

Data Privacy Update: Major Amendment to the Personal Information Protection Act of Korea

Korea's amendment to the Personal Information Protection Act ("PIPA") was passed by the National Assembly on February 27, 2023, more than two years after the Personal Information Protection Commission ("PIPC") of Korea had proposed the initial draft amendment bill in 2021. The amended PIPA will be promulgated on March 14, and will take effect on September 15, 2023.

The amended PIPA aims to give momentum to the growth of Korea's digital economy based on emerging technologies and data, and includes the following key changes: (i) strengthening the rights of data subjects by introducing the right to data portability and the right to object to automated decision-making, (ii) simplifying the application of the PIPA for all data controllers by removing special provisions for the online service providers, (iii) shifting from criminal sanctions towards economic sanctions, and (iv) providing additional grounds for overseas transfer of personal information (similar to EU GDPR's adequacy decision) in addition to the current stringent consent requirement.

Most provisions in the amended PIPA will take effect six months after the promulgation of the law (September 15, 2023). However, certain provisions, including the right to object to automated decision-making, shall take effect one year after the promulgation of the law (September 15, 2024). The right to data portability will take effect on a date to be determined by the Enforcement Decree of the PIPA ("**Enforcement Decree**"), which shall be between one year and two years after the promulgation of the law.

Below are some of the key provisions in the amended PIPA that we would like to introduce:

1. Strengthening the rights of data subjects

The amended PIPA enhances the rights of data subjects by introducing the right to data portability and the right to object to automated decision-making.

Related Areas

IP & Technology

Data & Technology

Contact

Doil SON

+82-2-528-5836
dison@yulchon.com

Sun Hee KIM

+82-2-528-5838
kimsh@yulchon.com

Dayeon AHN

+82-2-528-5254
dyahn@yulchon.com

Seung Jin HEO

+82-2-528-5567
sjheo@yulchon.com

Right to data portability

Article 35-2 of the amended PIPA grants data subjects the right to request that their personal information be transmitted to themselves or to a third party who satisfies the security standards specified in the Enforcement Decree.

Upon receiving a transmission request, a data controller must ensure that the requested information is transmitted within a reasonable timeframe, at a reasonable cost, and via reasonable means. The data controller may either reject or suspend a transmission request if the identity of the requesting data subject is not confirmed, or other conditions specified in the Enforcement Decree are met.

Also, please note that the scope of personal information that can be transmitted, the process of requesting transmission, the deadline and method of transmission, the method of revoking a transmission request, the method of rejecting or suspending a transmission request, and other related aspects will be prescribed in the Enforcement Decree.

The adoption of the right to data portability in the amended PIPA is expected to broaden the scope of the “My Data” service, which is currently confined to the financial industry under the Credit Information Use and Protection Act.

Right to object to automated decision-making

The amended PIPA also provides data subjects with the right to reject, object, and/or request explanations regarding decisions made by fully automated systems, including artificial intelligence systems, that process personal information and substantially impact the rights or obligations of the data subjects. If a data subject exercises this right, the data controller must cease applying an automated system or take necessary measures, such as manual re-processing of personal information, or providing explanations, etc., unless there are any justifiable reasons for not doing so.

2. Integrating the rules applicable to ordinary data controllers and the special provisions applicable to online service providers

Prior to the amendment to the PIPA, online service providers (“**OSPs**”)¹⁾ were subject to special provisions in addition to the general provisions applying to ordinary data controllers. However, with the amended PIPA, all provisions of the PIPA now apply equally to both general data controllers and OSPs.

1) An OSP is defined as an entity providing information or intermediating the provision of information for commercial purposes through the usage of information and communications services. In general, this definition is interpreted broadly, and may even include a company operating a company website to provide information about its products.

The following special provisions, which previously only applied to OSPs, will be applicable to **all data controllers**:

- Data controllers meeting the standards prescribed by the Enforcement Decree will be required to notify data subjects regularly about the use and third-party provision history of their personal information, or provide access to a system that shows the use and third-party provision history of their personal information.
- Data controllers meeting the revenue and personal information possession standards prescribed by the Enforcement Decree will need to take necessary measures such as purchasing insurance, joining mutual aid associations, or accumulating reserves to fulfill their liabilities to compensate for damages caused by violation of the PIPA.
- Data controllers with no address or business office in Korea meeting the criteria prescribed by the Enforcement Decree will be required to designate a local representative to act on their behalf.
- The current requirement under Article 39-4 of the PIPA, which required OSPs to notify data subjects and report to the Personal Information Protection Commission ("**PIPC**") or Korean Internet & Security Agency ("**KISA**") within 24 hours in case of any loss, theft, or leakage of personal information ("**Data Breach**"), has been deleted. Instead, all data controllers will be required to comply with the notification and reporting requirements under Article 34 of the amended PIPA.

According to Article 34, data controllers must promptly notify data subjects of any Data Breach, unless the data controller does not possess the contact information of the data subject (in which case alternative measures prescribed under the Enforcement Decree should be taken). Additionally, data controllers are required to report to the PIPC or KISA without delay if the scale of the loss, theft, or leakage exceeds a certain threshold as stipulated in the Enforcement Decree.

On the other hand, the special provision, which requires OSPs to delete or separately store the personal information of data subjects who have not used the services for one year, has been deleted.

In sum, these changes represent a shift towards increased consistency and clarity in the application of data protection requirements under the PIPA.

3. A shift from criminal sanctions to economic sanctions

Change in the scope of criminal penalties

The amended PIPA aims to substitute criminal sanctions with administrative penalties for certain violations of PIPA. These violations include but are not limited to, OSP's failure to obtain consent for the collection, use of personal information and failure to destroy personal information. Further, the amended PIPA removes criminal penalty for data breaches due to failure to take data protection measures.

However, it is important to note that, despite the general trend toward economic sanctions, the amended PIPA adds new types of violations that may be subject to criminal sanctions. These violations include obstruction of investigation by the authority by concealing, destroying, forging, or falsifying documents, or refusing access to premises (Article 73(1) Paragraph (5)).

Change in the scope of administrative penalties

Moreover, the amended PIPA aims to broaden the grounds for imposing administrative penalties. Before the amendment, ordinary data controllers (non-OSPs) were subject to administrative penalties only for violations such as the loss or leakage of Resident Registration Number or processing pseudonymized data to identify an individual, whereas the OSPs were subject to administrative penalties for a wider range of violations.

Under the amended PIPA, **all data controllers** can face administrative penalties for a wider range of violations. These violations include failure to obtain consent for collection, use and provision of personal information, failure to obtain consent from the legal representative in processing personal information of a child under the age of 14, failure to obtain consent for processing “sensitive information”, unlawful processing of “unique identification information”, a data controller’s failure to supervise or manage the data processing activities of the data processor thereby causing the data processor’s violation of the PIPA (in the context of outsourcing), processing pseudonymized personal information for the purpose of identifying a specific individual, violation of orders to cease overseas transfer of personal information, unlawful overseas transfer of personal information, and data breaches due to failure to take data protection measures.

Change in the administrative penalty amount

Under the current PIPA, the administrative penalty applicable to OSPs is up to three percent of the “**revenue related to the violation.**” Under the amended PIPA, the base amount for the administrative penalty has been adjusted to the “**total revenue**” (Article 64-2(1)). To ensure that the penalty amount remains proportional to the severity of the violation, “revenue unrelated to the violation” may be excluded from the calculation. However, if the data controller fails to submit the requested materials or provides false materials for calculating the base amount, “**total revenue**” will be used as the base amount (Article 64-2(2)). In effect, the burden of proving the relevant revenue now lies with the data controller.

4. Establishing additional legal bases for overseas transfer of personal information and the PIPC’s right to order a suspension of overseas transfer

Under the current PIPA, data controllers must obtain consent from data subjects before transferring personal information overseas. However, the amended PIPA has added new legal bases for the overseas transfer of personal information under Article 28-8. These include situations where a special provision,

treaty, or international agreement specifically allows the overseas transfer of personal information, where the recipient located overseas has obtained certification determined and announced by the PIPC, or where the transfer of personal information to a country or international organization with an adequate level of protection determined by the PIPC.

The amended PIPA will continue to allow overseas transfer of personal information for entrustment (outsourcing) or storage purposes, provided that certain information is disclosed in the privacy policy or notified to the data subjects. However, an additional requirement has been added, that the transfer is “necessary to execute and perform a contract with the data subject.” The impact of this additional requirement on the enforcement practices concerning overseas entrustment of personal data processing remains to be seen.

Furthermore, the amended PIPA authorizes the PIPC to suspend any ongoing or future overseas transfer of personal information. The PIPC can issue a suspension order if an overseas transfer of personal information violates Article 28-8 of the PIPA (e.g., when an overseas transfer took place without legal grounds, or when the transferring data controller enters into a written contract concerning overseas transfer in violation of the PIPA), or when a data subject has experienced or is highly likely to experience harm due to the recipient (an individual, country, or international organization) failing to provide an adequate level of protection according to the PIPA.

5. Key Takeaways

- All data controllers will need to update their privacy statements and policies to reflect the additional rights of the data subjects introduced by the amended PIPA, such as the right to data portability and their rights related to automated decision-making, to the extent applicable.
- All data controllers will need to update their privacy statements and policies to reflect changes in their privacy obligations resulting from the integration of the rules applicable to the online and offline services. In particular, ordinary data controllers (including offline businesses and data controllers in employer-employee contexts) will need to consider additional obligations due to the expanded scope of the integrated provisions under the amended PIPA.
- Given the increased risk of administrative penalties, we recommend that all data controllers review and strengthen their compliance practices to ensure that they are in fully compliance with the amended PIPA.