed exclusively within India while remaining integrated with broader enterprise systems – requires significant technical reconfiguration. Organizations must then layer contractual safeguards across vendors, affiliates, and partners to ensure restricted data is not inadvertently transferred. This demands cross-functional coordination across teams and entities, often spanning multiple jurisdictions. Accordingly, enforcing these provisions on compressed timelines, while foundational regulatory parameters remain unclear, will be challenging.

We strongly recommend that as the Rule comes into force, the Government expressly permit transfers that are subjected to well-understood contractual and legal requirements that protect data, such as contractual clauses, binding corporate rules, and similar commitments. At most, the Rule should be applied to only allow for restrictions when transfers are to specific countries where there are significant concerns that personal data may not be appropriately protected and no such commitments are in place.

Recommendation:

- MeitY should defer enforcement of Rules 12(45) and 14 to the original 18-month period.
- Include industry in the consultation processes for Rule 12(4) with respect to the details of the constitution of the "committee" and the criteria for data classification. Moreover, once the committee is formed and the data classification is completed, we urge that MeitY provide industry with sufficient compliance time of more than 18 months.
- Issue guidance under Rule 14 expressly permitting data transfers that are subject to well-understood contractual and legal requirements that protect data, such as contractual clauses, binding corporate rules, and similar commitments.
- GDA respectfully requests to be invited to similar or upcoming consultation meetings.

******

The GDA respectfully urges MeitY to maintain compliance timelines in the original schedule to enable businesses to implement the Act effectively.