2/15/2021

Personal Information Protection Commission (PIPC)
Deputy Director Min-joo Kim
mjkoo99@korea.kr

Re: *Proposed Amendment to the Personal Information Protection Act of 2011*

Dear Deputy Director Kim:

The Software & Information Industry Association (SIIA) welcomes the opportunity to provide written comments and feedback on South Korea's draft amendment to the Personal Information Protection Act of 2011 (PIPA). SIIA is the leading trade association for the digital content and software industries, and connects more than 700 data, financial information, education technology, specialized content and publishing and health technology companies. Our diverse members reflect the broad landscape of digital service and information providers and content producers, including B2B and B2C services, small and specialized publishers, and multinational industry leaders. Relying on the power of data, SIIA members help learners of all ages prepare to succeed in their future, manage the global financial markets, develop software that solves today's challenges, provide critical information that informs global businesses large and small, and innovate for better health care and personal wellness outcomes.

SIIA believes that privacy is a fundamental value that is essential to individual autonomy and a functioning democracy. We support privacy frameworks that protect these values while permitting socially beneficial uses of data, promoting innovation and competition, and ensuring interoperability with global frameworks.

We understand and appreciate Korea's interest in modernizing PIPA to align with global privacy frameworks, like the EU's GDPR. SIIA is concerned, however, that the proposed amendment misinterprets the intent of global frameworks by not taking a harm- and risk-based approach, overlying on consent, and not differentiating between the roles involved in data collection and processing. In particular, we have significant concerns with the proposed provisions relating to:

- overseas data transfers,
- the lawful bases for processing personal information,
- examination of privacy policies,
- the calculation of penalties,
- the right to data portability,
- the right related to automated decision-making, and
- dispute mediation.

Additionally, we request that the Korean government extend this commentary period or otherwise open a new period for stakeholder consultation. If passed, the draft amendment will result in sweeping changes to Korean privacy rules and have significant and broad-ranging implications for both Korean and global companies. The consultation period for the draft amendment was open only for a short period and did not include an English translation of the proposed changes. This inevitably will result in a loss of

critical feedback from stakeholders to help refine and strengthen the proposed amendment to better align with global privacy frameworks for the benefit of all stakeholders, including Korean consumers.

OVERSEAS DATA TRANSFERS
ARTICLE 28-8

Mechanisms and Standards for Overseas Data Transfers (Article 28-8)

SIIA's members rely on the ability to transfer personal data globally, including from Korea to the U.S., for a wide variety of routine and necessary commercial purposes, such as performing global HR functions, providing digital services to consumers, and implementing the systems necessary for banks and other companies to meet "Know Your Customer" and "Anti-Money Laundering" standards to combat financial fraud. To continue to rely on these outcomes, it is critically important that privacy frameworks both authorize the secure but free flow of data and treat data transfers as a normal rather than an extraordinary event in data processing. Indeed, Korea has recognized this need in the U.S.-Korea Free Trade Agreement (KORUS), which obligates it to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." *See* Ch. 15, Art. 15.8

Article 28-8 of the proposed amendment makes some important and significant headway in achieving these KORUS obligations. Notably, it proposes expanding the mechanisms for data transfers beyond consent, which is both necessary and an international norm. The proposed amendment, however, does not go far enough to enable data flows. **To better align with international standards for data flows, the proposed amendment should include additional data flow mechanisms enshrined in global privacy frameworks like the EU's GDPR and Brazil's LGPD, such as standard contractual clauses, binding corporate rules, and codes of conduct. Additionally, the proposed amendment can and should be "future proofed" by expressly recognizing bilateral, multilateral, and regional frameworks and certifications, like the APEC CPBR.**

In addition, the proposed amendment's requirements regarding consent in the context of data transfers is problematic. Although we agree that consent can be one basis for transferring data, it should not be the primary transfer mechanism. Moreover, when a personal information controller relies on consent, the standard for notice should not require a notice that acts as an implied signal to the data subject that the data transfer constitutes an extraordinary circumstance in data processing. As noted above, overseas data transfers are a routine aspect of modern data processing, and often required for seamless business operations and consumer experiences and interactions with digital goods and services. The proposed amendments, in contrast, require a personal information controller that relies on consent for a data transfer to include dense notifications that acts as red flags to the data subject and wrongly imply there is something extraordinary, wrong, or dangerous about the data transfer. The trade impact of overly onerous consent requirements should be considered before finalizing the amendment, particularly given Korea's obligations under KORUS.

Application Mutatis Mutandis (Article 28-10)

The proposed amendment includes a new provision that sets forth legal obligations for onward overseas transfers of data at Article 28-10. Problematically, the contemplated standard would convert companies that do not have any direct busines or relationship with Korea into "personal information controllers" subject to PIPA. Although we are not experts on Korean law, we assume that this raises difficult questions relating to extraterritorial jurisdiction and imposes an obligation that ultimately cannot be

enforced. And even if Korean law permits such an extraterritorial application of PIPA, any judgment from it would be meaningless if the company in question has no ties to Korea.

The better approach would be to use the amendment process to reflect the realities of modern data processing and introduce mechanisms to enable data transfers that ensure that the personal information controllers implement downstream controls to ensure that the appropriate PIPA protections flow with the data. For example, including standard contractual clauses or binding corporate rules as a mechanism for a data transfer would require the "personal information controller" (i.e. the data exporter) to ensure that the person or entity to whom the data is transferred overseas (i.e. the data importer) is contractually or otherwise bound by the data exporter's obligations under PIPA. Those mechanisms would then contemplate similar controls if the data were transferred onward for purposes of processing. This creates binding obligations with respect to the protections provided by PIPA while providing the Protection Commission with the appropriate jurisdictional oversight for the appropriate party should a violation occur.

Suspension Orders for Cross-Border Transfers (Article 28-9)

In Article 28-9, the proposed amendment provides the Protection Commission with the broad and blanket authority to order the suspension of the cross-border transfer of data. The Article sets forth the bases for an order for suspension including where it is highly likely the transfer may infringe the rights of the data subject. This standard, however, is highly subjective and undefined and risks an overbroad use of a suspension order even where there is no violation of PIPA. We note, for instance, that the proposed amendment does not define what constitutes a "significant risk" of a privacy invasion or any other objective standard by which the Protection Commission should abide. **To fix this, the proposed amendment should be revised at Article 28-9(1)(3) to tie the privacy invasion to a violation of PIPA: "where one's privacy rights are highly likely to be invaded due to violation(s) of PIPA."**

COLLECTION AND USE OF PERSONAL INFORMATION ARTICLE 15

We support the proposal to amend Article 15 to modify the bases for collecting and using personal information to include a new basis for the temporary processing of information when it is urgently necessary for public safety, security, and health. This is an important lesson from the COVID-19 pandemic we have globally endured over the last year, and from other public health and security emergencies that have arisen in modern memory. This is an important step forward for Korea and for global privacy frameworks.

Nevertheless, we are concerned that the proposed amendment does not go further and modify the existing bases for collecting and using personal information to better align with other global standards and the lessons learned therefrom, like the GDPR.

For instance, Article 15(6) sets forth a "justifiable interest" standard that is similar to the GDPR's "legitimate interest" standard. The latter, along with other lawful bases for processing set forth in the GDPR, have been important legal mechanisms to provide means for the processing of personal information that do not over rely on the consent of the data subject. As has been exhaustively discussed in recent years, data privacy frameworks that prioritize "notice and consent" place a heavy burden on

consumers to read and understand complex privacy practices in a way that is neither practical nor possible in the modern digital economy. Bases for processing data, like the GDPR's "legitimate basis", set forth alternative models that reduce the burden on consumers while ensuring appropriate privacy protections.

The "justifiable interest" standard in PIPA, however, misses this mark. Under this standard, a personal information controller can only collect and use the personal information if its interest in doing so is "manifestly superior to the rights of the data subject." This is an incredibly high standard and it disincentivizes the use of this basis for processing data, thereby likely forcing overreliance on consent and pushing the burden onto the consumer. In contrast, the GDPR's legitimate interest standard permits the use of the personal information when the "processing is necessary for the purposes of the legitimate interest…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject." Like PIPA's justifiable interest standard, this requires the personal information controller (who is the party better equipped to handle the burden) to engage in a balancing of interests that include care for the data subject. Unlike the justifiable interest standard, it does not open with the premises that the balance defaults to outweigh the interests of the personal information controller. **We encourage the Korean government to take this opportunity to amend PIPA to better align with the international standard that a "legitimate interest" in processing data is an appropriate basis on which to proceed unless that interest is overridden by the rights of the data subject**.

EXAMINATION OF PRIVACY POLICY
ARTICLE 30-2

We object to the proposal to include a new provision at Article 30-2 relating to the examination of privacy policies. Tis proposed amendment is concerning, particularly to the extent that it "deputizes" non-profits and NGOs with the authority to prompt a government investigation. As a practical matter for government operations, this will result in burdensome petitions for the Protection Commission to review privacy policies as the non-profits and NGOs will not be privy to the Commission's internal decisions on how to interpret PIPA and set its priorities for enforcement. Decisions on whether to investigate companies for violations of PIPA, including privacy policy failures, should rest solely within the discretion of the Protection Commission.

Even if we set aside the misplaced authority that is given to non-profits and NGOs, the standard set forth in Article 30-2 does little to guide when such requests should be made or other factors to guide the Protection Commission in addressing such petitions. For instance, Article 30-2 does not demand that the petition meet any minimum grounds or standards. This delegation of power to non-profits and NGOs will inevitably result in a gluttony of petitions for the Protection Commission to review and will unfairly and unnecessarily stymy and interrupt business operations while frivolous petitions are addressed.

Moreover, the proposed amendment is setting up companies to fail. The intention behind mandated privacy policies is transparency (both for data subjects and regulators) and to incentivize companies to engage in thoughtful recitation and review of their privacy practices. Mandated privacy policies, however, are not intended to correlate to a company's internal protocols for compliance. A privacy policy term alone is rarely, if ever, an indicum of a privacy law violation, the determination of which is a complex interplay of facts and internal and nonpublic company protocols. Article 30-2 does not recognize this. Instead, it sets up a "gotcha" regime that encourages both the Protection Commission,

non-profits, and NGOs to interpret a privacy policy in isolation as violative and then for the Commission to investigate to confirm if their understanding is correct without a nexus to the internal protocols that would be determinative.

IMPOSITION OF PENALTY SURCHARGES
ARTICLE 64-2

With respect to the proposed changes to Article 64-2 (originally Article 39-15), our primary concerns are the blanket expansion of the penalty surcharge calculation from 3% of the revenues related to the violation to global revenues and the failure of the proposed amendment to address the need for differentiating liability standards depending on whether the role of the personal information controller is as a "data controller" or a "data processor." We urge the government to use this amendment process to address both.

First, the proposed amendment contemplates modifying the provision to expand the calculation of penalties from 3% of the total revenues related to the violation at issue to global revenues irrespective of whether their source is related to the underlying violation. A penalty surcharge based on global revenues is excessive except in egregious instances of intentional violations or recidivism. **We urge the government to modify this proposed amendment to tie the penalty surcharge to the revenues relating to the violation except in these circumstances, and to provide other initial sanctions for relief, such as warnings and orders for corrective action.**

On this, other global frameworks are instructive. Brazil's LGPD, for instance, sets up an array of potential non-monetary sanctions, including a warning with a deadline for corrective measures and publicizing the infraction. With respect to monetary penalties, the LGPD assesses it at 2% of revenues but then provides a cap. Similarly, New Zealand's 2020 amendments to its privacy law contemplate both monetary and non-monetary penalties, including providing companies with written notice of the breach and a reasonable opportunity to remedy it, followed by the issuance of a compliance notice if the company fails to remedy the breach thereafter. Fines are then assessed for companies that failed to comply with the compliance notice, and are capped at $10,000 NZD.

Second, this provision, like the PIPA more generally, fails to distinguish between the roles that persons and companies can play with respect to data. This is a missed opportunity to better align with international frameworks like the EU's GDPR and Brazil's LGPB, and other emerging global frameworks like the California Consumer Privacy Act and its upcoming successor, the California Privacy Rights Act. **We urge the government to consider whether and how to amend PIPA to better address the different roles involved in data processing, often though not universally referred to as "data controller" and "data processor" roles.**

As currently proposed, Article 64-2 will result in the assessment of a significant penalty surcharge against a "personal information controller" even if that entity's role with respect to the data is merely to process the data upon the instructions and warranties of a data controller. In such instances, if there was a violation of the PIPA with respect to the data, the fault for that violation rests with the data controller that determined the methods and bases of collection and then instructed another company on the specifics of the processing of the data. For instance, a cloud provider acts a data processor when intaking personal data for storage purposes, but the cloud provider does not have "control" over the data beyond its agreement to provide storage services for the personal information controller. In such a case, if the actual

controller of the data violated PIPA by not having a lawful basis for collecting and using the data or not giving appropriate notices to the data subject, the liability should rest with that entity and not with the cloud provider. Any other result is unreasonable, and yet PIPA could be interpreted to require just that.

DATA PORTABILITY
ARTICLES 4(3) AND 35-2

Modern global privacy frameworks generally confer several core data subject rights, including the rights to notice, access, correction, deletion, and portability. Like other industry groups, SIIA supports these rights when privacy frameworks strike an appropriate balance between meaningful data subject control and other competing interests, such as freedom of expression, fraud prevention, assistance to law enforcement, data security, technical feasibility, and the protection trade secrets.

SIIA, therefore, generally supports the expansion of the data subject rights in PIPA to include a right to data portability in Articles 4(3) and in the newly inserted 35-2. We are concerned, however, that the data portability right as proposed in Article 35-2 does not meet the necessary balancing test with respect to technical feasibility and the protection of trade secrets.

First, proposed Article 35-2 contemplates an overly broad right for a data subject to request the transmission of personal information to other personal information controllers without accounting for whether this is technically feasible. This is in contrast to other global frameworks. The EU's GDPR, for instance, principally gives a data subject the right to receive a copy of their data in a form that is structured, commonly used, and machine-readable. The data subject can then exercise that right by having the data transmitted directly to another controller but only where it is technically feasible to do so. *See* Art. 20, GDPR. Not including this limitation in PIPA would require personal information controllers to either risk violating the data portability provision or force them to develop and maintain processing systems that are technically compatible with other personal information controllers. This is burdensome, unreasonable, infeasible, and unnecessary.

Second, the proposed data portability right for PIPA is not appropriately limited to the personal information provided by the data subject, thereby potentially infringing on a personal information controller's ability to protect its trade secrets. We agree that a data subject should have the right to a copy of the personal information he or she provided to the controller in a form that is readily accessible. But other information that a controller may hold, such as information that has been inferred or derived from the personal information provided should not be subject to that right. Such information inevitably constitutes trade secret or other confidential and protected business information that controllers should not be forced to give up by virtue of a right to data portability.

Third, the proposed amendment does not account for the potential risks when a data subject requests the transmission of their personal information to another personal information controller. Article 35-2 should be amended to make it clear that when a data subject requests such a transmission that the liability for any subsequent violations of PIPA rests with the personal information controller to whom the data was transferred and not with the original entity that facilitated the request as mandated by Article 35-2. Moreover, Article 35-2 should be amended to permit a personal information controller to deny a request for transmission to another controller when the personal information controller knows or has reason to

know that the data subject is request a transfer to a company that is suspicious or that the data will otherwise be at a high risk of infringement of PIPA.

AUTOMATED DECISION-MAKING
ARTICLES 4(6) AND 37-2

SIIA understands the impetus behind amending PIPA to include a new data subject right at Article 4(6) relating to automated decision-making, particularly with respect to developments in other global frameworks, like the GDPR, to do the same. As currently proposed, however, Articles 4(6) and the newly inserted 37-2 are ambiguous and therefore risk hindering innovation in using automated decisions for services without providing any benefit to data subjects.

For instance, as proposed, Article 37-2(1) permits a data subject to object or request an explanation of automated decisions, and in some instances even refuse the decision-making, if the decision is made solely by automated processing and "produces individual or legal effects concerning a specific data subject or significantly affects his/her life, body, mind, and property." It is unclear what would constitute an "individual effect" to trigger a company's obligation to comply with the requests through measures as required by Article 37-2(2). Similarly, it is ambiguous what constitute a significant affect on a data subject's life, body, mind, and property. Indeed, this requirement for exercising the right appears to be entirely subjective, which would require personal information controllers to respond to the requests based on the subjective assertions of the data subject rather than on an objective standard that can be applied equally and fairly across data subjects. **We urge the government to revisit this provision and either limit the requests to when automated decision-making will produce a legal effect concerning the data subject, which at least aligns with the GDPR, or set forth objective and reasonable standards for any expansion beyond that.**

REQUEST FOR MATERIALS AND FACT INVESTIGATION
ARTICLE 45(2)

SIIA objects to the addition of the newly inserted Article 45(2), which would give the Dispute Mediation Committee the authority to have the members and officials of the administrative organization enter a place of business related to a dispute in mediation to review and copy business records. This is a highly concerning delegation of authority, tantamount to a law enforcement action, under the auspices of a quasi-official entity that is formed to settle disputes not law enforcement investigations. If finalized as proposed, this provision will result in the seizing and review of business information that is covered by legal privileges and could result in the publicizing of trade secret and other confidential information. Actions such as accessing a business premises to review and copy business records should only be permitted within the parameters of an official law enforcement investigation and subject to due process rights, including concrete standards for when such an extraordinary invasion is appropriate and necessary. **We urge the government to strike Article 45(2) from the proposed amendment in order to ensure that the access and seizure of business records are subject to appropriate standards and carried out by trusted public authorities that are trained to meet obligations with respect to privileged, confidential, and trade secret information.**

CONCLUSION

On behalf of SIIA, thank you again for the opportunity to provide you with our feedback and comments on the proposed amendment to PIPA. We would welcome the opportunity to engage with you further on this process, and we will be available to answer any questions you may have regarding our feedback. If you do have any questions, you can reach me at **+1.202.789.4471** or sdepaul@siia.net. Our current mailing address is **PO Box 34340, Washington DC, 20043, USA**.

Dated: February 15, 2021 (USA)

Respectfully submitted,

/s/ *Sara C. DePaul*

Sara DePaul
Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
202-789-4471 Office / 614-439-4392 Mobile / @saracdepaul Twitter
siia.net/policy
