Proposed Amendments to the Presidential Decree of Personal Information Protection Act

Comments from BSA | The Software Alliance

May 11, 2020

Introduction and Summary of Comments

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Ministry of Internal Affairs and Security (**MOIS**) regarding the draft amendments to the Presidential Decree implementing changes to Korea's Personal Information Protection Act (**PIPA**) and related measures (**PIPA Decree**). Our comments focus on the measures designed to enhance the use of pseudonymized personal data as a means of enhancing the flexibility and utility of such data while ensuring that the information subjects' (**data subjects'**) privacy and other rights are protected.

BSA members are enterprise solutions providers that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. These enterprise software companies are in the business of providing privacy protective technology products and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

Therefore, BSA supports and welcomes the government of the Republic of Korea's (**ROK**) effort to support Korea's transition to the Fourth Industrial Revolution, including through amendments of the PIPA and related legislation. We have enormous experience engaging with governments around the world to promote effective, internationally interoperable legal systems that protect the privacy of consumers' personal information and provide strong consumer rights while

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 6369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

supporting responsible uses of data-driven technologies.[2] BSA members provide technologies that are trusted to advance social and economic goals, from empowering businesses to transition to remote working and ensure the continuity of their operations, to enabling researchers and first responders to address the spread of infectious diseases, such as COVID-19. We hope that our comments will assist MOIS in achieving these goals.

Attachments

- Appendix 1: BSA's article-specific comments in the MOIS's requested format.
- Appendix 2: The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation.[3] Both English and Korean versions included.

Recommendations

General Observations

As countries worldwide develop or modernize their personal information protection laws and regulations, it is critical that these frameworks are designed to provide effective consumer privacy protections in a manner that is internationally interoperable, flexible enough to account for rapidly evolving technologies and business models, and able to facilitate innovation and progress in promising areas of new technologies such as advanced data analytics and artificial intelligence (**AI**).

BSA supports frameworks that increase the transparency of personal data collection and use; provide consumers with control over their personal data; support robust security obligations; and promote the use of data for legitimate business purposes.[4]

The enacted amendments to the PIPA and related legislation assist in this regard by empowering the Personal Information Protection Commission (**Protection Commission**) and by introducing amendments to facilitate more flexible use of personal data, especially pseudonymized data. BSA urges MOIS to reinforce and support these objectives as you finalize the PIPA decree.

Distinguishing Data Controllers and Data Processors

At the outset, we note that the Korean data protection framework departs from an emerging international consensus in defining the types of entities subject to personal data protection laws. Specifically, the PIPA lacks a clear distinction between a "personal information controller" (**data controller**), defined in Article 2.5,[5] and a personal information processor (**data processor**). That fundamental distinction is critical to a host of global privacy laws, which distinguish between companies that decide when and how to collect and use data about

[2] See BSA Global Privacy Best Practices at:https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf.
In Korean at https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices_ko.pdf

[3] At: https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf;
In Korean at: https://www.bsa.org/files/policy-filings/kr05042020controllerprocessor.pdf

[4] BSA Global Privacy Best Practices *op. cit.*

[5] PIPA Article 2.5: "The term "personal information controller" means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities;"

individuals (data controllers) and companies that only process data on behalf of other companies (data processors).

This distinction is important because both data controllers and data processors have important roles in protecting personal information. For that reason, personal data protection laws should define both types of entities and subject them to obligations that reflect their role in safeguarding consumers' data. For example, data controllers generally interact with consumers and decide when and why to collect consumers' data. Data protection laws therefore generally place consumer-facing obligations on data controllers, including any requirements to obtain consent for processing and obligations to honor consumer rights requests.

In contrast, data processors generally do not have direct relationships with individual data subjects — but only process data on behalf of a data controller, often without looking at the underlying data. Indeed, a data processor may be contractually *prohibited* from accessing data it stores or otherwise processes for a controller. Data processors should accordingly be subject to important obligations to safeguard the data they hold, such as by enacting reasonable security measures. But placing consumer-facing obligations on data processors may ultimately undermine consumer privacy, since it may require processors to review significant amounts of data they otherwise would not (and in many cases, cannot) analyze in order to identify individuals they do not know and reach out to them to satisfy legal requirements.

As it stands, because the PIPA does not clearly distinguish between data controllers and data processors, it is extremely important for the MOIS to review carefully the broad obligations imposed on data controllers in the PIPA Decree. Therefore, we recommend MOIS to craft the PIPA Decree in a way that clarifies that many of these obligations do not apply to data processors, but only to data controllers that have knowledge of the data subjects and the personal data involved, and that make decisions on how such data is processed. As noted above, extending obligations meant for data controllers to data processors will weaken privacy as opposed to strengthening it, as players who were not originally intended to know who the data subjects are or what the collected data about them entails would need to have access to some of this information just so that they could comply with legal requirements.

Examples where MOIS should exclude data processors from the obligations of the PIPA include the consumer rights articulated in Chapter V, Articles 35-37, and in the corresponding PIPA Decree draft Articles 48-4, 48-5, 48-7, etc.) and the obligation to notify data subjects regarding a data breach (PIPA Article 34, PIPA Decree draft Article 48-3). The reason for this recommendation is that, as we state above, data processors (for example cloud computing service providers) may not have any information regarding the particular data subjects, nor might they even be aware of which data is personal data, and therefore subject to these laws. Indeed, many processors are under contractual obligations NOT to be aware of such details in the data they are processing on behalf of their customers The obligations to protect consumer rights, therefore, should fall on the data controllers, who must then be accountable for how any third party data processors manage such data.

Good Governance and Stakeholder Consultation

The amended PIPA grants the Protection Commission numerous opportunities and authorities to develop binding rules, requirements, and standards.[6]

It is important to clearly specify in the PIPA Decree that the standards and guidelines the Protection Commission will establish should be developed in a manner consistent with internationally recognized standards and emerging best practices. Rules should be outcome-oriented, and risk-based, to avoid overly prescriptive requirements that are inconsistent with emerging technological and business processes.

To assist the Protection Commission in these objectives, it is also critical that the PIPA Decree require the Protection Commission to undertake open and transparent consultations and work closely with private sector stakeholders, including both domestic and international companies. This will help to ensure that the work of the Protection Commission is aligned with international best practices, informed by the latest technological developments, and will work well to both effectively protect the privacy and personal information of the Korean people while at the same time fostering innovation and creating an Intelligent Information Society.

International Data Transfers

Because the ability to transfer data internationally is the lifeblood of the modern digital economy, we would like to emphasize the importance of ensuring that the PIPA and its implementation allows companies to responsibly transfer data internationally.

If the cross-border transfer of personal data is limited by restrictive requirements, those limitations will not only restrain the advancement of data protection goals, but also will trigger unintended consequences. Such restrictions disrupt companies' operations and make it costlier to provide services in Korea, even if that is not the intent, effectively depriving businesses in Korea of advanced services and putting them at a competitive disadvantage compared with companies in other countries.

Specific Recommendations

The following section describes our specific recommendations to adjust certain Articles of the draft PIPA Decree. These recommendations are summarized in the table in Appendix 1.

Combination of Pseudonymized Information Owned by Different Personal Information Controllers, etc.

Article 28-3 (1) of the PIPA requires the combination of pseudonymized information processed by different data controllers ***to be conducted by a specialized institution*** designated by the

[6] For example, Article 12 grants the Protection Commission the authority to establish the Standard Personal Information Protection Guidelines regarding personal information processing standards, types of personal information breaches, and preventive measures. Article 13 requires the Protection Commission to establish policies to promote and support self-regulating activities including introduction and facilitation of a privacy mark. The Protection Commission will prescribe rules regarding the procedures and methods of combination of pseudonymized information (Article 28-3), and storing, managing, and recording information about pseudonymized information (Article 28-4). The Protection Commission may certify whether the data processing and other data protection-related actions of a personal information controller comply with the law and determine the qualifications of individuals and institutions designed to administer such certifications (Article 32-2). And the Protection Commission is responsible for designating institutions to conduct privacy impact assessments (PIAs), fostering training of specialists, and developing and disseminating criteria for PIAs (Article 33).

Protection Commission or other government agencies. We view this as a very unfortunate requirement in the law. One of the stated objectives of the amendments was to enhance and promote better data analytics using pseudonymized personal information to facilitate important discoveries and outcomes.

The purpose of this requirement appears to be to minimize the chances of reidentifying pseudonymized data during the combination and analysis process. However, requiring the combination of pseudonymized data sets to be conducted by a separate "Expert Data Combination Agency" (**EDCA**) will likely represent a significant impediment to effective data analysis and inter-firm collaboration.

We urge that MOIS craft the PIPA Decree with as much flexibility as possible to permit entities to share and combine pseudonymized data sets, for commercial purposes as well as research and scientific objectives, pursuant to contractual arrangements committing each party to protect the data sets in accordance with the law. As the PIPA recognizes, there are many purposes for which pseudonymized data may be processed, and could be combined, without identifying the individuals whose data is included in a pseudonymized data set. These include statistical purposes, scientific research, and archiving purposes in the public interest.

For example, efforts to effectively respond to the COVID-19 pandemic have demonstrated, in the most stark terms possible, the importance of being able to maximize the efficiency by which firms and governments utilize even sensitive personal information in a privacy protective manner. In this light, the additional requirements to conduct such analysis via a specialized government institution is a step in the wrong direction.

Article 29-2 of the draft PIPA Decree goes further than the PIPA by requiring, except under specific circumstances, and subject to the approval of the EDCA, the data controller to view the results of such data combination only in a designated physical space (**Analysis Space**), provided by the EDCA in accordance with the specifications of the Protection Commission. We urge the MOIS to amend Article 29-2 (3) to make clear that the use of an Analysis Space is purely voluntary.

We also suggest that MOIS clarify in the Decree that the Analysis Space need not be a physical location within the premises of an EDCA but can refer to logically separated "virtual" spaces using cloud computing infrastructure.

If the requirement to seek approval of the EDCA to export combined data sets remains, we urge the MOIS to amend the PIPA Decree to require a) the EDCA to approve such requests unless there are specific reasons not to; b) the EDCA to specify the grounds for rejecting such a request; and c) to provide an applicant a legal basis to challenge a rejection.

Our recommendations are designed to assist the ROK to achieve its goal of fostering an Intelligent Information Society and to benefit from the revolution of advanced data analytics. Advanced data analytics, data sharing, and data combination can be conducted in a privacy protective manner. **The solution is not to make such efforts exceedingly cumbersome, but to ensure that data controllers remain accountable for the protection of the personal data they process, no matter by whom, where, or in what manner**.

Standards on Additional Use/Provision of Personal Information, etc.

The PIPA allows a data controller to, without the consent of the data subject, use (PIPA Article 15 (3)) or provide (PIPA Article 17 (4)) personal information for additional uses "within the scope reasonably related to the purposes for which the personal data was initially collected."

Article 14-2 of the draft PIPA Decree specifies 4 conditions that must be met for a data controller to meet the condition of using or providing data "within the scope reasonably related…" These conditions are: 1) the purpose is reasonably related to the original purpose of collection; 2) the additional use was foreseeable; 3) the additional use does not infringe on the user; ***and*** 4) if the additional use can be achieved using pseudonymized information, the information ***shall*** be pseudonymized.

We agree that data controllers should inform data subjects of the purpose for which they are collecting personal data and should use that data in a manner that is consistent with that explanation, the context of the transaction, or the reasonable expectations of the data subject, or in a manner that is otherwise compatible with the original purpose for which the data was collected. However, we are concerned that the current language of the draft PIPA Decree amendments may be overly restrictive.

To make clear that the concept of "reasonably related to" depends on the context in which the data was initially collected, we suggest amending the first part of Article 14-2 as follows:

> *Where prescribed by Presidential Decree" under Articles 15 (3) and 17 (4) of the Act shall refer to the case where all of the following conditions are satisfied**, taking into consideration the reasonable expectation of data subjects based on the compatibility of the use with the original purpose for which the data was collected**. In such case, "use" shall be deemed as "provision" for the purpose of Article 17 (4) of the Act.*

Of the first two conditions, the first, that the additional use is "reasonably related" to the original purpose of collection, seems to be most consistent with the stated obligations set out in the PIPA. The second condition, that the additional use is "foreseeable" could be considered as an example of being reasonably related, as a use that is foreseeable at the time of collection would likely be reasonably related to such collection. However, one might easily imagine a circumstance where, although the additional use is clearly "reasonably related" to the initial collection, it may not have been, at the time, "foreseeable" given changes in circumstances.

In addition, condition 3) requires the data controller to satisfy that the additional use will "… not unfairly infringe the interests of the data subject **or any third party**" (*emphasis added*). Including the interests of "any third party" as a mandatory condition for additional use goes beyond the language of the law, which only states that the data controller must consider "…whether disadvantages have been caused to the data subject…" (Article 15 (3) and Article 17 (4)). Also, requiring a data controller to ensure that the interests of "any" third party are not infringed is a very broad and undefined standard that would be difficult to ascertain and would therefore further limit legitimate additional uses of personal data counter to the intention of the amendments to the PIPA.

Therefore, we recommend combining conditions 1) and 2) and deleting reference to "any third party" in condition 3) as follows:

1) *The purpose of additionally using personal information is reasonably related to the original purpose for which the personal information was collected**, or otherwise foreseeable to the data subject, considering the circumstances and practices by which the personal information was collected**; **and***

~~***2) The additional use of personal information is foreseeable in light of the circumstances and practices by which the personal information was collected;***~~

2) ~~***3)***~~ *The additional use of personal information shall not unfairly infringe on the interests of the data subject* ~~***or any third party***~~*; and*

We also have specific concerns about condition 4), which states that ***if*** pseudonymized data ***may*** be used then the data ***shall*** be pseudonymized. This condition may be inconsistent with the intent of the PIPA and be difficult to interpret or implement in practice. We recognize the importance of encouraging the use of pseudonymized information. However, one can imagine circumstances where, although pseudonymized information ***may*** be used, such use could negatively impact the accuracy of the outcomes based on processing such data or otherwise reduce the value of the data to the data subject or the data controller.

Therefore, rather than requiring the pseudonymization of information in any case in which it ***can*** be used, we recommend adjusting draft PIPA Decree Article 14-2 to require data controllers to ***consider*** pseudonymizing the data. In doing so, data controllers should take into account the possible costs or trade-offs between the enhanced privacy protections from using pseudonymized data and the costs of sub-optimal processing outcomes for the data subjects or the data controller. We therefore recommend removing item 4 as a condition for additional use and revising the clause as follows:

> ~~***4.***~~ ***The personal information controller should also consider whether*** ~~***If***~~ *the purpose of additional use can be achieved with the personal information being pseudonymized*~~*,*~~ ***and, if appropriate for the purposes, should consider relying on*** ~~***then the personal information shall be***~~ *pseudonymized* ***personal information****.*

Scope of Sensitive Information

Article 18-3 of the draft PIPA Decree adds "Any information on physical, physiological, psychological, or behavioral characteristics of a specific individual" to the list of information to be designated as "sensitive personal information" pursuant to PIPA Article 23. We are concerned that these categories are far too broad to be practicable and urge MOIS to consider substantially narrowing the scope of this provision to specific biometric information used for the purpose of uniquely identifying a natural person.

Penalties

PIPA Article 28-6 imposes penalties of up to 3% total sales on data controllers that violate the PIPA by processing pseudonymized data in a way to identify individuals. Similarly, PIPA Article 39-15 imposes penalties of up to 3% total revenue on information and communications service providers violating certain prohibitions of the PIPA.

Draft PIPA Decree Articles 29-6 (4) and 48-10 (4) specify the method for calculating such penalties, referring to Table 1-3 and Table 1-5 of the Draft PIPA Decree, respectively.

Effective deterrents to willful or negligent violations of the law are important. However, it is important to highlight that remedies and penalties for violations of personal information protection laws should be structured to be effective and proportionate to the harm resulting from such violations.

In many cases, companies that are informed or warned that their conduct may be in violation of personal information protection laws will correct their conduct voluntarily. As a result, the draft PIPA Decree should provide an appropriate period for data controllers and information and communications service providers to implement measures in response to the Protection Commission's guidance, recommendations, or orders prior to the imposition of penalties. Penalties should only be applied if business operators do not take appropriate measures in a timely manner.

When penalties are imposed, the appropriate tools may include providing monetary relief to compensate individuals for any economic harm they suffer and imposing tailored conduct-based relief to prevent future violations.

Conclusion

BSA is grateful for the opportunity to provide these comments to the MOIS. We support the ROK's efforts to modernize Korea's personal information protection laws and requirements, and we look forward to working with the Protection Commission as it takes up its new responsibilities under the PIPA and the PIPA Decree. We hope that our comments will assist you as you try to best achieve your goals and objectives for managing Korea's transition to the Fourth Industrial Revolution and establishing and Intelligent Information Society.

Please do not hesitate to contact us if you have any questions or comments regarding our suggestions. We remain open to further discussion and look forward future opportunities to support the nation's work.

BSA | THE SOFTWARE ALLIANCE

APPENDIX 1: BSA's article-specific comments in the MOIS's requested format.

Amendment clause	Agree /Disagree	Reasons
Article 29-2: (Combination of Pseudonymized data between Different Personal Information Controllers, etc.) 1. If any personal information controller (hereinafter referred to as "Applicant") intends to request an expert agency (hereinafter referred to as "Expert Data Combination Agency") to combine pseudonymized information in accordance with Article 28-3 (1) of the Act, the Applicant shall submit the data combination request in the form prescribed by the Protection Commission's notification to the relevant Expert Data Combination Agency. 2. The Expert Data Combination Agencies shall combine pseudonymized information in a way that makes the individual unidentifiable in accordance with the procedures and methods prescribed by the Protection Commission's notification. In such case, the Expert Data Combination Agency may make Korea Internet and Security Agency provide relevant support work as necessary to make the particular individual unidentifiable. 3. A personal information controller shall analyze the combined data, in accordance with paragraph (2), in a physical space within an expert data combination agency designated by Protection Commission (hereinafter	Disagree	We support the establishment of a framework for the combination and use of pseudonymized data. However, we urge MOIS to amend the PIPA Decree to allow for commercially relevant combinations of pseudonymous and other data sets pursuant to contractual arrangements between the parties, rather than requiring data controllers to go through a third party Expert Data Combination Agency to conduct such operations. We also urge the MOIS to amend Articles 29-2 (3) and (4) to clarify that the use of an Analysis Space is purely voluntary. We also suggest that MOIS clarify in the Decree that the Analysis Space need not be a physical location within the premises of an EDCA but can refer to logically separated "virtual" spaces using cloud computing infrastructure. If the requirement to seek approval of the EDCA to export combined data sets remains, we urge the MOIS to amend the PIPA Decree to require a) the EDCA to approve such requests unless there are specific reasons not to; b) the EDCA to specify the grounds for rejecting such a request; and c) to provide an applicant a legal basis to challenge a rejection. The purpose of these recommendations to facilitate privacy protective means of conducting data analysis, including on pseudonymous data sets combined from different data controllers.

referred to as the “Analysis Space”) where technological, administrative, and physical measures to safety have been taken. 4. Notwithstanding paragraph (3), when the personal information controller deems that it is difficult to achieve its goal of combining the data or otherwise difficult to utilize the Analysis Space, and requests to release the combined data outside the Analysis Space, the Expert Data Combination Agency may approve the release of data after conducting an evaluation of the risk of re-identifying the individual, etc. in accordance with the criteria issued by Protection Commission under public notice.		
Article 14-2 (Additional usage/supply standard for personal information) “Where prescribed by Presidential Decree” under PIPA Articles 15 (3) and PIPA Article 17 (4) shall refer to the case where all of the following conditions are satisfied. In such case, the term “use” shall be deemed as “provision” for the purpose of PIPA Article 17 (4). 1. The purpose of additional use of personal information shall be reasonably related to the original purpose for which the personal information was collected; 2. The additional use of personal information is foreseeable based on the circumstances by which the personal information was collected and the practices by which it was processed;	Disagree	The PIPA Decree should make clear that the concept of “reasonably related to” is conditioned on the relationship between the data subject and the data controller. Please see our recommended adjustments to Article 14-2 below. Furthermore, because the terms “foreseeable” and “reasonably related” are similar, and “foreseeable” might be considered to be a sub-set of factors to determine whether additional use is “reasonably related”, rather than a separate and additional condition, we suggest combining paragraphs 1) and 2) as described below. We also propose removing reference to the interests of a third party, as this goes beyond the scope of the PIPA and, being to broad and underdefined, may be very difficult to ascertain, would make it far too

3. The additional use of personal information shall not unfairly infringe on the interests of the data subject or any third party; and 4. If the purpose of additional use can be achieved with the personal information being pseudonymized, then the personal information shall be pseudonymized.		difficult to reasonably use personal data for additional uses consistent with the law. Finally, while data controllers may be encouraged to use pseudonymized information when practicable, it would not be helpful, or consistent with PIPA Articles 15 (3) and 17 (4) to ***require*** the pseudonymization of personal data in every case where it ***could*** be pseudonymized. Instead, we suggest amending the PIPA Decree to instead encourage data controllers to consider using pseudonymized data when they can and when the costs of disadvantages of doing so do not outweigh the privacy enhancing benefits. Proposed amendments to draft PIPA Article 14-2: *Where prescribed by Presidential Decree" under Articles 15 (3) and 17 (4) of the Act shall refer to the case where all of the following conditions are satisfied****, taking into consideration the reasonable expectation of data subjects based on the compatibility of the use with the original purpose for which the data was collected****. In such case, "use" shall be deemed as "provision" for the purpose of Article 17 (4) of the Act.* ***1)*** *The purpose of additionally using personal information is reasonably related to the original purpose for which the personal information was collected****, or otherwise foreseeable to the data subject, considering the circumstances and practices by which the personal information was collected****; and***

		~~***2) The additional use of personal information is foreseeable in light of the circumstances and practices by which the personal information was collected;***~~ 2) ~~***3)***~~ *The additional use of personal information does not unfairly infringe on the interests of the data subject* ~~***or a third party.***~~ ***;*** ~~***and***~~ ~~***4).***~~ ***The personal information controller should also consider whether*** ~~***If***~~ *the purpose of additional use can be achieved with the personal information being pseudonymized* ***and, if appropriate for the purposes, should consider relying on*** ~~***then the personal information shall be***~~ *pseudonymized* ***personal information****.*
Article 18 (Scope of Sensitive Information) 1 ~ 2 (Remains) 3. Any information on physical, physiological, psychological, or behavioral characteristics of a specific individual that was produced using a particular technology with purpose to identify individual; 4. Any information relating to race or ethnicity that may be used to discriminate unfairly against an individual in light of the purpose or circumstances of processing such information	Disagree	Article 18-3 of the draft PIPA Decree adds "Any information on physical, physiological, psychological, or behavioral characteristics of a specific individual" to the list of information to be designated as "sensitive personal information" pursuant to PIPA Article 23. We are concerned that these categories are far too broad to be practicable and urge MOIS to consider substantially narrowing the scope of this provision to specific biometric information used for the purpose of uniquely identifying a natural person.

<table>
<tr>
<td>Articles 29 (6)-4, 48 (10)-4 and Annexes 1 and 3:

Article 29-6 (Imposition of Administrative Surcharges and its criteria for the Processing of the Pseudonymized information)
…
4. Criteria and process of imposition of administrative surcharges pursuant to Article 28 (6) is stated under Annex 1 and 3.

Article 48-10 (Special Cases for the Imposition of Administrative Surcharges)
…
4. Criteria and process of imposition of administrative surcharges pursuant to Article 39 (15)-4 is stated under Annex 1 and 5.

<u>Annex 1: Table 1-3</u>
(Criteria, etc. for Imposition of Penalty Surcharges) (Related to Article 29-6 (4))

1. Calculations of Surcharges
The surcharge must be calculated through comprehensively considering the impact of violation subject to Article 28-6 (1) of the Act through necessary and additional aggravating & mitigating the applicable standard amount.

2. Calculation Method and Reasons for the Criteria of Surcharge Calculation

A. Applicable Standard Amount
1) The applicable standard amount shall be the amount calculated by multiplying the related sales under Article 29-6 (1) by the following surcharges (applicable standard rate) according to the degree of seriousness of violation

<table>
<tr><th>Degree of Seriousness of Violation</th><th>Applicable Standard Rate</th></tr>
</table>
</td>
<td>Disagree</td>
<td>The draft PIPA Decree should provide an appropriate period for data controllers and information and communications service providers to implement measures in response to the Protection Commission’s guidance, recommendations, or orders prior to the imposition of penalties. Penalties should only be applied if business operators do not take appropriate measures in a timely manner.

When penalties are imposed, the appropriate tools may include providing monetary relief to compensate individuals for any economic harm they suffer and imposing tailored conduct-based relief to prevent future violations.</td>
</tr>
</table>

Very Serious Violation	27/1000
Serious Violation	21/1000
Violation	15/1000

2) Notwithstanding Section 1), in cases the violation is subjected to any subparagraph of Article 29-6 (2), depending on the gravity of the violation, the applicable standard amount shall be as follows.

Degree of Seriousness of Violation	Applicable Standard Amount
Very Serious Violation	KRW 360M KRW 60M
Serious Violation	KRW 280M
Violation	KRW 200M

3) Degree of Seriousness of Violation shall be determined by comprehensively considering whether it was intentional or negligence, whether it was done for profit, the level of personal information damage, whether personal information is exposed to the public, the level of profits acquired through the act of violation, etc.

B. Mandatory Aggravation and Mitigation of Surcharge

The surcharge must be aggravated or mitigated to the range of 50/100 of the applicable standard amount by considering the period, frequency of violation.

C. Discretionary Aggravation and Mitigation of Surcharge

The surcharge can be aggravated or mitigated to the range of 50/100 of

the applicable standard amount by comprehensively considering the level of efforts to protect personal information, level of cooperation to the investigation and whether the perpetrator cooperated with the investigation of the violation and whether the perpetrator led the violation, among others.

Annex 3: Table 1-5 (Standards and Procedures for Calculation of Penalty Surcharge in relation to Article 48-10 (4))

1. Steps of Calculating Penalty Surcharge

   Penalty surcharges shall be calculated by applying to the base amount mandatory aggravation/mitigation and discretionary aggravation/mitigation taking into account the totality of the considerations under each subparagraph of Article 39-15 (3) of the Act and any other acts having effect thereon.

2. Calculation Method and Considerations for Each Step of Calculating Penalty Surcharge

   A. Calculation of Base Amount

      1) The base amount shall be the sales revenue related to the violation under Article 48-10 (1) multiplied by the applicable penalty surcharge rate (imposition rate) below depending on the severity of the violation:

Severity of Violation	Applicable Standard Rate
Very serious	2.7%
Serious	2.1%

Ordinary	1.5%

2) Notwithstanding Section 1) above, for an act falling within any of the subparagraphs of Article 48-10 (2), the base amount shall be as follows depending on the severity of the violation:

Severity of Violation	Applicable Standard Amount
Very serious	KRW 360M
Serious	KRW 280M
Ordinary	KRW 200M

3) The severity of the violation shall be determined taking into account the totality of whether there was willful misconduct or gross negligence, whether the act was for profit, how much damage was caused to personal information due to the violation, whether the personal information was disclosed to the public and how much the perpetrator gained from the violation, among others.

B. Mandatory Aggravation/Mitigation

The base amount shall be aggravated or mitigated to the extent of 50/100, taking into account the period or number of violation.

C. Discretionary Aggravation/Mitigation

The amount after the mandatory aggravation/mitigation may be aggravated or mitigated to the extent of 50/100, taking into account the totality of how much effort the perpetrator used to protect personal information, whether the perpetrator cooperated with the investigation of the violation and whether the perpetrator led the violation, among others. 3. Detailed Standards Detailed standards for calculation of sales revenue related to the violation, standards for determination of severity of violation, detailed standards for mandatory aggravation/mitigation and discretionary aggravation/mitigation and any other matters required for imposition of penalty surcharges shall be prescribed and notified by the Protection Commission.		

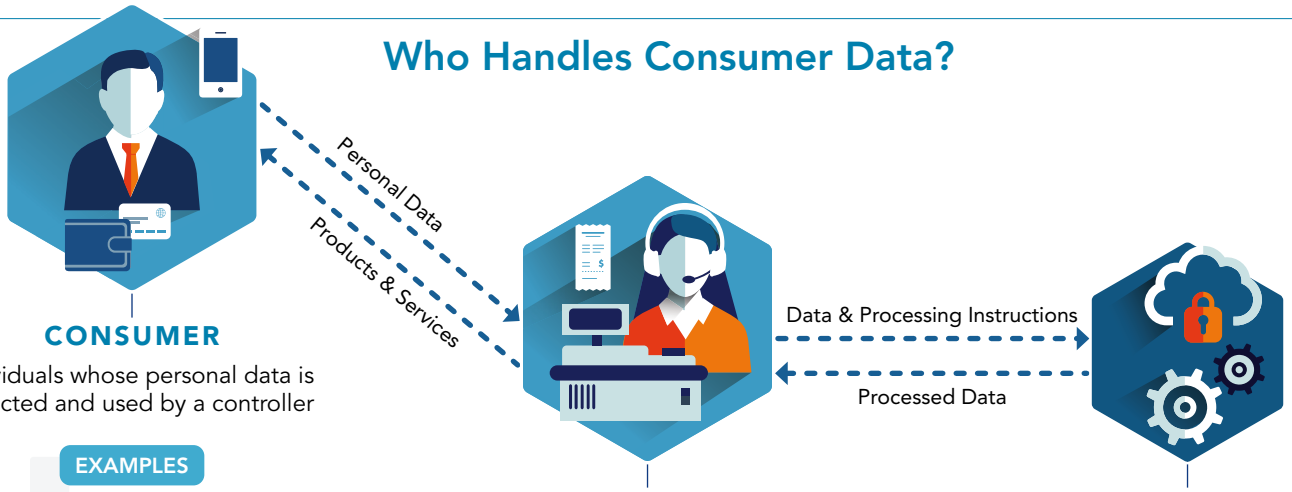
The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data on *behalf of* another company, which act as **processors** of that data

This fundamental distinction is critical to a host of global privacy laws, including the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?



CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Say no,** and opt out of broad types of use, not just sale
- **Access** information about them
- **Correct** that information
- **Delete** that information
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests for access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

Companies that decide how and why to collect consumer data.	Companies that process consumer data at the direction of others.
GDPR: Controllers Determine the "purposes and means" of processing.	**GDPR: Processors** Handle personal data "on behalf of" a controller.
CCPA: Businesses Determine the "purposes and means" of processing.	**CCPA: Service Providers** Handle personal information "on behalf of" businesses.

This distinction is crucial to a host of privacy laws beyond the GDPR and CCPA. In addition, leading international privacy standards, including ISO 27701, and voluntary frameworks that ensure data can be transferred across national borders, such as the APEC Cross Border Privacy Rules, also distinguish between controllers and processors.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

- Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like the GDPR and CCPA require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.