Business Software Alliance

Wednesday, February 4, 2026

Shri. S. Krishnan,
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

SUBJECT: BSA SUBMISSION ON PROPOSED REDUCTION OF DPDPA COMPLIANCE TIMELINES

Respected Shri S. Krishnan,

The Business Software Alliance (**BSA**)[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].

BSA 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 BSA members. The proposals fail to account for the scale of infrastructure upgrades, contractual alignments, and technical implementations required across enterprise operations. For example, the consent-based approach of the DPDPA and its stricter standards for processing children's data may require companies to revise their compliance practices, rather than simply apply their existing compliance programs

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[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

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. This runs directly counter to the spirit and intent of the Act by increasing rather than decreasing privacy risks. 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 (especially across distributed infrastructure) 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. Retention obligations intersect with security telemetry, diagnostic logging, lawful access, and erasure rights under the Act and other global laws. Compressing the timeline for companies to undertake this compliance work risks expanding data storage unnecessarily, increasing security exposure, and undermining consistency with existing global privacy commitments.

One way to narrow these concerns is to clarify that Rule 8(3) applies only to Data Fiduciaries specified in the Third Schedule, as with other parts of Rule 8.

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. It may also narrow the scope of Rule 8(3), by clarifying it only applies to Data Fiduciaries specified in the Third Schedule.

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. Additionally, because some of our members operate multi-tenant, globally integrated systems, they would need to coordinate legal, engineering, product, security, and contractual changes across a broad portfolio of services before implementation parameters are settled, creating risk of inconsistent compliance.

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 13(5) and 15 to the original 18-month period.
- Include industry in the consultation processes for Rule 13(5) with respect to "committee" for data classification.
- Issue guidance under Rule 15 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.

3. Significant Data Fiduciary (SDF) Obligations - Rule 13

Rule 13 imposes a range of new obligations on Significant Data Fiduciaries, but these companies are not the only ones impacted by Rule 13. Data processors and enterprise businesses may face indirect compliance impact of Rule 13 obligations. When SDFs are required to conduct Data Protection Impact Assessments or implement enhanced measures, these obligations flow downstream through contracts and operational dependencies. Providers must adjust infrastructure, provide audit documentation, and implement controls to align with the requirements of multiple SDF clients, who often have differing interpretations of compliance.

This creates a cascading timeline problem. Designation criteria for SDFs remains broad, meaning service providers cannot anticipate which clients will be classified as SDFs or when those classifications will be made. Once designations occur, providers will need time to respond, and compressed timelines leave no buffer for this downstream compliance. In effect, providers face a timeline that is even shorter than the one afforded to SDFs themselves: they cannot act until their clients are designated, however they must still undertake actions that enable SDF compliance almost immediately. Adequate lead time is essential to allow both SDFs and their service providers to coordinate implementation in a sequenced, workable manner.

Recommendation: MeitY should maintain the original 18-month implementation timeline and defer application of SDF-specific obligations until formal designation criteria are issued after adequate consultation. We also urge you to use the 18-month implementation period to establish criteria for determining if a company is an SDF and a process for notifying the company of the determination, to provide predictability for compliance obligations.

4. Information disclosure - Rule 23

Immediate enforcement of Rule 23's information-furnishing requirements will create concerns because it would create new powers for the Central Government to enforce the Act before the Act take effect.

This Rule would also benefit from additional guidance during the implementation period. For example, guidance could address request formats and scope limitations, to create clear expectations around new requests. That guidance should also recognize that requests should be

sent to the relevant company in the first instance, rather than to service providers that handle data on behalf of the company. This is particularly important because regulatory requirements for prompt disclosure by a service provider may create tension with its contractual duties to consult clients, required notifications, and conduct legal reviews. Adequate implementation time is necessary for organizations to establish internal protocols, train response teams, align client contracts, and build response mechanisms that satisfy both regulatory and contractual obligations.

Recommendation: MeitY should defer enforcement of Rule 23 to the original 18-month timeline and issue further guidance addressing the format and scope of such requests, while ensuring requests are directed to a company in the first instance rather than to a company's service provider.

******

BSA respectfully urges MeitY to maintain compliance timelines in the original schedule to enable businesses to implement the Act effectively. Please feel free to reach out to me at venkateshk@bsa.org if there are any questions or concerns. We look forward to continued engagement with the MeitY.

Yours sincerely,

Venkatesh Krishnamoorthy
Country Manager, India
Business Software Alliance