30 August 2024

Ministry of Public Security ("**MPS**")
Department of Legal and Administrative and Judicial Reform (V03)
30 Tran Binh Trong Street,
Nguyen Du Ward, Hai Ba Trung District,
Ha Noi City

To the Ministry of Public Security

Consultation Draft of the Data Law

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**", "**we**", "**our**" or "**us**"[1]) are pleased to submit this letter to the MPS. We seek to convey industry's views on the draft Data Law ("**Draft Data Law**"), and offer constructive ideas on how the Draft Data Law can be refined to encourage foreign investment into the Socialist Republic of Vietnam ("**Vietnam**"), enhance risk management and facilitate compliance by financial institutions ("**FIs**") with robust standards and obligations aligned with those of other emerging jurisdictions that are considered integral to the sustainable development of world markets.

Summary of key concerns

1. Clarify scope of application

From a business perspective, the scope of the Draft Data Law seems too wide and therefore potentially poses a challenge for FIs and other enterprises to comply with and operationalise. Specifically:

(1) **Purpose:** the Draft Data Law's purpose seems unclear. We recommend the MPS narrow the focus to the core goal outlined in the consultation paper: establishing a National Data Centre, creating a national database, and regulating data intermediary services and the data market. We are of the view that other aspects, especially those concerning general obligations related to data management and security, are already covered by existing laws and should not be duplicated in the Draft Data Law.

(2) **Territorial scope:** the Draft Data Law uses the term "agencies, organisations and

[1] *ASIFMA (Asia Securities Industry & Financial Markets Association) is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side. Our mission is to promote the development of liquid, deep and broad capital markets in Asia, which is fundamental to the region's economic growth. Through the Global Financial Markets Association ("GFMA") alliance with the Securities Industry and Financial Markets Association ("SIFMA") in the United States and the Association for Financial Markets in Europe ("AFME"), ASIFMA also provides insights on global best practices and standards to benefit the region.*

individuals involved in data activities in Vietnam" to define its applicable scope. This scope seems vague and may be interpreted in ways which result in conflicting legal obligations with respect to the activities conducted by international FIs and other organisations not located within the territory of Vietnam.

(3) **Scope of data:** the Draft Data Law uses the term "digital representation" to define "data", which creates uncertainty about whether the Draft Data Law pertains solely to digital activities or also extends to offline data (i.e. data in a physical scenario).

Clear scope of application of the Draft Data Law is vital for FIs and other organisations – both domestic and foreign-invested – to determine the applicability of the rules to their operations and adapt their practices accordingly to comply with the law.

2. Harmonisation with other laws and existing regulations from other authorities

We appreciate the effort that the MPS has and intends to play in coordination among it and other authorities in Vietnam. However, when it comes to industry-level enforcement of the Draft Data Law overseen by the competent authorities, depending on the specific type and business of an FI, its data management may be under the supervision of one or more of financial regulators. Based on our observations in other emerging jurisdictions, the requirements of different regulators may overlap or even conflict, such as different data classification criteria being set in rules released separately by multiple financial regulators. It would be difficult for FIs to observe different sets of rules if regulators do not coordinate among themselves in the area of supervision, i.e., data management in this case. We, therefore, recommend that the MPS coordinates with financial regulators as much as possible and:

(1) ideally, remove data classification and general data management obligations, as we suggest above in respect of the broader purpose of the Draft Data Law;

(2) align the requirements under the Draft Data Law with those under existing laws and regulations published by the MPS and other regulators, including any current technical requirements and financial industry standards;

(3) remove personal data from the scope of the Draft Data Law; and

(4) ensure implementation rules and industry-level regulations in future take a consistent approach in respect of formulating data management requirements.

Alignment with existing rules is not only critical for FIs' compliance with multiple rules released by different regulators, but also facilitates the stability and continuity of these organisations' businesses, such as ASEAN cross-border payments business – namely existing business models that are beneficial to the wider Vietnamese economy domestically and, in some cases internationally, would not be impeded by conflicting regulation – nor would a new business or management mechanism be needed in complex financial transactions if new rules are formulated to align with existing requirements.

3. Clarify principle-based obligations

We understand that the Draft Data Law sets out general principles and anticipates both the MPS and the relevant competent authorities will formulate more specific rules related to data management. To the extent that these obligations are retained in the Draft Data Law (notwithstanding our recommendation in section 1 (*Clarify scope of application*) above), we suggest:

(1) having a lead, or coordinating, regulator in implementing the Draft Data Law for the financial services sector, including for the purposes of formulating further rules or regulations in respect of the application of the Draft Data Law to the financial services sector, and how they are enforced;

(2) expressly acknowledging the relevant lead regulator's detailed guidance and practical examples on how FIs can discharge their obligations, with:

   (a) a transparent and inclusive process that engages with market participants (directly or through industry associations) in the drafting process, to ensure that the Draft Data Law is ultimately practicable and workable;

   (b) a collaborative approach between authorities to ensure the core aspects of the Draft Data Law are consistently implemented by each sector (including financial services), and reduce the likelihood of regulatory arbitrage;

(3) that rules, regulations or guidance applicable on a sectoral basis ("**sectoral rules**") should prevail over those:

   (a) set out in the framework of the Draft Data Law. Specifically, there should be a clear statement that sectoral implementing regulations are supplementary and prevail over the overarching provisions of the Draft Data Law; and

   (b) applicable based on the location of the data processing (that is, if a national financial regulator specifies certain sectoral rules, then these sectoral rules should prevail over any general rules specified by a local authority in the place where the data processing occurs);

(4) any new sectoral rules for the financial sector either replace or expressly supplement existing rules, to avoid overlap; and

(5) that sectoral rules take effect at the same time as the Draft Data Law, with an adequate implementation period. We suggest this period should be at least 24 months. If, for any reason, the sectoral rules cannot take effect at the same time as the Draft Data Law, we suggest an implementation period of 24 months after the sectoral rules are finalised to enable FIs to fully understand the implications and formulate and implement the necessary compliance measures.

4. Remove the data security assessment clauses

We notice that there is a framework in the Draft Data Law for the security assessment and approval of data exports from Vietnam, and this framework has similar requirements to those under Mainland China's Measures for Security Assessment for Outbound Data Transfer in Mainland China. A number of our members that have gone or continue to go through the assessment process in Mainland China are finding that that jurisdiction's broad framework intrinsically results in a burdensome process for both organisations and the regulator, especially in the modern world of finance where data flows are fluid to support a dynamic economy. When the measures in Mainland China negatively impacted foreign firms' willingness to invest in the market, the regulator later provided a more nuanced approach by limiting the scope to a large extent.

We urge the MPS to consider either (1) removing this approval process entirely and replacing it with other safeguards, or (2) if felt strictly necessary, to narrow down the scope of application and elaborate further on the process and frequency in implementing rules

and/or guidance published well in advance of the effective date of this framework under the Draft Data Law, to allow FIs and other businesses to adjust their operations as needed.

5. Definitions of important data and core data require further clarification

Article 3(24) and 3(25) of the Draft Data Law introduce the terms “important data” and “core data”. However, without sufficient clarification, our members strongly believe that it will be difficult for FIs and other businesses to comply in practice with the requirements that are attached to these types of data.

Based on our experience, FIs and other businesses have endured much disruption to data flows and business activities more generally where regulators in other markets have sought to introduce similar concepts but have not been able to promptly release either nationwide or industry-level implementation rules and/or guidance as to the exact scope of these concepts.

Therefore, we urge the MPS to consider removing these concepts of “important data” and “core data” to avoid similar issues. If the MPS sees it as strictly necessary to formulate a new category of data under the Draft Data Law, we suggest the MPS designate this through narrow, very clear numerical or other objective factors that all organisations and individuals can easily understand – any such designation being published well in advance of the effective date of the relevant provisions of the Draft Data Law to allow FIs and other businesses to adjust operations as needed. Alternatively, we suggest that the MPS makes it clear to firms that they do not hold such “important” or “core” data unless they are notified by relevant authorities.

6. Clarify the definition of “Data Intermediary Products and Services”

Article 3(4) of the Draft Data Law introduces the concept of “data intermediary products and services”. Article 47(2)(a) and Article 47(3) of the Draft Data Law further set requirements for organisations providing data intermediary products and services, including localisation requirements for the lead personnel and technical equipment of such organisations.

However, there is a lack of clarity around the definition and the specific types of services these arguably onerous requirements are intended to capture. It is also not certain whether the scope of the organsations, which would be subject to these requirements, extends to international FIs.

Moreover, the requirements may be duplicative for organisations that are already licensed under sectoral regulations. For example, financial services firms operating in Vietnam that are already subject to the regulation and oversight of the State Bank of Vietnam should be excluded from the scope of Article 47, 48 and all other applicable articles relating to the provision of data products and services.

We recommend that the MPS narrows the scope of data intermediary products and services and limits it to the types of products and services that carry the most risk, particularly in the context of international FIs and other multinational businesses.

7. Specify the government’s right to request data

Provisions empowering government information requests are seen in many markets. The key to them not negatively impacting private organisations’ cross-border operations (including those of international FIs) is to implement sufficient safeguards on these powers. Please find our detailed suggestions for Article 15 in the Attachment to this letter.

Without sufficient safeguards, Vietnamese FIs and other domestic champions looking to expand abroad may face regulatory barriers or even investigations where they seek to transfer personal information back to Vietnam in breach of the EU Law or similar regimes which seek to protect against data gathering powers of overseas regulators that seem unchecked by the rule of law.

To give international FIs and other businesses sufficient comfort on the scope and practical implementation of these powers to request data, we urge the MPS to release further implementing rules and/or guidelines to allow international FIs and other businesses to (1) make any required communications in good time to their internal and external stakeholders to allay concerns in respect of these powers, (2) prepare for receipt of and orderly compliance with these data requests, as well as (3) better understand the appeal system for challenging requests for information (as details on this important channel are omitted from the current form of the Draft Data Law)

Next steps

Our detailed considerations and suggestions in relation to the Draft Data Law are highlighted in the Attachment to this letter.

We appreciate the importance of the Draft Data Law for the business and economic environment in Vietnam. As a general suggestion, ASIFMA would urge the MPS and the other regulatory bodies with which it is liaising on the Draft Data Law to continue to consult with ASIFMA and other foreign stakeholders that can bring the unique benefit of insights from operating in multiple jurisdictions around the world and especially experience of other markets' data management and security laws.

In addition, to the extent that it is feasible, we recommend that a timetable for the release of further implementation measures, standards and/or guidance be published separately. ASIFMA strongly believes that such a timeline, if published, would enable government departments and market participants to be even more engaged to reach a set of regulations that benefits all stakeholders, as well as allow both domestic and foreign-invested businesses to plan for operational change as appropriate.

Should you have any questions in relation to this letter or would like to obtain further industry input, please contact Diana Parusheva, Managing Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

This submission was prepared with the assistance of the law firms Linklaters and Allens, based on feedback from the wider ASIFMA membership.

Yours faithfully

Diana Parusheva-Lowery
Managing Director, Head of Policy and
Sustainable Finance at Asia Securities Industry
and Financial Markets Association (ASIFMA)
F: +852 9822 2340
DParusheva@asifma.org

Attachment: Specific comments on Articles

Article No.	Article	Comments	Suggested action
1	Scope This law regulates the construction, development, processing and administration of data; applying science and technology in data processing; national synthesis database; national data center; data-related products and services; State management of data; responsibilities of agencies, organisations and individuals related to data activities.	From a business perspective, the scope of the Draft Data Law seems too wide and therefore potentially pose a challenge for enterprise to comply with and operationalise.	We suggest that the MPS considers limiting the Draft Data Law to the key purpose set out in the consultation paper – namely the creation of a National Data Centre and national database and regulation of the data intermediary services and the data market. Other aspects of the law, in particular, in respect of general obligations imposed on organisations and individuals relating to data management and security have been addressed in other laws specific to those subjects, and therefore should not be repeated here.
2	Applicable entities This law applies to agencies, organisations and individuals involved in data activities in Vietnam.	The current expression "agencies, organisations and individuals involved in data activities in Vietnam" is too vague and may lead to confusion regarding the scope of the Draft Data Law. This Article could be interpreted in ways which result in conflicting legal obligations with respect to activities for international FIs not in the territory of Vietnam. This has caused serious concerns amongst international FIs. For instance, to use an example relevant to modern investment activities, if an organisation or individual outside of Vietnam scrapes or otherwise accesses data from a website hosted in Vietnam, it is unclear whether that sort of activity falls within the scope of	We would suggest that the Draft Data Law is limited to the territory of Vietnam in as simple a manner as possible, or else be expressly stated.

Article No.	Article	Comments	Suggested action
		the Draft Data Law because the person is not in Vietnam.	
3(1)	Data is the digital representation of behaviour, things, events, information, including in the form of sound, images, numbers, writing, symbols or other similar forms.	Based on the definition of "digital representation", there is uncertainty about the definition of the scope of "data" and whether the Draft Data Law is intended to apply in online, physical; or both scenarios.	We recommend clarifying whether the Draft Data Law applies only to digital activities or also to offline ones, or if it is intended to cover both online and offline activities.

3(4)	Data intermediary products and services are products and services intended to establish a commercial relationship between data subjects and data owners, on the one hand, and data users, on the other hand, through technical, legal or other means for the purpose of sharing data and exercising data subject rights related to personal data, excluding the following products and services: (a) services which collect data from data owners and compile, diversify or transform data for the purpose of adding value to that data and grant licences to data users for using the collected data without establishing a relationship between the data owner and the data user; (b) services focused on providing copyrighted digital products; (c) data sharing services provided by State agencies are not intended to establish a commercial relationship.	The term "data intermediary products and services" has not been regulated under Vietnamese law before, but the proposed definition in the Draft Data Law is still quite ambiguous. For example, it is unclear what it means to "establish a commercial relationship between data subjects and data owners". Without further implementation rules and/or guidance under Vietnamese law, the scope and application of this term is difficult for FIs and other business to understand.	We suggest that the MPS further explains the intended scope and application of the term "data intermediary products and services". If this cannot be written in the Draft Data Law for the sake of time or due to the MPS' legislative approach to this law, we would suggest that the MPS at a minimum publishes some FAQ or similar guidance which can quickly and efficiently address uncertainties such as this. Experiences can be learnt from recent legislation in markets such as the EU (e.g. the Data Governance Act, which describes six categories of intermediary as (i) personal information management systems (PIMS), (ii) data cooperatives, (iii) data trusts, (iv), data unions, (v) data marketplaces, and (vi) data sharing pools).

Article No.	Article	Comments	Suggested action
3(17)	Data subject is an individual or organisation reflected by the data.	The concept of "data subject" is extremely broad where it relates to data "reflected by" both organisations and individuals. In a privacy law context, a law would typically refer to a data subject only as an individual. There is a risk that applying the term to both organisations and individuals may lead to ambiguities and additional burden on those seeking to comply with the Draft Data Law, if privacy and data protection concepts intended only to apply to individuals, then unintentionally apply also to organisations.	We suggest that the MPS reconsider the broad scope of this definition and its intention for the application of the Draft Data Law and individual provisions of it. Industry proposes that the MPS clearly articulates that personal information handling should follow the Decree on Personal Data Protection to avoid duplication and confusion for FIs and other business operators.
3(24)	*Important data* is data in fields, groups, and regions which can cause direct danger to national security, economic activities, social stability, public health and safety when such data is leaked, falsified or destroyed.	Notwithstanding the defined term, from a business and operational perspective for FIs handling their own, their customers', and their counterparties and other stakeholders' data, it is unclear what amounts to "important data". We understand from the text that the MPS sees the "importance" of data as likely to be measured with reference to the State and the general public, not from the standpoint of particular interest groups. However, without sufficient clarification, it will be difficult for FIs and other businesses to comply with this requirement in practice. Financial institutions and other businesses have endured much disruption to data flows and business activities more generally where regulators in other markets have sought to introduce similar concepts but	We note that Vietnamese laws already have the concept of State secrets which are extensively regulated and which already have restrictions and limitations on offshore transfer. Therefore, we urge the MPS to consider removing this concept of "important data" to avoid duplicate regulations. If the MPS sees it as strictly necessary to formulate a new category of data under the Draft Data Law, we suggest the MPS designate this through narrow, very clear numerical or other objective factors that all organisations and individuals can easily understand – any such designation being published well in advance of the effectiveness of the relevant provisions of the Draft Data Law to allow FIs and other businesses to adjust operations as needed.

Article No.	Article	Comments	Suggested action
		have not been able to promptly release either nationwide or industry-level implementation rules and/or guidance as to the exact scope of these concepts. Position papers of chambers of commerce in Mainland China, for example – which seems to have been a point of reference for some provisions in the Draft Data Law – have described the challenge of such concepts.[2]	Alternatively, we suggest that the MPS makes it clear to FIs and other businesses that they do not hold such "important" or "core" data unless they are notified by relevant authorities.
3(25)	Core data is important data with high coverage across fields, groups, and regions which has direct impact on political security when such data is used or shared illegally. Core data includes data related to important national security areas, data related to the vitality of the national economy, important people's livelihoods, major public interests, and other data provided by national agencies.	The concept of "core data" seems to be a subset of "important data" and, as such, our comments in respect of Article 3(24) above (on the later term) are equally applicable here.	The concept of "core data" seems to be a subset of "important data" and, as such, our comments in respect of Article 3(24) above (on the later term) are equally applicable here.
4(1)	Other laws that regulate data must not contravene the provisions of this Law. In cases where other laws do not stipulate or have regulations on data that are different from the provisions of this Law, the provisions of this Law shall apply.	In light of the Law on Protection of Personal Data, which is also being drafted, this may lead to confusion as to which law will prevail with respect to personal data.	We recommend making clear that matters pertaining to personal data will be governed by the Law on Protection of Personal Data.
4(2)	In the case of any discrepancies between	International FIs encourage prevalence being given to	To the extent that our members can act as a

[2] En-British-Business-in-China-Position-Paper-2023_compressed.pdf (britishchamber.cn)

Article No.	Article	Comments	Suggested action
	the provisions of this Law and an international treaty to which the Socialist Republic of Vietnam is a member on the same issue, the provisions of the international treaty shall apply.	international treaties in this manner.	sounding board to the MPS on the integration of the Draft Data Law and/or other rules into the wider international framework of data laws, our members would be delighted to assist the MPS in that regard.
6(8)	Developing, trading, and circulating data products and services which infringe national defence and security, personal privacy, and Vietnamese customs and traditions.	The concept of "Vietnamese customs and traditions" is vague and broad, such that the meaning is open to different interpretation by different stakeholders, in the context of modern business; the meaning is also likely to change with time and, for example, the increasing influence of the digital economy (as is particularly relevant to the scope of application of the Draft Data Law). In particular, this is relevant to the requirement under Article 50(3) that the construction, development, circulation and use of data analysis and synthesis products and services must comply with this prohibition.	We recommend that the Draft Data Law or the implementing regulations to be published at the time of promulgation of the Draft Data Law clarify the types and/or purposes of behaviour that should be within the scope of this concept, particularly in a modern business context as is relevant to FIs.
8(2)	(a) For the purpose of ensuring data quality, the agencies and organizations managing national databases and specialized databases must:…	The definition of "specialised databases" is not clear from the Draft Data Law itself. While that it appears not to be intended to capture databases of private organisations like FIs, the concept is not explained in great detail.	To avoid unintentionally catching the legitimate needs of private database operation by international FIs, we recommend that the Draft Data Law distinguishes between obligations for national databases and private databases to avoid the perception or actual imposition of an additional compliance burden on private organisations (if that is not the intention). In particular, we suggest clarifying that "national

Article No.	Article	Comments	Suggested action
			databases" and "specialised databases" are clearly defined as databases of the State authorities.
9(2)	Ministers, heads of ministerial equivalent bodies, Government agencies, and Chairmen of People's Committees of provinces and cities under central authority shall issue a list of important data within the scope of management.	As mentioned in respect of Article 3(24) above, we submit that the concept of "important data" is extremely vague and adds a significant level of uncertainty from the perspective of practical implementation by FIs and other businesses that process various types of data. In addition, we have seen in other markets – particularly Mainland China – that different authorised government bodies – whether split by industry or geography – can lead to contradictory (and even competing) lists. These contradictory lists are especially difficult for FIs to operationalise in a coherent manner, since they tend to serve customers from different industries and locations. These complications are exacerbated in today's digital economy – that the Draft Data Law seeks to promote – since there is convergence of sectors and business activities are less constrained by geographic boundaries. Alternatively, or in addition, this approach of relying on	Our suggestions in respect of Article 3(24) above are applicable here. However, to the extent that the concept of "important data" is retained and lists formulated by multiple government bodies, we would strongly recommend alignment of the definition and scope of important data among different lists, to avoid causing uncertainly for FIs and other businesses. Our members would be happy to be consulted by the MPS and/or its counterparts regulating financial services, in respect of our members' experience in other markets and the sort of framework for these lists that could lead to more acceptable outcomes for businesses that are seeking to serve Vietnamese stakeholders.

Article No.	Article	Comments	Suggested action
		multiple government bodies may lead to inertia among them as they wait for higher or associated authorities to formulate frameworks or rules for the first body to work to. This can leave FIs and other businesses uncertain as to how to comply, consequently potentially slowing or dissuading private capital investment and growth.	
9(3)	The Ministry of Public Security presides and coordinates with the Ministry of National Defence, the Ministry of Information and Communications and relevant units to submit a list of core data to the Prime Minister for promulgation.	Our comments in respect of Article 9(2) above (in relation to the issues that we expect to arise with the formulation of lists of "important data") are equally applicable to "core data" as an apparent subset of "important data". As a corollary to our comments in respect of Article 9(2) above, our members have experience in other markets – particularly Mainland China which would seem to have been a point of reference for some provisions in the Draft Data Law – where multiple government authorities are involved in the shaping of data laws. Where public security authorities lead the process of shaping these laws, our experience is that there can be an inherent challenge to find a sustainable balance between national/public security and economic considerations. Well publicised commentary is available on this topic.[3]	Our suggestions in respect of Article 3(24) above are applicable here. However, to the extent that the concept of "core data" is retained and lists formulated by multiple government bodies, as suggested in respect of Article 9(2) above, we would urge for collaboration between the MPS and financial services regulators as early as possible, to reduce uncertainty for FIs and lead to more acceptable outcomes for businesses that are seeking to serve Vietnamese stakeholders.
9(4)	The Government regulates this Article in	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules	We suggest that the MPS provides a definitive timetable for release of the relevant

[3] China Appears to Choose National Security Over Foreign Investment | TIME

Article No.	Article	Comments	Suggested action
	detail.	and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty as to the obligations and other requirements applicable to them as early as possible to allow for efficient compliance within the existing multi-market set of policies and practices.	implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them, if any.
10(2)	Organizations and individuals not specified in Clause 1 of this Article are encouraged to store and process data centrally and consistently, forming databases according to the models stated in Clause 1 of this Article.	Given the commercial value of data in today's digital economy, as international FIs, our members have seen inherent tensions between public and private sectors in respect of data sharing. While we agree that there should be sharing of certain types of data in various scenarios for the wider public interest, as well as clear access rights for individuals to information on themselves (under data protection law principles), provisions should come with sufficient guardrails to avoid the perception that government bodies could use them as leverage to require private organisations – FIs and others – to share proprietary and other commercial data in a manner that would not benefit the growth of a sustainable private sector (ultimately for the benefit of Vietnamese stakeholders).	We recommend clarifying the government's expectation on what data stored and processed in private database is encouraged to be shared with any state agencies, political organisations, socio-political organisations, other organisations or individuals, and setting parameters to avoid any perception that this discretionary obligation could be treated as a mandatory obligation.
11(1)	Data combination is combination of data from different sources into a single data set for later analysis or for storage in a data warehouse. Data needs to be prepared and standardized before	It is unclear if this is intended to apply for government agencies only, or also private entities. While it is correct that combining and standardising data before combining would increase the quality of the combined data set, it would be burdensome for international FIs	We suggest changing the term "Data needs to be prepared…" to "It is encouraged to prepare and standardise data…" to make this requirement a recommended process rather than mandatory.

Article No.	Article	Comments	Suggested action
	combining data together.	if this is set as a mandatory obligation. There is also lack of clear standard about to what extent data is considered as "prepared and standardised".	
11(3)	Any agency, organization which or individual who manages a database is responsible for adjusting and updating data regularly and continuously to ensure the accuracy and validity of the data in its database and information system, and notifying the parties with whom the data is shared of any such update and adjustment.	We note that this Article sets out requirements to adjust and update data regularly. However, this might lead to a heavy burden for international FIs' operation as they would be obligated to continually update third parties on adjustments of the database.	We suggest that notification relating to updates should relate only to existing obligations under data protection laws or should be limited to a finite period from creation of the database to no longer than every 12 months.
12	Data strategy	We note that this Article is general and covers scope broader than Chapter II.	We suggest moving this Article to Chapter I "General Rules".
12(3)	The State ensures that the expenditure on implementation of the National Data Strategy shall be at least 1% of the total annual state budget expenditure.	We are delighted to see the high-level commitment shown in this Article, which would add certainty and promote the faith of international FIs in the enforcement of the Draft Data Law.	We suggest clarifying the consequences and remedies if this Article is not met in the Draft Data Law.
12(4)	The Government regulates this Article in detail.	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and other requirements applicable to them as early as possible to allow for efficient compliance within the existing multi-market set of policies and practices.	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them, if any.

Article No.	Article	Comments	Suggested action
13(1)	A data administration organization must organize and develop policies, plans, programs and processes to continuously and effectively conduct data administration, ensuring the completeness, accuracy, timeliness of data.	On the face of the Draft Data Law, the role and make-up of these "data administrators" is not entirely clear as they are not defined. For example, it is unclear if they are intended to be government or quasi-government bodies or a body within any organisation such as a private corporate or institution (including international FIs with a presence in Vietnam). We note that the Draft Data Law also contains other overlapping definitions, including "database administrator" (Article 3(21)) and "data owner" (Article 3.22), which may conflict with the similar terms in other laws, such as "IT system administrator" in the Law on Cyber Information Security and Law on Cybersecurity, and "data controller"/"data processor" in Decree No. 13/2023/ND-CP.	We recommend that the MPS clarify the role and ultimate purpose of these "data management agencies" and harmonise other terms used in the Draft Data Law with other laws and regulations, so that FIs and other businesses understand the impact, and specific obligations imposed, on them, if any.
14(6)	The Prime Minister decides on the sharing of private-use data managed by ministries, ministerial equivalent bodies, Government agencies, and People's Committees of provinces and cities under central authority to resolve emergencies; unexpected and urgent cases in the prevention and control of natural disasters, epidemics, fires and explosions; emergency cases to solve problems that arise in practice.	We note that private-use data could be shared by the government for emergency purposes. However, the Draft Data Law does not cover the protection during the process of private-use data sharing, or any confidentiality requirements imposed on the government. Particularly for international Fis and other multinational businesses that are less familiar with government practices in Vietnam, this breadth may lead to concerns that the power could be abused. Therefore, relevant protection or confidentiality protocols would be highly valued by international FIs as they could ensure better security over their data. Further, limited access to private-use data by the	We suggest the MPS clarifies the confidentiality and data protection obligations when the government is processing or transferring the private-use data for emergency purposes.

Article No.	Article	Comments	Suggested action
		government might also be relevant to international FIs' compliance obligations to data protection laws in other jurisdictions.	
15(1)	Organisations and individuals must declare and provide data to state agencies in special cases when requested.	Provisions empowering government information requests are seen in many markets. The key to them not negatively impacting private organisations' cross-border operations (including those of international FIs) is to ensure that these powers (by reference, for example, to the European Data Protection Board's Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[4]) (i) are based on clear, precise and accessible laws; (ii) must be exercised in a necessary and proportionate manner; (iii) are subject to independent oversight; and (iv) provide effective remedies for individuals. Without these parameters, EU-based FIs and other business (to continue the example, given the importance of the EU as a trade partner to Vietnam) may be barred from transferring personal information to Vietnam. As such, to allow and promote cross-border business into Vietnam, implementing sufficient safeguards on this power is crucial. In addition, without these safeguards, Vietnamese FIs and other domestic champions looking to expand abroad may face regulatory barriers or even investigations where they seek to transfer personal	To give international FIs and other businesses sufficient comfort on the scope and practical implementation of these powers to request data, we urge the MPS to release further implementing rules and/or guidelines to allow international FIs and other businesses to (i) make any required communications in good time to their internal and external stakeholders to allay concerns on this power, and (ii) prepare for receipt of these data requests. In particular, industry seeks clarification on which types of "special cases" would warrant compliance with a request, and the exact process for challenging a request for information.

[4] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures | European Data Protection Board (europa.eu)

Article No.	Article	Comments	Suggested action
		information back to Vietnam in breach of GDPR[5] or similar regimes.	
15(2)	Special cases specified in Clause 1 of this Article include: (a) The requested data is necessary to respond to a public emergency status; (b) The lack of available data prevents a State agency from fulfilling a specific task in the public interest as expressly prescribed by law and the State agency cannot obtain such data by other alternative means.	While we appreciate that the MPS has sought to expressly limit the applicable circumstances in the Draft Data Law, the provisions remain relatively vague such as provides broad powers to a state agency to request data to perform its statutory public duties. Particularly for international FIs and other multinational businesses that are less familiar with government practices in Vietnam, the breadth of these scenarios may lead to concerns that the power could be abused.	Our suggestions in respect of Article 15(1) above are applicable here. Further, we recommend that the list of data that an authority may request must also be stipulated in law (and to the extent that they cannot obtain from other sources only).
15(3)	When requesting organisations or individuals to provide data in special cases, the state agency is responsible to: (d) … (e) Specify the time-limit for providing data. During that time-limit, the data holder can request the state agency to amend or withdraw the request.	We appreciate the apparent mechanism for FIs to appeal against a request, as this is a clear sign of rules being built to respect the rule of law. However, the appeal process is unclear under the current provision which could lead to abuse of the mechanism.	We recommend that the MPS sets out a clearer process for the appeal system under the Draft Data Law or its implementation rules and/or guidance well-in advance of the effectiveness of the relevant provisions of the Draft Data Law, to allow FIs and other businesses to adjust operations as needed.

[5] DPC launches two inquiries into TikTok concerning compliance with GDPR requirements relating to the processing of childrens' personal data and transfers of data to China | 14/09/2021 | Data Protection Commission

Article No.	Article	Comments	Suggested action
15(4)	A request for data provision made under Clause 5 of this Article must ensure: (a) Be expressed in a clear, concise and understandable language to the data holder; …	Although implied, it is not clear whether requests from state agencies must be made in written form. If requests could be made orally – or, at most followed up in writing to confirm the details of the request – there is a risk that this power could be abused in respect of what could be extremely sensitive proprietary, client or other sensitive and confidential data for FIs and other businesses.	We urge the MPS to state explicitly that requests – at least to private organisations and individuals – must be delivered in written form to ensure accountability of officials making these requests.
15(5)	Obligations of State agencies upon receipt of the requested data: (a) … (b) Implement technical measures and protect the legitimate rights and interests of the data subjects and the data providers; (c) …	As the MPS will appreciate, data and cyber security is multifaceted to deal with today's operational risks. As such, reference only to "technical measures" seems too narrow to provide the level of protection that FIs and other businesses would be expected to keep themselves, and therefore also have a right to expect from their regulators. In addition, it is not expressly stated whether state agencies can freely share information gathered among themselves (provided that this sharing does not go beyond the stated purpose of the original request).	We suggest that the measures referenced in this Article are extended to "technical and organisational measures" to follow similar rules in other contexts. In addition, we would recommend that the ability of state agencies to share information with other state agencies is clarified but also minimised to reduce the risk of advertent data leaks.
15(6)	The Government shall regulate in detail the provision of data to state agencies in special cases.	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and other requirements applicable to them as early as	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to prepare for receipt of these data requests.

Article No.	Article	Comments	Suggested action
		possible, to allow for efficient compliance within their existing multi-market set of policies and practices.	
18(1)	Public disclosure of data is announcement and provision of official information about a certain data set by an agency, organization, unit or individual.	It is unclear what qualifying impact the reference to "official" is intended to have on "information" in the context of an international FI and, we envisage, many other businesses. Without clarity on the scope of this activity, compliance with the prohibition under Article 18(4) on public disclosure, for example, is sufficiently more challenging.	We suggest that the MPS provides an explanation of the meaning and impact of the term "official" before "information".
18(2)(b)	Posting on data portals, electronic information portals, websites and mass media;	It is unclear what is the exact scope of "data portals, electronic information portals, electronic information pages and mass media". Are these portals and media of a public nature only, or do they also include semi-public membership platforms? For example, it cannot be inferred from the current expression whether posting data on a membership-only online platform would constitute data disclosure.	We suggest replacing the term "data portals" with "public data portals", etc. Alternatively, a reference to social media may be included directly in this sub-paragraph.
18(4)	Data not allowed to be made public includes: Personal data without the consent of the data subject; data being state secrets; data affecting national defence and security; data which if made public would harm the interests of the State and international relations; social ethics, community health; causing harm to the life, livelihood or property of others; information belonging to work secrets;	These broad categories of information prohibited from disclosure, although seen in at least one other Asian jurisdiction (namely Mainland China), are likely to have a similar effect of raising concerns among international FIs as to their scope of application. In particular in Mainland China, the broadening in July 2023 of the scope of data that triggers offences under the Anti-Espionage Law (to any "documents, data, materials and items related to national security and interests.") and the revision of the Law on Guarding	To avoid overlapping with the Law on Cybersecurity and other laws and regulations (such as on protection of State secrets or personal data), we urge the MPS to consider removing the prohibition on disclosure of data. If strictly necessary to formulate these distinct categories of data under the Draft Data Law, designate these through narrow, very clear numerical or other objective factors that all organisations and individuals can easily

Article No.	Article	Comments	Suggested action
	information about internal meetings of state agencies; documents prepared by state agencies for internal affairs.	State Secrets (to include the concept of "work secrets") caused concern among many international businesses at the lack of operationalized terms and created a perception that officials may not interpret the non-personal data concepts subjectively, thereby impacting normal cross-border business operations. We are concerned that similarly vague terms in the Draft Data Law may lead to inertia in marketing, research report distribution, and other activities requiring disclosure to the public of certain information. Furthermore, this prohibition may overlap with provisions in the Law on Cybersecurity which already prohibits the dissemination of certain specific categories of violating information in cyberspace.	understand – any such designation being published well in advance of the effectiveness of the relevant provisions of the Draft Data Law, to allow FIs and other businesses to adjust operations as needed. We recommend that – if retained – these categories of data should be clearly defined as soon as possible. For example, in some other jurisdictions (like Mainland China), in the majority of cases, state secrets should be expressly marked as such on the top of documents.
19(1)	(b) Write access: is the activity of writing data to a certain source. In the case where data is stored in applications, write access is used to update data to the database. (c) Edit access: is the activity of modifying the stored data. In the case where data is stored in applications, edit access is used to change data that is already stored in the database.	We notice that the definition of "write access" in sub-paragraph (b) and "edit access" in sub-paragraph (c) are not mutually exclusive, as the data flow for these two actions are the same (because modifying data also requires to update data to the database), especially in the cases where data is stored in applications.	We recommend merging these two subparagraphs as "(b) Write and edit access: is the activity of writing data to a certain source. In case data is stored in applications, write access is used to update data to the database".
19(2)	Data management agencies, organizations and individuals are	This Article may unintentionally create burden for organisations and individuals, if their data is passively	We propose to add the term "where appropriate" before "providing access tools

Article No.	Article	Comments	Suggested action
	responsible for providing access tools and granting rights according to the data access types.	held.	and…". This would grant organisations and individuals flexibility when complying with this Article, easing the compliance burden.
19(5)(a)	Relevant agencies, organizations and individuals using data retrieval tools are responsible for including technical measures to protect data into the design process from the beginning to protect data.	We welcome this "security-by-design" approach, which has been proved to be an effective method in data protection by laws and regulations in other jurisdictions, such as the GDPR.	We recommend expanding the scope of this sub-paragraph to cover personal data to provide more protection to individuals.
21	Copying, transmission, and transfer of data	We note that Article 21 sets out principles of data copying, transmission and transfer whose scopes are broad and vague. These requirements may lead to ambiguous interpretation and are generally hard to be implemented in enforcement. Moreover, with the rapid development of technology, it is also a common approach to include technology-related requirements in lower-level regulations or standards to avoid top-level laws becoming outdated.	We suggest omitting the requirements in Article 21 of the Draft Data Law, and separately issuing lower-level regulations or standards to cover them.
22(2)	The data classified as core data or important data that needs to be provided and transferred outside the borders of the Socialist Republic of Vietnam must be evaluated and approved by competent authorities.	Should the concepts of "core data" and "important data" be retained (see our comments on Articles 3(24) and 3(25) above, in particular), based on market examples elsewhere in Asia (principally Mainland China), this sort of government approval process must be implemented with extreme caution to avoid unduly hindering legitimate business activities. As can be seen from government released statistics in Mainland China (to continue the example, given the	To the extent feasible in the context of Vietnam's ambition stated in Article 22(1) (to protect national security and social public interests, but promote safe and automatic data flow), we would urge the MPS to consider removing this government-led approval process to free resources for other supervisory purposes. However, if it is felt that an approval process

Article No.	Article	Comments	Suggested action
		importance of Mainland China as a trade partner to Vietnam), it appears that there has been a slow approval rate for many companies required to complete the approval process – only 206 organisations in the first 21 months, notwithstanding the number and size of organisations in that key global market.[6] As mentioned in our comments to Article 3(24), foreign stakeholders cited data laws in Mainland China as one of their key concerns in 2023.[7] Furthermore, it should be considered that it is common practice for international FIs and other businesses to use "hubbed" infrastructure (for example, one data centre for all Asia-based operations) to benefit from economies of scale.	must be retained, we would suggest that it is administered by each respective industry-level regulator – such as the State Bank of Vietnam or the Ministry of Finance for FIs – so that officials should possess relevant industry-specific knowledge of key business activities, including data exports to make the process as efficient as possible. Moreover, the approval process should also be limited to a narrow scope of "important data" that warrants this level of rigour. In addition, given the regional nature of IT infrastructure in international FIs – particularly if the approval process is administered by an industry-level regulator – we would recommend that there is a mechanism for obviously regional businesses to be exempt from the process or put through a streamlined process subject to the in-scope data being secured with adequate standards for intra-group transfers. Preferably, we recommend that explicit exemptions are added to provide clarity to industry, such as outbound data transfers: (a) by onshore representative offices and branches of foreign entities.

[6] https://mp.weixin.qq.com/s/a0jfDFsTgDAiAhkSdv8VZw

[7] En-British-Business-in-China-Position-Paper-2023_compressed.pdf (britishchamber.cn)

Article No.	Article	Comments	Suggested action
			(b) to facilitate payments. (c) relating to personal information of legal/authorised representatives, senior management, individual shareholders, ultimate beneficiary owners, designated contact persons and individual signatories, as well as business contact information. (d) for risk management and compliance monitoring. (e) for operational, transactional and management purposes. (f) for offshore litigation, arbitration or other legal proceeding purposes. (g) for offshore regulatory compliance purposes. (h) relating to pre-investment due diligence, investment research, portfolio data and other information collected in relation to stewardship activities that (after being transferred offshore) will only be shared within the group or disclosed to the relevant investors (i) within a group of companies for HR management.

Article No.	Article	Comments	Suggested action
22(3)	The authority to decide on the provision and transfer of data abroad is prescribed as follows: (a) The Prime Minister decides on the provision and transfer of national core data. (b) The Ministry of Public Security conducts assessment and decides to provide and transfer important data.	Our comments in respect of Article 22(2) above are equally applicable to the approval process described here. In addition, given the resource-intensive process that can develop – as seen in the Mainland Chinese market – there may be concerns among businesses possessing "core data" that the requirement for the approval of the Prime Minister may lead to a subjective and even politised decision rather than one that is made objectively by industry-experts from (for instance) the relevant industry regulator. In addition, there seems to be a contradiction between this Article 22(3)(a)'s position that the Prime Minister will decide on the provision of core data abroad, and the statement in Article 22(4)(a) that the MPS will conduct the assessment.	Our suggestions in respect of Article 22(2) above are equally applicable to the approval process described here. In addition, it would provide more certainty for FIs and other businesses that may process core data, if the roles of the Prime Minister and the MPS in the security assessment and decision-making can be explained.
22(4)	When the data administrator needs to provide and transfer core data or important data abroad, they must meet the following conditions: (a) Pass the data security assessment conducted by the Ministry of Public Security according to the provisions of Clause 7 of this Article; (b) Sign a contract with the foreign recipient according to the	*Security assessment* While we appreciate that the framework for the security assessment set out in Article 22(7) has apparently drawn from a precedent with similar requirements under the Measures for Security Assessment for Outbound Data Transfer in Mainland China, we are cognisant that a number of our members that have or continue to go through the assessment process are finding that that broad framework intrinsically results in a burdensome process for both organisations and the regulator.	*Security assessment* We urge the MPS to consider either (i) removing this approval process entirely and replacing it with other safeguards, or (ii) if felt strictly necessary, to narrow down the scope of application and elaborate further on the process and frequency in implementing rules and/or guidance published well in advance of the effectiveness of this provision of the Draft Data Law, to allow FIs and other businesses to adjust operations as needed.

Article No.	Article	Comments	Suggested action
	standard contract developed by the Ministry of Public Security, agreeing on the rights and responsibilities of both parties; (c) Other conditions as prescribed by law.	In addition, it is unclear whether the security assessment requirement under item (a) of Article 22(4) constitutes a one-time process for each transfer, or if it covers repeated transfers of a similar nature. In particular, we are concerned that requiring assessments for each and every transfer would be disruptive to business. Cross-border transfers within financial services groups are too frequent in the modern world of finance. *Prescribed contract* In respect of the requirement to enter into a prescribed form of contract, the Draft Data Law does not provide any details on the necessary contractual terms.	*Prescribed contract* We suggest that if any contractual terms are mandatorily required, in order to allow FIs to understand their obligations in practice, including in respect of onward transfers from the first overseas recipient. In addition, we suggest that any implementing regulations or guidance should clarify that organisations can rely on contractual terms that conform to international standards (in place of the prescribed form). For example, the MPS may recognises standard contracts that have been recognised by other jurisdiction as they too uphold key obligations (as is the approach recently taken by the authorities in Thailand which have recognised as valid data transfer mechanisms both the EU's standard contractual clauses and ASEAN's Model Contractual Clauses for Cross Border Data Flows[8]).
22(6)	The data administration agency must apply necessary measures to ensure that the data processing activities of the foreign data recipient meets the data protection standards prescribed in this	Subject to the clarification sought in respect of Article 13(1) above, if responsibility for ensuring that data protection standards are met falls to an external data administrator, we submit that this could be an overly burdensome process for an international FI that	We recommend that ensuring that data protection standards are met is the responsibility of the organisation making the export, even if there are prescribed standards for the organisation to follow.

[8] Notification of the Personal Data Protection Committee on Criteria for the Protection of Personal Data Sent or Transferred to a Foreign Country Pursuant to Section 29 of the Personal Data Protection Act, B.E. 2562 B.E. 2566 (2023).

Article No.	Article	Comments	Suggested action
	Law.	needs to maintain numerous cross-border transfer channels.	
22(7)	Data security assessment for data provision and transfer abroad focuses on assessing the risks that data provision and transfer activities may bring to national security, public interests, legitimate rights and interests of individuals and organizations, including at least the following issues: …	We note that this Article is almost identical to Article 5 of the Measures on the Security Assessment of Data Export issued by the Cyberspace Administration of China. However, the Draft Data Law does not provide further information on the definition or scope of each item under this Article to be assessed.	As mentioned in our comment to Article 22(4), we suggest that the MPS either (i) removing this approval process entirely and replacing it with other safeguards, or (ii) if strictly necessary, to elaborate further on this data security assessment regime. If the latter, we further recommend the MPS to narrow down the scope of data where this requirement applies and provide more specific requirements and/or explanation on the items in this Article.
22(8)	Data security assessment for the provision and transfer of data abroad is carried out in a combination of assessment before the provision and transfer is carried out, continuous monitoring, and periodically re-assessment during implementation in order to prevent security risks and ensure the orderly and free flow of data in accordance with the law.	This provision of the Draft Data Law does not specify how frequently the re-assessment must occur, or whether this must be in response to a change in circumstances.	Given the potential burden on international FIs and other businesses to comply with continual assessment requirements, we urge the MPS to only require a re-assessment when there is a genuine deterioration in the protection for the data, such that may lead to danger to national security, etc.
22(9)	Competent Vietnamese agencies must resolve requests from foreign law enforcement or judicial agencies regarding provision of data according to	*Conflict with foreign regimes* We submit that the requirement on organisations and individuals to seek approvals for these data exports (as set out in the second sentence) will create major	*Conflict with foreign regimes* We recommend expressly clarifying that this Article does not apply:

Article No.	Article	Comments	Suggested action
	international treaties and international agreements that Vietnam has signed or participated in. Domestic organizations and individuals are not allowed to provide data stored in Vietnamese territory to foreign judicial or law enforcement agencies without the approval of Vietnamese competent authorities.	issues for international FIs headquartered outside of Vietnam, as it is likely to conflict with existing legal requirements under the laws of other jurisdictions. For example: • FIs may be required by the foreign regulator to respond within a time limit; and • if the Vietnamese authorities refuse to provide an approval to disclosure, then the FIs may be in breach of the law of the other jurisdiction. *Decision-making authority* In addition, it is not clear which authority a FI should apply to for approval. *Clarification on the receiving party* A regulator may take on different roles: sometimes as a day-to-day supervisory body and sometimes as an enforcement body. Reflecting on market practice elsewhere in Asia – principally in Mainland China – we submit that this prohibition should not seek to restrict transfers of data to a body in a non-enforcement capacity (even if the body has an enforcement role in other circumstances).	• to data that is not likely to endanger national security or public interest. Types of data which could have such an impact should be expressly dealt with under the approval mechanism in Article 22(2) or any other related rules; • to data stored in Vietnam merely by virtue of its storage in a cloud server located in Vietnam; • when the export of data is to facilitate intra-group assessment or reporting for anti-money laundering and counter-terrorism financing purposes; • to provision of data to international organisations (e.g. Interpol); or • to provision of data to foreign government authorities as required by applicable local laws. *Decision-making authority* We also suggest clarifying the intention of the MPS in respect of which party is authorised to make the relevant decision. *Clarification on the receiving party* We suggest clarifying that Article 22(9) only applies when the receiving party is an overseas regulator or similar body.

Article No.	Article	Comments	Suggested action
22(10)	The Government regulates this Article in detail.	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and other requirements applicable to them as early as possible, to allow for efficient compliance within the existing multi-market set of policies and practices.	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them, if any.
23(2) & (3)	Data deletion is the activity of removing data from the structure and environment where it is being stored. Data destruction is the activity of removing data from the structure and environment where it is being stored, ensuring the possibility of recovery is eliminated by overwriting or physical destruction.	We notice that the definition of "data deletion" in paragraph (2) and "data destruction" in paragraph (3) are not mutually exclusive, as the only difference these two terms have is whether data can be recovered. Based on our experience, in practice, using separate concepts for similar activities may frequently lead to confusion and add difficulty to enforcement.	We recommend the MPS to only keep the definition of "data deletion" in this Article, and separately add the requirements of "the possibility of recovery is eliminated by overwriting or physical destruction" where applicable.
24(5)	The Government regulates in detail the development and application of technology in data processing for the following applications: …	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and other requirements applicable to them as early as possible to allow for efficient compliance within the existing multi-market set of policies and practices.	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them, if any.
25(4)	Agencies, organisations and individuals processing core data and important data	This provision of the Draft Data Law does not specify how frequently the assessment must occur, or	Given the potential burden on international FIs and other businesses to comply with periodic

Article No.	Article	Comments	Suggested action
	must periodically conduct risk assessments for such data processing activities according to regulations. The risk assessment content includes at least information about the type and amount of data being processed, the circumstances of data processing activities, risks arising in data processing and solutions to resolve them.	whether this must be in response to a change in circumstances.	assessments, we urge the MPS to only require such an assessment when there is a genuine deterioration in the protection for the data, such that may lead to danger to national security, etc.
25(5)	Regulations on a number of measures to prevent risks arising in data processing including: (a) …	We note that the obligations set out in this Article are broader than those under the Law on Cyber Information Security. However, the extent of the additional compliance burden for FIs and other businesses will not be clear until further implementation rules and/or guidance is released. We note that FIs, such as credit institutions, may be subject to other sector-specific regulations already such as Decree No. 117/2018/ND-CP of the Government, Circular No. 09/2020/TT-NHNN of the State Bank of Vietnam, and various other regulations.	We recommend aligning the data management obligations under the different laws and regulations (possibly by referring to the existing obligations under sector-specific rules instead of creating new overlapping obligations) to ease the compliance burden of international FIs, which will also have an overlay of industry-level obligations and obligations flowing from their group's home market. We also suggest clarifying the extent of the final obligations through the prompt release of the implementation rules and/or guidance required to operationalise these obligations. Alignment with existing rules is not only critical for FIs' compliance with multiple rules released by different regulators, but also facilitates the stability and continuity of these organisations' businesses, such as ASEAN cross-border

Article No.	Article	Comments	Suggested action
			payments business [9] – namely existing business models that are beneficial to the wider Vietnamese economy domestically and, in some cases internationally, would not be impeded by conflicting regulation – nor would a new business or management mechanism be needed in complex financial transactions if new rules are formulated to align with existing requirements.
26	National Data Development Fund	Similar to our comment in respect of Article 12, we understand this Article sets out obligations on the public authorities, which seems out of the scope of Chapter II.	We suggest moving this Article to Chapter I "General Rules" together with Article 12.

[9] https://wtocenter.vn/an-pham/22818-vietnams-cross-border-payments-infrastructure-and-asean

Article No.	Article	Comments	Suggested action
33(2)	(a) Vietnamese individuals, Vietnamese organizations and enterprises, and foreign individuals, organizations and enterprises operating in Vietnam have the following responsibilities: Provide, share, synchronize, and update data for the National synthesis database according to the provisions of Article 15 of this Law upon written request from the National data center; (b) The State ensures necessary conditions to receive data provided by organisations and individuals according to the provisions of Article 15 of this Law.	Further to the comments made in respect of Article 15(5), FIs and other businesses may be concerned that potentially sensitive data requested by one state agency may be shared with other agencies, but this provision seems to extend that risk by suggesting that information can be sought for uploading to the national general database. This would raise more concern of data leaks.	We urge the MPS to ensure that the powers of state agencies to request and upload data relating to private organisations is kept to the bare minimum for the sake of confidentiality and preserving business secrets. We suggest that the MPS clarifies the scope of these powers in the Draft Data Law to remove ambiguity.

Article No.	Article	Comments	Suggested action
47(1)	(a) Conditions applicable to organizations providing data intermediary products and services, and data analysis and compilation services is a public professional unit or enterprise established or registered to operate in Vietnam in accordance with the law, meets the conditions for providing services and is licensed to provide services according to the provisions of this Law; (b) …	The "data synthesizing products and services" referred in Article 50(1), 50(2) and 24(5) is too broad and may cover entities that are already licensed by other regulators. It may also capture AI and generative AI products and services. To the extent that is correct, the localisation and licensing requirements could materially limit the deployment capability of international FIs and other businesses, if these activities are open to them. International FIs will need to understand more about the requirements envisaged in this provision. In particular, we note that similar registration requirements in Mainland China, for example, under the Interim Administrative Measures for Generative Artificial Intelligence Services only apply to "public-facing" products and services. The rationale for this is understood to involve the authorities' desire not to stifle innovation with a heavy compliance burden on AI developers.	Industry recommends that the MPS narrows down the scope of data products and services and limit it to the most risky types of products and services. The requirements may be duplicative for firms that are already licensed other sectoral regulations. For example, financial services firms operating in Vietnam that are already subject to the regulation and oversight of the State Bank of Vietnam should be excluded from the scope of sections 47, 48 and all other applicable sections relating to the provision of data products and services, or it should be clear than compliance with such sectorial regulations prevails. We recommend that any localisation, registration and licensing requirements for AI (and generative AI) products and services are limited to public-facing products and services, to similarly encourage innovation in Vietnam. We also recommend that the MPS clarifies the scope of these activities and whether they are open to foreign organisations providing the services. In addition, we request MPS to provide more implementation rules and/guidance on the process of obtaining a licence as soon as possible, given the current desire within the financial services industry to rollout AI tools.

Article No.	Article	Comments	Suggested action
47(2)	Conditions on personnel (a) The head of the organisation, the legal representative of the enterprise is a Vietnamese citizen, permanently residing in Vietnam; (a) The organization or enterprise must have personnel with a university degree or higher majoring in information security or information technology or electronics and telecommunications who are responsible for providing services, system administration, and system operation, ensuring system information security.	*Head of organisation* This requirement for a local head of an organisation involved in data analysing and synthesizing seems more appropriate for foreign direct investment legislation than a data law. *Personnel* We are cautious about being so prescriptive on qualifications for personnel in mandatory rules such as the Draft Data Law, as opposed to recommendatory standards, because it then limits the pool of potential candidates in a manner not necessarily relevant to the commercial objectives of private organisations.	We suggest that the MPS reconsider the appropriateness of these requirements in the context encouraging digital innovation, in particularly as it could limit the growth of services available to or developed by FIs operating in Vietnam.

Article No.	Article	Comments	Suggested action
47(3)	Conditions on physical facilities, technical equipment, service provision management process and plans to ensure security and order Organizations and enterprises applying for a certificate must have a service provision plan including the following contents: Service provision plan and process, including information technology system explanation; explanation of technical plans for technological solutions; storage plan, ensuring data integrity, ensuring information security of the service provision system; plans to protect personal and organizational data; plan to ensure security and order; fire prevention and fighting plans, disaster prevention and ensuring stable and smooth operation of services; technical equipment must be located in Vietnam and be inspected for information security and safety according to the provisions of law.	The localisation requirement under this Article appears to preclude international FIs deploying AI/generative AI and other data analysis and synthesizing tools hosted on regional or global IT infrastructure outside of Vietnam. This could limit the availability of internationally developed tools to the detriment of the relevant international FI and its Vietnamese stakeholders.	We would like to reiterate that the requirements may be duplicative for organisations that are already licensed under sectoral regulations. For example, financial services firms operating in Vietnam that are already subject to the regulation and oversight of the State Bank of Vietnam should be excluded from the scope of sections 47, 48 and all other applicable sections relating to the provision of data products and services. Hence, we recommend that the MPS narrows down the scope of data products and services and limit it to the types of products and services that carry the most risk. We strongly suggest that the MPS clarifies the intention of this localisation requirement and confirms the scope of its application, particularly in the context of international FIs and other multinational businesses.
47(4)	The Government regulates this Article in detail.	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them relating to the relevant

Article No.	Article	Comments	Suggested action
		other requirements applicable to them as early as possible, to allow for efficient compliance within the existing multi-market set of policies and practices.	products and services, if any.
50(2)	Organizations providing products and services for analyzing and compiling data related to the application of technology in data processing specified in Clause 5, Article 24 of this Law must be registered and licensed according to the provisions of this Law.	This Article 50(2) appears broad enough to capture AI and generative AI products and services. To the extent that is correct, international FIs will need to understand more about the registration and licensing procedures envisaged in this provision. In particular, we note that similar registration requirements in Mainland China, for example, under the Interim Administrative Measures for Generative Artificial Intelligence Services only apply to "public-facing" products and services. The rationale for this is understood to involve the authorities' desire not to stifle innovation with a heavy compliance burden on AI developers.	As in our suggestions in respect of Article 47(1)(a), we recommend that any registration and licensing requirements for AI (and generative AI) products and services are limited to public-facing products and services, to similarly encourage innovation in Vietnam. Financial institutions and other businesses would also benefit from more clarity on whether the Vietnamese authorities envisage that there will be algorithmic recommendation, data synthesis or separate AI/generative AI assessment requirements like in Mainland China. Understanding the degree of harmonisation (or lack of it) across markets is important for effective compliance by international FIs.
52(4)	Comply with service provision plans and procedures that have been appraised by the Ministry of Public Security.	This Article suggests that all organisations involved in data analysis and synthesis need to have their service delivery plans approved by the MPS. Presumably this is intended to be a corollary to the registration and licensing process mentioned in Article 50(2). Financial institutions will need to understand this better to prepare for compliant operationalisation.	We suggest that the MPS provides more implementation rules and/or guidance on the nature and process for this appraisal by it, well in advance of the effectiveness of the relevant provisions of the Draft Data Law to allow FIs and other businesses to adjust operations as needed.
52(5)	Submit six-month and annual or ad hoc	This Article suggests that all organisations involved in	We suggest that the MPS consider the

Article No.	Article	Comments	Suggested action
	reports on activities to the Ministry of Public Security upon request.	data analysis and synthesis have to submit periodic and, upon request, *ad hoc* activity reports to the MPS. If correct, this could potentially be a large burden in addition to other compliance and reporting requirements.	purpose of this reporting requirement and whether it can be modified to apply only to private organisations where there is a risk to data security or, possibly, other material changes in circumstances.
52(6)	The Government shall regulate this Article in detail.	We appreciate that the Draft Data Law is a framework law that requires more detailed implementing rules and/or guidelines. What is crucial for international FIs – in particular as typically complex, regulated businesses – is having certainty of the obligations and other requirements applicable to them as early as possible to allow for efficient compliance within the existing multi-market set of policies and practices.	We suggest that the MPS provides a definitive timetable for release of the relevant implementing rules and/or guidelines to allow FIs and other businesses to operationalise the requirements on them relating to the relevant products and services, if any.
55(2)	The Ministry of Public Security is the focal agency responsible to the Government for presiding over coordination with ministries and ministerial-level agencies to perform state management of data.	As mentioned in our comments in respect of Article 9(3) above, our members have experience in other markets – particularly Mainland China which would seem to have been a point of reference for some provisions in the Draft Data Law – where multiple government authorities are involved in the shaping of data laws. Where national/public security authorities lead the process of shaping these laws, our experience is that there can be an inherent challenge to find a sustainable balance between security and economic considerations. See also the footnote in our comments in respect of Article 9(3) above.	Our members would be happy to be consulted by the MPS and/or its counterparts regulating financial services, in respect of their experience in other markets and how alignment among authorities is key to creating more acceptable outcomes for businesses that seek to service Vietnamese stakeholders.
66	This Law takes effect from January 1, 2026.	We note that no timetable is stated for the effectiveness of the Draft Data Law if there are	We suggest that the period should be at least 18 months from finalising the form of the Draft

Article No.	Article	Comments	Suggested action
	This Law was passed by the 15th National Assembly of the Socialist Republic of Vietnam, 9th session, on June 2025.	revisions following this consultation process.	Data Law. If, for any reason, relevant sectoral and other implementation rules and/or guidance cannot take effect at the same time as the Draft Data Law, we suggest an implementation period of 24 months after the sectoral rules are finalised, to enable FIs to fully understand the implications and formulate and implement the necessary compliance measures.