9 April 2021

Submitted electronically

BSA COMMENTS ON DRAFT VIET NAM PERSONAL DATA PROTECTION DECREE

BSA | The Software Alliance (**BSA**)[1] thanks the Ministry of Public Security (**MPS**) for the opportunity to comment on the Draft *Personal Data Protection Decree* (the **PDPD**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that spark the economy.

BSA commends the Government of Viet Nam for soliciting stakeholder input on the draft PDPD and the proposal to establish a data protection authority in Viet Nam, the Personal Data Protection Commission (**PDPC**). Instituting a national personal data protection regime is an important step in growing a vibrant and innovative domestic digital economy and allowing Vietnamese companies to engage with the global digital economy.

This submission to the MPS provides recommendations on the following topics:

- Recognizing distinct roles of data controllers and data processors
- Disclosure of personal data
- Legal basis for processing personal data
- Cross-border transfer of personal data
- Registration provisions
- Technical requirements
- Sensitive personal data
- Penalties and compensation

Recognizing Distinct Roles of Data Controllers and Data Processors

A comprehensive personal data protection framework must create effective and enforceable obligations for all companies that handle personal data. These obligations will only be effective in protecting citizens' privacy and instilling trust if they reflect how a company interacts with consumer data.

---

[1] www.bsa.org

BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

The distinction between companies that decide how and why to collect and use data about individuals (frequently referred to as "data controllers") and companies that process data on behalf of other companies (frequently referred to as "data processors") is important because both data controllers and data processors have important, but distinct, roles in protecting personal information.

Personal data protection laws worldwide clearly distinguish between these two types of entities and assigns each with responsibilities that reflect their different roles in safeguarding personal data.[2]

Article 2 of the PDPD provides for two different personal data handling entities — "personal data processors" and "third parties". However, the definitions of these terms do not align with the globally recognized roles of data controllers and processors and instead combine their scope and responsibilities. This results in a lack of clarity that creates significant challenges in implementing the law for all stakeholders, including data subjects, companies handling personal information, and government authorities.

The current definition of "personal data processor" under the PDPD refers to an agency, organization, or individual inside or outside the country that performs personal data processing activities. This open-ended definition does not make the distinction, found in global privacy laws, between separate entities based on whether they decide how and why personal data is processed (data controllers) and those that merely process personal data on behalf of others (data processors).

The definition of "third parties" raises similar concerns, as it also does not reflect the concepts of personal data processors and data controllers. For example, although third parties appear able to process data for other entities, the definition of third parties does not specify the critical requirement that such entities carry out processing "on behalf" and "at the direction" of the main controlling entity (data controller).

We recommend the PDPD revise these definitions and obligations in two ways:

- First, the definition of the "personal data processor" should be revised to align with the definition of data controllers in other legislation and the role of these entities should be reflected in the substantive obligations assigned to them. For example, as data controllers have a direct relationship with data subjects, the PDPD should assign primary responsibility to data controllers for satisfying many of the data protection and security obligations including, among other things, determining the legal basis for processing personal data, obtaining consent from data subjects where necessary, and notifying data subjects of data breaches or other incidents that present a material risk of harm to the individuals. Data controllers should also be the entities to comply with data rights such as those provided under Article 5 of the PDPD.

- Second, the definition of "third parties" should be revised to align with the definition of data processors in other legislation and their obligations should accordingly fit this role. For example, because data processors process data on behalf of data controllers, they generally have no direct relationships with data subjects and may have limited authority or ability to access the data being processed. Data processors are therefore unable to directly obtain consent from data subjects, fulfill data rights requests, or notify data subjects in cases of breach. Rather, data processors' primary responsibilities should be to process data on behalf of the controller consistent with the controller's instructions; they also may be required to employ reasonable and appropriate data security measures and to provide controllers with the tools necessary to collect data needed to respond to data subjects' requests. These obligations are typically specified in the contractual agreements between the data controller and data processor.

[2] The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation, https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation

Combining these roles under the current PDPD affects several provisions. While there is differentiation in the roles and responsibilities between "personal data processors" and "third parties" in some of the provisions such as "technical measures" (Article 17) and "development of regulations on personal data protection" (Article 18), the distinction is less clear for other provisions. This includes several data subject obligations imposed by the PDPD that should be assigned explicitly to data controllers (personal data processors in the PDPD), such as obligations to obtain data subjects' consent to process their data (Article 8), the requirement to notify the data subject of processing activity (Article 11), the ability to disclose personal information without consent (Article 6), and the obligation to honor data subjects' rights requests, such as requests to access, delete, or transmit personal information (Article 5).

The current lack of clear definitions and the conflation of these roles will likely render data subjects unable to understand which entity they should contact to exercise their personal data rights. To the extent these consumer facing obligations fall on data processors (third parties) that a data subject does not generally interact with, it may also create security and privacy risks for data subjects by forcing those processors (third parties) to disclose personal data to individuals with whom they have no prior direct relationship and whose identity they may be unable to authenticate. Moreover, many data processors (third parties) are contractually prohibited from accessing or reviewing the data they are processing on behalf of their data controller customers; forcing processors (third parties) to access that personal data undermines the privacy protections which contracts and the PDPD are designed to establish.

Finally, we note that the lack of clear definitions and distinctions is inconsistent with the approach taken by other privacy laws around the world, such as the European Union's General Data Protection Regulation (**GDPR**),[3] Singapore's Personal Data Protection Act (**PDPA)**,[4] and Japan's Act on the Protection of Personal Information (**APPI**).[5]

In sum, **BSA recommends** the following:

- To amend the definitions in Article 2 for personal data processor and third party to align with the more commonly accepted roles of data controller and data processor.

- To explicitly state that consumer-facing obligations such as those under Articles 5, 6, 8, and 11 apply only to entities with a direct relationship with the consumer, which in the case of the PDPD is the personal data processor (internationally known as data controller).

Disclosure of Personal Data

Article 6 of the PDPD outlines the conditions under which data can be disclosed by personal data processors and third parties and provides for five exceptions to requiring consent which are commonly observed in other data protection frameworks.

Establishing mechanisms to disclose personal data is important as this provides companies with the regulatory certainty to transfer personal data to other entities for essential business activities. Article 6, as it is currently drafted, can be read narrowly to limit any form of data transfer between entities absent consent to only those five exceptions and this has the potential to disrupt essential business activities. For example, it could prohibit legitimate personal data transfers between a data controller and their data processors (third parties), or between business units within a single corporation.

BSA recommends that the PDPD ensure that personal data can be disclosed for the same purposes and on the same basis as those for which the data may be processed under the PDPD. This will help ensure that Article 6 does not prevent disclosures of personal data in connection with legitimate

[3] EU Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[5] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

business activities that are reasonable to provide a product or service to the data subject. Similarly, it should be made clear that when a company transfers data to a third party that processes data on the company's behalf, that action does not amount to a "disclosure" requiring consent or an exception to consent. This ensures that companies can use data processors (third parties) to carry out the products and services requested by customers, without subjecting customers to additional consent requests.

Legal Basis for Processing Personal Data

Under Article 3, the PDPD provides for personal data to be collected and processed with the consent of the data subject or with the permission of the competent authority — the proposed PDPC. The PDPD also provides limited exceptions for processing without such consent (Article 10). It further requires consent to process personal data by automated means (Article 13) and to transfer personal data outside of Viet Nam (Article 21). The PDPD also separately addresses the issue of disclosure of personal data (Article 6).

Privacy and personal data protection regulators around the world have long debated the challenges and limitations presented by consent-based models of protecting personal data. We recognize that consent is an important legal basis for the collection, use, and disclosure of personal information. However, it should not be the only legal basis for processing personal data. Indeed, there is widespread recognition that consent-based frameworks may increase burdens on data subjects, because they may require data subjects to provide consent to many types of processing they already expect, such as processing to deliver the goods and services they request.

We accordingly urge MPS to incorporate in the PDPD a broader range of legal grounds for processing, without relying on consent as the primary ground upon which data processing is authorized.

In particular, we encourage MPS to revise Article 10 to recognize a broader set of grounds in addition to consent for processing personal data — and in doing so to recognize that each of these grounds is an appropriate basis for processing rather than an exception to consent requirements. Specifically, Article 10 should be amended to specifically allow for:

- processing personal data in connection with entering into, or performance of, a contract with the data subject;
- to fulfill a legal obligation to which the data controller is subject;
- for the legitimate interests pursued by the data controller or processor (third party);[6]
- to protect the vital interests of the data subject or another natural person; and
- where 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 data controller.

Recognizing these additional grounds for processing data will help to ensure that data controllers and processors (third parties) may use data in ways that consumers expect and allow them to enhance cybersecurity, to detect and deter fraud, and to improve business processes. Moreover, by recognizing additional grounds for processing personal data beyond consent, personal data protection laws can reduce the burden on data subjects to consent to each expected use of their personal

[6] Legitimate interests include processing for purposes of fraud detection and prevention; monitoring, detecting, and protecting a network via cybersecurity measures; and updating products and services to ensure they are as accurate and reliable as possible. As enumerating the range of these legitimate interests in statutory language is impractical, including a ground such as "reasonable purpose" or "legitimate interest" provides companies the flexibility and regulatory certainty to process personal information for these legitimate purposes.

information. Consent is then reserved for situations in which it is most meaningful to data subjects — when a use may involve sensitive personal information or may be unexpected in a given context. This reduces "consent fatigue" among data subjects in which individuals either begin to ignore privacy notifications and requests for consent or are deterred from using digital products and services.

These grounds for processing are well-established features of data protection frameworks globally that aim to facilitate the use of personal data for innovative purposes while ensuring that the risks to individual personal data protection rights are appropriately considered. They enhance the protection of individuals' personal data while promoting responsible use of personal data by businesses.

BSA recommends that MPS amend the PDPD to explicitly include these additional legal bases for processing. In doing so, these grounds should be presented as alternative grounds for processing, rather than exceptions to a consent requirement.

Cross-Border Transfer of Personal Data

The ability to transfer data, including personal data, across international borders is the lifeblood of the modern digital economy. For this reason, it is critical that the PDPD allows companies to responsibly transfer data internationally. The Government of Viet Nam has agreed to ensure the cross-border transfer of information in its international commitments to the parties of the Comprehensive and Progress Trans-Pacific Partnership.[7]

We are deeply concerned with the restrictive requirements on cross border transfers of personal data. Under Article 21(1), personal data may only be transferred out of Viet Nam if all the following conditions are met: a) the data subject has agreed to the transfer of the data; b) the "original personal data" is stored in Viet Nam; c) the country of to which the data is transferred imposes the same or higher level of data protection (must have a document proving the same); and d) the PDPC agrees to the transfer in writing. Several of these requirements are impractical individually; collectively they threaten to undermine the ability of global companies to do business in Viet Nam and, by the same token, threaten the ability of companies in Viet Nam to operate globally.

Companies in all industries require the ability to transfer data across international borders. In sectors as diverse as agriculture, healthcare, manufacturing, and banking, businesses that produce a broad range of products and services are united by the need to send data across international borders. Indeed, everyday technologies like cloud storage services, customer relationship management software, human resource management programs, identity management services, workplace collaboration software, cybersecurity solutions, and supply chain management services all depend on the ability to transfer data across national boundaries. Cross-border transfers are also vital to consumers and workers who expect to use global services that connect them with others worldwide in a manner that protects the privacy and security of their data.

Article 21's restrictions on cross-border transfers will harm the ability of companies in Viet Nam to provide global services. Moreover, the restrictions do not advance the data protection goals of the PDPD. For example, requiring copies of personal data to be stored in Viet Nam will do nothing to enhance personal information protection as the security of data depends on the policies, procedures, and technologies employed by the entity storing the data and not upon the physical location or legal jurisdiction of such data. In addition, requiring the PDPC to approve data transfer in advance will be enormously costly to the PDPC and disruptive to normal business operations. Even the requirement for individual companies to determine if the jurisdiction in which data is stored meets the same level of protection afforded in Viet Nam is subjective and labor intensive.

We highlight below concerns about the broad nature of these conditions, the narrowly drafted exceptions, and the impractical results of additional obligations imposed on transferred data.

Broad Conditions: Requiring all four conditions to be fulfilled concurrently under Article 21(1) is not practical and risks upsetting the ability of companies, workers, and consumers in Viet Nam to benefit from global services. The compliance costs and transaction delays for companies and administrative

[7] CPTPP Article 14.11 at https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf

burdens on the PDPC would not be sustainable. Nor is it clear that the exceptions set out in the PDPD under Article 21(3) provide sufficient flexibility to facilitate international data transfers.

We encourage MPS to amend Article 21 to enable more flexibility in transferring data across borders.

Narrow Exceptions: As currently drafted, Article 21(3) provides for four conditions that can exempt organizations from having to meet these initial conditions. These are: a) the data subject grants consent for the transfer; b) the PDPC provides written approval; c) the personal data processor (internationally referred to as data controller) provides a "commitment to protect personal data"; and d) the personal data processor provides a "commitment to apply personal data protection measures". It is unclear whether an organization needs to meet only one of these conditions or if the organization must meet all four to legally transfer personal information without meeting the obligations of Article 21(1). Furthermore, the conditions under Article 21(3)(a) and (b) appear to simply restate the conditions in Article 21(1)(a) and Article 21(1)(d).

We urge MPS to revise Article 21(3) to clearly state that meeting either of the requirements in Article 21(3)(c) or Article 21(3)(d) individually is a sufficient basis for transferring data.

Under Article 21(3)(c) and Article 21(3)(d) companies may transfer data on the basis of commitments to protect that data regardless of the data's location. These provisions appear to reflect the accountability principle which was first established by the Organisation for Economic Cooperation and Development (**OECD**)[8] and was subsequently endorsed and has been integrated in many legal systems including the EU,[9] Japan,[10] New Zealand,[11] Singapore,[12] and Canada.[13] The accountability principle is also a significant feature of the APEC Privacy Framework,[14] the APEC Privacy Recognition for Processors (**PRP**) system,[15] and the APEC Cross Border Privacy Rules (**CBPR**) system.[16] Under this principle, organizations that transfer data globally should implement procedures to ensure that when data is transferred to countries other than where it was collected the data will continue to be protected.

We encourage MPS to make clear that meeting either Article 21(3)(c) or(d) individually will be sufficient to internationally transfer personal data, consistent with the accountability principle discussed above.

Impractical Additional Obligations: In addition to the overly restrictive conditions for cross border data transfer in Article 21(1), the provisions in Article 21(4), (7), and (8) contain additional burdensome requirements for personal data processors (internationally referred to as data controllers) to store data transfer history for three years, register with the PDPC for cross-border transfers of sensitive personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by personal data processors. These obligations are not practical and may create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

We encourage MPS to avoid posing such obligations on cross border transfers.

---

[8] The Accountability Principle states that a data controller should be accountable for complying with measures which give effect to the other OECD principles including the Security Safeguards Principle. OECD Privacy Framework 2013 (p15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[9] EU Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] Japan's Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[11] New Zealand Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23376

[12] Singapore's Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[13] Canada's Personal Information Protection and Electronic Documents Act fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[14] APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[15] APEC Privacy Recognition for Processors, http://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-3.pdf

[16] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

BSA recommends the following amendments to Article 21 to enable more flexibility for organizations that depend on the ability to provide companies and consumers with products and services that require transferring data across borders, while ensuring a high level of data protection:

- Revise Article 21(1) to eliminate the requirements in Articles 21(1)(b), (c), and (d) and to clarify that consent by the data subject to process data is one basis that is sufficient to allow for international data transfers in pursuance of purpose of processing.

- Revise Article 21(1) to recognize additional bases for international data transfers, including corporate binding rules, international trustmarks, regional certifications, and contractual arrangements. These mechanisms are incorporated in other global data protection frameworks to promote cross-border data flows, including the APEC CBPR and PRP schemes, the EU GDPR, and Japan's APPI. Recognition of these mechanisms will also better align the PDPD with recent initiatives in ASEAN such as the development of the ASEAN Model Contractual Clauses[17] and other ongoing work under the ASEAN Cross Border Data Flows Mechanism.[18]

- Revising Article 21(3)(c) and Article 21(3)(d) to highlight the obligations of companies (both data transferor and recipient) to protect data regardless of its location of storage and recognize that commitments by companies to protect data, regardless of the location of the data's storage, are independent bases for transferring data internationally. As noted above, this approach would align with the accountability principle that has been implemented in data protection laws worldwide.

- Eliminate the requirement under Article 21(4) for personal data processors to store data transfer history for three years which may lead to unintended privacy and security risks by forcing companies to store and access data they otherwise would not.

- Eliminate the requirement to submit an application for registration to transfer sensitive personal information internationally under Article 21(7)(a). Any requirements imposed by other provisions in the PDPD for processing sensitive personal information (e.g., conducting a privacy impact assessment) should already address the privacy concerns raised by the collection and use of sensitive personal data; likewise, a company's reliance on the mechanisms described above for transferring data with appropriate privacy protections ensures those privacy protections continue to apply to the data regardless of where it is stored. The additional registration requirement is thus unnecessary.

- Incorporate additional flexibility for organizations under Article 21(8) by permitting companies to submit independent third-party audits and supporting documentation in lieu of additional or duplicative audits conducted by the PDPC.

Registration Provisions

The PDPD contains numerous provisions requiring registration with the PDPC, including registration requirements for processing sensitive data (Article 20) and for transferring personal data outside of Viet Nam (Article 21). These requirements would amount to a de facto licensing scheme leading to unnecessarily delays in processing of data and are at odds with the data protection requirements of most jurisdictions around the world. They impose unnecessary costs on businesses and additional obligations on government authorities with respect to reviewing and approving applications for registration, and do not achieve added protection for individual data subjects. That is why the EU,

[17] ASEAN Model Contractual Clauses for Cross Border Data Flows, https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

[18] ASEAN Data Management Framework, https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf

even as it significantly strengthened its data protection regime in adopting the GDPR, eliminated the data registration requirements that existed under the prior Data Protection Directive.

BSA therefore recommends:

- Eliminating the registration requirements in Article 20 and Article 21(7) and (8) that function as de facto licensing arrangements. This will encourage both the PDPC and businesses to apply their limited resources to the more important objective of ensuring reliable privacy outcomes for data subjects.

- Revising, for purposes of internal consistency, provisions that reference registration requirements. For example, the requirement for processing to be carried out strictly based on "purposes registered" (Article 3(2)) should also be eliminated from the PDPD.

Technical Requirements

Article 17(1) requires organizations to implement a variety of administrative, technical, and physical measures to protect personal data. Not all of the requirements would be relevant for every organization handling personal information. As such, we suggest MPS make clear that the measures need only be applied "where appropriate",[19] and are not required to be implemented by all data controllers in all circumstances.

Also, **BSA urges** MPS to avoid mandating prescriptive security approaches, and instead recommends adopting a flexible, technology-neutral, risk-based approach to securing personal data, in line with internationally recognized standards and best practices. For example, Article 17(2)(g) requires personal data processors to store information regarding the type of equipment and software that is used to process personal data. This information does not contribute to the safety or responsible processing of data and BSA recommends that this requirement should be eliminated.

Sensitive Personal Data

The current definition of sensitive data provided under Article 2(3) is unnecessarily broad. The definition encompasses special categories of data,[20] as well as financial data, personal location data, and personal data about social relationships. It also does not specifically limit these sensitive data types to where they are clearly attributable to or able to identify a data subject, potentially broadening the applicability of this provision beyond personal information.

BSA recommends that MPS amend the definition to better align with international norms on sensitive personal data and specifically limit the provision to where the data is clearly attributable to or able to identify a data subject.

Penalties and Compensation

A central regulator should have the tools and resources necessary to ensure effective enforcement. Effective enforcement of a personal data protection law is critical to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. A personal data protection law can create effective enforcement without introducing criminal sanctions or including a private right of action.

Remedies and penalties imposed upon violations of personal data protection laws should be proportionate to the harm resulting from such violations. Criminal penalties are not proportionate remedies in this case.

Accordingly, **BSA recommends** that MPS revise Article 4(1) to eliminate the reference to criminal penalties.

Article 5 provides data subjects the ability to file legal complaints if their personal data is compromised or processed incorrectly or the exercise of their personal data rights are not implemented correctly. It

[19] See Article 32, EU GDPR.

[20] See Article 9, EU GDPR.

also provides data subjects with the right to seek compensation where there are "grounds to believe that their personal data has been breached".

Providing consumers with a private right of action will introduce unhelpful and unnecessary uncertainty in how the law will be enforced. Placing enforcement powers in a government agency, the PDPC in the case of the PDPD, will afford effective and consistent enforcement of the law and provide organizations and consumers with certainty in terms of how the rights and obligations specified in the PDPD are to be applied.

Accordingly, **BSA recommends** that MPS limit Article 5(5) to making complaints to the PDPC and remove Article 5(6) from the proposed PDPD.

Once again, BSA commends the Government of Viet Nam for taking the important step of developing a national data protection regime and thanks the MPS for the opportunity to comment on the proposed provisions. If MPS requires any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher
Director, Policy – APAC
BSA | The Software Alliance