ASIA VIDEO INDUSTRY ASSOCIATION

Shri S Krishnan
Secretary,
Ministry of Electronics and Information Technology Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi – 110003

5 March, 2025

Dear Sir/ Ma'am,

Submission to the Ministry of Electronics and Information Technology on the Consultation for the Digital Personal Data Protection Rules, 2025

On behalf of the Asia Video Industry Association (AVIA), we welcome the opportunity to comment on the Draft Digital Personal Data Protection Rules, 2025 (i.e. the Rules), as proposed by the Ministry of Electronics and Information Technology (MeitY). AVIA is the trade association for the video industry and ecosystem in Asia Pacific. It serves to make the video industry stronger and healthier through promoting the common interests of its members. AVIA is the interlocutor for the industry with governments across the region, leading the fight against video piracy, as well as publishing reports and hosting industry conferences. It aims to support a vibrant video industry for the benefit of all stakeholders.

Our membership consists of a combination of local, regional and multi-national companies, many of which are substantial cross-border investors; creating and purchasing video content to meet rapidly-expanding consumer demands and investing in India's communications and creative industries.

AVIA welcomes the first comprehensive legislation on data protection in India and the implementing rules for the Digital Personal Data Protection Act 2023 (DPDPA 2023), which aims to protect personal data and preserve the rights of individuals and align with global standards such as those found in the European Union's General Data Protection Regulation (EU GDPR) and Singapore's Personal Data Protection Act (PDPA) to mandate transparent, accessible, and detailed notices which explain data collection, purpose, and rights. However, we would like to provide feedback on some concerns regarding implementation and compliance with these rules so that they align with global standards.

Implementation Timeline

First and foremost, we acknowledge MeitY's consideration for a staggered implementation of some provisions. However, we would like to note that there is an absence of a compliance window, with most of these rules and provisions coming into force upon publication of the Rules. Given that our member companies would need to make extensive technical and

20/F Leighton Centre, 77 Leighton Road, Causeway Bay, Hong Kong | 5008 Ang Mo Kio Avenue 5, #04-09 Techplace II Singapore 569874 avia.org

operational changes to comply with these Rules, we humbly request a transitional timeline of at least two years for companies to do so.

Notice by Data Fiduciary to Data Principal

It is important to emphasise that the notification requirements established by the Data Fiduciary to the Data Principal, as outlined in the Rules, are consistent with global standards. Nevertheless, given that the Rules allow for considerable flexibility in how the notification is presented, implementing a prescriptive format specific to India for multinational corporations operating globally presents challenges, as it may diverge from global norms. Therefore, the current flexibility incorporated in the Rules concerning the notification requirements is welcome and we would urge that this flexibility is retained.

However, the requirement to renotify all the Data Principals who have previously consented to the processing of their personal data by a Data Fiduciary (and deleting their personal data if they do not issue any response to the notice) may not be feasible. Illustratively, news organisations, media houses, documentary filmmakers, film producers, etc. may find it difficult to comply with this requirement given the sheer volume of personal data from contributors that they process. While we understand the rationale of the requirement to re-notify Data Principals, we recommend that Data Fiduciaries should only be required to stop the processing of personal data if the Data Principals specifically revoke their previous consent.

Registration and Obligations of the Consent Manager

The DPDPA 2023 introduces the role of Consent Managers through which Data Principals may manage their consent to Data Fiduciaries. However, the Rules only set out the (1) conditions to register as a Consent Manager with the Data Protection Board (DPB) and (2) obligations of the Consent Manager with respect to the Data Principals. As such, given the Rules' emphasis on simplicity, we would ask for additional clarification and further consultation, prior to operationalising the Consent Manager framework. Furthermore, we urge MeitY to issue guidelines to assist businesses in complying with the Consent Manager framework. These guidelines should address interoperability between Data Fiduciaries and Consent Managers, as well as clarify the accountability of Consent Managers in the event of any data breaches that may expose Data Principals

Intimation of Personal Data Breach

While the intimation of data breaches is significant, there exists the concern regarding the lack of a threshold for reporting such breaches, as well as the stipulation that all data breaches must be reported to the DPB and the Data Principal, irrespective of the severity of the breach, and that the breach must be reported without delay with a detailed report submitted within 72 hours. This can mean that even the breach of a single e-mail address must be reported, and with such a brief reporting timeline and numerous reporting requirements that do not conform to global standards, it becomes onerous not only for data fiduciaries but also for the

20/F Leighton Centre, 77 Leighton Road, Causeway Bay, Hong Kong | 5008 Ang Mo Kio Avenue 5, #04-09 Techplace II Singapore 569874 avia.org

DPB. We would request that consideration be given to extending reporting timelines and, more importantly, should also include a specified threshold based on the services provided, nature of personal data processed to ensure that breaches which pose a real risk of harm to Data Principals are reported while avoiding potentially overwhelming the DPB.

We note that other overlapping obligations for reporting breaches are already in place, such as those to the Computer Emergency Reporting Team (CERT) in India and other sectoral regulators with differing timelines and compliance requirements. As such, adding to these requirements already in place by other agencies may lead to compliance challenges for corporations. To align with the nation's overarching goal to support the Ease of Doing Business (EoDB), multiple reporting requirements across different agencies should be consolidated under a single authority once the DPDPA takes effect.

We recommend that the Data Protection Board serve as a single-window to report personal data breaches, thus doing away with the onerous process of reporting to multiple authorities. In addition, to simplify compliance for businesses, we recommend that a first report should be filed within 72 hours of the discovery of the personal data breach, instead of the "layered" approach in rule 7(2).

Determining When a Specified Purpose is No Longer Served

The Rules provide overly prescriptive provisions regarding the maximum retention period for certain categories of Data Fiduciaries, as well as the obligation to notify Data Principals prior to the deletion of personal data once the "specified purpose" for retention has elapsed. Therefore, we recommend that the Rules be aligned with global norms and security practices instead. Specifically, we would recommend that, in cases where Data Principals continue to pay for a service, data erasure requirements should not be enforced as paying customers should be regarded as active users. Secondly, we request that it should be clarified that any obligation to erase personal data should only be applicable when a Data Principal terminates a service or subscription. Moreover, as is currently common practice, service providers may retain certain customer data for a reasonable period of time after a subscription is canceled. In the event a customer signs up again, this retention enables a good consumer experience. Lastly, the requirements to delete personal data while retaining user accounts for Data Principals to access should be removed due to their technical complexity and impracticality. Finally, notifying Data Principals before deleting personal data imposes undue burdens on businesses and we would urge this requirement to be revisited.

Additional Obligations of Significant Data Fiduciary

Pursuant to Section 10 of the DPDPA, the Central Government is empowered to notify entities as Significant Data Fiduciaries (SDFs) based on an assessment of relevant factors, including "the volume and the sensitivity of the personal data processed". It is our position that further clarification is required on the "sensitivity" and "volume" thresholds for classification as an SDF. Specifically, in light of the additional compliance obligations applicable to SDFs, the

classification should be primarily determined by the "sensitivity of the personal information", which pertains solely to the type of personal data and the associated scope of data processing activities rather than purely focusing on "the volume" processed. Moreover, the Rules do not envisage a compliance window once an entity has been classified as an SDF. We recommend that the Rules should provide a reasonable time frame of two years for entities to comply with the additional requirements applicable to SDFs, such as that of providing Data Protection Impact Assessments (DPIA). This timeline will allow Data Fiduciaries to make the necessary operational and technical adjustments to meet compliance standards.

Despite the fact that similar DPIA assessments are already required during the auditing process, the Rules mandate that additional DPIAs be conducted by third parties as well. There is no clear distinction between DPIAs and audits. We suggest that the audit and the requirement for the additional independent DPIA should not be made compulsory, as this would lead to redundancy. Furthermore, Data Fiduciaries should have the flexibility to conduct these assessments in-house as third parties may lack knowledge of internal processes. We also recommend establishing clear thresholds to trigger the requirement for DPIAs. For instance, we propose that DPIAs be conducted only when a Data Fiduciary processes sensitive personal information or on an event-driven basis (i.e., prior to the launch of a new product), rather than on an annual basis, and it should not be necessary for these DPIAs to be submitted to the DPB.

Data Localisation Requirements & Cross-Border Data Transfer Restrictions

Cross-border data flows are integral to the functioning of the 21st-century economy. This necessity applies to businesses of all sizes across industries, not just those focused on digital activities. Introducing these cross-border data transfer requirements and establishing a committee represents a significant departure from the initial DPDPA, and reintroducing data localisation mandates for SDFs contradicts the government's intent to implement principles-based and business-friendly data protection legislation. Likewise, such restrictions on cross-border data flows will adversely impact the ease of doing business in India.

The Rules require SDFs to undertake data localisation, and the cross-border transfer restrictions under Rule 14 conflict with Section 16 of the DPDPA, which only envisages a list of countries to which personal data cannot be transferred as notified by the Central Government. Given this conflict, we suggest consideration be given to excluding this provision from the Rules. Additionally, we recommend that such restrictions on transferring personal data outside India should only be introduced under the notification mechanism provided for under Section 16 of the DPDPA. Moreover, if the Central Government notifies a list of certain foreign states to which personal data cannot be transferred, it should subsequently prescribe measures (in line with global standards) that may be put in place to enable transfers to such foreign states and companies should be provided with sufficient time to implement such measures. Therefore, it is essential that provisions on data transfers do not create uncertainty among stakeholders and align with international best practices.

We also seek greater clarity regarding what constitutes algorithmic software and the due diligence requirements that Significant Data Fiduciaries must deploy for the verification of such software. Clear definitions and guidelines will aid in compliance and ensure that SDFs can effectively manage their obligations

Language Requirements for Notices

Data Principals have the option of receiving notices and requests for consent in the processing of personal data in either English or any language specified in the Eighth Schedule of the Constitution. This creates a significant operational burden for Data Principals as it disproportionately burdens smaller companies. We suggest offering flexibility at the discretion of the Data Fiduciary to determine the appropriate language, including English, for notices.

Age Verification/ Parental Consent

The proposed requirements are operationally challenging. Furthermore, our members' Online Curated Content (OCC) services provide professionally curated content and already have a range of mechanisms in place to ensure safe, informed, and age-appropriate viewing for children and adults. As such, a less onerous approach is recommended for such services. In addition, we would like to point out that services providers can take reasonable steps to verify ages; however, users should also take responsibility to provide service providers with accurate information. We believe more consultation is required on this front.

Conclusion

Although we recognise the Government of India's commitment to safeguarding personal data while fostering a regulatory environment that supports innovation, global alignment, and business competitiveness, we believe that the implementing rules should take into consideration the position already passed in the DPDPA 2023, and any other overlapping regulations or processes that are already in place to support the ease of doing business in India. To ensure effective implementation, we urge MeitY to consider providing a clear compliance window, streamline reporting requirements, and align key provisions with global standards. Specifically, we believe that introducing a risk-based threshold for data breach reporting, offering greater flexibility in data retention obligations, and clarifying the criteria for Significant Data Fiduciaries (SDFs) will be instrumental in reducing compliance burdens while maintaining robust data protection standards that align with international best practices. Additionally, avoiding restrictive data localisation and cross-border data transfer constraints will further support India's digital economy and global trade ambitions.

Finally, we would request that MeitY undertake an exercise to ensure consistency and alignment of requirements with other rules, in particular related to the maintenance of logs. As an example, the Maintenance of logs by Data Fiduciary {Rule 6 (1)(e)} requires Data Fiduciaries to maintain logs regarding unauthorized access, its investigation, remediation, and the continued processing of related personal data for a period of one year. However, this requirement

20/F Leighton Centre, 77 Leighton Road, Causeway Bay, Hong Kong | 5008 Ang Mo Kio Avenue 5, #04-09 Techplace II Singapore 569874 avia.org

contradicts the Cyber Security Directions issued on April 28, 2022 (CERT-In Directives), under Section 70B(6) of the Information Technology Act, 2000, which mandates that logs be maintained for a period of 180 days on a rolling basis. Although the language in the Rules specifies that compliance with other laws in force is expected, it does not clarify whether the provisions of those laws would take precedence over the requirements of this Rule or the DPDPA. We would welcome clarity or additional guidance on which takes precedence.