



August 14, 2023

## BSA COMMENTS ON THE PERSONAL INFORMATION PROTECTION ACT DRAFT REGULATIONS ON OVERSEAS TRANSFERS OF PERSONAL INFORMATION

### Submitted Electronically to the Personal Information Protection Commission (PIPC)

BSA | The Software Alliance (**BSA**)<sup>1</sup> welcomes the opportunity to provide our comments on the Personal Information Protection Act's Draft Regulations on Overseas Transfers of Personal Information (**PIPA** and **Draft Regulations** respectively).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software.

BSA has followed the development of the PIPA closely and provided comments on the PIPA's recently released Draft Enforcement Decree.<sup>2</sup> We note that the purpose of the Draft Regulations is to "prescribe matters necessary for the transfer of personal information abroad" pursuant to the Draft Enforcement Decree.<sup>3</sup> In this regard, BSA appreciates that the PIPA amendments have established additional legal bases for the overseas transfer of personal information. Currently, under Article 28-8 of the amended PIPA, the legal bases pursuant to which personal information may be transferred out of Korea include:

1. When the data subject has separately given his or her consent;
2. When there are special provisions regarding the cross-border transfer of personal information in laws, treaties, or international agreements;
3. When the: (i) outsourcing of the processing of personal information or the storage thereof is necessary for the execution or performance of a contract; and (ii) information that must be notified to data subjects when obtaining consent for the cross-border transfer of personal

---

<sup>1</sup> 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.

<sup>2</sup> See: BSA Comments on Personal Information Protection Act Draft Enforcement Decree, June 2023, <https://www.bsa.org/policy-filings/korea-bsa-comments-on-personal-information-protection-act-draft-enforcement-decree>.

<sup>3</sup> Draft Regulations (2023), Article 1.

information has been disclosed in the privacy policy or notified individually to data subjects via methods prescribed by the Enforcement Decree of the PIPA (e.g., by email);

4. If the overseas recipient has obtained data protection certification prescribed by the PIPC and has taken all of the following measures: (i) security measures necessary for the protection of personal information and measures necessary to guarantee the rights of data subjects; and (ii) measures necessary to conduct data processing in accordance with data protection certification in the country where personal information is to be transferred; and
5. When personal information will be transferred cross-border to a country or international organization recognized by the PIPC as having essentially equivalent levels of data protection as those required under the PIPA.

BSA has two recommendations for PIPC's further consideration.

## **Contract-based and other mechanisms for cross-border transfers of personal information**

While the amended PIPA substantially expanded the legal bases for transferring personal information overseas, it is not clear if contract-based transfer mechanisms, including Standard Contractual Clauses (**SCCs**), fall within these legal bases. SCCs offer a workable model for cross-border transfers of personal information that is consistent with the requirements in the PIPA. Many global companies have widely adopted contract-based transfer mechanisms to protect personal information as it is transferred between countries and regions. Our member companies have also adopted SCCs such as the European Union's SCCs (**EU SCCs**) and the UK's International Data Transfer Agreements (**UK IDTAs**). Korea's recognition of transfer mechanisms under such arrangements will provide further legal certainty and reduce business compliance burdens.

**In respect of the Draft Regulations, BSA recommends that the PIPC should interpret "certification" more broadly and consider recognizing other accepted legal instruments for data-transfers, such as the SCCs. PIPC and the Specialized Committee would be able to assess the "adequacy" of the internationally recognized SCCs, such as the EU SCCs and the UK IDTAs, pursuant to the criteria specified under Articles 12 to 14 and Table 1 of the Draft Regulations. If these SCCs are determined to provide adequate levels of protection, they can be notified and listed as certifications approved by the PIPC under Table 2 of the Draft Regulations. This would allow businesses that have adopted these SCCs to seamlessly transfer and receive personal information from Korea, without requiring the data subject's separate consent or adopting another certification.**

At a broader level, BSA is also encouraged that the Specialized Committee is allowed to evaluate third party certification processes under Articles 12 to 14 and Table 1 of the Draft Regulations. This will help to create more flexibility in supporting cross-border data transfers. For example, the Specialized Committee can recommend the use of internationally recognized certifications such as the ISO 27701, the Global and APEC Cross Border Privacy Rules (**CBPR**) and other such certifications that would allow the transfer of personal information outside of Korea without requiring the data subject's consent. These certifications have proved beneficial for several global companies in demonstrating their compliance with globally interoperable and trustworthy data privacy standards. 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.

## **Assessing the personal information protection level of other countries**

Following the PIPA amendments, cross-border transfers of personal information without consent are permitted when the information is transferred to a country or international organization recognized by the PIPC as having essentially equivalent levels of data protection as those required under the PIPA. The factors which the PIPC are required to consider when determining if a country provides an equivalent level of personal information protection as the PIPA are set out in Article 29-11 of the Draft Enforcement Decree.<sup>4</sup>

When conducting an assessment pursuant to Articles 18 to 22 of the Draft Regulations, the Specialized Committee and PIPC should note that not all countries have an overarching privacy law. An example of such a country is the US – while many states have passed or introduced privacy bills regulating the commercial collection and use of personal information, no comprehensive, federal-level privacy law exists. **In this regard, we urge the Specialized Committee and PIPC to look beyond the absence or presence of an overarching privacy law and consider *all* relevant laws and regulations when assessing if a country provides an equivalent level of protection.**

There is also no clear guidance for when the process for assessing a country's personal information protection level will begin, and how long the process will take for each country. **In this regard, BSA urges PIPC to stipulate a timeline for assessing a country's protection level, and to seek inputs from the industry on which countries Korea should prioritize. Relatedly, PIPC should also provide further information on its methodology for prioritizing countries for assessment. For example, PIPC could advise which countries are considered to offer an equivalent level of data protection.**

## Conclusion

We hope that our comments will assist with the implementation of the PIPA amendments and the Draft Regulations. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,



Tham Shen Hong  
Manager, Policy – APAC

---

<sup>4</sup> These factors include:

1. Whether the personal information protection system, such as laws, rules, or regulations of the Subjected Countries, etc. is consistent with the principles of personal information protection set forth in Article 3, and whether sufficiently guarantees the rights of data subject set forth in Article 4
2. Whether there is an independent supervisory authority responsible for ensuring and enforcing compliance with the personal information protection system under Paragraph (1)
3. Whether there is a damage relief procedure that can be easily accessed by the data subject in the Subjected Countries, etc. and whether the damage relief procedure effectively protects the data subject.
4. Whether there are existence and practical guarantees of protection measures for data subjects, including legal basis, procedure, and damage relief, when personal information is processed by public institutions in the Subjected Countries, etc.
5. Whether the supervisory authority of the Subjected Countries, etc. can cooperate with the PIPC on the basis of mutual understanding on the rights of data subject.
6. Other matters prescribed by the PIPC.