

Asia Internet Coalition (AIC) Industry Feedback on Vietnam Draft Personal Data Protection (PDP) Law

22 November 2024

To:

Senior Lieutenant General Luong Tam Quang,
Minister of Public Security, Government of Vietnam

Cc:

Lieutenant General Nguyen Minh Chinh, Director General of the Department of Cybersecurity & High-Tech Crime Prevention, Government of Vietnam

The [Asia Internet Coalition \(AIC\)](#) and its members express our sincere gratitude to the Ministry of Public Security (MPS) for the opportunity to submit comments on the [Vietnam's Draft Personal Data Protection \(PDP\) Law](#). The AIC is an industry association of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region.

We appreciate MPS for exploring avenues to proactively address new issues regarding personal data protection and welcome the opportunity to contribute to the development of Vietnam's data protection framework.

While we support these efforts, we also wish to express our recommendations about some of the requirements proposed. As such, **please find enclosed to this letter detailed comments and recommendations in Annex A**, which we would like MPS to consider when preparing the Personal Data Protection Law.

Summary of key issues:

- 1. Definitions:** The definition of "basic personal data" should be exhaustive to avoid regulatory uncertainty, and the concept of "sensitive personal data" should either be removed or defined in a closed manner, focusing on actual risks. Cross-border data transfers should be limited to data exchanged between legal entities across jurisdictions, while "de-identification" should adopt a flexible, reasonableness-based standard to allow for evolving technologies. Behavioral advertising should be clearly distinguished from marketing in data use definitions to avoid confusion. Cloud service providers should not be required to proactively monitor data compliance due to technical and resource limitations. Finally, the roles of external personal data protection organizations and credit ranking agencies should be clarified to ensure their feasibility and effectiveness in practice.
- 2. Cross-Border Data Transfers:** The draft PDP Law's provisions on cross-border data transfers are overly broad, impractical, and misaligned with internationally recognized frameworks like the GDPR, Singapore's PDPA, and ASEAN MCC. Article 45(1) defines data transfers abroad in an unworkably expansive way, while Articles 33(1) and 45(g) impose a restrictive consent requirement, limiting flexibility for businesses. Additionally, Article 45(9), allowing the government to suspend transfers based on undefined national interest violations, creates significant legal uncertainty. To foster responsible data transfers while supporting Vietnam's integration into the global digital economy, the law should provide a range of interoperable legal bases for transfers, including adequacy determinations, contractual necessity, public interest, and recognition of multilateral frameworks like Global CBPRs. Vietnam should also align with global standards like EU SCCs and ASEAN MCCs, ensuring clarity by limiting transfer definitions to cases involving changes in data controllers or processors. Robust consultation with stakeholders is critical to developing technically feasible, scalable, and widely accepted mechanisms.
- 3. Data Subject Rights:** The draft PDP Law's requirement to fulfill data subject rights within 72 hours is impractical and not aligned with international standards. Deleting data, for example, is a complex process that requires identifying all relevant data points, balancing user rights,

ensuring sufficient processing power, and managing potential human error. Thus, the law should be amended to require responses to data subject requests "as soon as reasonably possible" or "without undue delay" rather than adhering to rigid 72-hour timelines.

Furthermore, the draft lacks exceptions to the provision of data subject rights, which are common in global privacy frameworks. It is recommended that the law include exceptions for requests that are manifestly unfounded, excessive, repetitive, technically infeasible, or would infringe on commercial or trade secrets, and allow refusal if requests interfere with legal obligations, law enforcement, or system integrity. These exceptions would ensure that organizations can manage requests effectively and prevent abuse of the law.

4. **Right to Consent:** We recommend deleting the requirement for consent as a data subject right in Vietnam's Draft Law on Personal Data Protection, as it is inconsistent with international frameworks and poses practical challenges. Requiring consent for all personal data processing activities is not always feasible or appropriate, particularly in scenarios like fraud detection, where obtaining consent from a malicious actor is impractical. Moreover, overreliance on consent risks creating consent fatigue, where frequent or lengthy consent requests overwhelm users and lead to disengagement, ultimately undermining data protection. Globally, jurisdictions like Australia have recognized that excessive reliance on consent places an unrealistic burden on individuals to navigate complex data practices, often without improving privacy outcomes. To align with international best practices, the law should allow organizations to use other legal bases for processing personal data, such as legitimate interests or compliance with legal obligations, to ensure practical and effective data governance.
5. **Over-reliance on consent:** The draft PDP Law's reliance on consent as the primary legal basis for all personal data processing is problematic from both business and privacy perspectives. Over-reliance on consent risks "consent fatigue," reducing users' engagement and undermining privacy protections. Consent is not always practical or feasible, especially for critical activities like fraud prevention, law enforcement cooperation, or everyday digital interactions like social media posting. Robust data protection laws, such as the GDPR and Singapore's PDPA, offer multiple legal bases for processing personal data, balancing user rights with operational needs. The draft law should follow this approach, including bases like contractual necessity, compliance with legal obligations, legitimate interests, public interest tasks, and vital interests, to support both privacy and innovation.
6. **Processing of children's personal data:** Ensuring age-appropriate experiences and privacy for young users is vital, but online age determination remains an industry-wide challenge with no foolproof method. To address this, the term "age verification" should be replaced with "age assurance," emphasizing privacy-friendly solutions without excessive data collection. Additionally, requiring parental consent for data processing should apply only to children under 13, aligning with international standards. Provisions such as subsection (4)(c), which vaguely addresses processing affecting children's legitimate rights, risk over-enforcement and should be removed.

We are grateful to MPS for upholding a transparent, multi-stakeholder approach and further welcome the opportunity to offer our inputs and insights, directly through industry meetings and participating in the official consultations / workshops. Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you.

Sincerely,

Secretariat
Asia Internet Coalition (AIC)

Annex A: Detailed Comments and Recommendations

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
Interpretation of Terms Article 2	Key definitions in the draft Law are as below: 1. Basic personal data is basic information of citizens or other information that is not sensitive personal data associated with the identity of citizens, including... Other information associated with the identity of the citizen other than the provisions of 4 of this Article. 2. Sensitive personal data means information that, when infringed, will directly affect the legitimate rights and interests of organizations and individuals, associated with the privacy of individuals, including... Other personal data prescribed by law is specific and requires necessary security measures.	Basic Personal Data (BPD): The definition of “basic personal data” is open-ended. It should be exhaustive. Alternatively, the language in the Draft Law should replace the phrase “associated with the identity of the citizen” with the phrase <i>“that is linked or reasonably linkable to an identified or identifiable natural person.”</i> - The definition of BPD should contain an exhaustive list. This is because any change in the categories of data that are basic personal data would require a widespread reconsideration of the basis for processing data. This would lead to uncertainty for businesses, significant compliance costs, an increased cost of doing business, and ultimately lower market competitiveness. Open lists give open-ended powers to regulators to add BPD types without meaningful consultation, economic modeling, and fair compliance runways. An open list is also disadvantageous to data subjects who look to data privacy legislation to be educated on, understand, and manage their privacy rights. - Personal data protection laws must make clear that they are limited to data that can reasonably be linked to	Recommendation: On Basic personal data - Option 1: The definition of “basic personal data” should be exhaustive or closed rather than open-ended (Article 2(3)(l)) - Option 2: Replace the phrase “associated with the identity of the citizen” with the phrase <i>“that is linked or reasonably linkable to an identified or identifiable natural person.”</i> On Sensitive Personal Data - Option 1: Remove the category of Sensitive Personal Data - Option 2: The definition of “sensitive personal data” should be <i>exhausted/closed and limited to Personal Data.</i> “Overseas transfer of personal data” should be defined as <i>“the transfer of personal data between two legal entities, in which one is located in a jurisdiction outside of Vietnam.”</i> “De-identification of personal data” should be non-prescriptive on how to perform the action. It should establish “reasonableness” as the standard for

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	3. Overseas transfer of personal data means the use of cyberspace, equipment, electronic means or other forms of transfer of personal data of Vietnamese citizens from a Data Controller or Data Processor to another Data Controller or Data Processor based in a jurisdiction other than Vietnam to a location outside the territory of the Socialist Republic of Vietnam or the use of a location outside the territory of the Socialist Republic of Vietnam for the processing of personal data. 4. De-identification of personal data means altering data relating to a data subject through the use of reasonable and available technical means the process of anonymizing or removing identifiable contents or replacing them with other imaginary names or codes to create new data so that such data cannot reasonably identify a specific individual. 5. Use of personal data for marketing means activities related to calling,	an identified or identifiable individual or natural person. Classifying all “basic information” or “other information” “associated with the identity of citizens” as personal data can lead to overregulation where there are unnecessary restrictions on data processing that doesn’t actually pose risks to individual privacy. This could create barriers to innovation and pose extremely burdensome – if not technically infeasible – compliance challenges for organizations. Sensitive Personal Data (SPD): The definition of “sensitive personal data” is very broad and open-ended, when it should be closed/exhaustive. “Information” is not limited to Personal Data. - It is important to note that not all data protection laws include a concept of sensitive personal data. - For example, Singapore’s, Hong Kong’s, and New Zealand’s long-standing privacy laws do not include this concept. India’s newly-enacted Digital Personal Data Protection (DPDP) Law deliberately doesn’t recognize the concept of sensitive personal data. - There is good reason for this. Removing the concept of sensitive personal data from a data protection law can be beneficial for several reasons: - Recognition that data use—not data type—matters: What can give rise to privacy risks is not merely what a data type is, but how it is used. Privacy laws that deem certain data types inherently	determining effective deidentification within the definition. Please also confirm that the processing of encrypted or hashed data is not considered personal data processing. “Use of personal data for marketing” should exclude “Use of personal data for behavioral advertising or with specific objectives” from its definition. “Use of personal data for behavioral advertising or with specific objectives” should exclude “Use of personal data for marketing” from its definition. On Personal Data Protection We seek clarification: To clarify if this requires organizations to actively undertake measures to proactively detect / prevent violations of personal data laws. Cloud service providers does not have access to customers’ content and cannot undertake such measures proactively. We suggest deletion of such wording on the basis this will be very onerous for online service providers to comply with (given the multi-faceted nature of such services and constant information flows between end-users and the online services). Implementing effective monitoring and

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	sending emails, messages, letters or other marketing information to consumers through the customer's personal data previously collected. Use of personal data for marketing does not include the use of personal data for behavioral advertising or with specific objectives. 6. Use of personal data for behavioral advertising or with specific objectives, namely the use of personal data of customers or behavioral data of customers for targeted advertising. Use of personal data for behavioral advertising or with specific objectives does not include the use of personal data for marketing. 7. <i>Personal Data Protection</i> means activities of propagating, guiding, ensuring, managing, operating, protecting, detecting, preventing and handling acts of violating the provisions of law on personal data protection.	sensitive fail to recognize this reality; they impose blanket prohibitions on any uses of certain data types, even when only certain uses of those data types may actually pose privacy risks. 2) Simplicity: Removing the concept of sensitive personal data simplifies the regulatory framework – making it easier for businesses to understand and comply with the law, and for governments who must enforce the law. 3) Flexibility and Support for Emerging Technologies: Emerging technologies such as artificial intelligence, machine learning, and Internet of Things (IoT) often rely on diverse datasets to deliver innovative solutions and services. Removing barriers to accessing and utilizing various types of data can accelerate the adoption and integration of these technologies into business operations and industry sectors. This will be beneficial for businesses of all sizes, especially SMEs and startups. 4) Strengthened Competitive Position: Businesses operating in jurisdictions with more flexible data protection laws may gain a competitive advantage over those facing regulatory complex regimes	enforcement mechanisms across the entire range of online services and customer use cases would be technically challenging and resource-intensive – instead, having a mechanism to reactively respond to known or reported issues would more effectively balance data privacy concerns whilst preserving the core functionality of the online services. ● On Developer involved in personal data protection ○ We suggest that this is removed. ● On Business services of Personal Data Protection Organisation means ○ We seek clarification: Does this mean that organisations can now appoint these external entities to act as data protection departments rather than employees? (Ref. Art 48 - 49) Other than law firms, which other companies does MPS foresee being able to provide these services? Auditors? ○ Recommendation: Change “technological and legal capacity” to “technological <u>or</u> legal capacity”. Article 36 suggests that the draft envisions there being personal data protection organizations that have either only legal or only technological capacities. (Ref. Art 36 – 37) ● On Organisation providing credit ranking service on personal data protection ○ We seek clarification: How will the ‘credit rating agency’ differ from the ‘certification

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	8. <i>Developer involved in personal data protection</i> means an individual or organisation involved in the development of programmes, applications, software, and information technology systems that collect, process, and store personal data. 9. <i>Business services of Personal Data Protection Organisation</i> means the provision of business services of personal data protection organisation by an organisation, enterprise with technological and legal capacity in personal data protection in order to meet the needs of the Data Controller, Data Controlling and Processing Entity, Third Party, Cross-Border Data Transferor, Cross-Border Data Recipient of a Vietnamese citizen. 10. <i>Organisation providing credit ranking service on personal data protection</i> means an organisation certified or authorised by the Specialised Personal Data Protection Authority and is capable of assessing,	with challenging implementation requirements. This advantage can stem from greater agility to respond to market demands, faster time-to-market for new products and services, and the ability to leverage data insights more effectively to meet customer needs and preferences. A more flexible data protection regime can also attract greater foreign direct investment (FDI), and lead to job creation and growth of the local economy. - That said, a majority of privacy laws do establish SPD. If Vietnam were to similarly take this approach, we recommend following these principles: (i) The definition of “sensitive categories of data” should focus on whether a data point is actually used to identify something sensitive about someone, not whether there is merely any theoretical possibility that the data point could be combined with any other data points to reveal such information. - If SPD were broadly defined as any personal data that could theoretically be combined with any other personal data points to reveal something sensitive about someone, then all personal data would be sensitive. To avoid this outcome, laws and implementing regulations should focus on whether a	organization’? The certifying organization will already need to review the credential of organizations applying to be ‘personal data protection organization / expert’ service providers. - Which type of companies does MPS foresee being able to provide these services? Auditors (e.g. EY/KPMG)? (Ref Art 41) Recommendation: For the identity of the ‘Specialised Personal Data Protection Authority’ to be defined. On Automated personal data processing means Recommendation: This definition should be revised to cohere with existing standards of automated profiling by including the nuance “without human intervention”.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	inspecting, confirming, and ranking the level of credibility in personal data protection. 11. <i>Automated personal data processing means</i> a type of personal data processing in which an electronic device assesses, analyses and predicts activities of a specific person, such as habit, interest, level of trust, behaviour, location, tendency, capability and other cases.	controller actually uses a data point to reveal someone’s membership in a protected group or possession of a sensitive trait. ■ Such a risk-based approach allows for more flexibility and adaptability in addressing data protection challenges in a rapidly evolving digital landscape. A flexible approach will allow business to innovate and develop new products and services, which will fuel economic growth and global competitiveness. (ii) SPD provisions should contain an exhaustive list of sensitive classes and traits. Statutory lists should be exhaustive because: ■ Any change in the categories of data that are sensitive personal data would require a widespread reconsideration of the basis for processing data. This would lead to uncertainty for businesses, significant compliance costs, an increased cost of doing business, and ultimately lower market competitiveness. ■ Open lists give open-ended powers to regulators to add SPD types without meaningful consultation, economic modeling, and fair compliance runways. ■ An open list is also disadvantageous to data subjects who look to data privacy legislation to be educated on,	

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
		understand, and manage their privacy rights. ■ SPD provisions' most important contribution to privacy laws is guarding against downstream discrimination. Exactly what classes and traits are listed may vary slightly between jurisdictions, as the historical contours of discrimination vary between cultures. ■ That said, laws should generally not include classes or traits beyond the following: race; ethnicity; criminal record; religious, philosophical, or political opinions; health conditions or diagnoses; sex life or sexual orientation; citizenship; and gender identity beyond cisgender Cross-border data transfers: <i>“Overseas transfer of personal data”</i> - Is currently defined as a physical transfer of data. ● The global internet is built on the principle of cross-border data flows. Cross-border data flows are beneficial for economic growth, data privacy, and cybersecurity. They underpin innovation, research and development across multiple sectors; support international cooperation; and enable us to stay emotionally and socially connected to one another. However, 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 legal entities, in which at least one is based in a</i>	

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
		<i>different jurisdiction, which are therefore subject to different laws.</i> This definition aligns with globally recognized frameworks such as EU’s GDPR (see Guidelines 05/2021 by the European Data Protection Board), 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 including those which are wholly domestic and there is no change in data controller or data processor. Indeed, cross-border data flows are technically necessary for the internet to function, beneficial for economic growth, enable local businesses to access state-of-the-art services from around the world, promote best practices for data security, and allow millions of people to keep in touch with friends and family who live all over the world. De-identification: De-identification should be non-prescriptive on how to perform the action. It should establish “reasonableness” as the standard for determining effective deidentification within the definition (taken from the Virginia Consumer Data Protection Act).	

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
		- Laws and regulators should adopt a flexible and pragmatic approach for determining whether data have been deidentified. They must also recognize that deidentification is not a purely technical question, and assessing it should be a holistic exercise taking into account both what technical measures—such as Privacy Enhancing Technologies (PETs)—have been applied and what non-technical measures—such as access controls, policies, procedures, and legal mechanisms—have been adopted. - This is why regulations should establish “reasonableness” as the standard for determining whether an organization has anonymized data. Such determinations should not require companies to irrefutably prove with numerical evidence that they have achieved de-identification through burdensome documentation like impact assessments. Rather, companies should be able to demonstrate compliance based on reasonable efforts to use PETs and other measures, including non-technical ones, consistent with industry best practices. Lastly, the definition of de identification should be non-prescriptive in order to allow for the evolution of updated technologies and strategies used for the process of de-identification. Use of personal data for marketing: Should exclude “Use of personal data for behavioral advertising or with specific objectives” from its definition. - This is to ensure there is no confusion in their	

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
		interpretation. Use of personal data for behavioral advertising or with specific objectives: Should exclude “Use of personal data for marketing” from its definition. • This is to ensure there is no confusion in their interpretation. Developer involved in personal data protection • “Developer” is only used once in the entire draft. In any event, this concept would be more relevant to the development of new technology in general rather than just personal data. (ref: Art 28.5)	
Prohibition of sale and purchase of data Article 3	1. Personal data may not be bought or sold in any form.	• This vague, wide-ranging provision would prohibit a wide range of standard commercial activities, such as when necessary for purposes of providing a product or service requested by the consumer, when the customer has consented to the sale and purchase of their personal data, or when it involves the disclosure of information that the consumer intentionally made available to the general public. • This provision would also take choice away from consumers who do consent if the purchase and sale of personal data is necessary for the provision of requested services. • Furthermore, it is unclear how this Article interacts with	Recommendation: • Remove Article 3(1).

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
		(Article 33(2)), which imposes a consent requirement for the “purchase and sale of personal data.”	
Article 5.2	To build and organise the implementation of strategies, policies, programmes and plans on personal data protection.		Recommendation: This should be done in an iterative manner, in consultation with the industry. This will increase the chance of successful implementation across the industry and avoid unintended consequences that the regulator may have inadvertently overlooked (i.e. a one-size-fits-all approach incompatible with the diverse and rapidly-evolving digital landscape.).
Prohibited acts Article 8	1. Processing personal data in contravention of the law on personal data protection. 2. Processing personal data to create information and data against the State of the Socialist Republic of Vietnam. 3. Processing personal data to create information and data that affect national security, social order and safety, lawful rights and interests of other organizations and individuals. 4. Obstructing the personal data protection activities of competent authorities.	- Articles 8(2) & 8(3) provide a vague and wide range of prohibited acts of personal data processing. The lack of clarity is such that businesses would have no certainty as to whether certain data processing activities would be considered in violation of these provisions. This uncertainty would make compliance efforts extremely challenging, and businesses would operate in an environment which would be viewed as unpredictable, and thus leading to views that the business environment in Vietnam is unnecessarily burdensome. - In addition, it could be interpreted in ways that negatively impact data processing activities through unfair and non-transparent regulatory targeting and enforcement. - Whether or not a service provider is ‘suitable’ for a specific purpose should be assessed by the data controller depending on the use case. But if the service provider turns out to be ‘unsuitable’, it would be unreasonable to penalise the data controller. The	Recommendation: - Remove Articles 8(2) & 8(3). - Article 8.7 on restrictions on data transfers should be removed.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	5. Taking advantage of personal data protection activities to violate the law. 6. Illegally collecting, processing and transferring personal data and trading personal data. 7. Transferring personal data to organizations and individuals inconsistent with the purpose of data processing.	preceding articles would already capture data transfers that are not authorized by the data subject or that are not allowed.	
Data Subject Rights Articles 9, 11, 12, 13, 14, 15, 16	Data subject rights include: • Right to know • Right to consent • Access • Right to withdraw consent • Right to data erasure • Right to restriction of data processing • Right to provide data • Right to object to data processing • Right to complain and denounce • Right to self-protection	This section provides technically infeasible timelines for compliance - 72 hours. • The existing requirement to fulfill data subject right requests within 72 hours of receipt is technically infeasible and not aligned with international standards. For example, the data deletion process is technically challenging and time-consuming as it includes: accurately identifying all of a data subject's data and relevant dependencies; balancing user rights; ensuring sufficient processing power (machine and manual); and accounting for and rectifying unintentional internal human error during the deletion process. The processing power to enact a single account deletion can be significant, and, in certain instances, may	Recommendation: • Data subject rights timelines should be changed to "as soon as reasonably possible" or "without undue delay." • Data subject rights should include standard exceptions, and should include the following: ○ if the request is manifestly unfounded, excessive, repetitive, frivolous, technically infeasible, or would infringe on commercial or trade secrets; ○ if the request would compromise the legal rights, security, or integrity of other people or businesses; ○ if the request interferes with the exercise or defense of legal claims, or compliance with a legal obligation; ○ if it would interfere with law enforcement, judicial proceeding, or investigations; ○ if it would undermine the controller's efforts to guard

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
		involve deleting millions of data points, intersecting across data subjects and applications. Therefore, the prescriptive timelines for data controllers to respond to data subjects' requests should be removed and replaced with an obligation to respond “as soon as reasonably possible” or “promptly” to recognise that different cases require different response times, depending on the complexity of the request, while still ensuring the organizations prioritize such requests. The draft Law lacks standard exceptions to the provision of data subject rights. It is a globally-recognized principle that people should have certain rights with respect to their personal data. However, when it comes to implementation, practicality and feasibility must also be considered. User rights must therefore strike a balance between giving people meaningful control over their data, while also recognizing pragmatic exceptions. With this in mind, best practice internationally includes clear and reasonable limitations on user rights, including: technical feasibility; if allowing access to the data would reveal confidential commercial information;	against, detect, or investigate malicious, unlawful, or fraudulent activity, or enforce contracts to which it is a party; - if it would require re-identifying or otherwise linking data that is not considered personal data; - if it would compromise the controller’s efforts to maintain the function and health of the service; - if the data cannot be made human readable; or - if the personal data has been de-identified.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
		if the information could reasonably interfere with the rights of others; and if the requests are repetitious, systematic, frivolous or vexatious in nature. Controllers should also have a right to refuse to facilitate the exercise of a data subject right if the request is “manifestly unfounded, excessive, repetitive, technically infeasible, or would infringe on commercial or trade secrets.” This exception is recognized in exceptions under recognized privacy legislation in California and Virginia in the United States. Such exceptions would prevent individuals from abusing the law to harass an organization and disrupt its operations, would reflect the reality that it is not always possible to fulfill some requests due to technical limitations (such as personal data which has been deleted or encrypted), and would reflect the reality that companies may not necessarily have access to particular forms of data (such as data that is only created and used in real time or data that is solely collected and stored on user devices).	
Right to consent (Article 9(2))	2. Right to consent The data subject may or may not consent to the processing of his/her personal data, unless otherwise provided for by law.	<i>We recommend deleting the right to consent. This data subject right is not aligned with international standards or frameworks, and it seems to imply that consent is required for all personal data processing activities. This is concerning because</i>	Recommendation: Remove Article 9(2).

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
		<i>obtaining consent is not always practical or feasible for each purpose of data processing.</i> ○ An example of this is data processing for purposes of fraud detection. In this example, it is not reasonable to expect a data subject (who is, for example, a malicious, fraudulent individual) to provide consent for the processing of his or her data, if the objective of the organization is to prevent or detect the fraudulent activity). In this instance, another legal basis for processing personal data should be available for the organization, and consent should not be required. ● Requiring consent for all personal data processing activities can also lead to <i>consent fatigue</i> where – either through length or frequency – the demand of users becomes too onerous and causes them to disengage. This risks undermining data protections for individuals. ○ In their recent Review of the Australian Privacy Act, the Australian Government observed that <i>“an over-reliance on notice and consent can place an unrealistic burden on individuals to understand the risks of complicated information handling practices and may not result in improved privacy outcomes.”</i>	

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
		- An overreliance on consent can significantly impede the processing required for data-reliant companies to provide services. - Privacy laws should therefore not require consent for all data processing activities, and <i>allow organizations to choose from several equally-valid legal bases for processing personal data.</i>	
Article 9.6.b	Restriction of data processing shall be implemented within 72 hours after receiving a request of the data subject, and all personal data that the data subject requests shall then be restricted, unless otherwise prescribed by law.	A 72-hour deadline <u>after a data subject's request is improbable</u> given that companies will require further verification of the requestor and additional information to fully understand the context of the request before carrying it out. This verification and clarification process will already take longer than 3 days. In addition, for security reasons access to systems that store personal data cannot be granted to a wide pool of people so any changes must necessarily go through strict review and approvals which will require additional time.	Recommendation: This should be extended to 'within a reasonable period' instead of a prescriptive deadline. Or that the obligation is imposed <u>on data controllers</u> to respond to such requests <u>within one month</u>. Please note that the proposed timeline of one month is consistent with existing international standards such as the GDPR.
Right to object to data processing Article 9(8)	The data subject may object to the Personal Data Controller, the Personal Data Controller and the Processing Party to process his/her personal data in order to prevent or restrict the disclosure of	This right could potentially unreasonably prohibit the ability of organizations to serve personalized ads. Giving data subjects the right to object to the use of their personal data for marketing purposes would often mean forcing organizations to provide their services for	Recommendation: Remove Article 9(8).

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	personal data or use it for advertising or marketing purposes;	free and/or at a loss. Any individuals that do not find any form of the service valuable have the choice to delete their accounts or otherwise abstain from the service. This is fundamentally at odds with the economic systems adopted in many countries. It would significantly disincentivize innovation and investment in a variety of sectors, leading to fewer jobs and economic opportunities on which economies—particularly developing ones—depend.	
Article 9.8.c	The Personal Data Controller and Personal Data Controller and Processor shall comply with the request of the data subject within 72 hours after receiving the request, unless otherwise prescribed by law.	A 72-hour deadline <u>after a data subject's request</u> is <u>improbable</u> given that companies will require further verification of the requestor and additional information to fully understand the context of the request before carrying it out. This verification and clarification process will already take longer than 3 days. In addition, for security reasons access to systems that store personal data cannot be granted to a wide pool of people so any changes must necessarily go through strict review and approvals which will require additional time.	
Right to complain and denounce Article 9(9)	9. Data subjects have the right to complain, denounce or initiate lawsuits in accordance with the Law on Complaints, the Law on Denunciations and other relevant legal documents.	This provision seems to provide data subjects with a private right of action to claim compensation for damages.	Recommendation: Remove Article 9(9) & 9(10)

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	10. The right to claim compensation for damage in accordance with the provisions of law when a violation of regulations on personal data protection occurs, unless otherwise agreed by the parties or otherwise provided for by law.	It is unclear what is meant by “damage,” and what distinguishes it from a “violation of regulations on personal data protection.” • Providing data subjects with a private right of action will be harmful for innovation, create uncertainty, discourage foreign investment, and inhibit growth in the Vietnamese digital economy. • Internationally, it is not clear whether this right actually protects data subjects or resolves underlying privacy matters. Instead, private rights of action result in vexatious litigation, leading to a significant burden - especially on small and medium businesses - without creating additional privacy protections for people. • Another risk is that private rights of action could lead to inconsistent interpretation of rights and obligations in the courts, which would lead to confusion for companies seeking to comply with the law. • Furthermore, the costs for businesses that have to defend lawsuits that are often frivolous or unwarranted can be daunting for any company, but especially for small businesses. Ultimately, these costs have to be passed down to the consumer and the price for providing services to residents in Vietnam will increase.	
Article 9.10	Right to claim compensation for damages in accordance with law when regulations governing the protection of his/her personal data are violated unless		Clarification: How does MPS propose damages are calculated?

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	otherwise agreed by the parties or otherwise prescribed by law.		
Article 9.11	Right to self-protection The data subject has the right to self-protection in accordance with the provisions of the Civil Code, other relevant laws and this Law, or to request the relevant agencies and organisations take measures to protect his/her civil rights, as specified in Article 11 of the Civil Code.		Clarification: How does MPS envision individuals ‘self-protecting’ against personal data protection infringement?
Article 11	Consent of data subjects		We recommend explicitly stating that consent must be freely given, specific, informed, and unambiguous, as per GDPR requirements. Need to provide more guidance on what constitutes valid consent, especially for children's personal data.
Article 11.1	The data subject’s consent is required for all activities in the processing of personal data, unless otherwise prescribed by law.	Consent in the specific format set out in this draft is not always possible to obtain, and this obligation will likely stymie emergency rescue efforts and the performance of legal obligations as well. We further note that exceptions to consent are also set out in Article 17 of Decree 13.	Recommendation: That lawful bases other than ‘consent’ to be included: ● processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ● processing is necessary for compliance with a legal obligation to which the controller is subject; ● processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
			- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; - processing is necessary for the purposes of the legitimate interests pursued by the controller 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, in particular where the data subject is a child.
Article 11.3	It must not be a condition of compulsory consent to transfer personal data of the data subject to other services for improper purposes. The data subject has the right to reject this condition.		We seek clarification on what is “compulsory consent” (for example, whether no provision of service without consent will be deemed as “compulsory”) and what is “improper purpose”.
Processing of personal data obtained from audio and video recording activities in public places Article 18	1. Government agencies and organizations or those at the direction of the government may record and video record and process personal data obtained from audio and video recording activities in public places for the purpose of protecting national security, social order and safety, legitimate rights and interests of organizations and individuals without the consent of the data subject. unless otherwise provided for by law.	As written, this article could impact a number of everyday activities, such as individuals taking photos or videos in public places. It is nearly impossible for individuals or private organizations to notify each and every individual that may or may not be recorded. The draft Law should clarify that Article 18 only applies to personal data collected by the government or at the direction of the government.	Recommendation: Clarify that Article 18 only applies to personal data collected by the government or at the direction of the government.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	2. In case of audio or video recording as prescribed in Clause 1 of this Article, government agencies and organizations or those at the direction of the government shall have to notify others so that they can understand that they are being recorded, unless otherwise provided for by law.		
Processing of children's personal data Article 20	1. The processing of children's personal data shall always be carried out in accordance with the principle of protection of children's rights and in the best interests of children. 2. Before processing children's personal data, the Personal Data Controller, the Personal Data Processor, the Controller and Processor of Personal Data, and the Third Party must assure verify the age of the child under the age of 13 and obtain the consent of the parent or guardian, except for the cases specified in Article 17 of this Decree as prescribed. 3. Do not process personal data of children without the consent of children aged full 7 years or older and of their parents or guardians, except for the cases specified in Article 17 of this Decree.	Age verification and parental consent requirements Understanding age online is a complex, industry-wide challenge. Protecting our users – particularly young people – is of paramount importance. Moreover, ensuring age-appropriate experiences and robust privacy settings for young users is imperative. However, addressing this challenge requires thoughtful industry-wide solutions that appropriately balance privacy, effectiveness and fairness if we are to meet the needs of parents and teens. No single method of age verification can achieve 100% accuracy; there will always be ways to circumvent even the most robust measures. This is why the term “age verification” should be replaced with “age assurance”, which still requires companies to provide age-appropriate experiences but without compelling additional data collection.	Recommendation: - Replace the term “verify” with “assure”. - Adjust Section (2) to require parental consent for processing data of a child younger than 13 years old. - Remove Section (3), because requiring user and parental consent is both duplicative and onerous for businesses.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	4. Stop processing children's personal data, irretrievable deletion or destruction of children's personal data in the following cases: a) Processing data for improper purposes or having completed the purpose of processing personal data with the consent of the data subject, unless otherwise provided for by law. b) The child's parent or guardian withdraws his/her consent to the processing of the child's personal data, unless otherwise provided for by law. c) At the request of competent functional agencies when there are sufficient grounds to prove that the processing of personal data affects the legitimate rights and interests of children, unless otherwise provided for by law.	Delete subsection (4)(c): It is unclear what is meant by the processing that “affects the legitimate rights and interests of children”, and (c) could lead to potential over-enforcement and investigatory overreach into the practices and data use of Data Controllers and Processors. • All data processing must be in accordance with the best interest of the child, and where such processing is found to be in violation of this principle, would not be allowable under this act. Any violation should be enforced through the enforcement process provided for under the act without separate, potentially arbitrary or inconsistent deletion “at the request of functional agencies”. • It is also not specified which agencies would be allowed to make such requests, broadening the scope of which agencies may try to enforce this provision on data controllers or processors.	
Over-reliance on consent Articles 2, 3(4), 11(1), 11(4), 11(7),	Consent requirement for all personal data processing (11(1)) - Article 3(4) - Consent required for different entities in the same group - The consent of the data subject to a company does	The draft PDP Law uses consent as the primary and default legal bases for all personal data processing activity. This is harmful from a business and privacy perspective. • Consent is not a silver bullet. Laws that rely on legal bases should neither mandate consent nor treat it as the default legal basis for all types of data processing.	Recommendation: • <i>Any comprehensive, robust data protection law should provide a <u>range of legal bases for the collection, use and disclosure of personal data</u>. A range of legal bases is important to ensure that reasonable and expected protection of data subjects can take place, and that data processors</i>

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
11(8), 12, 14, 19, 22, 30 33(2)	not mean consent for all companies in the members of the economic group or corporation to process personal data. - Consent required for third party data collection for advertising purposes (Article 22) - No deemed or implied consent (Article 11(4) & (7)) - Partial consent (undefined): “The data subject may give consent in part or with accompanying conditions” (Article 11(8)) Consent required for establishment of software systems, technical measures or the organization of activities of collection, transfer, purchase and sale of personal data. (Article 33(2)) Consent required for location tracking. Mobile app platforms should inform users “about the use of location data and take measures to prevent the collection of location data by irrelevant organizations and individuals” (Article 30)	Repeated consent requests can lead to “consent fatigue” where – either through length or frequency – the demand of users becomes too onerous and causes them to disengage. This risks undermining data protections for individuals. In their recent Review of the Australian Privacy Act, the Australian Government observed that “<i>an over-reliance on notice and consent can place an unrealistic burden on individuals to understand the risks of complicated information handling practices and may not result in improved privacy outcomes.</i>” Consent is not always practical, feasible or, indeed, expected by people. Some data processing activities can be legitimate in the absence of consent, particularly where it creates community value. For example, fraud prevention, detecting illegal behavior, cooperation with law enforcement, CSAM prevention, or each and every time a person wishes to post to a social media platform, or send an email/message. An overreliance on consent can significantly impede the processing required for data-reliant companies to provide their services. Consent is just one of several tools to underpin and support a balanced data relationship between companies and the user. Providing users with transparency, education and opt-out controls can give them a high level of privacy control without disrupting their browsing experience.	<i>can responsibly process personal data.</i> • This is why a range of legal bases for personal data processing is included in internationally-recognized frameworks such as GDPR and Singapore’s PDPA. ○ <u>The draft PDP Law should include a wide range of legal bases for processing including when:</u> ■ necessary for the performance of a contract between the data subject and the data controller/processor; ■ necessary for compliance with a legal obligation to which the controller is subject; ■ necessary for the purposes of the legitimate interests pursued by the controller 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, in particular where the data subject is a child; ■ necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or ■ necessary in order to protect the vital interests of the data subject or of another natural person.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	No other legal bases for processing personal data. Can be withdrawn (Article 12). Youth data processing must be ceased if parent/guardian revokes consent (Article 2). Consent required for sharing data with other organizations or individuals (Article 14). PD processing of missing or deceased persons must be consented to by parents, spouses, or adult children (Article 19) - except a) To protect the life and health of the data subject or other person in an emergency situation, b) The disclosure of personal data in accordance with law, c) The processing of data by competent state agencies in case of national defense and security emergencies, social order and safety, major disasters or dangerous epidemics; when there is a risk of threatening national security and defense but not to the extent of declaring a state of		

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	emergency; fight riots, terrorism, crime prevention and combat and law violations in accordance with law, d) To perform the obligations under the contract of the data subject with relevant agencies, organizations and individuals in accordance with the provisions of law.		
Social network rules (Article 31)	1. Organizations and individuals providing social network services and communication services provided directly to viewers through cyberspace (OTT) shall: a) Protect personal data of Vietnamese citizens when operating in the Vietnamese market or appearing on mobile application warehouses provided to the Vietnamese market. b) Clearly notify the content of personal data collected when the data subject installs and uses social networks and OTT services. Do not illegally collect personal data and outside the scope of the agreement with the customer. c) It is not allowed to take a photo of a citizen's identity card or identity card as an account authentication factor. d) Provide an option that allows users to	- Organizations may not use a citizen's identity card as a form of account authentication - Requires organizations to provide a "do not track" option or only monitor social networks or services with user consent. It is not clear what is meant by "monitor," which is vague and could be misinterpreted by regulators and organizations seeking to comply. - Requires data subject consent to eavesdrop, record calls, or read text messages. It is unclear what is meant by "eavesdrop," which is vague and could be misinterpreted by regulators and organizations seeking to comply.	Recommendation: - Remove Article 31(1)(c), (d), (dd). - Remove "eavesdropping" from Article 31(1)(g) since it is a vague term and undefined. Amend Article 31(1)(g) so that it does not prevent organizations from responding to lawful government requests for data.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	opt out of the collection of cookies and share cookies. dd) Provide the option of "do not track" or only monitor the use of social networks and OTT services with the consent of the user. e) Notify in detail, clearly and in writing the sharing of personal data as well as the application of security measures when carrying out advertising and marketing activities based on customers' personal data. g) Eavesdropping, eavesdropping or Recording calls and reading text messages without the consent of the data subject is a violation of law. <i>This does not prevent organizations and individuals providing social network services and communication services from responding to lawful governments requests for data.</i> 2. Personal data registered for social network accounts and OTT services is not public data and is not subject to processing without the consent of the data subject.		
Cross-Border Data Transfers	1. Personal Data may be transferred from a Data Controller or Data Processor to another Data Controller or Data Processor	Article 45(1) contains extremely broad examples of what constitutes a transfer of personal data abroad, such as sharing personal data with recipients outside of	Recommendation: - Remove Article (45)(1). - Remove Article (45)(3)(g).

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
Article 45	where at least one of the Controllers or Processors is based in a jurisdiction other than Vietnam in one of the following circumstances: - when the transfer is necessary for: - the provision of services; - the performance of a contract to which the data subject is a party; - the protection of the vital interests of the data subject; - the purposes of the legitimate interests pursued by the controller 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; - the transfer is pursuant to a code of conduct issued by the Regulator or Government; - important reasons of public interest;	Vietnam, sharing personal data at an overseas meeting or conference, sending documents or emails with personal data to recipients outside of Vietnam, and publishing personal data online that is received by persons outside of Vietnam. Such examples are unworkably broad, and are not aligned with internationally recognized frameworks such as GDPR, Singapore's PDPA, and ASEAN MCC's which recognize overseas data transfers as transfers between legal entities in which one is located outside of their respective jurisdiction. - Articles 33(1) & Article 45 (g) impose a consent requirement for the transfer of personal data abroad. Similar to needing a range of legal bases to process personal data, a range of data transfer mechanisms / legal bases for international data transfers is important to ensure that reasonable and expected protection of data subjects can take place, and that organizations can responsibly transfer personal data. - Article 45(9) states that the government may suspend overseas transfers if the transferred personal data is "used in activities that violate the national interests and security of the Socialist Republic of Vietnam." This article is vague and could constitute a number of undefined activities.	- Remove Article 45(9). - Include a <u>range of data transfer mechanisms</u> for international data transfer including: - adequacy determinations, - necessity for the performance of contract, - necessity for the establishment or defense of legal claims, - necessity for the provision of services, - necessity for the protection of the vital interests of the data subject, - necessity for important reasons of public interest, or - any other instrument, treaty or international certification recognized by the Government. Such data transfer mechanisms exist in internationally-recognized frameworks such as EU GDPR, Singapore, Sri Lanka, Malaysia, Thailand, and more. Additionally, Vietnam should consider including the Global Cross Border Privacy Rules (Global CBPR) as a valid mechanism for international data transfers. In today's tech integrated world and because of how the global internet was built and has evolved, the broad types of international data transfers specified by the bill occur as part of almost every online communication or activity (for example, using search engines, chatting with friends, doing online banking or making purchases). Therefore, it's not technically feasible for

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	vii. the establishment, exercise or defense of legal claims; or b. when the transfer is pursuant to: i. data subject consent; ii. an international judicial cooperation required under relevant international obligations; iii. a binding contractual mechanism/agreement or intra-group transfer scheme; iv. any other instrument, treaty or international certification recognized by the Government; or v. if the transferee is accredited under the Global CBPR system. 1. Cases of transfer of personal data abroad: a) Sharing personal data with recipients outside the territory of the Socialist Republic of Vietnam; b) Sharing personal data at an overseas conference, seminar, meeting or discussion;	Lastly, any regulations of cross-border data transfers should recognize a range of legal bases and mechanisms for data transfers that are interoperable and give companies flexibility and scalability, equally valid irrespective of the nature of the data and volume, and inclusive of initiatives for multilateral cross-border data transfers agreements like Global CBPRs. A range of legal bases is important to ensure that reasonable and expected protection of data subjects can take place, that organizations can responsibly transfer personal data, and to ensure that organizations operating in Vietnam can contribute to the global digital economy.	organizations to inform the specialized agencies upon each completion of such types international data transfer. This is why the draft Law should clarify that international data transfers only occur when there is a change in controller or processor rather than any physical movement of data. Vietnam should also recognize widely accepted standard contractual clauses, such as the EU Standard Contractual Clauses (SCC) and ASEAN Model Contractual Clauses (MCC). We strongly recommend Vietnam to carry out thorough and robust consultation with relevant stakeholders prior to the formulation of the standard contractual clauses. This will ensure that the standard contractual clauses will be technically feasible, interoperable, and cognizant of stakeholders needs.

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	c) Sending documents or emails containing personal data to recipients living with recipients outside the territory of the Socialist Republic of Vietnam; d) Publishing personal data in cyberspace that is received by persons outside the territory of the Socialist Republic of Vietnam; dd) Providing personal data to other organizations, enterprises and individuals for the purpose of carrying out business activities; e) Providing personal data on the fulfillment of legal obligations abroad or according to the laws of the host country. 2. An offshore data transferor is an organization or individual that performs the activities specified in Clause 1 of this Article and must make a dossier of impact assessment of the transfer of personal data abroad. 3. A dossier of assessment of the impact of transfer of personal data abroad comprises: a) Information about the type of entities		

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	and contact details of the data transferor and the recipient of receiving personal data of Vietnamese citizens; b) Information about the personal data protection organization and the personal data protection expert; c) Describe and explain the objectives of the personal data processing activities of Vietnamese citizens after they are transferred abroad; d) Describe and clarify the types of personal data transferred abroad; dd) Describe and clearly state the compliance with the personal data protection regulations in this Law, detailing the personal data protection measures applied; e) Assessment of the impact of the processing of personal data; possible unexpected consequences and damages, measures to minimize or eliminate such risks and harms; g) The consent of the data subject as prescribed in Article 11 of this Law on the basis of knowing the mechanism for		

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	Impact assessment / Comments / Rationale	Recommendations
	feedback and complaints when incidents or requests arise; h) There is a document showing the binding and responsibility between organizations and individuals transferring and receiving personal data of Vietnamese citizens for the processing of personal data. 4. The dossier of impact assessment of the transfer of personal data abroad must always be available to serve the inspection and assessment activities of the specialized agency for personal data protection and send 01 original copy to the agency in charge of personal data protection within 60 days from the request to access from the specialized agency date of processing of personal data. 5. The data transferor shall notify the specialized agency for personal data protection of information about the data transfer and contact details of the organization or individual in charge after the data transfer takes place successfully. 6. The agency in charge of personal data protection shall evaluate and request the personal data controller, the personal data controller and processor, and the personal		

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	data processor to complete the dossier of impact assessment of the transfer of personal data abroad in case the dossier is incomplete and in accordance with regulations. 7. The personal data controller, the personal data controller and the personal data processor shall update and supplement the dossier of impact assessment of the transfer of personal data abroad when there is a change in the content of the dossier sent to the specialized agency for personal data protection. 8. Based on the specific situation, the specialized agency in charge of personal data protection shall decide on the inspection and transfer of personal data abroad 01 time per year, except for cases of detecting violations of the provisions of law on personal data protection in this Law or causing incidents of disclosure and loss of personal data of Vietnamese citizens. 9. The specialized agency in charge of personal data protection shall decide to request the suspension of overseas data transfer of organizations, enterprises and individuals when detecting that the		

Topic	Relevant Article / Recommended red-line to the text of the Draft Law	impact assessment / Comments / Rationale	Recommendations
	transferred personal data is used in activities that violate the national interests and security of the Socialist Republic of Vietnam.		