Revised Personal Information Protection Act Bill

Comments from BSA | The Software Alliance

November 17, 2021

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the National Assembly regarding the revised Personal Information Protection Act (**PIPA**) Bill. BSA is the leading advocate for the global software industry before governments and in the international marketplace. We have extensive experience engaging with governments around the world to promote effective, internationally interoperable legal systems that protect personal information and provide strong consumer rights while supporting responsible uses of data-driven technologies. BSA supports privacy frameworks that increase the transparency of personal data collection and use; provide individuals with control over their personal data; enhance robust data security obligations; promote the use of data for legitimate business purpose; and enable the international transfers of data.[2]

BSA members create the technology products and services that power other businesses. Our members offer enterprise tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Companies entrust some of their most sensitive information to BSA members, and our members work hard to keep that trust.

Our comments to the revised PIPA Bill build on our February submission on the PIPA and focus on measures designed to protect consumer privacy and personal data while supporting an interoperable approach to data protection. Our comments also focus on areas in which the PIPA Bill could be further aligned with leading international approaches to privacy and data protection to strengthen consumer protections

Our recommendations, discussed in greater detail below, address the following topics:

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

[2] See BSA Global Privacy Best Practices at: https://www.bsa.org/files/policyfilings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf. In Korean at https://www.bsa.org/files/policyfilings/A4_2018_BSA_Global_Privacy_Best_Practices_ko.pdf.

300 Beach Road
#25-08 The Concourse
Singapore 19955

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

Regional Representative Office
UEN: S97RF0005K

- Revise the Roles and Responsibilities of "Outsourcees" (Data Processors) To Ensure Obligations Do Not Inadvertently Undermine Privacy
- Provision on Periodic Notification to Data Subjects
- Facilitating International Data Transfers
- Data Portability Requirements
- Thresholds for Data Breach Notification
- Potentially Excessive Onsite Inspections Requirement
- Review Maximum Civil Penalties

Recommendations

Revise the Roles and Responsibilities for "Outsourcees" (Data Processors) to Ensure Obligations Do Not Inadvertently Undermine Privacy

BSA appreciates that there is distinction between the concepts of data controller and data processor in the PIPA Bill as outlined in Article 26(5), which covers the entrustment or outsourcing of personal information processing by a "personal information controller" (frequently referred to as "data controller" or "controller") to an "outsourcee" (frequently referred to as "data processor" or "processor"). At the same time, we are concerned that several substantive obligations reflected in the PIPA Bill conflate these two roles — in ways that may inadvertently but significantly undermine the privacy and security goals of PIPA.

Definitions. At the outset, we want to recognize the PIPA Bill's approach of defining these two separate roles sets a critical foundation for a strong privacy and data protection law. Distinguishing between companies that decide how and why collect and use data about individuals (data controllers) and companies that only process such data on behalf of other companies (data processors) is critical because both data controllers and data processors have important, but distinct, roles in protecting personal information. For that reason, leading personal data protection laws worldwide clearly distinguish between these two different entities and assign each with respective responsibilities that reflect their different roles in safeguarding personal data. In contrast, failing to recognize these different roles can ultimately undermine consumer privacy and security — including by requiring processors that do not interact with consumers to begin reaching out to them, thus exposing processors to more personal data than necessary. Although PIPA recognizes these two distinct concepts, BSA strongly encourages that the PIPA further clarifies the dividing line between these two roles by defining a "personal information controller" as the entity that determines the purposes and means of processing data.

Substantive Obligations. We have significant concerns about the substantive obligations placed on outsourcees (data processors) — which distort their role in handling personal data. By placing consumer-facing obligations on outsourcees (data processors) who often have no direct relationship with a consumer, the PIPA Bill risks undermining consumer privacy and is inconsistent with the

approach taken by other leading privacy laws around the world, such as the European Union's General Data Protection Regulation (GDPR)[3] and Singapore's Personal Data Protection Act (PDPA).[4]

Most critically, consumer-facing obligations should not apply to data processors. To protect consumers' personal data, a privacy law can and should impose a range of obligations on the companies that decide how and why that data is used. Those companies are the data controllers — which often have a direct relationship with individual data subjects. For this reason, leading privacy laws worldwide impose consumer-facing obligations on data controllers — but not on data processors. For example, the GDPR places on controllers the obligation to honor consumer rights requests and the obligation to provide data subjects with certain information about their processing. Processors, in turn, are not subject to those obligations under the GDPR — and instead, are required to assist controllers in fulfilling certain obligations and to process data pursuant to the controller's instructions. This approach is designed to ensure that personal data remains protected when handled by processors. The approach embodied in the PIPA Bill risks undermining such protections.

These concerns are particularly high with two types of obligations:

- *Consent*. Consent obligations are among the consumer-facing obligations that are appropriately placed on data controllers, not outsourcees (data processors). A consumer buying a good or service typically interacts with the controller providing that service — and may rightly expect the controller to ask their consent to process their personal data for certain purposes. But consumers do not expect all of the outsourcees that a controller may rely on to provide its products – which can be dozens or more – to also reach out to them requesting their consent to process personal data for the purposes for which the controller has already obtained consent. Article 26(8) of the PIPA Bill could be read to impose exactly such an obligation, thus, creating significant security risks if outsourcees must ask for consent from individuals they do not know and whose identity they may not be able to authenticate. Instead, the obligation to obtain consent should fall only on the controllers. Outsourcees (data processors) should be required to process data on behalf of those controllers and in line with their instructions — an approach that ensures the data remains safeguarded when handled by an outsourcee.

- *Responding to Consumer Rights Requests.* Responding to consumer rights requests to access, correct, or delete personal data often requires authenticating the identity of the consumer making the request and understanding whether the information requested should be provided. Those decisions should be made by controllers, which generally interact with consumers and that decide when and why to collect personal data. For that reason, laws like the GDPR require controllers to respond to consumer rights requests, but not the processors. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold. These obligations are ill-suited to outsourcees, which are often not privy to information about the nature of the data they are processing or the purposes for which such processing is being conducted — because those purposes are determined by the data controller. Moreover, outsourcees may be contractually *prohibited* from accessing data they store or otherwise process for a controller and may design their processing activities to minimize the amount of personal data they need to access — all of which better protects the privacy of that data. Requiring outsourcees to access and review personal data they otherwise would not, undermines such protections.

[3] Article 28, GDPR, https://gdpr-info.eu/art-28-gdpr/

[4] PDPA https://sso.agc.gov.sg/Act/PDPA2012

Of course, personal data should remain protected when it is handled by an outsourcee — but the outsourcee's obligations must reflect its role in processing data, which is to handle data on behalf of a controller and pursuant to the controller's instructions. Data protection laws therefore appropriately focus on ensuring processors act only on the documented instructions of a controller, assist the controller in carrying out certain obligations, and adopt reasonable data security and organizational measures to safeguard data held by the processor.

We have significant concerns with Article 26(8), which continues to impose consumer-facing obligations on outsourcees (data processors). These include, among others, the obligations for "outsourcees" to:

- obtain consent from data subject to process their data (Article 22, 22-2);
- notify the data subject in case of transferring data due to business transfer (Article 27);
- obtain consent from the data subject in case of cross-border transfer and to respond to data's subject's request to stop the cross-border transfer (Article 28-8, 28-9);
- notify the data subject in case of a data breach (Article 34),
- respond to a request made by data subjects to transfer its data (Article 35-2),
- respond to consumer rights request, including requests made by data subject to delete its data (Article 36); requests to stop the processing of its data (Article 37), and requests made by the data subject to explain the of automated decision-making process (Article 37-2).

BSA recommends the following changes to the PIPA Bill's approach to these issues:

- **First, further clarifying the distinct roles of "personal information controllers" and "outsourcees" by defining a personal information controller as the entity that determines the purposes and means of processing.**
- **Second, revising Article 26(8) to clarify that outsourcees are not subject to consumer-facing obligations**. **These include: Articles 15 to 18, 21, 22, 22-2, 27, 28-2, 28-9, 34, 35-2, 36, 37-2.**
- **Third, revising Article 26 to ensure that outsourcees remain subject to important obligations to safeguard the data they hold. Specifically, we recommend revising this provision to make clear that outsourcees be required to assist a controller with certain obligations and should put in place reasonable security measures to safeguard personal data and to establish corporate privacy programs that adopt a risk-based approach to managing privacy and security concerns.**
- **Fourth, and in the event that Article 26(8) is not clarified along the lines suggested above, we strongly recommend revising the penalties and remedies provisions in Articles 64 and 70-75 so that they are only available against outsourcees that knowingly violate a substantive obligation. As set out above, outsourcees in many cases will only have limited information about the types of data processed on behalf of a controller – and the concerns about applying consumer-facing obligations to outsources are compounded by these penalty provisions. For example, an outsourcee may be subject to administrative penalties for processing sensitive information without a data subject's consent. However, as mentioned earlier, outsourcees are often not in a**

position to know the nature of the personal data they are processing, nor should they be interacting with the data subject directly. At minimum, to the extent that Article 26(8) is retained, the penalties and remedies provisions in Articles 64 and 70-75 should be revised so that they are only be available against outsourcees that knowingly violate the relevant substantive obligation.

Provision on Periodic Notification to Data Subjects

Article 20-2 lays down the obligation for data controllers to ***periodically*** notify the data subjects of their statement of use, the matters relating to the processing of personal information and the rights available to data subjects, thereof. We believe that providing privacy notices to consumers when there have been no changes in the content of the notification, data handling practices of the organization or where no new personal information is being processed, could potentially confuse the data subjects and inundate them with notifications without serving the purpose of enhancing privacy protections.

We therefore recommend that the provision be amended to require notification to the data subjects of the statement of use or other information on processing of personal information, only upon any material changes in the processing practices, new information being collected, or any updates to the existing statements of use and/or privacy notices.

Facilitating International Data Transfers

BSA appreciates the proposed inclusion of several data transfer mechanisms under Article 28-8(1). Enabling personal information controllers to use different mechanisms to transfer personal information across international borders affords businesses the flexibility to determine the mechanisms that will be most optimal and relevant for them.

However, we continue to have concerns with the PIPA Bill's approach to international data transfers, which underpin today's global economy. We reiterate three recommendations designed to facilitate cross-border transfers:

- *First*, we remain concerned about the requirement to obtain "separate consent" for those transfers undertaken on the basis of consent under Subparagraph 1 of Article 28-8(1). Requiring entities to obtain "separate consent" is impractical and may result in consumers receiving a much higher volume of consent request, compounding concerns about the potential for consent fatigue. **We recommend that the PIPA Bill treat the original consent for processing as sufficient for a transfer rather than requiring a "separate consent."**

- *Second*, BSA recommends **deleting the requirements in Article 28-8(2), which require companies to provide data subjects with a long list of information about data transfers if they undertake such transfers on the basis of consent**. These not only include the "particulars of the personal information to be transferred" but also, the "countries, times and methods of transfer", the "name and contact information of the person to whom personal information is transferred," the "purpose of using personal information and the period of use and retention" by the recipient, and the "methods and procedures for refusing to transfer".

  These prescriptive notification requirements create significant burdens for both Korean and non-Korean businesses delivering global services, and much of this information would not be meaningful or relevant to a data subject in understanding how these transfers might impact the processing of their personal data. For example, requiring companies to provide information such as the methods of data transfer and the period of use and retention of the personal information to be transferred, including those of the recipient's, risks inundating

consumers with information that does not meaningfully enhance their privacy or the protection of their personal information. Moreover, requiring a controller to provide specific contact information for each recipient could reduce the ability of companies to engage new subprocessors, including in situations where new subprocessors need to be obtained quickly to address security concerns or continue providing services during a potential outage.

Alternatively, if such requirements are maintained, we recommend that the provision be amended to limit the information to the categories of the personal information transferred, the purposes, the recipient countries, categories of the recipients, the rights available to data subjects and data storage or retention criteria or periods, as feasible. This would also align this provision with the requirements envisaged under the GDPR.

- Third, **we continue to urge the recognition of additional data transfer mechanisms under Article 28-8(1), such as intra-corporate binding rules, international trustmarks and regional certifications** which can help create more flexibility in supporting cross-border data transfers. These mechanisms are incorporated in other global data protection frameworks to promote cross-border data flows, including the APEC Cross Border Privacy Rules (CBPR) of which Korea is a participant, the European Union's General Data Protection Regulation (GDPR), and Japan's Act on the Protection of Personal Information. Given that Subparagraph 4 of Article 28-8(1) allows an entity that has attained certification under Article 32-2 to transfer personal information, recognizing international trustmarks and other regional/domestic certifications with standards consistent with the PIPA will further enhance interoperability and facilitate international data transfers seamlessly.

Data Portability Requirements

The proposed draft amendments provide data subjects with new rights, such as the right to request a personal information controller to transmit their personal information to themselves, another personal information controller, or a personal information management-specialized organization.[5] The new right under Article 35-2 resembles the right to data portability found in Article 20 of the GDPR[6] and Article 26F-J of Singapore's PDPA.[7] While the Article itself specifies that the right may be exercised by the data subject only against a personal information controller to transmit their personal information to themselves or another personal information controller or a personal information management-specialized organization, when Article 35-2 is read together with the provision under Article 26 (8), it would place the data portability obligation 'mutatis mutandis' on the data processor as well. This departs from the data portability provisions envisaged under the GDPR and PDPA, both of which place the obligation only upon the personal information controllers.

To the extent individuals are allowed to exercise this right against companies acting as outsourcees (data processors), it would create potential privacy and security concerns. As noted above, data processors act on behalf of their business customers and generally do not interact with consumers – so may be unable to verify the identity of an individual seeking to exercise this right. In addition, a processor may not have the right to access or analyze data subjects' data. To the extent a processor is nonetheless required to honor such requests, there is a security risk that they could be obligated to provide a data subject's information to an individual they cannot authenticate as the appropriate data

[5] PIPA Articles 35-2 and 35.3.

[6] https://gdpr.eu/article-20-right-to-data-portability/

[7] https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210#pr14-

subject. **We therefore reiterate our recommendation in the earlier section to exclude data processors (outsourcees) from the obligation under Article 35-2.**

Article 35-2 also requires a transferring entity to confirm that the data recipient fits into one of the three categories outlined in Article 35-2(1). However, it is not clear whether the obligation to ensure that the data recipient meets the applicable standards in sub-paragraph 3 falls on the data subject or transferring entity; whether the request can be rejected if there are reasonable grounds to believe that the recipient does not meet these applicable standards; and, whether the transferring entity would be liable if the data recipient turned out to be a fraudulent entity. We would encourage the PIPA Bill to establish clearer guidance on these issues.

Article 35-3 further sets out the tasks and competencies required of a "personal information management-specialized organization" to support data subjects' requests to transmit their personal information. It is currently unclear if the "personal information management-specialized organization" would be a public or private entity, the data protection obligations that such an entity would be subject to, and the requirements for personal information to be transmitted to the "personal information management-specialized organization" (besides a data subject's request to do so). While we support a user-centric approach to data protection that provides consumers with rights and the mechanisms to control their personal data in a safe and deliberate manner, these rights must be implemented in a manner that does not raise new privacy and security concerns. We would also encourage that such a right be flexibly implemented based on internationally recognized practices to minimize conflicting legal obligations on organizations.

Thresholds for Data Breach Notification

BSA supports reasonable and appropriate personal data breach notification requirements that are consistent with global best practices. Such requirements provide incentives to ensure robust protection of personal information, and to enable data subjects to take actions to protect themselves from serious harm.

BSA reiterates that it is critically important to set the correct threshold for reporting and to allow sufficient time for data controllers to report. We therefore recommend amending Article 34(1) to make clear that personal information controllers should only be required to notify data subjects **without undue delay** after establishing that a **breach involves the unauthorized access to, or loss of, unencrypted or unredacted personal data that creates a material risk of harm to an individual**, such as identity theft or financial fraud.

Potentially Excessive Onsite Inspections Requirement

BSA reaffirms its support for mechanisms designed to resolve disputes efficiently. However, the proposed amendments in Article 45 (2) that empower the Dispute Mediation Committee to conduct onsite investigations may be excessively intrusive and burdensome, especially considering that mediation processes are typically not supposed to be adversarial in nature. The current provisions under Articles 45 (1) and 45 (3) already provide the Dispute Mediation Committee with sufficient authority to request the materials necessary to mediate the dispute and the submission of data or opinions related to the dispute from disputing parties. BSA accordingly urges **removing the Dispute Mediation Committee's authority to conduct on-site inspections in dispute mediation cases**.

Review Maximum Civil Penalties

BSA strongly supports the revisions in Article 64-2 (3) addressing factors the PIPC would consider when imposing a civil penalty. These include mitigating factors such as the degree of harm to data subjects, the nature of the data breach, and the recovery and management measures put in place by

organizations, when deciding the level of penalty surcharges to be imposed on infringing organizations.

In our view, civil penalties should be proportionate to the harm caused to the data subjects and reflect the presence or absence of any aggravating or mitigating factors. We recommend clarifying Article 64-2 to recognize that civil penalties in Article 64-2(1) are only imposed in light of the harm at issue in each case and in light of these mitigating circumstances. Specifically, the PIPA Bill could adopt language similar to the GDPR, which provides that monetary fines are to be imposed "in each individual case" if "effective, proportionate, and dissuasive." We also encourage further guidance on these provisions that can explain the imposition of fines should be a last resort, taking into account a list of mitigating or aggravating factors.

We recommend the PIPA Bill's maximum civil penalty of "3% of annual turnover" **be tied to the degree of violation and harm caused to data subjects.** If the Government of Korea nonetheless imposes the revenue-based maximum financial penalty, it can help to ensure those penalties are proportionate to harms caused by the violation of PIPA by expressly recognizing that the turnover calculation is based on **turnover "in Korea"**.

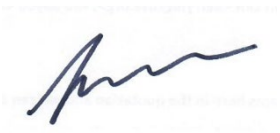
Conclusion

BSA is grateful for the opportunity to provide these comments and recommendations on the proposed PIPA Bill. We strongly support the Korean Government's efforts to review and update the personal data protection regime in Korea, responding to the ever-evolving needs of the digital economy and data innovation. We look forward to continuing to collaborate with the National Policy Committee on privacy and personal data protection policies. Please do not hesitate to contact us if you have any questions or comments regarding our suggestions.

Sincerely,

Geun Kim

Country Manager Korea



BSA | THE SOFTWARE ALLIANCE