Draft Partial Amendments to the Personal Information Protection Act

Comments from BSA | The Software Alliance

February 16, 2021

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Personal Information Protection Commission (**PIPC**) regarding the draft partial amendments to the Personal Information Protection Act (**PIPA**). 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.

Our comments to the draft partial amendments focus on measures designed to protect consumer privacy and personal data while supporting an interoperable approach to data protection that enables companies to deliver the global services demanded by the individuals and businesses they serve.

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

- Recognizing Distinct Roles of Data Controllers and Data Processors
- Enabling International Data Transfers
- New Data Rights for Data Subjects
- Expanding Legal Bases for Processing Personal Information
- Designating Self-Regulatory Organizations
- Thresholds for Data Breach Notification
- Notification on Statement of Use and Privacy Policy
- Potentially Excessive Onsite Inspections Requirement
- Proportionate Civil Penalties Based on Consequences of Violation

BSA members create the technology products and services that power other businesses. Our members offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. BSA members are enterprise software companies that are in the business of

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

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, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

providing privacy protective technology products and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

Companies entrust some of their most sensitive information to BSA members, and our members work hard to keep that trust. Companies also rely on BSA members to provide technologies that can advance social and economic goals, from helping businesses transition to remote work and ensuring the continuity of their operations[2] to empowering researchers and first responders with new tools to address the spread of infectious diseases such as COVID-19.[3] We hope our comments will assist the PIPC to ensure that revisions to the PIPA advance the objectives of enhancing consumer privacy and personal information protection, while ensuring the law is internationally interoperable with emerging global norms and enables and facilitates innovative uses of data to drive economic growth and job creation in Korea.

General Observations

As countries worldwide develop or update their personal information protection laws and regulations, it is critical that they ensure those frameworks are designed to provide effective privacy protections in a manner that is internationally interoperable, flexible enough to account for rapidly evolving technologies and business models and are able to facilitate innovation and progress in promising new technologies such as advanced data analytics and artificial intelligence (**AI**). 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.[4]

BSA strongly supports the Government of Korea's commitment to improve Korea's personal information protection regime while enhancing flexibility for the responsible use of personal information to drive innovation and economic growth. The proposed partial amendments to the PIPA assist in this regard by empowering the PIPC and by introducing amendments to facilitate more flexible use of personal data.

In the sections below, we respond to proposals within the draft partial amendments and suggest additional proposals to amend the PIPA in line with emerging policy developments and internationally recognized approaches.

[2] BSA's Response & Recovery Agenda at: https://www.bsa.org/files/policy-filings/05272020bsaresponserecoveryagendaa4.pdf

[3] COVID-19 Response: Software Solutions Enable Vaccine Research, Security, Safe Distribution at: https://software.org/news/covid-19-response-software-vaccine-research-security-distribution/

[4] 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.

Recommendations

Recognizing Distinct Roles of Data Controllers and Data Processors

Article 26 of the PIPA allows a "personal information controller" (frequently referred to as "data controller") to outsource the processing of personal information to an "outsourcee" (frequently referred to as "data processor"). The distinction between companies that decide when and how to collect and use data about individuals (data controllers) and companies that only process data on behalf of other companies (data processors) is an important one because both data controllers and data processors have important, but distinct roles in protecting personal information. For that reason, personal data protection laws worldwide reflect a global consensus that clearly distinguishes between the two types of entities and assigns each type of entity responsibilities that reflect their different roles in safeguarding personal data.

In its current form, several PIPA provisions conflate these two distinct roles and risk undermining the goal of furthering consumer privacy. We accordingly urge the PIPC to consider two related issues as you revise the PIPA.

- **First, we urge the PIPC to clarify that consumer-facing obligations do not apply to "outsourcees".** These include obligations to obtain data subjects' consent to process their data and the obligation to honor data subjects' rights requests, such as requests to access, delete, or transmit personal information.

  These obligations belong on data controllers because such companies often have a direct relationship with individual data subjects and decide when and why to collect consumers' data. In contrast, data processors generally do not have direct relationships with individual data subjects and process data on behalf of a data controller, usually pursuant to a contractual relationship and in line with the data controller's instructions. In this role, data processors may not be privy to 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, data processors may be contractually *prohibited* from accessing data they store or otherwise process for a controller or from processing that data for purposes other than those directed by the controller.

  Placing consumer-facing obligations on data processors may inadvertently undermine consumer privacy since it may require data processors to review significant amounts of data they otherwise would not review and could require them to access and analyze such data to identify individuals to whom they must reach out to satisfy their legal requirements. This can create a host of privacy and security issues, particularly to the extent that data processors could be required to provide data to individuals they do not know and whose identity they may be unable to rightfully authenticate. The obligation to interact with those individuals should instead fall on data controllers to ensure these important rights and obligations are not exercised in a manner that inadvertently undermines PIPA's privacy protections.

- **Second, we urge the PIPC to ensure that data processors remain subject to important obligations to safeguard the data they hold**. These obligations include enacting reasonable security measures to safeguard the data and putting into place corporate privacy programs that adopt a risk-based approach to managing privacy and security concerns.

To accomplish these two objectives, we recommend the PIPC amend the PIPA to clarify that many of PIPA's consumer-facing obligations do not apply to "outsourcees" (data processors) but only to "personal information controllers" (data controllers). This can be achieved by amending Article 26(8), which identifies other articles within PIPA that are applied to outsourcees. We recommend Article 26(8) be revised to exclude outsourcees from the following sets of obligations: (1) the consumer-facing obligations imposed by Articles 15 to 25-2 and 27-28 that impose obligations based on the purpose for which data is processed; as noted above, the data controller determines the purposes of processing — which may not be known to the outsourcee; (2) the obligations subject to a privacy impact assessment under Article 33 and to notify data subjects of a breach under Article 34; and, (3) the consumer rights articulated in Articled 35-38. As noted above, data controllers are best positioned to interact with individual data subjects while data processors are unlikely to know those data subjects and may lack information needed to authenticate their identity.

While the PIPA's consumer-facing obligations are critical for effectively protecting personal information privacy, we urge the PIPC to ensure these obligations are not inappropriately applied to entities that have very different roles in handling consumers' data. Doing so will undermine, not strengthen, privacy and data security. Instead, these consent-based obligations and consumer rights requests should apply to data controllers, whereas data processors should be accountable for handling data securely and in line with a controller's instructions.

Enabling International Data Transfers

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 PIPA allows companies to responsibly transfer data internationally.

BSA appreciates the proposed inclusion of several data transfer mechanisms under Article 28-8(2). This approach will enable personal information controllers to use different mechanisms to transfer personal information across international borders and afford businesses the flexibility to determine the mechanisms that will be most optimal and relevant for them. However, we encourage Article 28-8(2) be revised to recognize additional transfer mechanisms and to create more flexibility in supporting cross-border transfers. In particular, we recommend:

- **Revising Article 28-8(2) to recognize additional transfer mechanisms**, including intra-corporate binding rules, international trustmarks, regional certifications, and contractual arrangements as additional acceptable mechanisms that can support international 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.

- **Revising the consent requirements in Article 28-8(2),** which require personal information controllers to obtain "separate consent regarding cross-border transfer from the data subject". BSA recommends in cases where the cross-border transfer of personal information is needed to fulfil the purpose of collecting the personal information, the original consent for processing should suffice to support the transfer rather than requiring a "separate consent."

BSA further recommends **deleting the requirements in Article 28-8(3),** which requires companies to provide data subjects with a long list of information about data transfers. These include the "particulars of the personal information to be transferred" but the "countries, times and methods of transfer" and the "name of a 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 requirements create significant burdens for both Korean and non-Korean businesses delivering global services without helping data subjects understand how their information may be handled. 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 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.

The effectiveness of data security and personal information protection has less to do with where data is physically stored or processed than the technologies, systems, and procedures in place by the companies handling the information. **Thus, instead of the requirements listed in Article 28(3), we recommend requiring the company transferring personal data to retain responsibility to ensure that it is processed appropriately and in compliance with Korea's laws, and for addressing individuals' requests for access, information, deletion, correction, or other rights.**

New Data Rights for Data Subjects

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 draft amendments also grant data subjects the rights to refuse, raise objection against, and request to explain of automated decision-making that may have a significant impact on their lives, body, or property.[6]

BSA supports 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. However, these rights must be implemented in a manner that does not raise new privacy and security concerns — which could ultimately undermine the goals of a data protection framework. The new right under Article 35-2 resembles the right to data portability found in Article 20 of the GDPR[7] and Article 26F-J of Singapore's Personal Data Protection Act (**PDPA**).[8] However, Article 35-2 departs from the data portability rights in the GDPR and PDPA as the obligation is placed on both personal information controllers outsourcees (data processors) under the PIPA.

As phrased, the proposed right may create meaningful data privacy and security concerns. To the extent individuals may exercise this right against companies acting as outsourcees (data processors), it creates potential privacy and security concerns. As noted above, data processors act on behalf of their business customers and generally do not have rights to access or analyze data subjects' data. Data processors also do not generally have direct relationships with individual data subjects and may therefore be unable to verify the identity of a data subject seeking to exercise this right. To the extent

[5] PIPA Articles 35-2 and 35.3.

[6] PIPA Articles 37-1 and 37-2

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

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

a processor is nonetheless required to honor such requests, there is a privacy risk that they could be obligated to provide a data subject's information to an individual they cannot authenticate as the appropriate data subject. We accordingly recommend that the PIPC exclude outsourcees (data processors) from the obligation under Article 35-2 and encourage the PIPC to ensure that such a right be flexibly implemented based on internationally recognized practices which will minimize conflicting legal obligations on organizations.

In addition, the draft amendments could require personal information controllers to explain to and exclude data subjects from certain types of automated decision-making. We recommend narrowing the scope of this proposed right to focus on an individual's right to object to decisions based solely on automated processing rather than broadening that right to include requiring an explanation of such decision-making. Automated decision-making activities are now commonly used in applications and services across many sectors for a range of activities. It may be appropriate to empower individuals in some circumstances to opt out of automated decision-making that can create certain legal effects. At the same time, we encourage the PIPC to support international efforts and the development of internationally recognized standards that will improve the "explainability" of automated decision-making activities to help ensure data subjects understand and trust automated decision-making processes.

Expanding Legal Bases for Processing Personal Information

Article 15(1) of the PIPA currently permits personal information controllers to rely on several independent legal bases for the collection and use of personal information. These include processing with consent; in connection with the performance of a contract; in the public interest or the vital interest of the data subject; necessary for compliance with a legal obligation; and "justifiable interest" of a personal information controller. BSA further notes the proposed inclusion of Paragraph 7 under Article 15(1) which will allow the temporary processing of personal information for public safety and well-being.

BSA supports Article 15(1) which provides a range of grounds for processing personal information on bases other than consent. This approach has strong foundations in other globally recognized data protection frameworks and reduces the burden on consumers to consent to the use of personal information when that processing is needed to carry out a contract they have entered or to perform certain other types of processing. At the same time, we are concerned that some of the existing grounds for processing under Article 15(1) are framed too narrowly.[9]

We recommend further expanding the grounds for processing under Article 15(1) Paragraph 6, to align it with the "legitimate interest" basis for processing contained in other global data protection laws. The "legitimate interest" ground for processing is a well-established feature of data protection frameworks that aims to facilitate the use of personal data for innovative purposes while ensuring that the risks to individual rights and freedoms of individuals are appropriately taken into account. While the "justifiable interest" ground for processing personal data in Paragraph 6 of Article 15(1) appears similar to the "legitimate interest" ground for processing, it is framed more narrowly. This is particularly true as Paragraph 6 may require proof that a personal information controller's "justifiable interest" is "manifestly superior" to the data subject's rights. The legitimate, or justifiable, interest basis should be permitted if it does not adversely affect the data subjects' rights and interests. For instance, companies should be able to rely on legitimate or justifiable interests for the beneficial processing of personal information for purposes of fraud detection and prevention; monitoring, detecting, and protecting a network via cybersecurity measures; or updating products and services to ensure

[9] Article 15(1), Paragraph 6.

accuracy and reliability. BSA accordingly recommends that the PIPC consider broadening the scope of Paragraph 6 of Article 15(1) to create more flexibility and regulatory certainty in line with other leading data protection frameworks.

Designating Self-Regulatory Organizations

The draft amendments in Articles 13(2) and 13(3) allow the PIPC to establish "self-regulatory organizations" representing personal information controllers in different sectors which will be tasked to regulate personal information with the assistance of the PIPC.

BSA generally supports initiatives that promote and enhance organizations' accountability in their data protection measures. We are also encouraged that the proposed "self-regulatory organization" initiative is envisaged to take the form of a private-public partnership, with the PIPC providing technical, administrative, and financial support to "self-regulatory organizations", where appropriate. However, given that "self-regulatory organizations" are expected to draft voluntary industry covenants, there is a need for clearer distinction between the PIPC's guidelines and the covenants that will be established by the self-regulatory organization to avoid regulatory overlaps and confusion by the industry.

BSA also notes that there are no specific incentives in the current amendments of Articles 13(2) and 13(3) that will encourage "self-regulation". As the PIPC refines its approach to the "self-regulatory organizations" and develops language of the Presidential Decree that will prescribe the implementation details, BSA urges the PIPC to conduct meaningful stakeholder consultations on the designation, roles, and responsibilities of the "self-regulatory organizations", including incentives or measures of self-regulation that will encourage personal information controllers to move towards "self-regulation". This is especially important given that the "self-regulatory organizations" are expected to represent and regulate specific sectors through industry covenants. BSA looks forward to contributing our input and recommendations to these stakeholder consultations.

Thresholds for Data Breach Notification

BSA supports reasonable and appropriate personal data breach notification requirements that are consistent with global best practices to provide incentives to ensure robust protection of personal information. These actions enable data subjects to take actions to protect themselves from serious harm. To achieve these goals, it is critically important to set the correct threshold for reporting breaches based on risk of harm to individuals, to allow sufficient time for data controllers to report, and to provide appropriate exceptions to the notification requirement.

In this regard, BSA recommends amending Article 34(1) to make clear that personal information controllers should 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.

Notification on Statement of Use and Privacy Policy

The newly proposed Article 20-2 appears to require personal information controllers and outsourcees to periodically notify data subjects of their use of the data subject's personal information, as may be prescribed by the Presidential Decree. Requiring the publication of a privacy policy to inform data subjects of how their personal information is being collected, processed, and handled by personal information controllers improves transparency and is found in many privacy frameworks such as the

EU GDPR,[10] Canada's Personal Information Protection and Electronic Documents Act, [11] and Australia's Privacy Act.[12] Consumers are accordingly able to access these privacy policies as they interact with services over time. BSA recommends clarifying that the periodic notification requirement under Article 20-2 be to state clearly that the obligation can be met by keeping the personal information controller's privacy policy, as set forth under Article 30, up-to-date and accessible to data subjects.

Relatedly, BSA notes that the proposed amendments in Article 30-2 will give the PIPC powers to review if a company's privacy policy is in violation of the PIPA upon the request of certain entities or persons. However, the details of the review process and how such a request may be raised are to be addressed by the Presidential Decree. BSA encourages the PIPC to conduct meaningful stakeholder consultations as it develops the procedures for submitting a review request and the review criteria. Such procedures should be based on international best practices.

In addition, as noted previously, given that "outsourcees" (data processors) generally do not have a direct relationship with the data subjects, we urge excluding "outsourcees" from obligations under Articles 20-2 and 30

Potentially Excessive Onsite Inspections Requirement

The newly proposed amendments in Article 45 (2) provide the Dispute Mediation Committee the authority to conduct fact-finding and onsite investigations if deemed necessary. While BSA supports mechanisms designed to resolve disputes efficiently, the measures should not be overly burdensome and excessive. The current provisions under Articles 45 (1) and 45 (3) already provide the Dispute Mediation Committee with the authority to request the materials necessary to mediate the dispute and the submission of data or opinions related to the dispute from disputing parties. Therefore, BSA urges PIPC to remove the Dispute Mediation Committee's authority to conduct on-site inspections in dispute mediation cases.

Proportionate Civil Penalties Based on Consequences of Violation

Civil penalties should be proportionate to the harm caused to the data subjects and whether there are any aggravating or mitigating factors. Mitigating factors could include (a) how actively and promptly the organization has tried to resolve the matter with the data subject; (b) whether the organization took reasonable steps to prevent or reduce the harm caused by the breach or violation; and (c) whether the organization has provided affected data subjects with remedies. Aggravating factors could include (a) whether the breach was intentional or repeated or (b) whether the organization knew or should have reasonably known of the risk of the breach or violation but continued with its operations without taking measures to minimize the risk or remedy the breach. BSA urges PIPC to review the civil penalties taking into consideration the mitigating factors highlighted earlier.

Conclusion

BSA is grateful for the opportunity to provide these comments and recommendations on the proposed amendments to the PIPA. We support the Korean Government's efforts to review and update the

[10] https://gdpr.eu/article-12-how-controllers-should-provide-personal-data-to-the-subject/

[11] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/

[12] https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy/#:~:text=A%20privacy%20policy%20is%20a,agency%20handles%20your%20personal%20information.&text=The%20Privacy%20Act%20covers%20organisations,Australia%2C%20and%20some%20other%20organisations

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 PIPC on privacy and personal data protection policies. Please do not hesitate to contact us if you have any questions or comments regarding our suggestions.

BSA | THE SOFTWARE ALLIANCE