November 7, 2024

H.E. Pham Minh Chinh
Prime Minister
Socialist Republic of Vietnam

Dear Prime Minister Pham Minh Chinh:

We write to you on behalf of the undersigned associations representing global and regional industries engaged in trade and investment with Vietnam, to express our concerns with Vietnam's draft Data Law. We are supportive of the Government of Vietnam's objective to update the country's data laws and encourage the Government to allow for further deliberation, review and consultation before promulgating the data law.

If enacted, the draft Data Law ("the law" or "draft law") would greatly hinder data processing in Vietnam, impacting the ability of foreign businesses to operate and invest in Vietnam across industries and create a chilling effect on the entire digital and data ecosystem that underpins the economy. The ability to process data (whether personal or non-personal data) for reasonable purposes, without prohibitive or prescriptive regulation, enables businesses large and small to offer state-of-the-art innovative services, while still responsibly handling data.

Therefore, we urge the Ministry of Public Security to delay the passage of the Data Law in order to conduct further consultation and address industry's concerns with the scope and applicability of the Data Law's provisions.

We have outlined several pressing concerns below, that are based on version 5 of the draft law.

The Data Law should not apply to personal data: Personal data protection should be governed by dedicated regulations (such as the existing Personal Data Protection [PDP] Decree and the Personal Data Protection Law, which is already in the drafting process). To avoid conflicting provisions, overlapping scopes, and to ensure consistency and clarity, matters pertaining to personal data protection should be excluded from the Data Law. The Data Law should include an explicit provision that the PDP Law should supersede the Data Law in case of any inconsistencies between them.

Restrictions on cross-border flows for a broad set of ambiguously defined data (Articles 3.25, 3.26, 22, and 25): The broad yet unclear definition for "important data" and "core data", coupled with the onerous restrictions on cross-border data transfers, effectively means that most data will be required to be localized within Vietnam, unless companies receive prior written approval from the Vietnamese government. The security of data is determined by the quality and relevancy of the security controls applied to protect it, not where it is located. Studies have shown that data localization/residency requirements do not actually improve data security. What

matters is the security controls that are in place to protect the data and mitigate risks of unauthorized access or disclosure. Implementing such requirements will limit organizations' ability to access some of the most secure computing environments and impede Vietnamese businesses and citizens' access to cost-effective, state-of-the-art technology needed for a country's digital transformation.

Moreover, a disproportionate implementation of restrictions around important and core data is likely to undermine Vietnam's efforts to attract foreign investment, including in strategic sectors such as the semiconductor industry. The approach taken in this framework is similar to the Measures for Security Assessment for Outbound Data Transfer in Mainland China where foreign firms expressed strong reservations about their willingness to invest in the market in response to the proposed measure.

To avoid these unintended consequences, we recommend definitions of "core data" and "important data" be more clearly defined in an exhaustive list and be consistent with existing laws, or to remove the approval requirement and rely on other safeguards. We urge MPS to consider alternative pathways to address any concerns with cross-border data flows, such as developing guidelines on security best practices to be implemented by service users when transferring data offshore, leveraging well-reputed international security accreditations (e.g. ISO 27018), or setting up data transfer frameworks that set out clear responsibilities between the transferor of data and the offshore recipient.

The requirements within the draft law would likely contravene Vietnam's international trade commitments, as foreign service suppliers would be put at a distinct disadvantage to operate in the country and serve Vietnamese customers (or foreign customers based in Vietnam). Vietnam's obligations under the World Trade Organization's General Agreement on Trade in Services (GATS) include providing trade partners with non-discriminatory treatment (national treatment) for services in 39 different sectors or subsectors. These services suppliers include a broad sweep of participants, including tax preparation, data processing, insurance, and more. Each of these sectors could very likely require sending what Vietnam defines as "important information" abroad to function and to complete service transactions. Transactions that are entirely domestic would not be subject to the draft law's impact assessment and approval requirements, meaning domestic suppliers would receive preferential treatment. The law also has the potential to strongly discourage Vietnam-based companies from contracting with cross-border suppliers. Accordingly, this discriminatory treatment of cross-border suppliers is likely inconsistent with Vietnam's trade obligations.

Further, under the CPTPP, Vietnam has made commitments to not prohibit or restrict cross border data flows (Article 14.11). Even when there are legitimate public policy objectives, restrictions should not be greater than required to achieve these objectives. The Data Law, as drafted, exceeds this threshold.

Requiring data subject consent for combining, adjusting or updating data (Article 14.2): The requirement that all private organizations that are data owners must seek data subject consent in order to combine, adjust or update data is unnecessarily onerous and will impede the progress of cutting-edge digital applications, such as the Internet-of-Things technologies and AI. There are many circumstances in which data subject consent is not practicable or not desirable. For example if an organization is collecting sensor data in a public area, where the data subject is not identifiable or contactable (as contact information was not collected at the point at which the IoT data was obtained), it would not be possible for the organization to subsequently obtain consent from the data subject if they wanted to combine or update the data. We therefore recommend

that the clause be amended to, "Data owners other than those specified in Clause 1 of this Article have the right to combine, adjust and update data, and should obtain the consent of data subjects, where appropriate or practicable."

Disproportionate obligations imposed on data intermediary service providers and data managers (Articles 3.4, 50.4): Businesses that connect Vietnamese companies to third party providers of large datasets or training models will be considered "data intermediary service providers" by virtue of Article 3 paragraph 4. This classification is misguided as such service providers may not themselves have any control over the content in the datasets or models. Accordingly, the obligation to label such content and to 'notify data owners about unauthorized access may not be possible for all service providers that fall into this broad definition. Similarly, "data managers" is so broadly defined that it could include service providers that offer database services but who do not get visibility or control over the content of users of the database service. It is therefore not possible for such service providers to distinguish between datasets uploaded by different users and the data in real-time as it is not the source of the information nor is it possible for service providers to apply for real-time approval before the transmission of data across borders. Rather, the obligations relating to the subject matter of any content should be imposed on the source of the content rather than the host of any information or an intermediary.

Broad Powers of data expropriation right by the Party, State Agencies, and socio-political organizations, from private sector without clear due processes (Articles 18 and 34.4*):* We are extremely concerned that Article 18 provides broad powers for the government to request that the private sector provide specified data for "special cases" including for "national interest" and "public interest" which are broadly defined categories. Article 34, paragraph 4 likewise allows the Prime Minister to request "private use data" for a broad range of scenarios. Such requirements, without sufficient due process, safeguards for situations in which private organizations can dispute such a request, or assurances that data provided will be kept confidential, will have a chilling effect on investments into Vietnam. Any requests by the government to organizations to provide data should require a court order, include the opportunity for organizations to dispute the request (e.g. if data is proprietary or a trade secret; provision of the data will result in a conflict of law internationally or will result in a breach of international commitments; or providing the data will be extremely costly), and be directed to the party producing the data rather than service providers that do not control the data.

Further, Vietnam has an obligation to protect investments against expropriation, both direct and indirect, under the CPTPP (Article 9.8). Overly broad data expropriation rights by the State, without sufficient due process or guarantees on protection of IP and/or proprietary data, could constitute a direct or indirect expropriation as it interferes with the intangible property rights/interest (i.e. data/IP) of a foreign investor.

Unduly prescriptive obligations for data intermediary service providers (Articles 49, 50 and 51): There are several provisions across Chapter V that are unnecessarily prescriptive and dictate how data intermediary service providers should conduct their operations in Vietnam. Some examples include: (1) Article 49(2)(a), which requires "the legal representation of the enterprise " to be a "Vietnamese citizen or permanently residing in Vietnam"; and (2) Article 49(2)(b) which requires organizations to employ people with university degrees to be responsible for the provision of services, administering the system *etc*. These requirements are overly prescriptive and may impede the ability of providers to employ the most qualified individuals for these roles.

Such requirements will stifle digital innovation hamper the accessibility of services in Vietnam. Alternatively, the Government's objectives could be met by principles-based guidelines that are

outcome-focused and align with international norms, for how data intermediary service providers should operate with necessary guardrails without unduly restricting innovation and business models.

Data subject rights must consider technical feasibility, authenticity and reasonableness, and trade secrets (Article 26): The data subject rights granted in Article 26 apply to all data (not just personal data), and do not empower organizations to discern whether a request is genuine, reasonable, or even technically feasible. It is not clear how organizations can be expected to provide data subject rights to data that cannot be identified. Without reasonable exceptions, these rights could leave organizations vulnerable to vexatious or inauthentic/invalid requests that they would be constrained to oblige. Further, the right to data recovery is infeasible and broad, and could prohibit certain types of processing that are essential to providing services. This right should be removed as it would impede the processing required for data-reliant companies to provide services in Vietnam.

Exempt open source AI or utilize existing international standards to ensure consistency (Article 27): The scope of Article 27 is broad and empowers the government to impose prescriptive regulations governing Generative AI services. Open source should be exempted from this provision. Open source drives innovation, and creates better, safer, products that everyone can benefit from. It also requires a more flexible, responsive, and adaptive regulatory environment to reach its potential. Alternatively, the regulations should, at minimum, harmonize with existing international baselines to ensure consistent standards around the world and avoid internet fragmentation.

While this is a non-exhaustive list of concerns with the draft law, we hope this list highlights the need for further consultation and review before the law is promulgated. We look forward to further discussion as the Draft Data Law and others with similar remits are considered.

Sincerely,

ACT | The App Association
American Council of Life Insurers
American Property Casualty Insurance Association
Asia Internet Coalition
Coalition to Reduce Cyber Risk (CR2)
Coalition of Services Industries
Computer & Communications Industry Association
Consumer Technology Association (CTA)
Information Technology Industry Council
National Foreign Trade Council
Semiconductor Industry Association
U.S. Chamber of Commerce
United States Council for International Business
World Innovation, Technology and Services Alliance (WITSA)

cc: H.E. Luong Tam Quang, Minister of Public Security
H.E. Nguyen Hong Dien, Minister of Industry and Trade
H.E. Nguyen Quoc Dzung, Ambassador of Vietnam to the U.S.