

Asia Internet Coalition (AIC) Industry Letter on the Draft Data Law, Vietnam

7 November 2024

To
Senior Lieutenant General Luong Tam Quang,
Minister of Public Security (MPS)
Socialist Republic of Vietnam

The [Asia Internet Coalition](#) (AIC) writes to express our concerns with Vietnam's draft Data Law. AIC is an association of leading Internet and technology companies that promotes the understanding and resolution of Internet policy issues in the Asia Pacific region. Our mission is to represent the Internet industry and participate in and promote stakeholder dialogue between the public and private sectors, sharing best practices and ideas on Internet technology and the digital economy. 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. Firstly, we would like to convey two primary recommendations through this submission:

1. **Delay the passage of the Data Law:** Our primary and immediate concern and recommendation is for Vietnamese policymakers to conduct further consultations on the Data Law. Given the significant concerns in the draft Data Law which we've outlined below, we urge Vietnamese policymakers to conduct further consultations on the draft Data Law before it is enacted. Within a matter of weeks, multiple versions of the draft Data Law have been released, providing extremely limited time for careful evaluation and meaningful, genuine consultation. Considering the broad, significant impact of the Data Law on multiple industries, more thought needs to be put into carefully drafting the Law, to ensure it achieves its goals of (among other things) protecting data and providing for rights and obligations related to data activities, without imposing undue burdens on organizations and individuals and hindering Vietnam's digital economic growth.
2. **Scope the Data Law so that it does 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):** Having multiple laws and regulations on the same subject matter, such as personal data protection, with conflicting, inconsistent, and duplicative requirements lead to significant uncertainty and tremendous operational burden on the part of industry, in terms of compliance. 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.

We urge the Ministry to carefully consider the proposed changes detailed in the **Annex of this submission**. A balanced approach that supports economic growth, encourages foreign investment, and maintains a competitive business environment is essential for Vietnam's continued success. Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your attention on this matter and we look forward to further discussion with the Government on this important policy.

Sincerely,
Secretariat
Asia Internet Coalition (AIC)

Annex: Detailed Comments and Recommendations

A. Summary of Comments and Recommendations

1. Data definitions, classification, and management

The law introduces broad terms like "core" and "critical" data, which could lead to significant ambiguity in interpretation. These categories include data that impacts national security, public health, or the economy—areas that organizations, without access to government insight, may struggle to accurately assess. This lack of clarity could increase the risk of misclassification, leading to either over-compliance, which drives up costs, or under-compliance, which could leave critical data inadequately protected. With severe penalties for non-compliance, organizations may become overly cautious, limiting innovation and data use. This uncertainty could undermine Vietnam's ambition to become a regional data hub. To address these issues, the MPS should reconsider the long list of data terms in the draft law and provide clearer definitions so organizations can better understand which data is in scope and how to comply with the proposed laws. Issuing guidance with concrete examples of the types of data that fall under each definition could further help businesses navigate the complexities of compliance. Clearer and more specific definitions will enable organizations to strike the right balance, ensuring that data is properly protected without imposing unnecessary burdens.

2. Amend the mandatory data sharing provisions to protect commercially sensitive information, avoid creating international conflicts of law, and consider technical feasibility

- a. The provisions for mandatory data sharing (for personal and non-personal data) in certain situations, such as public emergencies or specific tasks to fulfill the public interest are extremely problematic. The requirements would create conflicts of law with foreign governments, may force companies to reveal trade secrets or other commercially sensitive information, and will lead to reduced foreign investment as companies may favor markets with less burdensome costs of entry. In addition, the requirement should clarify the conditions for public sector bodies to access data in instances where there is a clear and meaningful public interest.
- b. **Concerns regarding IP rights and proprietary data:** The requirement to provide data to government agencies raises considerable IP, confidentiality, and possibly also privacy issues for organizations with proprietary data and personal data. Sensitive business information, trade secrets, and other proprietary and personal data could be subject to government oversight under the draft law. See Article 5(7), which expressly states that data subject to IP rights must comply with this draft law.

3. Rather than focusing only on consent requirements for specified data processing activities, include a range of legal bases for processing data
 - a. Several articles of the bill (Art. 14, 21, 22) impose requirements to obtain data subject consent when performing specified data processing activities. This is onerous and will significantly impede the processing required for data-reliant companies to provide their services. (i) First, this requirement is not technically feasible insofar as it pertains to non-personal data. How can an organization obtain data subject consent if the data does not relate to an identified individual? (ii) Second, it is not always practical nor desirable to obtain data subject consent for certain data processing activities. For example, in cases of fraud prevention and detecting illegal behavior - it is not practical to expect the bad actors to consent to the processing of their data, so that their illegal activities can be thwarted. Instead, the bill must include a range of legal bases for data processing activities such as legitimate interest; contractual necessity; vital interest; legal obligation; and public interest.
4. Ease the restrictions on cross-border data transfers
 - a. Cross-border data transfers are the lifeblood of the digital economy and will ensure Vietnamese businesses' competitiveness in the global economy. As drafted, the restrictions on cross-border data transfers deviate from international norms and may lead to data localization, which would undermine best practices for data security and privacy and harm local businesses. (i) First, the bill should clarify that "core data" and "important data" are only limited to data collected by or at the direction of the Government. If the intent is to protect state and national security secrets, we recommend limiting the definitions to data collected by or at the direction of the Government. (ii) Second, we strongly recommend that the bill limit the definition of "*Transferring data abroad to foreign organizations and individuals*" to "*the transfer of personal data between two legal entities, in which one is located in a jurisdiction outside of Vietnam*". The current definition regulates any physical movement of data around the world. Due to the nature of the global internet in which physical international transfers routinely occur in every online interaction, this is not technically feasible to accomplish. Our recommended definition that regulates transfers between legal entities (such as data controller or data processors) aligns with internationally recognized frameworks (EU's GDPR, see [Guidelines 05/2021](#); Singapore's PDPA; and ASEAN's Model Contractual Clauses for Cross Border Data Transfers), and takes technical feasibility into account. (iii) Lastly, if the above two recommendations are not accepted, the Law must include multiple cross-border data transfer mechanisms, including contractual necessity; legitimate interest; public interest; contractual clauses (such as Standard Contractual Clauses and ASEAN Model Contractual Clauses for Cross Border Data Transfers); adequacy; Global CBPRs, and when necessary for the establishment, exercise, or defense of legal claims relating to the data subject. Furthermore, the mandatory impact assessment and approval requirement, combined with the vague and broad data definitions, implies international data transfers will be risky and cumbersome.
 - b. The draft data law requires "*critical*" and "*core data*" to be stored centrally in the National Data Centre (NDC), or on infrastructure approved by the government for data security and long-term retention, upon written request - Article 10(4) and 33(2). Once data is in the NDC, organizations lose some direct control over the data. We may want to clarify whether data localization in the draft data law applies to commercial businesses. If it does, there are concerns regarding unauthorized access, potential misuse, or even just inadequate protection of any data stored at the NDC.

5. Data subject rights must consider technical feasibility, authenticity and reasonableness, and trade secrets
 - a. The data subject rights granted in Art. 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 to honor it. (i) First, it is not clear how organizations can be expected to provide data subject rights to data that cannot be identified. (ii) Second, without reasonable exceptions, these rights could potentially leave organizations vulnerable to vexatious or inauthentic / invalid requests that it 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.
6. Exempt open-source AI or rewrite Art. 27 to align governing principles with existing international standards to ensure consistency
 - a. The scope of Art. 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, but it 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.
7. Remove the registration requirements to appoint a local representative within Vietnam or limit them to local organizations that operate from entities incorporated in Vietnam
 - a. Requirements for all foreign providers to appoint a local representative are onerous and ignore the realities of the ways in which global platforms operate. This obligation would hinder Vietnam's attractiveness as a digital hub to foreign providers, discourage foreign providers from doing business in Vietnam, and create unnecessary barriers to cross-border services on trade.
8. Alignment of Data security and protection measures with international standards

We Urge the MPS to align its regulatory framework with international standards to ensure greater interoperability and harmonization. Alignment with international standards is also necessary as Article 22(6) only permits cross-border data transfers to offshore data recipients that meet the data protection standards prescribed in the draft law.

B. Details on the key issues with the draft law are set out in the table below

Topic	Description	Initial impact assessment / Comments	Recommendations
Article 4 Application of the Data Law	Where future laws that regulate similar data issues differ from this law, the provisions of this law will apply unless specified in the future law.	Article 4 seems to make other future laws/regulations that govern data – such as the future Personal Data Protection (PDP) Law, CASD, Digital Technology Industry (DTI) Law – inferior to the Data Law, unless specified. It is also unclear how Clause 2 in Option 1 & 2 will be applied in practice. It is unusual and a potentially significant overreach for legislation to state that it will prevail over all future regulations governing data. As a matter of statutory interpretation in Vietnam, the more recent law will typically prevail over older ones in case of conflict. The non-obstante provision in Article 4 represents a steep digression from established legislative practice to prevail in posterity over any future data laws, particularly given the broad scope of this bill which governs all <i>data</i>. It will likely pose substantial concerns for organizations if this law were to prevail over other specific decrees that they are already aiming to comply with (e.g., the PDPD, the CASD, etc.). Introducing new, similar regulations will undermine the compliance work that organizations have already undergone and, if passed as is, will present unnecessary burdens. This design of the Draft Law, therefore, presents significant uncertainties and concerns for organizations' ability to offer services in Vietnam.	Recommendation: Option 1: - The bill should operate without prejudice to the existing, draft, or future Vietnamese laws/regulations that govern data, or at the very least, personal data. - The bill should mirror or cut any provisions that overlap or are redundant with other laws that regulate data.
Article 6 Prohibited acts		Article 6 contains a list of broad prohibitions.	Recommendation:

Topic	Description	Initial impact assessment / Comments	Recommendations
			The objective of this provision is unclear as the prohibitions in it are generally prescribed by (other) laws (see Article 6(9)). We urge the MPS to delete this provision.
Article 49 Conditions for provision of data analysis and synthesis Article 52 Responsibilities of organizations providing products and services of data analysis and synthesis	Data analysis and synthesis is the process of applying tools, technologies, and processes to convert available data into actionable insights, to find trends, and to support data-driven decision-making. Based on the above definition, this concept will likely cover various forms of artificial intelligence (AI) and algorithmic content recommendation systems since such systems collect, synthesize, and analyze input data to generate outputs such as predictions, content, recommendations, or decisions. Article 19 of the Draft Law states that if the data analysis and synthesis are related to activities as prescribed under Article 27.5 of the Draft Law (including (i) manipulating the cognitive behavior of people or vulnerable groups; (ii) classifying people based on behavior, socioeconomic status, personal characteristics; (iii) Identifying biometrics; (iv) Being used in products that affect peoples' safety; (v) Being used in fields that affect basic human rights), the person who conduct the data analysis and synthesis will be subject to	The draft law imposes a requirement for certain organizations to i) be public non-business units or enterprises established or registered to operate in Vietnam, ii) be licensed to provide services, and iii) appoint a Vietnamese citizen or someone that permanently resides in Vietnam as the head of the organization or legal representative. It is not clear how this provision is intended to apply to foreign companies and it may ignore the realities of the way in which global platforms are operated. This obligation should be reconsidered to ensure that the law is workable for foreign providers that want to offer services in Vietnam, does not hinder Vietnam's attractiveness as a digital hub to foreign providers, does not discourage foreign providers from doing business in Vietnam, and does not create a restriction on free trade.	Recommendation: • Option 1: Remove the requirements. • Option 2: The requirements should be limited to local data controllers that operate platforms from entities incorporated in Vietnam, with a clear exemption for open source AI.

Topic	Description	Initial impact assessment / Comments	Recommendations
	requirements under Article 52 of the Draft Law (eg being a public non-business unit or an enterprise established or registered to operate in Vietnam; obtaining a license/registration under the Draft Law). Article 52.2 reconfirms that the provider of the data analysis products/services falling within Article 27.5 will be subject to licensing/registration under the Draft Law.		
Article 18 Providing data to Party agencies, the State, socio-political organizations Article 37 Responsibilities for providing data of Party agencies, State agencies, socio-political organizations, individuals and other organizations	An organization (processing or handling data) must declare or provide data to party, state agencies, or socio-political organizations: 1. When requested data is necessary to respond to a public emergency, serving national defense and security, and ensuring national interests; and 2. When the lack of available data prevents the Party, State agencies or socio-political organizations from fulfilling a specific task in the public interest prescribed by law and the Party, State agencies or socio-political organizations cannot obtain such data by other alternative measures.	This appears to be a mandatory obligation to share data (personal and non-personal) with public bodies and socio-political organizations. The Draft Law prescribes certain specific scenarios in which it may be invoked; however, the Article applies to all types of data – personal, non-personal as well as original data. Although such data sharing can be useful for dedicated purposes, it is essential that any such measures to promote it are carefully constructed and take into account the rights, obligations and interests of all parties involved, including individual data protection rights, the right to privacy and business secrets. The draft Data Law as currently drafted will place foreign companies in an impossible position of being caught between conflicting global laws. For instance, US communications providers are subject to US law, which places strict limits on their ability to disclose contents and most metadata. As a result, US-based organizations looking to invest may forgo markets with mandatory	Recommendation: • Clarify conditions for public sector bodies to access data in instances where a clear and meaningful public interest is established. • Add a provision to Article 18(4), which states that requests for data supply must ensure the request: ○ is technically feasible for the data manager or data owner to access or share; ○ does not reveal trade secrets, proprietary information, and/or commercially sensitive information; and ○ does not create international conflicts of law. • For Article 37(2)(a), limit it to the provision of information about the individual, organization or enterprise to whom the request is addressed, as opposed to their customers or users.

Topic	Description	Initial impact assessment / Comments	Recommendations
	The state agency requesting data is required to clearly state what data is sought, the purpose of the request, the legal bases for the data request, the duration of expected use, etc. In addition to the above mandatory data sharing obligation, organizations may also voluntarily share data under their ownership with state agencies for public purposes, research, etc. Article 37 requires foreign individuals and enterprises operating in Vietnam to provide, share, synchronize and update data for the National General Database as prescribed in Article 18 of this Law upon written request of the National Data Center.	government data sharing regimes in favor of markets with less burdensome costs of entry. This requirement would also be in tension with other global data governance laws, such as the GDPR. The overbroad framing of Article 18 could lead to situations where broad categories of personal data (such as EU user data) could become incidentally subject to or collateral in this mandatory data sharing provision, potentially conflicting with existing mechanisms of cross-border data transfers or cross-border data sharing channels. We recommend that Vietnam utilize existing legal channels, such as signing an MLAT (US Mutual Legal Assistance Treaty) with the US, and acceding to the Budapest Convention in order to better facilitate law enforcement requests for data from foreign-based providers. Finally, Vietnam should establish a single point of contact for government-to-government requests. This would ensure that requesting agencies are familiar with US legal and constitutional requirements, and have reviewed requests to ensure they meet US standards. It is unclear whether organizations will have any grounds to challenge or seek amendment to data sharing requests, such as in instances where the request would require the production of data that are technically infeasible to access or share, where doing so could create an international conflict of law, or if sharing such data would reveal trade secrets, proprietary information, and/or commercially sensitive information.	

Topic	Description	Initial impact assessment / Comments	Recommendations
		Moreover, the purpose and public interest should be clearly defined and proportionality and accountability should be ensured in order to prevent misuse. The Draft Law should clarify conditions for public sector bodies and socio-political organizations to access data in instances where a clear and meaningful public interest is established. Indiscriminate data sharing requirements would be inefficient and could put people’s privacy at risk without clear benefits. Access to data for public purposes should not be indiscriminate and should be subject to a predictable process as well as appropriate privacy, integrity, security protections. The government should also consider protections to help preserve intellectual property rights and trade secrets when crafting data sharing requirements. These interests often conflict with data sharing requests. Private entities should not be required to share data where insights are developed by combining different data points typically involving trade secrets, algorithms, computational techniques, advanced analytics, etc. More generally, any data sharing exercise should not harm the data collector and the data source.	
Article 3 Interpretation of terms	Key definitions in the Draft Law are as below: 1. <i>Data</i> means a digital representation of a thing or event, including audio, image, numerals,	In general, the definitions appear to be overly vague and broad. As this could lend itself to inconsistent or uncertainty in interpretation, it poses a concern for organizations.	Recommendation: • Clarify which provisions of the bill apply to the different types of data. • <i>Transferring data abroad to foreign organizations and individuals</i> should be defined as <i>the transfer of personal data between two legal entities, in which one is</i>

Topic	Description	Initial impact assessment / Comments	Recommendations
	writing, symbols or other similar forms. 2. <i>Transferring data abroad to foreign organizations and individuals</i> is the use of cyberspace, equipment, electronic means or other forms of data transfer to a location outside the territory of the Socialist Republic of Vietnam or using a location outside the territory of the Socialist Republic of Vietnam to processing data or transferring data to foreign organizations and individuals. 3. <i>Non-personal data</i> means data that is not personal data in accordance with the law on personal data protection. 4. <i>Core data</i> means important data affecting many other fields, groups and regions, including data related to national defense, security of foreign affairs activities, the national economy, important livelihoods of people, major public interests and other data as decided by the Prime Minister. 5. <i>Important data</i> means data in fields, groups or areas that directly pose a direct danger to	For example, the scope of the bill extends beyond “personal data” (not defined in the bill), and regulates the term “data” (broadly defined and open-ended), which includes the digital representation of things, events, images, numbers, sounds, and symbols. Such broad application and prescriptive requirements will have a chilling effect on the entire digital and data ecosystem. <i>Transferring data abroad to foreign organizations and individuals</i> is currently defined as any physical movement of data or data processing outside of the physical territory of Vietnam. For the purpose of the regulation at issue, we want to underline that overseas data transfers should be defined as <i>data that are transferred between separate legal entities, where at least one such entity is based in a different jurisdiction, and is therefore subject to different laws as a result of the transfer.</i> This definition aligns with globally recognized frameworks such as EU’s GDPR, Singapore’s PDPA, and ASEAN’s Model Contractual Clauses for Cross Border Data Transfers. Other types of cross-border data flows for routine transfers of data that are technically necessary for the internet to function and fall outside that narrow scope should not be covered. Because of how the global internet was built and has evolved, international physical data transfers occur as part of almost every online communication or activity (for example, using search engines, chatting with friends, doing online banking, or making purchases), often	<i>located in a jurisdiction outside of Vietnam.</i> This is seen in EU’s GDPR (see Guidelines 05/2021), Singapore’s PDPA, and ASEAN’s Model Contractual Clauses for Cross Border Data Transfers. • Limit the scope of <i>important data</i> and <i>core data</i> to <i>data that is collected by or at the direction of the Government.</i> • Limit the definition of <i>data subject</i> as <i>relating to individuals reflected by personal data only.</i> For example, in GDPR a <i>data subject</i> is an identified or identifiable natural person [whose personal data concerning him or her is processed].

Topic	Description	Initial impact assessment / Comments	Recommendations
	national defense, security, external relations, economic activities, social stability, public health and safety when leaked, forged or destroyed. Data owned by the data owner and only related to the data owner itself shall not be considered important data, except for the case where the competent authority decides as prescribed in Clause 2, Article 12 of this Law. 6. <i>Data subject</i> is an individual or organization reflected by data.	including those which are wholly domestic and there is no change in data administration. Indeed, cross-border data flows are technically necessary for the global internet to function. Regulations that attempt to regulate all physical movements of data online will weaken local and global economies, threaten data security, and lead to internet fragmentation. The term <i>core data</i> encompasses a wide range of data types, and is extremely broad. If <i>core data</i> is broadly defined as “<i>important data affecting many other fields, groups and regions including data related to national defense, security, foreign affairs activities, the national economy, important livelihoods of people, public interests and other data as decided by the Prime Minister.</i>” then all data could be considered to be <i>core data</i>, or later on decided to be <i>core data</i>. The terms used to define core data are wide and vague, and the category itself can be expanded by a decision by the Prime Minister. This provides little certainty to organizations that must comply with the law. The definition of <i>core data</i> should be limited to <i>data collected by or at the direction of the Vietnamese government.</i> As it currently is defined, <i>core data</i> could lead to data localization. While it is important for government entities to control their networks and data based on what’s best for them, to the extent that Vietnam is considering these goals, private sector entities that are not acting at the direction of the government should not fall into the scope of the data transfer restrictions in this regulation.	

Topic	Description	Initial impact assessment / Comments	Recommendations
		Restrictions on data transfers of private sector entities providing goods and services to individuals and other private sector entities will make data less safe while disadvantaging local businesses by restricting their ability to access international markets, and generally harming the Vietnamese economy. <i>Data subject</i> is not defined in relation to personal data, which appears unreasonably broad. It would be technically challenging to apply the concept of a data subject when implementing the law with respect to data that is not personal data.	
Article 24 & 25 Overseas Data Transfers	Article 24(1): The data owner shall have the right to decide on the reproduction, transmission or transfer of his/her data. Article 25: Any international data transfer must ensure the protection of rights and interests over personal data, national security and public interests. The cross-border transfer of core data and important data is subject to restrictions such as prior assessment and approval by a competent local authority. <u>Personal data shall comply with the provisions of the PDP Law, except in cases where personal data is core data or important data.</u>	The intent of Article 24(1) is ambiguous and seems to grant undefined rights to data owners to “decide” on the transfer of his/her data. The intent of this article is unclear and contradicts with the cross-border data transfer provisions that already exist in the PDP Decree, the draft PDP Law, and Article 25 of the draft Data Law. The term “important data” is broadly defined and – according to Article 12(2) – empowers the government with the authority to promulgate lists of what is considered important data. The provision remains vague with respect to whether any data generated by organizations’ AI systems or processed by them will be treated as core data. <i>Core data</i> is defined broadly, and it is unclear if any data that organizations collect or produce as part of its services will amount to core data. If yes, then this will impose additional onerous obligations on the transfer of core data outside Vietnam in	Recommendation: Option 1: - Clarify that “data owner” in this instance does not refer to a data subject. - For Article 25, the draft Law should provide multiple, but effective mechanisms for cross-border data transfers, which support accountability, national security, and digital economic growth. Some suggested mechanisms include: - Adequacy of the target country’s laws and enforcement mechanisms; - Pre-approved contractual clauses by the data regulator (Standard Contractual Clauses and ASEAN Model Contractual Clauses for Cross Border Data Transfers); - Approved binding corporate rules for data sharing by multinationals and their service providers across the world;

Topic	Description	Initial impact assessment / Comments	Recommendations
	The Ministry of National Defence assesses and approves the impact of the transfer of core and important data in the fields of military, national defense or cipher. The Ministry of Public Security will conduct an impact assessment and approve the transfer of important and core data other than in the fields of military, national defense or cipher. The cross-border transfer of core and important data abroad is subject to restrictions such as prior impact assessment and approval by a competent local authority, a contract with the transferee, and other conditions as prescribed by law. Data managers transferring core data and important data abroad to foreign organizations and individuals shall be responsible for conducting periodic impact assessments in the course of implementation in order to prevent risks, protect data, serve inspection activities, and supervision of competent agencies specified in Clause 3 of this Article.	addition to existing data transfer requirements under the PDP Decree. We urge the Government of Vietnam to commit to cross border data flows and provide clarity on the conditions for data transfers. As written, the stringent requirements for cross border data transfer in the Draft Law deviate from international norms and will lead to data localization. Data localization is an extraordinary provision that creates burdensome data storage costs, is impractical, discourages investment in Vietnam, undermines best practices for data security and privacy, and can lead to economic consequences that will harm local businesses that heavily rely on global internet platforms to export their products and services around the world. It presents a barrier to international trade, reduces foreign direct investment in Vietnam, and restricts the availability of services to local customers as multinational companies may look to alternative markets that have lower costs of entry. Localization obligations would further make it difficult for growing businesses in Vietnam to compete in global markets as it will result in an immediate increase in the cost of doing business because it would no longer be possible to store their data in the most affordable and business-efficient manner and location. Cross border data flows will benefit Vietnam’s economy and ensure Vietnamese businesses’ competitiveness in the global economy, by 1) promoting innovation, productivity, and efficacy; 2) lowering costs for businesses and consumers; 3) lowering international trade and investment barriers; 4) increasing access to global	4. Certification mechanisms approved by authorized regulator; and 5. Code of Conduct produced by industry and regulators. - We further recommend introducing exceptions in line with international benchmarks such as Article 49 of the GDPR to accommodate situations where, for example, the transfer is necessary for: - the performance of a contract between the data subject and the controller; - the establishment, exercise or defense of legal claims relating to the data subject; - the purposes of the legitimate interests pursued by the organization or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data; or - important reasons of public interest. - We also recommend incorporating an additional legal basis / data transfer mechanism of ‘necessity for the provision of services’ to enable routine transfers that are fundamental for business services and operations. - Lastly, in line with international best practices, we would also recommend allowing cross-border transfer of personal data based on recognized certifications, such as the Global CBPR certification. Option 2:

Topic	Description	Initial impact assessment / Comments	Recommendations
		products and services; and 5) ensuring businesses in Vietnam can service consumers both at home and abroad. We recognize that governments may have reasonable grounds for protecting data of particularly sensitive nature, such as data used for national security purposes. If the intent is to protect state and national security secrets rather than impact all private services that operate in Vietnam, we recommend limiting the definitions of <i>core data</i> and <i>important data</i> to data collected by or at the direction of the Government.	• Cut Article 24(1) • Limit the definitions of <i>core data</i> and <i>important data</i> to data collected by or at the direction of the Government.
Article 26 Retrieval, deletion, destruction of data	The right to recover, delete, or destroy data is provided to all individual data subjects under the Draft Law. These rights extend beyond personal data and to all forms of data that has been shared with organizations. Data recovery is defined as “the activity of data owners and data managers to revoke the right to use data that has been provided or shared with agencies, organizations and individuals, or publicized on the mass media.” The right of data destruction refers to “destroying data from the storage structure [and/or] environment and ensuring the elimination of its resilience by means of physical overwriting or destruction.”	The provision presents risks for organizations as it creates a mandatory, disproportionate, and onerous obligation to honor all requests for recovery, deletion, and destruction of data. This provision appears excessive as it extends these data rights to individuals over not just personal data but other data types as well. It also does not empower organizations to discern whether a request is genuine, reasonable, or even technically feasible to honor it. It could potentially leave organizations vulnerable to vexatious or inauthentic / invalid withdrawal or destruction requests that it would be constrained to oblige. Furthermore, data recovery is defined as “the activity of data owners and data managers to revoke the right to use data that has been provided or shared with agencies, organizations and individuals, or publicized on the mass media.” This right is infeasible and broad (particularly as it relates to data that cannot be tied to an individual), and	Recommendation: Option 1: • Cut the right to data recovery. • Limit data subject rights to personal data as defined by the PDP Decree. • The rights provided in Article 23 should be subject to the following limitations, i.e. where complying with the request to exercise rights would: ○ disclose trade secrets or proprietary information; ○ be infeasible on technical grounds or require disproportionate effort; ○ interfere with law enforcement, judicial proceedings, and/or investigations; ○ undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts; ○ violate laws or the rights of other persons; ○ involve non-human understandable data; ○ compromise the controller’s efforts to implement

Topic	Description	Initial impact assessment / Comments	Recommendations
	The Article does not carve out reasonable restrictions to the exercise of these rights. Data managers are required to establish policies and procedures for data recovery, deletion or destruction at the request of data subjects.	could prohibit certain types of processing that are essential to providing services. This will significantly impede the processing required for data-reliant companies to provide services in Vietnam. Multinationals looking to invest may forgo markets with data localization requirements in favor of markets with less burdensome costs of entry. This would restrict the ability of local businesses to access and benefit from state-of-the-art tools, resources, and economies of scale that multinational companies offer.	- security and integrity systems; - require access to data that cannot be made human readable; - require re-identifying or otherwise linking data that is not considered personal data; - infringe upon a data controller’s ability to process data to perform a contract to which the data controller is a party or to provide a service requested by the data subject; - infringe upon a data controller’s ability to process data to store personal data for disaster recovery or legal and compliance purposes; - facilitate manifestly unfounded, substantially similar, repetitive and/or vexatious requests. Option 2: - Cut the right to data recovery. - Limit data subject rights to personal data as defined by the PDP Decree. - Align data subject rights and exceptions to the GDPR.
Article 27 Application of science and technology in data processing, management, administration, use and exploitation	This Article states that: - The use of science and technology in data processing, management, administration, use, and exploitation will be prioritized to protect national security, public interests, and citizens' rights. <u>Principles for developing and applying technology in data processing include not producing prohibited content, preventing</u>	The scope of this Article is overly broad and appears to empower the government to frame isolated, potentially prescriptive regulations for 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, but it requires a more flexible, responsive and adaptive regulatory environment in order to reach its potential. Creating a structure for potentially prescriptive regulations is	Recommendation: - Exempt open source AI from Article 27. Alternatively: Rewrite Article 27 to align with existing international baselines to ensure consistent standards around the world. - Rewrite Article 27(3) to discuss the misuse of technology, obligations and liability related to it, outside of its development and application.

Topic	Description	Initial impact assessment / Comments	Recommendations
	<u>discrimination, respecting intellectual property rights, and respecting others' rights and interests.</u> 3. The Government will prescribe regulations for technological development and application in <u>data processing for specific applications, such as manipulating cognitive behavior, classifying people based on behavior or personal characteristics, identifying biometrics, and affecting fundamental human rights.</u> 4. Regulations for technological development and application in data processing will include requirements before launching new products or services, assessment of product security and ethics, requirements for daily operation, training data and labeling, censoring input and output data, labeling general contents, protecting users' rights, periodically assessing algorithms, managing data safety, and handling false information and complaints.	antithetical to this, beyond being technically infeasible for some technologies, including open source AI. Regulations on data processing development and application for private companies should be built through stakeholder input, also taking into account technical feasibility and other established international standards for such regulations Alternatively, government regulations should, at a minimum, be harmonized with existing international baselines. Globally-harmonized frameworks are necessary to ensure consistent standards around the world. Further, Article 27(3) describes a set of unreasonable expectations of providers or developers of technologies, both from a technical and legal perspective. The building of technology itself should not be limited or prohibited simply because of the potential for its misuse. In fact, in some cases, like artificial intelligence, it is impossible for a company to, during development, prevent its AI model from being used to discriminate or infringe on any of the enumerated principles. Article 27(3) should be rewritten to discuss the misuse of technology, obligations and liability related to it, outside of its development and application.	

Topic	Description	Initial impact assessment / Comments	Recommendations
Article 14 Combining, adjusting, updating data	Data owners (other than Party agencies, the State, the Vietnam Fatherland Front, and socio-political organizations) must obtain consent from data subjects to combine, adjust and update data.	The requirement for all data owners (other than Party agencies, the State and socio-political organizations) to obtain consent from data subjects to combine, adjust, and update data is onerous and will significantly impede the processing required for data-reliant companies to provide their services. Indeed, it is not always practical or feasible to obtain consent, particularly where the data cannot be linked to an individual.	Recommendation: ● Option 1: 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. ● Option 2: Provide a range of legal bases for combining, adjusting, and updating data including legitimate interest; contractual necessity; vital interest; legal obligation; and public interest.
Article 15 Data sharing obligations	Non-exhaustive list of special cases when data sharing is obligatory:	The draft law requires organizations to provide data to government agencies upon request in “ <i>special cases</i> ” - Article 15.	Recommendation: We suggest the following amendment: “ <i>Special cases as prescribed in Clause 1 of this Article include refer to: ...</i> ”
Article 21 Data disclosure	“Data disclosure” is broadly defined as: a) Posting information; b) Posting on data portals, web portals, websites and mass media; and c) Other forms as prescribed by law. Prohibits data disclosure in following conditions: 1. Personal data without data subject consent 2. The data is a state secret; data affecting national defense and security; 3. The data, if made public, will harm the Party, State, national interests and external relations; social ethics and community health;	This article is unclear in its intent, and sets vague and/or infeasible restrictions on data disclosure. For example, it is not clear what “posting information” means in Article 21(1). This could cover a wide range of activities that are not in fact harmful. Furthermore, Article 21(1)(c) allows the government to prescribe other forms of data disclosure in the future. Any change in the categories of data disclosure would require a widespread reconsideration which would lead to uncertainty for businesses, significant compliance costs, an increased cost of doing business, and ultimately lower market competitiveness. The list should be exhaustive and closed. Concerning item (3)(a) under the list of data prohibited from publication (personal data without the consent of the data subject) and (4)(a) (data related to trade secrets with	Recommendation: ● Option 1: ○ Delete Article 21. ● Option 2: ○ Clearly define terms for data prohibited from disclosure or data subject to conditional disclosure. ” We recommend limiting “secrets” to those that are collected by or at the direction of the Vietnamese government. ○ Data disclosure that deals with personal data should be regulated in the PDP Law rather than the Data Law. ○ Provide additional legal bases for data disclosure including legitimate interest; contractual necessity; vital interest; legal obligation; and public interest.

Topic	Description	Initial impact assessment / Comments	Recommendations
	endangering the life, health, legitimate rights and interests of organizations and individuals. Data subject to conditional disclosure includes: 1. Data related to trade secrets shall be disclosed in case the owner of such trade secret agrees in accordance with law; 2. Data related to private life secrets and personal secrets shall be disclosed in case of consent from such persons; data related to family secrets shall be made public in case of consent of family members; 3. In the course of performing his/her functions, tasks and powers, the heads of the Party, State agencies and socio-political organizations shall decide on the provision of data related to business secrets, private life, personal secrets and family secrets in case of public interest, the health of the community in accordance with relevant laws without the consent specified at Points a and b of this Clause; 4. Heads of Party, State agencies and socio-political organizations	data owner consent) - it refers to consent as the only basis for data disclosure. It is not always practical or feasible to obtain consent, particularly where the data cannot be linked to an individual. Relying on consent as the only legal bases for data disclosure is onerous and will restrict many activities required for data-reliant companies to provide their services. Concerning Article 21(2) & (3), terms such as “will cause harm to the interests of the Party, the State,” “social ethics and community health,” “legitimate rights and interests,” “state secrets,” “data that affects national defense and/or security,” and “social ethics,” are broad and undefined. Furthermore under Article 21(4), the terms “private life secrets,” “trade secrets,” “personal secrets,” and “family secrets” are vague and will confuse private organizations seeking to comply. Such requirements are technically infeasible to accomplish because it is not possible for organizations to know what data are considered “secrets” for private individuals.	

Topic	Description	Initial impact assessment / Comments	Recommendations
	shall decide on the provision of information on internal meetings of Party agencies, State agencies and socio-political organizations; documents drafted by the Party, State agencies and socio-political organizations for internal affairs.		
Article 17 Connect, share, and coordinate data	Data sharing means the provision of data by data subjects, data owners, and data managers to data users for the purpose of common or separate use of such data, based on voluntary agreements or as prescribed by law, directly or through an intermediary. Government agencies and socio-political organizations shall be responsible for sharing and coordinating data and ensuring conditions for data sharing for organizations and individuals permitted to exploit data.	This article seems to empower the government and socio-political organizations to coordinate data sharing which enable organizations and individuals to exploit and use such data (personal and non-personal) and make it available for third parties. Similar to Article 18, this Article should be carefully constructed and take into account the rights, obligations and interests of all parties involved, including individual data protection rights, the right to privacy and business secrets.	Recommendation: • The bill should clarify that data sharing should be exempted if it: ○ would reveal trade secrets, proprietary information, and/or commercially sensitive information; ○ is technically infeasible for the data manager or data owner to access or share; or ○ violates the data protection rights of others.
Article 9 Prohibited acts	The Draft Law prohibits the following activities: 1. Taking advantage of data processing and data management to infringe upon national interests, ethnic minorities, security, national defense, social order and safety, public interests, legitimate	The over broad phrasing of this provision is concerning. First, it applies to all data (personal, non-personal, or original), making the provision's scope onerous and vague. It is also unclear how narrowly or rigorously the provisions of this law will be implemented. It is important for the government to clarify and very narrowly define the provision.	Recommendation: • Option 1: ○ Cut Article 9. • Option 2: ○ Clarify which provisions of Article 6 apply to the different types of data. ○ Provide clear definitions for what constitutes prohibited activities.

Topic	Description	Initial impact assessment / Comments	Recommendations
	rights and interests of agencies, organizations and individuals. 2. Illegally obstructing or preventing the process of data processing or data management or committing other acts aimed at sabotaging information systems in service of data processing. 3. Illegally collecting, providing, using, accessing, disclosing data, displaying, disseminating or sharing. 4. Falsifying, falsifying, losing, damaging or deleting, destroying, copying, illegally sharing or illegally moving part or all of the data. 5. Illegally appropriating or using data. 6. Deliberately providing false data or failing to provide data as prescribed by law. 7. Illegally trading, trading and exchanging data, products and services on data. 8. Developing, trading and circulating data products and services that infringe upon security, national defense and		

Topic	Description	Initial impact assessment / Comments	Recommendations
	privacy of individuals, contrary to Vietnamese customs and customs. 9. Arbitrarily using data copying tools and software without the permission of the data owner; accessing or deliberately accessing or attacking the database without the right or permission of the data controller. 10. Other prohibited acts as prescribed by law.		
Article 16 Data administration and management	Article 16 1. Data owners and data managers must organize and formulate policies, plans, programs and processes to implement data management in a continuous and effective manner, ensuring the completeness, accuracy and timeliness of data.	This provision is ambiguous. It appears exceedingly broad in scope and places an infeasible requirement on data owners and data managers to ensure the accuracy of data. It is not possible for data owners and data managers to edit, change, and regularly ensure the accuracy of user generated data, particularly in large volumes.	Recommendation: • Delete “accuracy” from Article 16(1)
Article 19 Data analysis and synthesis	Organizations and individuals may analyze and synthesize data from sources that they are allowed to use.	The Article states that organizations may analyze and synthesize data collected from sources they are allowed to use. It is unclear whether this creates a prohibition or an obligation on organizations to demarcate allowed sources and whether the provision creates consequences for non-compliance.	Recommendation: • Such objectives should either be deleted or set out in the preamble as objectives, not regulatory requirements.