COMMENTS TO THE GOVERNMENT OF INDIA

ON

THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

February 14, 2025

The International Trademark Association (INTA) would like to thank the Ministry of Electronics and Information Technology for the opportunity to provide comments on the Draft of the Digital Personal Data Protection Rules, 2025 ("Rules"), which, together with the Digital Personal Data Protection Act, 2023 ("Act"), will bring in an overhaul of India's personal data protection regime.

We hope you will find these comments helpful, and we welcome the opportunity to further engage in discussions on the topic.

The International Trademark Association (INTA) is a global association of brand owners and professionals dedicated to supporting trademarks and complementary intellectual property (IP) to foster consumer trust, economic growth, and innovation, and committed to building a better society through brands. Members include nearly 6,500 organizations, representing more than 34,350 individuals (trademark owners, professionals, and academics) from 185 countries, who benefit from the Association's global trademark resources, policy development, education and training, and international network. We have 221 members in India, some of which include brand owners such as: Reliance Industries Ltd, Mahindra & Mahindra Limited, Aditya Birla Fashion and Retail Limited, Viacom18, TVS Motor Company Limited, and Sun Pharmaceutical Industries Limited. Founded in 1878, INTA, a not-for-profit organization, is headquartered in New York City, with offices in Beijing, Brussels, Santiago, Singapore, and Washington, D.C., and a representative in New Delhi. For more information, visit inta.org.

General Comments

In addition to providing our comments on the present Rules hereunder, we take this opportunity to reiterate our comments to the Draft India Data Accessibility & Use Policy titled "Data Privacy Principles and Considerations for India", and our comments on the Digital Personal Data Protection Bill, 2022.

Our position is that data privacy rights under legislation must be balanced with the obligation to protect consumers from counterfeiting, fraud, and contraventions of intellectual property rights, and that the legitimate rights of brand owners protecting their intellectual property must be considered while developing legislation relating to personal data privacy.

Provisions should be explored within the legislative framework of data protection that allow brand owners and law enforcement agencies to access records which may be required for the protection and policing of their valuable IP rights – for instance, to initiate enforcement action against otherwise

‘unknown’ infringers and IP violators. Of course, the legitimate interest of a brand owner vs. the privacy of an individual / third-party will have to be carefully balanced. Nonetheless, the provisions should be clear that brand owners have a right to obtain personal information when there is a reasonable suspicion that domain name abuse, infringement, counterfeiting and/or piracy are suspected.

Privacy legislation should facilitate, rather than hinder, the protection of the public from infringement or counterfeiting. Therefore, it should expressly allow for an expeditious process to provide access to non-public information (such as domain name registration data) necessary for identifying bad actors. Section 7(d) of the Act allows a Data Fiduciary to process personal data of a Data Principal “*for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force.*” As currently written, this is rather broad. In contrast, Section 7(i) of the Act, which addresses employer rights for processing personal data without consent of the employee, explicitly refers to safeguarding intellectual property rights, including trade secrets. While there was an opportunity to address this gap in the Rules, it has not been done. INTA proposes that the final version of the Rules include provisions to clarify this, ensuring that the privacy law supports IP enforcement and does not inadvertently exclude it with overly broad or vague language.

This issue is particularly pressing in cases of domain name infringements, which have been on the rise in recent years. Much of the domain name registration data, which is crucial for resolving complaints under both the Uniform Domain Name Dispute Resolution Policy (UDRP) and the .IN Domain Name Dispute Resolution Policy, is now masked. As a result, legitimate trademark owners face significant challenges in accessing this essential information. This process often involves paying fees to WIPO or NIXI when filing complaints, and sometimes even again after making amendments to the complaint, creating additional obstacles for rights owners. Given the increasing complexity and financial cost of this process, trademark rights holders require clarity on how the Act will accommodate their needs. We request a clear right of access for trademark rights holders to accurate domain name registration data (WHOIS data) for investigative purposes, including without limitation for the establishment, the exercise, or the defense of cybersecurity, intellectual property, consumer protection or any other legal claims whether criminal or civil in nature. This would not only benefit trademark owners but also support the broader industry in effectively addressing domain name infringements.

Specific Comments

We highlight our comments to the following Rules for consideration:

1. Rule 2: Section 2 (u) of the Act defines "personal data breach" as “*any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, which compromises the confidentiality, integrity or availability of personal data*”. The term "processing" in relation to personal data has been defined under Section 2 (x) of the Act as “*wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing,*

disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction". Given the broad scope of these definitions, one could argue that the processing of personal data into non-personal data - without specific consent from the Data Principal - could fall under the definition of a "personal data breach." As such, the aggregation of personal data and its anonymization into non-personal data may be explicitly exempted from the requirement of obtaining consent under the Act. Permanent anonymization of data is allowed in many jurisdictions. This is especially important for INTA members, as brands necessarily rely on advertising and other kinds of commercial communication – for which anonymized data and analytics are essential business intelligence. Since behavioral profiling and targeted advertising, without the explicit consent of the Data Principal, may not be possible, companies may at least be permitted to convert personal data into non-personal data for the purpose of serving contextual ads.

2. Rule 7 of the Rules also mentions that on becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, and without delay intimate each affected Data Principal and the Board. Intimating for any personal data breach, regardless of the severity or impact may result in an unnecessary compliance burden on the Data Fiduciaries. There would also be a negative impact on the Data Principals as receiving frequent notifications for minor breaches may result in them ignoring major breach notifications. It is recommended that a distinction be made between major and minor breaches for notification purposes.

3. Rule 10: The Act requires Data Fiduciaries to obtain verifiable parental consent prior to processing personal data of a minor. In this regard, Rule 10 of the Rules provides further guidance as to the responsibility of the Data Fiduciary to obtain such parental consent, and the threshold for meeting the standard of such consent being verifiable under the legislation. However, the Rules only specify that Data Fiduciaries must take appropriate technical and organizational measures and conduct due diligence to ensure the legitimacy of parental consent, and state that consent may be verified through verifiable details of the parent's identity and age already available to the Data Fiduciary, or such details being provided and authenticated through government-issued services (such as the DigiLocker service). Additionally, while the Act allows for the Rules to provide exemptions to this requirement of parental consent, the exemptions which have been provided under the Rules are extremely limited in nature. This requirement of parental consent and the lack of clarity regarding the level of accountability on Data Fiduciaries to verify parental consent is likely to create implementational issues for many classes of Data Fiduciaries which provide services to a substantial demographic of minors such as social media, content streaming OTT platforms, gaming companies, etc. The lack of specific thresholds also creates a potential risk of a wide net of unsubstantiated complaints being made and enforcement actions being taken against Data Fiduciaries on this point, which could have an adverse effect on both the operations of Data Fiduciaries and the burden on the Board. To avoid such risks, the Rules may be revised to provide more specific requirements relating to the responsibility of Data Fiduciaries for verifying parental consent.

4. Rule 12: The provisions of the Rules prescribe requirements in relation to data localization and cross-border data transfers. Specifically, Rule 12(4) of the Rules places an additional obligation on Significant Data Fiduciaries wherein the government may notify certain categories of

personal data on the basis of recommendations by a committee appointed by it, and Significant Data Fiduciaries may not transfer such categories of personal data outside India. This leaves foreign brand owners potentially in the dark regarding their continuing compliance with local rules and localisation requirements. Category changes and notifications that may be made at an indefinite point in the future, especially without stakeholder consultation, may entail significant changes in digital infrastructure, increase compliance burden and operational costs, while also leaving the data in question in a temporary flux and possibly at risk. We request that the Rules include clarity on the manner of such categorisation, compliance requirements and timelines, as well as consequences of non-compliances (if any), to help foreign brand-owners be in a better position to plan and implement the necessary changes to their digital infrastructure and ongoing compliances.

In addition to the data localization requirement discussed above, Significant Data Fiduciaries are required to comply with some additional obligations under the Act and Rules. Specifically, Rule 12 of the Rules prescribes conducting a data protection impact assessment and an audit for compliance with the provisions of the Act and Rules on an annual basis, and submission of a report regarding the assessment and audit to the regulatory authority – the Data Protection Board of India ("Board"). Additionally, Significant Data Fiduciaries are required to ensure that any algorithmic software employed by them to process personal data is not likely to cause a risk to the rights of Data Principals under law. These requirements, in the current version of the Rules, have been imposed without clear guidance on the specifics needed to meet compliance. In the absence of more clarity, Significant Data Fiduciaries, who may include foreign brand owners, may face issues in ensuring that their systems and policies are adequate for the standards required by Indian authorities under the new law.

5. Rule 15: Section 17(2)(b) of the Act allows an explicit exemption for the government from the Act's provisions when processing personal data necessary "*for research, archiving, or statistical purposes, provided the personal data is not used to make decisions specific to a Data Principal.*" Rule 15 and the Second Schedule of the draft Rules outline the standards for such processing. Given that the majority of research occurs in the private sector and considering some industry-specific exceptions (such as in the medical field), the private sector should also be allowed to process personal data for research, subject to the same standards prescribed under the Rules.

6. Rule 18: Rule 18 sub clause 9 provides that an inquiry by the Board shall be completed within a period of six months from the date of receipt of the intimation, complaint, reference or direction under Section 27 of the Act, unless such period is extended by it, for reasons to be recorded in writing, for a further period not exceeding three months at a time. A period of 6 months for completing an inquiry with the provision of a 3-month extension creates critical concerns for all parties involved. For example, pending inquiries for 9 months shall be detrimental to the reputation and goodwill of any Data Fiduciary. It is recommended that the inquiry period be reduced, and extensions be provided only in rare cases with reasons recorded in writing. We propose a cap of 3 months within which complaints should be disposed of – so as to maintain balance on both sides and ensure a speedy and fair redressal process.

We are pleased to answer any questions that the Ministry of Electronics and Information Technology may have and are available to discuss our recommendations in more detail. Please contact Lori Schulman (lschulman@inta.org) or Gauri Kumar (gkumar.consultant@inta.org).

Thank you for considering our comments and suggestions.

Sincerely,

Etienne Sanz De Acedo
Chief Executive Officer
International Trademark Association