



Comments to the Draft Partial Amendments to the Personal Information Protection Act

The Global Data Alliance (**GDA**)² welcomes this opportunity to provide our comments to the National Assembly regarding the revised Personal Information Protection Act (PIPA) Bill. While member companies may have interests and concerns on a range of issues raised in the draft amendments, the GDA is focused on policies related to cross-border data transfers. Accordingly, this submission builds on our [February 2021 submission](#) on the PIPA and reiterates our views regarding the relevant provisions related to cross-border data transfers.

Cross-border data transfers power innovation and growth across the globe and all sectors of the economy — from manufacturing and farming to local start-ups and service providers. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.³

GDA members share a deep and long-standing commitment to protecting personal data across technologies and business models, as they recognize that today's cross-border economy depends on the trust of consumers and the general public. The GDA, therefore, supports policies that protect personal data while enabling data to move across borders.

We urge the National Assembly to ensure that the PIPA amendments will promote robust personal information protection through a flexible, pro-innovation legal framework that allows companies to responsibly transfer data both internally and externally to other entities, within and outside the Republic of Korea.

The seamless transfer of data across international borders enables the deployment of modern and emerging technologies and services that underpin the economy, across all sectors and at the local, national, and international level. This includes technologies and services enabled by data transfers, such as AI-related data analytics and machine learning technologies, as well as cloud computing, blockchain, and new privacy-enhancing technologies. These technologies and services, which are often accessed across borders or rely on data transferred across borders (or both), support many important economic activities and priorities, including remote work and virtual collaboration, distance education, telemedicine, cybersecurity, fraud monitoring and prevention, anti-money laundering, investigation of dangerous counterfeit products, and a broad range of other activities relating to the protection of health, privacy, security, and intellectual property. These technologies and services are particularly important in a country

² The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. GDA members include BSA members and American Express, Amgen, AT&T, Citi, ITB360, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, RELX, Roche, United Airlines, Verizon, Visa, UDS Technology, and WD-40 Company. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: <https://www.globaldataalliance.org/downloads/aboutgda.pdf>

³ Please see Global Data Alliance paper "The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector" available at <https://www.globaldataalliance.org/downloads/GDAeverysector.pdf>.

such as the Republic of Korea, in which jobs and exports depend upon these emerging technologies in the advanced industries where it is globally competitive, including advanced electronics, automobiles, shipbuilding, telecommunications, as well as media and content distribution. A forward-leaning policy on cross-border data transfers, which is interoperable with international frameworks, is a particularly effective tool to aid policymaker efforts to drive innovation, increase employment, and create other economic and societal benefits for government, businesses, consumers, and society.

Accountability Model and International Data Transfers

The ability to transfer data, including personal data, across international borders is the lifeblood of the modern global economy. For this reason, it is critical that the PIPA allow companies to responsibly transfer data internationally.

The GDA strongly supports the accountability model for international data transfers. This model was, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles. The accountability model provides an approach to cross-border data governance that effectively protects the privacy and consumer rights of individuals and fosters streamlined, robust data flows by requiring entities that collect personal information (often defined as personal data controllers) to be responsible for its protection no matter where or by whom it is processed.

To benefit from cross-border data transfers while simultaneously ensuring the responsible processing and protection of data, the focus of privacy policy and regulation needs to be on the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. The accountability model, therefore, continues to be an important tool in increasing privacy and security by requiring entities to ensure that data will continue to be properly protected, regardless of where the data is located.

The GDA appreciates the proposed inclusion of several data transfer mechanisms under Article 28-8(1) as they provide a range of international data transfer mechanisms that personal information controllers can choose from. However, **we recommend 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, without helping data subjects understand the utility of such information or how this impacts 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 recipients’ 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 sub-processors, including in situations where new sub-processors 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.

Flexibility and Interoperability

Personal data protection and privacy frameworks that are based on a common set of international consensus-based principles facilitate cross border data transfers and drive innovation and business investment in local markets by promoting international interoperable legal frameworks upon which businesses of all sizes can rely. These coordination mechanisms also help to bridge current gaps in international privacy norms while facilitating the safe and secure international transfer of personal

information. Such mechanisms may include private codes of conduct, contractual arrangements such as standard contractual clauses, certifications such as the APEC Cross Border Privacy Rules (CBPR), seals or marks, and mutual recognition arrangements such as the adequacy with the European Union General Data Protection Regulation (GDPR).

As noted above, the GDA welcomes the proposed inclusion of several international data transfer mechanisms under Article 28-8(1) but urges this provision be expanded to recognize additional transfer mechanisms and create more flexibility in supporting cross-border data transfers. 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. In particular, the GDA recommends:

- **Revising Article 28-8(1) to recognize additional transfer mechanisms**, including intra-corporate binding rules, international trustmarks, and regional certifications 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**), Brazil's data protection law that recently entered into force, 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.
- **Revising the consent requirements in sub-paragraph 1 of Article 28-8(1)**, which requires personal information controllers to obtain "separate consent regarding cross-border transfer from the data subject". GDA 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."

We appreciate the opportunity to share these views and hope that they will be helpful as the National Assembly considers its next steps on the PIPA, promoting a robust data protection environment, while allowing responsible stewardship of data to continue benefiting the citizens and economy of Korea.

Please do not hesitate to contact us with any questions regarding this submission.

Sincerely yours,



Eunice Lim
Senior Manager, Policy – APAC
BSA | The Software Alliance