August 31, 2026

BSA COMMENTS ON REVIEW OF KOREA'S DATA PROTECTION REGIME

Submitted Electronically to the Personal Information Protection Commission (PIPC)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to provide recommendations in response to the PIPC's comprehensive review of Korea's data protection regime.

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. Many BSA members provide their products and solutions to Korean businesses across the economy. We are proud that Korean businesses continue to rely on our members' offerings to operate and grow.

We have actively engaged with the PIPC on privacy-related issues,[2] and we are encouraged to see that the PIPC is examining if the current consent-focused data protection regime remains best suited for the AI era. We agree with the PIPC's observation that the current regime may no longer be fit-for-purpose. In today's environment, consent obtained at the point of collection often provides less protection while placing significant constraints on responsible data use. Individuals face a growing volume of consent requests, which weakens the meaningfulness of their choices, and organizations are left without practical legal bases for beneficial, low-risk processing. We therefore welcome the PIPC's decision to reassess the regime.

Summary of BSA's Recommendations

Recommendation 1: Broaden the Legitimate Interest Basis for Data Processing

- Broaden Article 15(1)6 of the Personal Information Protection Act (**PIPA**) to align it with the legitimate interest bases in other privacy laws worldwide, and treat it as a legal ground equal to consent, rather than as an exception to consent.
- Processing on this basis should be permitted where it does not adversely affect the rights and interests of data subjects, assessed under a balancing test in which privacy risks are

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] See: BSA Comments on Draft Amendments to PIPA Enforcement Decree, July 2026, https://www.bsa.org/policy-filings/korea-bsa-comments-on-draft-amendments-to-pipa-enforcement-decree; BSA Comments on PIPA Draft Enforcement Decree, June 2023, https://www.bsa.org/policy-filings/korea-bsa-comments-on-personal-information-protection-act-draft-enforcement-decree; BSA Submission on Proposed Revisions to the PIPA, November 2021, https://www.bsa.org/policy-filings/korea-bsa-submission-on-proposed-revisions-to-personal-information-protection-act.

mitigated, rather than requiring the controller's interest to be "manifestly superior" to those rights.

Recommendation 2: "Personal Information Controllers" and "Outsourcees" Must Have Distinct Responsibilities

- Adopt definitions that align with other privacy laws worldwide, with the "personal information controller" defined as the entity that determines the purposes and means of processing personal data, and the "outsourcee" defined as an entity that processes personal data on behalf of the controller.
- Tailor obligations to each entity's role. Consumer-facing responsibilities, such as obtaining consent and responding to consumer rights requests, should be assigned to "personal information controllers". "Outsourcees" should be subject to obligations that reflect their role, including safeguarding personal information and processing it only on the controller's instructions.

Recommendation 3: Facilitate Cross-Border Data Transfers

- Adjust the "separate consent" requirement so that, where a transfer is needed to fulfil the purpose for which the personal information was collected, the original consent for processing suffices to support the transfer.
- Recognize internationally accepted transfer instruments, such as the EU Standard Contractual Clauses (**SCCs**), the UK International Data Transfer Agreements, the Global and APEC Cross-Border Privacy Rules (**CBPR**), the ASEAN Model Contractual Clauses, and ISO/IEC 27701.
- Make the equivalence route under Article 28-8(1)5 predictable by stipulating timelines, publishing the prioritization methodology, seeking industry input on which countries to prioritize, and considering the totality of a country's laws rather than the presence or absence of a single overarching privacy law.

Recommendation 1: Broaden the Legitimate Interest Basis for Data Processing

Current Status & Situation (Problem Case)	The PIPA is a consent-focused law. Generally, a company must obtain the data subject's consent before collecting or processing personal information. However, companies collect and process personal information regularly for purposes where obtaining consent is impractical and provides little meaningful protection. Such purposes include detecting and preventing fraud, monitoring networks for cybersecurity threats, and updating products and services to ensure accuracy and reliability. Article 15(1)6 of the PIPA allows processing for the legitimate interest of a personal information controller, but only where that interest is "manifestly superior" to the rights of the data subject. The language in the PIPA is vague but also suggests that a very high

	threshold must be met for a company to rely on the legitimate interest basis.
Relevant Regime & Standards	PIPA, Article 15(1)6.
Issues	• **The "manifestly superior" threshold means that the legitimate interest basis in the PIPA is significantly narrower and less flexible than data protection frameworks in other leading jurisdictions.** For example, Article 6(1)(f) of the EU General Data Protection Regulation (**GDPR**) permits processing necessary for the legitimate interests of the controller except where those interests are "overridden by the interests or fundamental rights and freedoms of the data subject". Similarly, under Singapore's Personal Data Protection Act (**PDPA**), an organisation may collect, use, or disclose personal data without consent where the "legitimate interests of the organisation or another person outweigh any adverse effect on the individual". Consequently, not only can companies can more easily rely on the legitimate interest basis in markets such as EU and Singapore, but companies are also clearly incentivized to improve their practices to mitigate any privacy harms. In contrast, as a result of the "manifestly superior" threshold, companies in Korea are subject to a stricter and less predictable standard. • **Relatedly, because companies cannot assess in advance whether their interests would be considered "manifestly superior", they tend to over-rely on consent for all processing activities.** This burdens individuals with a growing volume of requests, produces consent fatigue, and devalues consent in the situations where it is genuinely meaningful. Consent should be reserved for high-impact processing, involving sensitive data or secondary uses genuinely outside an individual's reasonable expectations. The over-reliance on consent also chills processing that protects the very individuals whose data is involved. Fraud detection and prevention, cybersecurity and network monitoring, and updating products and services to ensure accuracy and reliability all benefit data subjects directly.[3] A legal framework that makes companies hesitate before conducting this processing does not improve

[3] The EU GDPR expressly recognizes such processing as legitimate interests, per Recitals 47-49.

	privacy outcomes. It creates risk for the people the law is meant to protect. • **Over-reliance on consent could also hinder responsible AI development.** Consent requirements can discourage AI-model training or AI-development by companies with lawfully collected personal data where consent is not feasible to obtain, such as research drawing on large or historical datasets where data subjects cannot practicably be reached . This can also distort training datasets where certain groups are more likely to withhold consent, leading to sampling bias and ultimately resulting in AI systems that perform poorly for underrepresented groups. Access to diverse and representative data, including Korean-specific data, is essential for building AI systems that are accurate and fair for Korean users.
Recommendation(s)	**Broaden Article 15(1)6 of the PIPA to align it with the legitimate interest bases in other global data protection laws, and treat it as a legal ground equal to consent.** Processing on this basis should be permitted under a balancing test that assesses purpose legitimacy, necessity, reasonable expectations, potential impact, and the presence of safeguards, and in which privacy risks are mitigated. Processing should be permitted where it does not adversely affect the rights and interests of data subjects, rather than requiring the controller's interest to be manifestly superior to those rights. This revised legitimate interest basis should operate as an equal legal ground alongside consent, rather than as an exception to consent.

Recommendation 2: "Personal Information Controllers" and "Outsourcees" Must Have Distinct Responsibilities

Current Status & Situation (Problem Case)	The PIPA recognizes two entities that handle personal information. The first is the "personal information controller" (Article 2(5) of the PIPA), which is the entity that "processes personal information directly or indirectly… as part of its own activities". The second is the "outsourcee" (Article 26 of the PIPA), the entity entrusted by a controller to process personal information on the controller's behalf and in accordance with its instructions. **Importantly, despite defining two separate entities, the PIPA obligations equally apply to both the "personal information controller" and the "outsourcee".** Such obligations include

	obligations to obtain consent, to notify data subjects of a breach, and to respond to data subject requests (for access, deletion, transmission of data, etc.). In the absence of a meaningful distinction between the two entities' roles and obligations, both consumers and businesses face increased uncertainty, and also defeats the purpose of having two separate entities defined in the first place. Consumers lack clarity about which entities are responsible for safeguarding their data and how to exercise their rights, while businesses lack clear guidance on their obligations, leading to potential gaps in accountability and compliance.
Relevant Regime & Standards	PIPA, Articles 2(5) and 26
Issues	• **Many obligations applied to "outsourcees" are consumer-facing obligations, which "outsourcees" cannot properly discharge.** Obligations such as obtaining consent, notifying data subjects, and responding to rights requests assume that an entity knows what personal information it holds and can identify and communicate with the data subject in question. That is not always the case. For example, many enterprise cloud and software-as-a-service providers act as "outsourcees" and process personal information strictly on the instructions of their customers (i.e., the "personal information controller"). The "outsourcees" are often contractually prohibited from accessing the data at all, may not know its contents, and have no means of authenticating the individuals to whom the data relates. Requiring an "outsourcee" to comply with consumer-facing obligations would undermine privacy because the "outsourcee" must access and analyze data it would otherwise never examine and risks disclosing personal information to a requester it cannot authenticate. In contrast, the "personal information controller" decides why and how personal information is collected and used, and holds the direct relationship with the data subject. It knows what personal information it has collected, can verify the identity of the individual making a request, and can communicate the outcome to them. The "personal information controller" is therefore the entity best positioned to take on consumer-facing obligations in the PIPA. • **Relatedly, applying the same obligations to both entities is misaligned with international standards and incompatible**

	with the emerging AI-era ecosystem. Data protection laws worldwide distinguish between "data controllers" (entities which determine the purposes and means of processing personal data) and "data processors" (entities that handle personal data on behalf of controllers pursuant to their instructions). Both data controllers and processors are assigned obligations they can actually perform. For example, the EU GDPR places consumer-facing obligations on controllers, while processors must act on the controller's documented instructions, assist the controller, and secure the data they hold. This distinction is present in other leading privacy laws, such as Singapore's PDPA, and the California Consumer Privacy Act. Korea's PIPA is unusual in defining the two roles but applying the obligations equally to both roles. This complicates compliance for companies that have built their data protection programs, contracts, and technical architectures around the internationally recognized division of responsibilities.
Recommendation(s)	• **Adopt definitions that align with other privacy laws worldwide.** The "personal information controller" should be adjusted to refer to an entity that "alone, or jointly with others, *determines* the purposes and means of processing personal data", whereas an "outsourcee" should be defined as an entity that "processes personal data on behalf of the personal information controller". This clearly distinguishes the roles of both entities, which consequently allows for more precise allocation of responsibilities between them. • **Ensure that that obligations for "personal information controllers" and "outsourcees" are appropriately tailored according to their roles.** Importantly, consumer-facing responsibilities, such as obtaining consent from individuals and responding to consumer rights requests, should be assigned to "personal information controllers" rather than "outsourcees". This reflects the fact controllers are entities that decide how and why to collect a consumer's personal information. "Outsourcees" should be subject to other obligations, such as requirements to safeguard personal information and to process personal information only on behalf of the controller and pursuant to the controller's instructions. Such an allocation of responsibilities is also consistent with global norms.

Recommendation 3: Facilitate Cross-Border Data Transfers

Current Status & Situation (Problem Case)	The PIPA regulates the transfer of personal information out of Korea through Article 28-8. Cross-border transfers are prohibited unless one of five legal bases applies: 1) the data subject gives separate consent to the transfer; 2) the transfer is authorized by statute, treaty, or international convention; 3) the transfer is necessary to conclude and perform a contract with the data subject and prescribed matters are disclosed in the privacy policy or notified to the data subject; 4) the overseas recipient holds a certification determined and publicly notified by the PIPC and takes required protective measures; or 5) the destination country or international organization is recognized by the PIPC as providing a level of protection substantially equal to the PIPA. In practice, cross-border data transfers out of Korea remain difficult for various reasons (see "Issues" section below). This is especially problematic given that companies delivering global service increasingly rely on cross-border data transfers for AI development and training purposes.
Relevant Regime & Standards	PIPA, Article 28-8
Issues	• **The consent basis is impractical and does little to protect data subjects.** Where a transfer rests on consent, the controller must obtain "separate consent" specific to the transfer, even where the transfer is needed to fulfil the very purpose for which the personal information was collected and the data subject has already consented to that processing. Before obtaining consent, the controller must also inform the data subject of a prescribed list of items under Article 28-8(2), including the particulars of the personal information, the destination country, the transfer date and method, the name of the recipient, and other such information. Much of this information, such as the transfer date, is not meaningful to a data subject in understanding how the transfer affects their personal information. It is also not practical for the name and contact person of the recipient corporation to be set out in the privacy notice as those details may change and may not be readily available. The combined effect is to inundate individuals with consent requests and detail, which compounds consent fatigue while adding little protection. This also increases operational costs.

	• **The alternative transfer mechanisms are narrow compared with international practice.** Standalone contract-based transfer instruments concluded between the transferring company and the overseas recipient, such as SCCs, are not recognized as a basis for transfer. Consequently, companies that have built global compliance programs around these instruments cannot use them for Korea, and must consider other options, such as only transferring the data to overseas recipients who have obtained Korea-specific certifications e.g., the Information Security and Personal Information Protection Management System (**ISMS-P**) Certification. • **The equivalence route is slow and lacks a predictable process.** The recognition of the European Union in September 2025 was the PIPC's first equivalence decision under Article 28-8(1)5, and it remains the only one. There is no stated timeline for assessing other countries, no published methodology for how countries are prioritized, and no mechanism for industry to provide input on which destinations matter most to Korea's economy. The assessment approach also risks disadvantaging countries that protect personal information effectively but through a different legislative structure, such as the United States which regulates the commercial collection and use of personal information through a combination of state privacy laws and sectoral federal rules rather than one omnibus statute. An assessment that turns on the presence or absence of an overarching law, rather than on the totality of relevant laws and regulations, would leave transfers to such countries without an equivalence pathway indefinitely. • **Cumulatively, the above concerns with the cross-border data transfer landscape in Korea create significant costs and burdens for any business delivering global services.** These concerns carry particular weight in the AI era, where the development and training of AI systems depend on the ability to move data, including personal information, across borders at scale.
Recommendation(s)	• **Adjust "separate consent" requirement.** Where the cross-border transfer of personal information is needed to fulfil the purpose for which the information was collected, the original consent for processing should suffice to support the transfer, and "separate consent" under Article 28-8(1)1 should not be

	required. This would align the provision with the approach taken under the EU GDPR. • **Recognize additional transfer mechanisms through the certification route in Article 28-8(1)4.** The PIPC should recognize internationally accepted transfer instruments, such as the EU SCCs, the UK International Data Transfer Agreements, the Global and APEC CBPRs, the ASEAN Model Contractual Clauses, and ISO/IEC 27701. Many global companies have adopted these instruments to protect personal information as it moves between countries, and they share substantial common ground with what the PIPA requires of overseas recipients. Recognizing them would allow businesses to transfer and receive personal information from Korea without obtaining separate consent or a Korea-specific certification. Enabling personal information controllers to choose among recognized mechanisms gives businesses the flexibility to determine the arrangement most suitable for their operations. It would also provide greater legal certainty, reduce compliance burdens for both Korean and non-Korean businesses delivering global services, and align Korea with the multi-mechanism approach of other global data protection frameworks. • **Make the equivalence route under Article 28-8(1)5 predictable.** The PIPC should stipulate timelines for assessing the protection level of other countries, publish its methodology for prioritizing countries for assessment, and seek input from industry on which destinations to prioritize. In conducting assessments for equivalence, the PIPC should look beyond the presence or absence of a single overarching privacy law and consider the totality of relevant laws and regulations that protect personal information in the destination country, so that countries which protect personal information through state privacy laws and sectoral federal rules are not left without an equivalence pathway.

Conclusion

We thank PIPC for the opportunity to contribute to this comprehensive review of Korea's data protection regime. We support the PIPC's efforts to ensure that the regime continues to protect personal information effectively while enabling responsible data use. We would welcome the opportunity to discuss any of them further and remain available as a resource to the PIPC throughout this process. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Yours sincerely,

Tham Shen Hong
Director, Policy – APAC