March 6, 2026

GLOBAL DATA ALLIANCE COMMENTS ON VIETNAM DRAFT DECREE ON THE CYBERSECURITY LAW

The Global Data Alliance (**GDA**)[1] appreciates the opportunity to provide feedback on the Draft Decree detailing a number of articles in the Cybersecurity Law of Vietnam to the Ministry of Public Security (**MPS**) and the Ministry of Justice (**MOJ**). To avoid unintended harms, the GDA recommends that Vietnam explore alternative approaches to the data localization mandates proposed in the Draft Decree.

The GDA has provided comments on numerous Vietnamese proposed requirements to localize data or restrict data transfers. Those comments can be found here.[2]

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. The GDA supports policies that help instill trust in the digital economy without imposing undue cross-border data restrictions or localization requirements that undermine data security, innovation, economic development, and international trade.

GDA member companies are significant investors in Vietnam, investing millions of dollars and supporting thousands of jobs. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.

As the Government of Vietnam considers revisions to the Draft Decree on the Cybersecurity Law, we wish to provide our recommendations to enhance the effectiveness of the legislation, reduce unnecessary impacts on businesses, and better align the legal framework with international practices. Failure to do so could negatively impact the ability of Vietnamese enterprises and other organizations for developing and adopting cutting edge digital technologies, including cloud computing and artificial intelligence.

Data Localization Requirements

Article 28 requires domestic enterprises to store certain types of data in Vietnam: a) Data on personal information of service users in Vietnam; b) Data generated by service users in Vietnam: Account names using the service, time of using the service, credit card information, email addresses, latest login/logout network (IP) addresses, and registered phone numbers attached to accounts or data; c) Data on the relationships of service users in Vietnam: friends and groups that users connect with or interact with. Further, Article 28.3 requires foreign enterprises—including those providing data storage and sharing in

[1] For more information on the Global Data Alliance, please see www.globaldataalliance.org

[2] *See* Global Data Alliance, GDA Comment to the Government of Vietnam (2020 – 2025), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-vietnam&sector=&language=&posts_filtered=1

cyberspace, online applications, among others—to set up branches or representative offices in Vietnam in specific cases related to violating the Cybersecurity Law and they have been notified by the MPS.

The GDA's interpretation is that the requirements in Article 28 are similar to those the data localization requirements outlined in the Decree No. 53/2022/ND-CP dated August 15, 2022, detailing a number of articles of the Law on Cybersecurity 2018 (**Decree 53**).

The scope of services proposed for data localization is very broad and is likely to cover entities, including those that often act in the capacity of a data processor, i.e., service providers processing personal information on behalf of another entity (i.e., a data controller). Both these parties have distinct roles and responsibilities in the data processing ecosystem, which have been clearly distinguished under the Personal Data Protection (PDP) Law of Vietnam that took effect in January 2026. The PDP Law assigns data controllers the primary accountability for the processing activities as the data processors act on the data controllers' instructions.

If both data controllers and data processors are held to strict data localization standards, it presents additional costs to the digital economy, in the form of additional storage requirements, information security issues, regulatory uncertainty, and overlapping compliance burdens.

Cross-border data transfers underpin the global economy and are vital to the security of networks and information systems. Data localization requirements do not ensure information security and are likely to have the opposite effect of reducing information security instead. Such requirements can frustrate efforts to implement effective security measures, protect data, and defend critical networks, just as they can impede business innovation and limit services available to consumers.

As noted in our previous submissions, data localization requirements have a chilling effect on the local economy as they restrict domestic enterprises and other organizations from fully benefiting from cutting edge technology and services available in the global marketplace. For instance, restrictions on cross-border data transfers may prevent domestic companies, including small and medium-sized enterprises (**SMEs**) and larger organizations such as hospitals, airlines, and banks, from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Vietnam. Such services frequently provide best-in-class security capabilities. Domestic companies subject to data transfer restrictions are likely to find it difficult to access such services, reducing their competitiveness, especially internationally, and exposing them to greater data security risks. Restrictions on international data transfers are also resource-intensive for government authorities to manage.

Moreover, it is inadvisable to require localization of broad categories of data that could include data that is commonplace in everyday business operations. Such data is unlike the type of highly sensitive government data that implicates national security concerns. Accordingly, we urge Vietnam to avoid the imposition of unnecessary or arbitrary restrictions on cross-border data transfers, given Vietnam's relatively high restrictiveness score on international indices of cross-border data transfer policies.[3] Vietnam's regulatory efforts should focus on enabling cross-border data transfers in the digital economy – consistent with Vietnam's treaty commitments, such as under Article 12 of the WTO Agreement on E-Commerce to seek to "facilitate public access to and use of government data" and Article 14.11 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**CPTPP**) – while considering a more nuanced approach towards data governance at the same time, that does not impinge its national security and public policy objectives.[4]

[3] Global Data Alliance, *Cross-Border Data Policy Index* (2023), at: https://globaldataalliance.org/resource/cross-border-data-policy-index/

[4] Open Data - Bridging the Data Divide (2021), https://www.bsa.org/files/policy-filings/061120bsaopendata.pdf

Recommendation: Remove the localization requirement under Article 28 for covered organizations to store data on personal information, data on relationships of service users, and data created by service users in Vietnam. If the MPS wishes to retain the data localization requirements against our recommendation, we recommend that the MPS clarify that so long as the data itself is stored in Vietnam, the proposed requirement does not (a) prevent organizations from transferring a copy of the data overseas for legitimate business purposes, nor (b) prevent organizations from using global cloud-based services that do not or cannot store data in Vietnam.

Sincerely,

Joseph P. Whitlock
Executive Director
Global Data Alliance
josephw@bsa.org