June 30, 2023

BSA COMMENTS ON THE PERSONAL DATA PROTECTION DECREE NO. 13/2023/ND-CP

Respectfully to: The Ministry of Public Security

On behalf of BSA | The Software Alliance (**BSA**),[1] we send you our sincere regards. BSA has been actively participating in the developments related to the Law on Cybersecurity and its various implementing decrees. For instance, BSA provided comments on Decree 53 in September 2022[2] and attended the Workshop organized by the Ministry of Public Security (**MPS**) in November 2022. BSA also commented on proposed amendments to the draft Decree 72 in September 2021[3] and December 2021,[4] as well as the draft Decree Implementing Law on Cybersecurity in December 2018[5].

We are writing now to raise concerns about several issues in the final Decree No. 13/2023/ND-CP on the Protection of Personal Data (**PDP Decree**), which was published on April 17, 2023 and is scheduled to enter into force on July 1, 2023. We are raising these issues to your attention so that they may be addressed through implementing regulations or explanatory guidance to clarify how a range of provisions contained in the PDP Decree will function in practice.

Additional bases for processing personal data

Articles 11 and 12 set out a consent-based personal data protection regime, which will require individuals to review disclosures regarding and provide consent to a wide range of processing activities. While several exceptions to processing personal data without consent of the data subject are provided for in Article 17, such as protecting the life and health of individuals in an emergency, fulfilling contractual obligations and reasons related to security and national defense, these exceptions are far narrower than many data protection laws adopted globally. As a result, companies doing business in Vietnam and consumers accessing products and services in Vietnam may be forced to seek and provide consent resulting in consent-fatigue,

[1] BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Vietnam: BSA Comments on Decree 53 to Implement the Law on Cybersecurity

[3] Vietnam: BSA Comments on Proposed Amendments to Draft Decree 72 | BSA | The Software Alliance

[4] Vietnam: BSA Comments on Proposed Amendments to Draft Decree 72 | BSA | The Software Alliance

[5] Vietnam: BSA Comments on Draft Decree Implementing Law on Cybersecurity | BSA | The Software Alliance

300 Beach Road
#30-06 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

for a long list of activities that may be reasonably expected by the consumer, and/or are consistent with the initial purposes of processing.

Recommendation: As MPS implements the PDP Decree through regulations and guidance, we recommend recognizing that companies may process data without a data subject's consent for a wide range of activities. For instance, a company should be permitted to process personal data as necessary for purposes of legitimate interests it pursues, except when those interests are overridden by the rights and freedoms of a data subject. Globally, this ground for processing is often used in connection with activities including processing designed to prevent fraud, to improve the network and information security of a company's IT systems, or to improve the functionality of a product or service used by the data subject, among other pertinent activities in the usual course of business. One way is to integrate this basis of processing by taking a broader interpretation of "conditional consent" articulated under Article 11 (7) of the PDP Decree, where a data subject could be considered to have conditionally consented to the processing for legitimate purposes, if appropriate notice is provided and such processing does not adversely impact the rights and freedoms of the data subject.

Creating a workable timeline for responding to data subject requests

While we welcome the establishment of many data subject rights within the PDP Decree, requirements in Articles 14.3b, 15.2b, 16.5j could be read to require controllers to respond to certain data subject requests within 72 hours.

Because that result would in many cases be either impractical or impossible, we encourage MPS to clarify that only an initial response to a consumer must be made within 72 hours, but that a full response may be provided thereafter, within a reasonable timeframe. Below we identify a range of practical concerns with reading this provision to require a complete response within the 72-hours window referenced in the PDP Decree.

First, for all data subject requests, an organization must verify the identity of the requestor and ensure that it is indeed the data subject requesting their personal data be corrected, deleted, or provided to them in response to an access request. This process may require companies to ask the data subject for additional information, which may not be feasible within a 72-hour period, especially if multiple time zones are involved.

Second, in many instances, a data subject's request will be unclear. In these cases, the company must clarify with the data subject on the scope of the specific request. In the case of a request for deletion, it is important for a company to understand the specific personal data the consumer is requesting be deleted, because that data is irretrievable once deleted.

Third, even if a company receives a clear request from a data subject whose identity it may readily authenticate, responding to each request will take time to do properly. Companies also expect to receive large volumes of requests, meaning it may be impractical to respond to each request within 72 hours. For instance, if a data subject request comes in on a Friday evening after close of business, an organization may find that it has effectively has less than one working day to respond to the request if the 72 hours is read to mean calendar hours rather than business hours.

Recommendation: Clarify that the response time of 72 hours should be read to apply to a controller's initial response to a data subject, while permitting the full response to be provided thereafter. For example, providing a full response to a data subject request within 30 days would align with international practices. The EU General Data Protection Regulation (**GDPR**) allows controllers 30 days to respond to a data subject access request. Similarly, the Singapore Personal Data Protection Act (**PDPA**) also allows organizations 30 days to respond to an access request from a data subject.

Cross-border data transfers

While we welcome the removal of data localization requirements that were contained in an earlier draft of the PDP Decree, we remain concerned that the PDP Decree will still lead to the same result: a severe restriction of international data transfers.

Under the Decree, cross-border transfers of personal data may proceed only through a single mechanism: consent. Furthermore, in addition to the data subject's consent, each transfer requires: (1) a transfer impact assessment, and (2) reporting that transfer impact assessment to the MPS, with the requirement to submit updates and amendments accordingly. In practice, these provisions will create significant barriers to cross-border data transfers.

As noted in our prior submissions, restrictions on cross-border transfers will have a chilling effect on the local economy as they restrict domestic enterprises and other organizations from fully benefitting from cutting edge technology and services available in the global marketplace. For instance, restrictions on cross-border data transfers may prevent domestic enterprises, both small and medium-sized enterprises (**SMEs**) and larger organizations such as hospitals, airlines, and banks, from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Vietnam. Such services frequently provide best in class security capabilities. Due to such restrictions, domestic companies are likely to find it difficult to access such services, reducing their competitiveness, especially internationally, and exposing them to greater data security risks. The implementation of this requirement would not only be resource-intensive for government authorities to manage and review an enormous number of administrative processes in the form of impact assessments, and will result in additional administrative burden and operating costs for local and international businesses investing in Vietnam. Although we support efforts to ensure data is protected commensurate with the risk its compromise poses, the Decree's onerous restrictions on cross-border data transfers may ultimately undercut data protection and increase the risk that such data may be compromised, by reducing access to privacy-protective and secure products and services.

Recommendation: Adopt an accountability-based approach to support cross-border data transfers, under which the transferring organization remains accountable for ensuring that the receiving organization protects the transferred personal data to the same standard required under Vietnamese law. At minimum, we strongly recommend that the MPS issue implementing guidance that permits companies to transfer data internationally on a basis other than the consent of the data subject and that avoids requiring companies to conduct individual transfer impact assessments. Accordingly, we recommend recognizing interoperable mechanisms for cross-border data transfers, such as contracts, including model contracts such as the ASEAN Model Contractual Clauses; intra-group schemes like binding corporate rules; and certifications like the APEC Cross-Border Privacy Rules (**CBPR**) system.

We also recommend that any data processing and cross-border transfer impact assessments be submitted to the MPS only upon request, as opposed to mandatorily in every case. This would be consistent with international best practice and would free up both corporate and government resources in engaging on material instances.

Roles and responsibilities of controllers and processors

We strongly support the PDP Decree's recognition of the distinct roles of personal data controllers and personal data processors. The longstanding distinction between these two types of companies is foundational to privacy and data protection laws worldwide.[6]

At the same time, Article 39.4 raises specific concerns about the obligations of personal data processors under the PDP Decree. This provision holds the personal data processor responsible to the data subject for damage caused by the processing of personal data. In practice, most business arrangements are such that the personal data controllers are in control of the relationship with the data subjects, and not the personal data processors. Indeed, most personal data controllers do not want personal data processors that act on behalf of the controller to contact the data subject. In practice, it is therefore more appropriate for the personal data controller to be responsible to the data subject for damages caused by the processing of personal data.

Recommendation: Implementing guidance should clarify that the responsibility to the data subject should be held by the personal data controller. Personal data controllers and personal data processors should also be permitted to work out the distribution of responsibilities within their own contractual arrangements.

Notification of violations

Article 23 sets out requirements for notifying MPS and other entities in the case of violations of regulations implementing the PDP Decree. However, it does not set out materiality thresholds for those notifications. As a result, it could be read to require reporting of violations that create only low risks to data subjects. This would result in notification fatigue to both the MPS and the personal data controllers, eroding the effectiveness of the notification requirement.

Recommendation: Implementing regulations should set a suitable threshold for notifications, so that only high-risk breaches of personal data need to be reported to the MPS. For example, notification may be appropriate in circumstances involving the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of harm to the data subject. Creating a clear threshold that focuses this notice requirement on high-risk violations will allow the MPS and personal data controllers to appropriately focus their efforts and resources on addressing such violations.

[6] See BSA, Controllers and Processors: A Longstanding Distinction in Privacy, available at https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf.

Transition period

The PDP Decree is scheduled to enter into force on July 1, 2023. This provides very little time for companies to implement its requirements. That is particularly problematic because the Decree also calls for a range of implementing guidance, including guidance to be issued by MPS.

Recommendation: We strongly recommend extending the implementation date for the PDP Decree. For example, MPS could extend the eligibility of the grace period in Article 43.2 to all organizations, allowing all a two-year transition period to adjust their systems and processes to comply with the PDP Decree. Alternatively, MPS could issue guidance recognizing that enforcement of the PDP Decree will not begin until at least one year after MPS has issued guidance implementing the Decree.

A two-year transition period with the introduction of new personal data protection regulations is in line with practices in other jurisdictions. In the European Union, the European Parliament adopted the GDPR in April 2016, with a two-year period before taking effect in May 2018. In Singapore, the Personal Data Protection Act was enacted in 2012, and came into force in 2014. In Thailand, the Personal Data Protection Act was enacted in 2019 and took effect in 2022, providing a three-year transition period.

Conclusion

We would like to thank the MPS for considering our comments on the Draft Law and hope that the MPS will positively implement our recommendations. We urge the MPS to continue to engage in dialogue with the private sector and to continue open discussions to achieve common goals for developing a vibrant and competitive digital economy. This could include deeper collaboration between the MPS and other government agencies with the private sector such as through roundtable discussions on how the PDP Decree should be enforced.

Please do not hesitate to contact us if you require any clarification or further information. Thank you once more for your time and consideration.

Sincerely,

Wong Wai San

Wong Wai San
Senior Manager, Policy – APAC