Asia Internet Coalition (AIC) Industry Comments on the Dossier of Application for the Development of the Law on Personal Data Protection

4 April 2024

To
Mr. To Lam, Minister of Public Security (MPS)
Government of Vietnam

Mr. Nguyen Minh Chinh, Director General of the Department of Cyber Security and High-Tech Crime Prevention and Control
Minister of Public Security (MPS)
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 **Dossier of Application for the Development of the Law on Personal Data Protection** (Personal Data Protection 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. Our member companies would like to assure MPS that they will continue to actively contribute to online safety on digital platforms, products and services in support of the digital ecosystem of Vietnam.

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. We hope that the process for stakeholders proves valuable in promoting Vietnam's goals and can become more formal and public soon, such as recent steps that have been elsewhere in ASEAN and across the globe.

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

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,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

Article/Concern	Issues and Recommendations
Definition of Personal Data and scope of a Personal Data Protection Law	The purpose of personal data protection laws is to protect individuals from the harms that arise from potential misuses of their personal data. These risks arise when data can be tied back to or associated with an individual who can be identified. When data cannot be associated with an identifiable individual, then the risk is much lower. A definition of personal data that is too broad will create significant implementation challenges for both government and businesses, and dilute the overall protection of citizens under the law. International principles embedded in show that personal data protection laws (and the definition of personal data) must be limited to data that can reasonably be linked to an identified or identifiable individual, and data protection laws should not expand to cover circumstances where the personal data is already available to the public. This means the definition of personal data should also exclude anonymized or de-identified data. Non-personally identifiable information is important to companies who analyze large amounts of data to improve their products, security, operations, and customer service. Imposing additional protections on this type of data does not significantly benefit individual data protection since it does not identify

Article/Concern	Issues and Recommendations
	the person. In fact, it could restrict the ability of businesses to innovate and compete effectively in the modern, digital economy. **<u>Our recommendation</u>**: We recommend modifying the definition of Personal Data to mean *"any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include anonymised, de-identified data or publicly available information."*
Definition of Sensitive Data	Sensitive personal data (a.k.a. "special categories of personal data" or "SCD") is a subset of personal data that reveals particularly sensitive or private aspects of a person, such as their race, religion or political opinions, and usually other aspects that cannot be changed by a person. SCD provisions are most responsive to concerns over potential discrimination, designed to protect vulnerable individuals. However, the definition of SCD should be very clear. If SCD is 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. Having a precise, *exhaustive* list of the categories of SCD provides greater certainty for those subject to the law. Without such an exhaustive list of the categories of SCD in the Personal Data Protection Law itself, any later addition to or change in the categories of data that are considered sensitive personal data (such as, for example, those that could be made through issuances subsequent to the enactment of a Personal Data Protection Law) would require a widespread reconsideration of the basis for processing SCD, which would generate uncertainty and increased compliance burden for businesses. Having an exhaustive list of the categories of SCD would also be beneficial to data subjects who look to data protection legislation to be educated on, understand, and manage their privacy rights. The definition of "sensitive personal data" is broad and unclear. It is currently defined as "personal data associated with the privacy of an individual that, when… infringed upon, will directly affect the legitimate rights and interests of [such] individual, *comprising of*:…" and goes on to list specific types of data. a. It is unclear if the data types listed are exhaustive or only a subset. The government should clarify this. "Directly affect the legitimate rights and interests of an individual" is a

Article/Concern	Issues and Recommendations
	very broad phrase that provides little clarity to businesses on what data types require special protection. This creates huge regulatory uncertainty for businesses. **<u>Our recommendation:</u>** We recommend modifying the definition of Sensitive Data to mean *"personal data used to identify racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, related to a natural person."* We also recommend that the government aligns the definition of sensitive personal data with the GDPR, and removes the following definitions because they are unclear and potentially very broad: a. "Customer information of credit institutions, foreign bank branches, payment intermediary service providers [or] other authorized organizations" – it is unclear whether this only applies to credit institutions etc., or broadly encapsulates financial information. b. "location data of an individual as determined by location services" – it is unclear whether this applies to all location data or otherwise what "as determined by location services" means.
Age of Digital Consent	Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to their respective age groups. For example, if a 15-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. Setting the age of digital consent at 13 years old would give teens better access to: (a) health information, which are vital at their stage of development; (b) educational resources and tools, which they may use in and out of school; (c) resources that would inform them of relevant and current issues, raising their civic and political understanding and consciousness; and (d) ready support resources and platforms, that are already available online. This would align with the US federal Children's Online Privacy Protection Act (COPPA); the Advisory Guidelines from Singapore's Personal Data Protection Commission ("PDPC"); and Singapore's

Article/Concern	Issues and Recommendations
	recently released "Advisory Guidelines On The PDPA For Children's Personal Data In The Digital Environment" which defines "child" as an individual under 18 years of age, but specify that children aged 13-17 may consent on their own behalf and provide for a flexible range of methods for age assurances. Furthermore, several countries have also adopted 13 as the relevant age of consent, including the UK, Belgium, Denmark, Estonia, Finland, Latvia, Malta, Norway, Portugal and Sweden. **Our recommendations**: We recommend that the Bill should define the "age of consent" as 13 years old or older. Several key jurisdictions have adopted 13 years old as an appropriate threshold.
Parental and Minor Consent	Parental consent and verifying parental relationships would require the collection of more, not less, sensitive data from users. In order to ensure parental relationships, companies may need official government documentation not limited to driver's licenses, birth certificates, and records of the familial relationships of minors and their parents, in order to be able to verify it. There is a risk that making parental consent mandatory will lead to a higher volume of teenagers misrepresenting their age to avoid seeking the mandatory consent, and also trying to come up with ways to bypass our ability to identify their real age when on the platform. This will not only undermine the effectiveness of parental consent requirements but also our ability to ensure that teens have age-appropriate experiences online.
Very limited legal grounds other than Consent	Personal data protection laws (and the definition of personal data) must be limited to data that can reasonably be linked to an identified or identifiable individual, and data protection laws should not expand to cover circumstances where the personal data is already available to the public. This means the definition of personal data should also exclude anonymized or de-identified data. As it is currently drafted, the Decree is a consent-first regime, with limited exceptions and no "legitimate interest" ground as under the General Data Protection Regulation (GDPR). a. The requirements for consent are onerous and require active consent, so consent cannot be implied or deemed. Where there

Article/Concern	Issues and Recommendations
	are multiple processing purposes (which, in practice, would likely be the case for the vast majority of controllers), the controller must list the purposes for the data subject to give consent to one or more of the specific purposes, implying that data subjects should be able to choose the purposes for which their data is processed. This is inconsistent with international norms and is impractical to operationalise since controllers generally cannot customise their specific purposes for each data subject. b. The exceptions to consent are limited. For example, the "contractual necessity" basis only allows processing to "fulfil the contractual obligations of the data subject towards relevant agencies, organisations or individuals in accordance with a Law". This requires clarification and is significantly narrower than the contractual basis in other jurisdictions such as GDPR, which permits processing where necessary for performance of a contract to which the data subject is a party, without any further requirement to be in accordance with "a law". We propose broadening the exception to align with the GDPR. c. This may result in consent fatigue, which may have a negative impact on individuals. In addition to the possibility of consent fatigue, consent, especially "written consent" may not be practicable in certain situations. For example, "written consent" would not be obtainable when transacting with a company over the phone, or when signing up for an off-the-shelf product which the company is unable to customise for individual users. Very few services, especially online products and services, are able to be customised for individuals. Withholding consent is meaningless, because it would simply mean that companies cannot provide the service. Another example where it is difficult to imagine consent being freely given includes those situations where the data subject is under a degree of influence by the controller (for example, an employee, or a student). In either example, data subjects may be driven to simply give consent - regardless of their actual preferences - so that they are not deprived of services they rely on every day or do not suffer adverse consequences. d. A consent-first regime also impacts the ability to use data for innovation, and to drive economic growth and social progress. To

Article/Concern	Issues and Recommendations
	transform Vietnam into a truly digital nation, we propose introducing "legitimate interests" as an alternative to consent. This is more flexible and appropriate to cover innovative data processing activities that are key for the development of the digital economy, whilst still giving due consideration to the rights and interests of the data subject. In many cases "legitimate interests" can provide a more privacy protective standard, since it requires data controllers to balance the rights and freedoms of the individual against the interests of the organisation processing the data and justify the processing based on that test. **Our recommendations**: The Decree currently suggests that consent may be "partial" or that a data subject can include other conditions when giving their consent. This is unclear, inconsistent with global best practice, and not reflective of how internet-based businesses work. The Law should allow for implied, or deemed consent for processing that aligns with the reasonable expectations of the consumer. We recommend that either this concept be removed from the Law or to broaden the exceptions to consent to be consistent with international norms such as the GDPR. Either of these amendments will provide greater clarity to businesses, and to prevent an unreasonable compliance burden on those businesses. We would also like the government to clarify if third party transfers can be done on grounds other than Consent.
Requirement to submit "Dossiers" for Personal Data Processing and Overseas transfers	The requirement to submit detailed dossiers for routine processing requires material operational resources and is inconsistent with international norms. Assuming the requirement is retained, we would like clarification that this is a "one-time" requirement. Requiring regular submissions would be very impractical and require huge amounts of resources on the parts of the government and private industry. It is also unclear how this requirement would provide better privacy protection for individuals, compared to a "records of processing" requirement similar to the GDPR. **Our recommendation**: We propose that this requirement be changed to something similar to

Article/Concern	Issues and Recommendations
	the maintenance of records of processing that are available upon request (similar to the GDPR requirement), or a pared down version of the requirement which focuses on high risk processing (similar to the requirements for conducting a Data Protection Impact Assessment under the GDPR).
Overseas transfers	Like the Personal Data Protection Impact Assessment (PDPIA), the requirements in the Overseas Data Transfer Impact Assessment (OTIA) are extremely onerous. In addition, the controller also needs to notify authorities in writing after 'successful' overseas data transfer and update authorities within 10 days of any changes. This could mean that companies need to prepare - and the authorities would need to receive - a large volume of OTIAs in relation to companies' standard, day-to-day operations. These requirements are consistent with international standards or the technological realities of current cloud implementations, and do not meaningfully increase privacy protections. In the vast majority of cases, companies are not able to accommodate an individual customer's request not to transfer their data overseas without ceasing to provide the service in a meaningful manner to them. The broad definition of overseas personal data transfer is also problematic: directly processing personal data of Vietnamese citizens by automated systems located outside of Vietnam is considered as overseas personal data transfers. This means an automated teller machine located outside of Vietnam would also be transferring personal data overseas and be required to comply with the requirements relating to overseas transfers. This is unlikely to be the intention of the decree. **Our recommendations**: We recommend that instead of the OTIA requirement, the Law should recognise other legal grounds for transfers that are aligned with international benchmarks and encourage interoperability (e.g. consent, contractual clauses, contract necessity, etc.). It is important that these requirements are not overly prescriptive so that they can be easily adopted at a multinational level - in this respect it would be helpful to adopt interoperability frameworks such as the APEC Cross-Border Privacy Rules or leverage regional frameworks such as the ASEAN Model Contractual Clauses. We also suggest that the scope of overseas personal data transfers be

Article/Concern	Issues and Recommendations
	narrowed to products and services targeted at Vietnamese users only.
Age Verification and Children's Personal Data	The Decree requires age verification and, for children aged 7 years or older, both parental consent and the consent of the child is required. Aside from the steep administrative burden in obtaining two sets of consent, this creates a risk that companies would need to implement privacy-intrusive methods to verify age, including of very young children (under 7), which may result in an overall less privacy protective position requiring collection of more personal data. Age verification thus mandates the collection and storage of more – not less – sensitive, personally identifiable information on *all* Vietnamese users (not just teens), and an even greater level of data about children and their family. Age verification should therefore be viewed not as a single tactic, but rather as part of a collection of ongoing efforts that work dynamically to provide effective solutions. It is important for data controllers to evaluate the effectiveness of age verification holistically, based on the outcomes resulting from a range of measures applied across different points in the user experience. This enables data controllers to achieve the necessary level of confidence proportional to the risks presented in a particular use case, while applying a floor of protections to users for whom we have lower confidence levels in the accuracy of their age. **Our recommendations**: 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. Companies should be allowed to take *reasonable* steps to assure a user's age. This amendment would make the Bill consistent with international best practices.
Mandatory Data Breach Notification requirement without a materiality threshold	The requirement to notify the Government of "all violations" of personal data regulations is inconsistent with international norms. This would also result in the regulator being inundated with trivial notifications that do not have a material impact on individuals' privacy. **Our recommendations**: The trigger for notification should be limited to breaches of security that lead to "significant harm" or "serious harm". The overarching goal

Article/Concern	Issues and Recommendations
	should be to help regulators identify incidents that pose an actual risk to users so that they can focus their oversight and guidance on these.
Legal Bases for Processing	A range of legal bases for processing is important because there are a variety of practical reasons why one legal basis might be more suitable than another, even where more than one might be available. In some circumstances, multiple bases may be applicable. It is international best practice for any comprehensive, robust data protection law to have a range of legal bases for processing personal data. Common legal bases include (but are not limited to): informed notice, consent; legitimate interest; contractual necessity; vital interest; legal obligation; and public interest. All legal bases for processing data should be equal – meaning that there is no "default" legal basis, and no hierarchy amongst them. It is the data controller's and/or processor's responsibility to determine which legal basis is most appropriate, and to take steps to establish that legal basis, given the circumstances in which they will be processing personal data. *Legitimate interest* is a particularly important legal basis and is recognised in privacy laws across the world. Legitimate interest requires the entity processing the data to consider the balance between their own interest, and the rights of data subjects. Therefore, the legal basis of legitimate interests offers a flexible way for organizations to process data in a manner that respects privacy and data subject rights. Legitimate interest facilitates many beneficial uses of data. For example, many companies' data can be shared with third party researchers to advance research on important issues or to help make their services safer for security purposes, such as fraud, network security, criminal acts, and possible threats to public security. In addition, it should be flexible enough to support alternative business models, such as "freemium" services that offer services free to consumers and business users, and rather fund that service through the processing of personal data in a transparent, informed manner. The interpretation of the legitimate interest legal basis should be sufficiently broad and flexible to allow for businesses to conduct essential and beneficial processing operations. **<u>Our recommendations</u>**: We recommend the following for your consideration.

Article/Concern	Issues and Recommendations
	Processing shall be lawful only if and to the extent that at least one of the following applies: ● The data subject has given consent to the processing of his or her personal data for one or more specific purposes; ● 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; ● 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; ● The rights and interests of the data subject will not be infringed upon by the processing; ● The controller has taken reasonable steps to inform the data subject of the processing that it wishes to undertake.
Using Personal Data for Advertising Purposes	Personalization is at the heart of what makes the modern internet valuable. Personalized advertising enables various online and digital services to provide people with valuable services for free. It is the most efficient way for businesses to find new customers and grow their business – which is particularly important for small businesses. Personalized advertising, and the free services that it supports, drives economic growth and have provided crucial benefits. It is essential then that personalized advertising be designed with privacy and data protection in mind. Mandating consent for all data processing for marketing and advertising activities shifts the burden to the users themselves to ensure that their personal information is being processed appropriately. When users sign up for a free online service, they understand that they are also signing up to fund that service by being served personalized online ads. A risk-based approach to personalization is the more appropriate path to provide users with a high value service. This includes providing users with protections so that they can have transparency, education, and reasonable restrictions and controls to provide users with a high

Article/Concern	Issues and Recommendations
	level of privacy control without disrupting their browsing experience. Over-reliance on consent for processing personal data is inconsistent with internationally recognized frameworks, which will economically harm Vietnam by reducing foreign investments and undermining local businesses. **<u>Our recommendations</u>**: We recommend that over-reliance on consent for processing personal data for advertising purposes should be avoided. The Law should provide a wide range of legal bases in which to process personal data for advertising purposes.
Cross-border data transfers	Cross-border data flows are beneficial for economic growth, data privacy and security, and the protection and exercise of privacy and other human rights. They underpin innovation, research and development across multiple sectors; support international cooperation; and enable us to stay emotionally and socially connected to one another. For the purpose of this Law, we define cross-border data transfers as international data transfers should be defined as data that are transferred between data processing agents, in which at least one is based in a different jurisdiction, which are therefore subject to different laws. Due to the decentralized nature of the internet, it is not technically feasible to regulate every international physical transfer of data that occurs outside of a country. Networks are generally agnostic of the physical "journey" of the data and instead optimize routing in real time to reduce latency and increase network resilience. Therefore, any regulation that attempts to regulate every international physical transfer of data threatens to break the network connections that are necessary for the internet to function. **<u>Our recommendation</u>**: We recommend amending the definition of cross-border data transfers to *"data that are transferred between data controllers or data processors, in which at least one is based in a different jurisdiction"* rather than any physical transfer of data outside Vietnam.

Article/Concern	Issues and Recommendations
Data Subject Rights	We would like to highlight four main issues under Data Subject Rights. First, 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, international best practice includes clear and reasonable limitations on user rights, including: technical feasibility; if allowing access to the data would reveal confidential commercial information; 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 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). Controllers could also be given the ability to charge a reasonable fee to cover the administrative cost of producing burdensome data. By allowing controllers to charge a reasonable fee where applicable, users could still have access to this data, while controllers would be able to better handle unreasonable requests. Second, based on our experience of implementation of Decree 13/2022 on Personal Data Protection ("Decree 13"), the existing requirement to fulfil 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

Article/Concern	Issues and Recommendations
	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 may involve deleting millions of data points, intersecting across users 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. Third, the Decree allows users to exercise provision of data subject requests through email, Fax, Post or Online. Organizations should be able to meet the requirement by making one method available (rather than all four). A requirement for organizations to meet all four methods is against international norms, will reduce the competitiveness of Vietnam, and imposes onerous costs and administrative challenges for businesses of all sizes. Lastly, data subject rights should not include the right to restriction and objection of personal data processing for marketing and advertising purposes. Forcing organizations to provide their services to individuals who object to or restrict personal data processing for marketing and advertising purposes would often amount to forcing them to provide their services for free and/or at a loss. 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. Forcing service provision also ignores the value of providing transparency and control tools. Just like treating consent as the primary or default legal basis ignores the value of transparency and control tools, so does forcing service provision when individuals do not consent, or opt out of, data processing. Transparency and control tools give individuals the power to customize their experiences; individuals that prefer the fullest user experiences can select them, while individuals that prefer less rich experiences and less data processing can select them. And individuals that do not find any form of the service valuable can delete their accounts or otherwise abstain from the service. But bluntly forcing service provision based on one consent moment would remove these valuable choices.