July 13, 2026

BSA COMMENTS ON DRAFT AMENDMENTS TO PERSONAL INFORMATION PROTECTION ACT ENFORCEMENT DECREE

Submitted Electronically to the Personal Information Protection Commission (PIPC)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to respond to the PIPC's draft amendments to the Enforcement Decree of the Personal Information Protection Act (**Enforcement Decree** and **PIPA** 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. 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.

BSA has followed the development of the PIPA closely and participated in past consultations on the PIPA and the Enforcement Decree.[2] The latest proposed amendments to the Enforcement Decree seek to implement the PIPA amendments which were promulgated in March 2026 (**2026 PIPA amendments**). Given that the 2026 PIPA amendments substantially increased both the compliance obligations placed on industry and the penalties for falling short of them, we encourage the PIPC to consider our recommendations below, which seek to ensure that the Draft Enforcement Decree provides companies with clear and workable guidance while also appropriately recognizing the security and governance investments that companies have already made.

Summary of BSA's Recommendations

On the mandatory requirement to obtain Information Security and Personal Information Protection Management System (**ISMS-P**) Certification:

- The Draft Enforcement Decree should establish that personal data processed by an outsourcee (i.e., a personal data processor) on the instructions of a personal information

[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 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.

controller does not count toward the outsourcee's own threshold for mandatory ISMS-P certification under Article 34(9)(4).

- The Draft Enforcement Decree should also establish a clear pathway for companies holding internationally recognized security and privacy certifications, including ISO/IEC 27001, Service Organization Control 2 (**SOC 2**), ISO/IEC 27701, the EU General Data Protection Regulation (**GDPR**), or the Global/APEC Cross-Border Privacy Rules (**CBPR**) system, to obtain ISMS-P certification that builds on those existing frameworks without requiring full-scale duplicative assessments.

On the scope and threshold of notification requirements:

- The Draft Enforcement Decree should not require notification of data subjects based on a mere possibility of a breach. Where notice is required, it should be limited to incidents presenting a material risk of significant harm to data subjects, with clear definitions of "objective circumstances" and "high likelihood" supported by concrete and specific examples.
- In addition, notification and reporting obligations for falsification, alteration, or damage of personal information should be triggered only where the incident presents a material risk of harm to the rights and interests of affected data subjects, rather than wherever such an incident has technically occurred.

On the penalty framework:

- The Draft Enforcement Decree should specify that the nature and sophistication of the threat actor responsible for a breach is a relevant consideration in assessing mitigation under Article 64-2(6) of the PIPA, to be weighed alongside the scale and continuity of the company's investment in personal data protection. It should also expressly state that demonstrating security measures consistent with prevailing industry standards at the time of a breach should weigh significantly in favour of mitigation.
- The Draft Enforcement Decree should also establish a transition period of at least 12 months following the entry into force of the amended PIPA obligations, to give companies adequate time to align their compliance programs with the new requirements.

Mandatory ISMS-P Certification

The 2026 PIPA amendments converts the ISMS-P certification from a fully voluntary regime into one that is mandatory for personal information controllers meeting criteria to be set out in the Enforcement Decree, based on revenue and the scale of personal data processed. Notably, the scope of covered entities extends to "large-scale personal data processors meeting a combined threshold of KRW 1 trillion or more in total revenue, KRW 10 billion or more in ICT service revenue, and an average of 30 million or more domestic data subjects per day".[3]

[3] Article 34(9) of Draft Enforcement Decree. The other three categories of entities include: 1) public system operators under Article 30-2 designated by the Protection Commission through official public notice; 2) entities that have been allocated frequencies pursuant to Article 10 of the Radio Waves Act to provide mobile telecommunications services and that have entered into service use agreements with data subjects; and 3) identity verification institutions under Article 23-3(1) of the Act on Promotion of Information and Communications Network Utilization and Information Protection.

BSA appreciates that the scope of covered entities is anchored in specific figures, which gives companies more certainty as to whether the mandatory ISMS-P requirement would apply to them. However, the following issues remain unaddressed.

First: The data subject threshold should focus on controllers

The Draft Enforcement Decree sets a threshold for covered entities that have an "average of 30 million or more domestic data subjects per day."

This threshold is difficult to apply to companies that act as "outsourcees" rather than as "personal information controllers" under the PIPA. Modern privacy laws worldwide distinguish between controllers, which determine the purposes and means of processing personal information, and processors (or "outsourcees" under PIPA) which process personal information on behalf of, and in accordance with the instructions of, a controller.[4] While PIPA defines both of these roles, it departs from many modern privacy laws by applying the same obligations to both entities instead of assigning controllers with obligations, that reflect their role in deciding why and how to process individuals' personal data.[5]

Accordingly, the Draft Enforcement Decree's threshold should apply only to controllers, which decide how and why to process individuals' personal data and therefore are in a position to know the number of domestic data subjects whose personal data they process each day. In contrast, outsources may not know this information.[6] Enterprise cloud and Software-as-a-Service (**SaaS**) providers, for example, typically process personal data strictly as instructed by their business customers, who are the controllers determining why and how the data is processed and who maintain the direct relationship with the affected data subjects. These providers, in their capacity as outsourcees, may in aggregate process very large volumes of data across their customer base, but they generally have no independent authority over how that data is used, no direct relationship with the individual data subjects whose data they hold, and in many cases, no practical ability to identify which data subjects are domestic data subjects for purposes of the threshold calculation. If data processed by an outsourcee on behalf of multiple controllers is counted toward the outsourcee's own threshold under Article 34(9)(4), the certification mandate risks applying to entities that lack the authority and direct relationship with data subjects, while the controllers who do hold that authority and that relationship may fall outside scope entirely.

Recommendation: The Draft Enforcement Decree should establish that personal data processed by an outsourcee (i.e., personal data *processor*) on instructions of a personal information controller do not count towards the outsourcee's own threshold for mandatory ISMS-P certification under Article 34(9)(4).

---

[4] Controllers and Processors: A Longstanding Distinction in Privacy, April 2025, https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

[5] Article 26 of PIPA.

[6] For example, a processor that handles personal data purely on a controller's instructions, and that may be contractually prohibited from accessing or using that data for any other purpose, is often not in a position to know the content of the data it processes, to identify the specific individuals to whom that data relates, or to authenticate the identity of a given data subject. A controller, by contrast, has decided what data to collect, for what purpose, and maintains the direct relationship with the data subject.

Second: Companies should be encouraged to build on existing international frameworks and certifications.

Another issue not addressed by the current draft is how the new mandate should treat companies that already maintain rigorous, independently audited security and privacy programs under major international frameworks. These companies typically have global compliance programs built around internationally recognized security certifications, including ISO/IEC 27001 and SOC 2 reports, as well as privacy frameworks such as ISO/IEC 27701, the EU GDPR and the Global/APEC CBPR system.

These frameworks share substantial common ground with ISMS-P's requirements. As such, a company that has already built and independently audited a security management system to ISO 27001 or a personal data governance program to GDPR/CBPR standards has, in substance, already implemented much of what an ISMS-P assessment is designed to verify. Mandating the company to undergo a full, ground-up ISMS-P assessment, with no recognition of this existing work, is duplicative, adds cost and administrative burden without a proportionate gain in actual data protection. The result will be to limit Korean government agencies and businesses to more expensive, less functional, and less secure services.

We also encourage the PIPC to ensure that the ISMS-P requirements are coordinated with related developments in Korea's information security certification landscape, including the Cloud Security Assurance Program (**CSAP**) and the move toward a unified National Information Security (**NIS**) framework for public-sector cloud services, to avoid overlapping or conflicting certification requirements applying to the same cloud services.

Recommendation: The Draft Enforcement Decree should establish a clear pathway for companies with certifications and processes, including ISO/IEC 27001, SOC 2, ISO/IEC 27701, the GDPR, or the Global/APEC CBPR system, to obtain ISMS-P certification that builds on the existing certifications and frameworks, without requiring full-scale duplicative assessments.

Scope and Threshold of Notification Requirements

The PIPA now requires notification of data subjects not only once a personal data breach is confirmed, but also where there is a "possibility" that one has occurred. We have significant concerns with this approach, which is likely to inundate individuals with information about incidents that may never materialize and undermine the ability of data subjects to identify and focus on notices about actual harms from real breaches.

The amendments to the Enforcement Decree implement this obligation by specifying two situations which will trigger the notification requirement: 1) where a personal data processing system or device has been subject to unauthorized access and there are “objective circumstances” indicating a breach may have occurred, but the specific affected data subjects cannot yet be identified; and 2) where it is objectively confirmed that personal data is being unlawfully traded or distributed, and there is a “high likelihood” that other data subjects' data has also been compromised.[7]

[7] Article 39(2) of Draft Enforcement Decree.

In addition, the amendments expand the scope of incidents that trigger notification obligations. The current definition of a notifiable incident is limited to the loss, theft, or leakage of personal information. The amendments expand this definition to also include the "falsification, alteration, or damage of personal information".[8] We have concerns at each step.

First: The "possibility" threshold should be removed or, alternatively, tied to specific material harms

As a general principle, notice should not be required when there is a mere possibility of a breach. Requiring companies to notify data subjects of a mere possibility of a breach will lead to various concerning outcomes. Notably:

- Companies may over-notify as a precaution, even where the underlying incident does not ultimately involve any compromise of personal information. Over-notification driven by an undefined standard works directly against the aim of the Decree and risks desensitizing data subjects to notifications more broadly, making it harder for them to identify and respond to genuinely serious incidents when they occur.
- Companies may apply the standard inconsistently, given the absence of clear guidance on what evidence or indicators are sufficient to trigger notification. Companies facing materially similar facts may reach different conclusions about whether the threshold has been met, producing inconsistent practice across industry and unpredictable enforcement outcomes. This uncertainty is compounded by the scale of the penalties now at stake, which gives companies strong reason to default to over-notification simply to avoid the risk of being found non-compliant after the fact.
- Requiring notice of any possibility of a breach also diverts resources at precisely the moment they are most needed elsewhere. In the immediate aftermath of detecting unauthorized access, a company's security and compliance teams have limited capacity, and that capacity is best directed toward containing the incident, determining its actual scope, and remediating any harm. Requiring notices of a possible breach forces companies to divert some of that same capacity toward documenting and justifying a notification decision under uncertain criteria, rather than toward the technical and operational work of resolving the incident itself. This is precisely the wrong allocation of effort at the stage when speed and focus matter most to limiting harm to data subjects.
- Premature disclosure of unverified incidents may inadvertently assist threat actors. Notifications issued before a company has confirmed whether an incident has actually occurred could provide cybercriminals with feedback on the effectiveness of their methods and techniques. There is also a risk that the obligation incentivizes attackers to trigger non-material alerts deliberately, knowing that doing so will divert company resources and distract incident-response teams from more serious intrusions at a critical moment.

Recommendation: The Draft Enforcement Decree should:

- Not require notice to data subjects of "potential" incidents. Rather, notice should only be required when there is a material risk of significant harm to data subjects. The Decree

[8] Article 30-2(2)(1) of Draft Enforcement Decree.

should ensure that all obligations are tied to breaches that create a material risk of significant harm to data subjects.

- When notices are required, they should be tied to clear definitions for "objective circumstances" and "high likelihood" under Article 39(2). These should be tied to concrete examples of the evidence and indicators that would satisfy each threshold and focus on situations that create material risks to data subjects of significant harms.

Second: The expanded scope of notices does not reflect actual risk to data subjects

The expanded scope of a notifiable incident to cover "falsification, alteration, or damage of personal information" is significant. BSA is concerned that there is no materiality threshold tied to this expanded scope. In other words, the notification requirement is triggered regardless of whether the incident in question poses any actual risk to data subjects.

In practice, this means that a company that suffers a ransomware attack affecting the availability of personal data, but that results in no actual loss, theft, or leakage of that data (e.g., through encrypting and backing up the data), could fall within scope as an incident involving damage to personal information, even where no data subject's information has been viewed, accessed, or exfiltrated by an unauthorized party. At the same time, routine operational incidents, such as a database error that temporarily alters a subset of records and is fully remediated through automated backup and recovery systems, could also technically fall within the same definition. Treating a serious attack resulting in actual data exfiltration and a routine, fully remediated system error as equivalent for notification purposes does little to help data subjects distinguish between incidents that warrant their attention and those that do not, and risks diverting both company and PIPC resources toward incidents that present no meaningful risk of harm. A materiality threshold is needed to avoid these results.

Recommendation: The Draft Enforcement Decree should clearly set out that notification and reporting obligations for falsification, alteration, or damage of personal information are triggered only where the incident presents a material risk of harm to the rights and interests of affected data subjects, rather than wherever such an incident has technically occurred. This would ensure that notification and reporting obligations are reserved for incidents that genuinely warrant the attention of data subjects and the PIPC.

Penalty Framework

The 2026 PIPA amendments increased the maximum penalty for a breach to 10% of a company's "total revenue" for specific circumstances.[9] The Draft Enforcement Decree introduces mitigating criteria which the PIPC may consider when calculating the penalty, which include the scale and continuity of a company's investment in personal data protection, the maturity of its governance framework, and additional security-strengthening efforts.[10] BSA welcomes the mitigating criteria and highlights the following areas which can be improved

[9] Per Article 64-2(2) of the PIPA, "total revenue" refers to a company's global revenue, excluding revenue unrelated to the violation. This enhanced penalty applies where a company commits a willful or grossly negligent violation and repeats it within three years; where a single incident involving intentional or grossly negligent conduct affects 10 million or more data subjects; or where a breach occurs after a company has failed to comply with a PIPC corrective order.

[10] Article 64-2(6) of the PIPA

First: Differentiate companies that have invested in security from companies that have not

Companies that build and maintain rigorous security programs, employ qualified privacy and security personnel, and invest continuously in their defences can still be the victims of sophisticated attacks. Such a company is in a fundamentally different position from a company whose breach results from a failure to invest in basic security measures at all. Treating these two companies as equivalent under the same penalty framework does not serve the Act's deterrent purpose, since the company that invested seriously had no meaningful additional step available to it that would have prevented the breach, while the company that failed to invest did.

Article 64-2(6) of the PIPA states that the PIPC "may" consider a company's investment in personal data protection as a mitigating factor, without specifying how this factor should be weighed against the nature of the attack itself, including whether the company faced a sophisticated, targeted, state-sponsored, or otherwise unusually capable threat actor. A mitigation framework that does not explicitly account for the sophistication of the attack a company faced, alongside the investment that company made, would be applying the same severe penalty exposure to companies in fundamentally different positions.

The Draft Enforcement Decree should distinguish between a company that maintains rigorous, well-resourced security infrastructure and is nonetheless compromised by a sophisticated attacker, and a company whose breach results from systemic underinvestment or neglect.

Recommendation: The Draft Enforcement Decree should:

- Specify that the nature and sophistication of the threat actor responsible for a breach is a relevant consideration in assessing mitigation under Article 64-2(6) of the PIPA, to be weighed alongside the scale and continuity of the company's investment in personal data protection.
- Expressly state that, where a company can demonstrate that it maintained security measures consistent with prevailing industry standards at the time of the breach, this should weigh significantly in favour of mitigation, even where a breach ultimately succeeded.

Second: Provide a transition period before pursuing financial sanctions

The penalty framework discussed in this section takes effect alongside the amended obligations in the PIPA in September 2026.[11] Companies will need time to train relevant personnel and align global incident response and governance architectures with the newly clarified regulatory requirements discussed throughout this submission. Moving directly to the full exercise of the PIPC's enhanced penalty powers from the moment these obligations take effect, without any period for companies to operationalize the changes, risks penalizing companies for compliance gaps that reflect the practical realities of implementation timelines rather than any unwillingness to comply.

Recommendation: The Draft Enforcement Decree should establish a defined transition period of at least 12 months following the entry into force of the amended PIPA obligations. This would give

[11] BSA notes that the requirement to obtain ISMS-P certification is an exception, insofar as it only takes effect from July 2027.

companies adequate time to align their compliance programs with the new requirements while preserving the PIPC's full enforcement authority once that transition period has concluded.

Conclusion

We appreciate the PIPC's continued engagement with industry as it implements the 2026 PIPA amendments, and hope that these comments are useful as the PIPC finalizes the Draft Enforcement Decree. We offer our recommendations in the spirit of helping PIPC implement the 2026 PIPA amendments through rules that are clear, proportionate and workable for the companies that need to comply with them. We would welcome the opportunity to discuss any of the issues raised in this submission further and remain available as a resource throughout this process.

Yours sincerely,

Tham Shen Hong
Director, Policy – APAC