Journal of Korean Law | Vol. 17, 33-52, December 2017

Cross-Border Transfers of Personal Data and Practical Implications*

*Inhwan Lee** and Jennifer S. Keh****

Abstract

The cross-border transfer of personal data is an important and often-discussed issue in South Korea. As Korea's representative personal data protection regulations, namely, the Personal Information Protection Act ("PIPA") and the Act on the Promotion of IT Network Use and Information Protection ("Network Act"), distinguish between the third-party provision of personal data and the delegation of personal data processing, it is helpful to analyze the overseas provision of personal data separately from the overseas delegation of personal data processing. Regarding the overseas provision of personal data, the requisite consent is deemed valid only if each third-party recipient is disclosed prior to obtaining the data subject's consent. Thus, it is difficult to obtain consent initially and when new recipients are added. In addition, as the PIPA and the Network Act do not address the issue of whether personal data can be submitted to foreign government authorities pursuant to foreign laws, it is difficult for companies to respond to requests for personal data from foreign government authorities. As for the overseas delegation of personal data processing, although the Network Act includes an exception to the consent requirement for the overseas delegation of personal data processing, companies that want to rely on this exception must carefully analyze the underlying scope of the delegation and the delegated tasks, as there is a lack of precedents and guidance from regulators on exactly when this exception applies. Moreover, companies that delegate the processing of their personal data overseas should ensure that they and their overseas delegatees comply with PIPA and the Network Act's various security requirements for protecting personal data. Last, companies should stay current on the latest international developments in light of Korea's recently joining the APEC CBPRs and Korea's ongoing efforts to obtain an adequacy decision from the European Commission.

* The views and opinions expressed in this article are solely those of the authors and do not reflect the view of the firm or any of the firm's current or past clients.

** Inhwan lee is a senior attorney in Kim & Chang. He received his B.A. in political science from College of Social Sciences, Seoul National University in 2006, M.A. from Graduate School of Law, Seoul National University in 2010, and LL.M. from School of Law, New York University in 2016. He is a member of the Korean and New York Bars.

*** Jennifer S. Keh is a member of the California Bar. She received her B.A. from the University of Chicago in 2004 and J.D. from the UCLA School of Law in 2007. She was a foreign attorney at Kim & Chang when this article was prepared.

KEY WORDS: *personal data, cross-border transfer, third-party provision, delegation of personal data processing*

Manuscript received: Nov. 30, 2017; review completed: Nov. 23, 2017; accepted: Dec. 1, 2017.

Introduction

Interest in cross-border transfers of personal data has continued to increase along with the exponential growth in IT network and communications technology. Related regulations have evolved as lawmakers aim to facilitate the free flow of information across borders while protecting data subjects' rights to the protection of their personal data. Recently, such regulations are increasingly aiming to regulate not only how personal data are processed within their jurisdictions, but also how personal data are processed once transferred overseas.

Korea has also enacted and enforced various data protection statutes, which explicitly address cross-border transfers of personal data. While these laws have been praised for promoting the protection of personal data and data security, they have also been criticized for failing to take into account the practical realities of widespread information sharing and technological developments.

This article summarizes the provisions of the Personal Information Protection Act ("PIPA"), which is the general privacy law in Korea, and the Act on the Promotion of IT Network Use and Information Protection ("Network Act") as they relate to cross-border data transfers and aims to highlight the real-life implications and challenges experienced by companies subject to these laws. First, this work explains the PIPA and the Network Act's approach to cross-border data transfers and their requirements for lawfully making such transfers. Second, it highlights several practical issues that companies must consider regarding their cross-border transfers of personal data, both directly and through third-party service providers. Third, it briefly discusses recent international developments involving Korea and cross-border data transfers.

II. Overview of Korea's privacy regime

1. Major laws concerning the protection of personal data

1) The PIPA

In Korea, the PIPA is the overarching, general law concerning personal data protection.[1] The PIPA was enacted on September 30, 2011, and has been amended several times since then. It is currently composed of nine chapters and 76 articles.

To protect personal data, the PIPA imposes requirements on the "Personal Data Controller," which is defined as all persons, organizations, corporations, and governmental agencies that process personal data files directly or indirectly for business purposes, regardless of sector.[2] As reflected in this definition, "Personal Data Controller" is a broadly defined concept. Consequently, most corporations that handle personal data in the course of business would be considered a Personal Data Controller. It is notable that the definition of "Personal Data Controller" is not limited to corporations established under Korean law or the personal data of Korean residents.

Besides the requirements for processing personal data, the PIPA includes provisions on matters such as the establishment and operation of the Personal Information Protection Commission,[3] the establishment and operation of the Personal Information Dispute Mediation Committee,[4] and class-action lawsuits for data breach incidents.[5]

2) The Network Act

The Network Act, which was enacted before the PIPA, prescribes requirements that online service providers ("OSPs") must follow to protect the personal data of users. The term "OSP" is defined as "(i) the

1) PIPA, Art. 6.

2) PIPA, Art. 2.5.

3) PIPA, Art. 7 and 8.

4) PIPA, Chapter 6.

5) PIPA, Chapter 7.

telecommunications service providers as prescribed in Article 2(viii) of the Telecommunications Business Act, and (ii) other persons who provide information or act as an intermediary with respect to the provision of information for the purpose of earning profit utilizing the services rendered by telecommunications service providers."[6] The term "user" is defined as "an individual who uses the telecommunications services provided by OSPs."[7]

The most representative example of an OSP that is subject to the Network Act is a for-profit website or mobile app that collects and uses the personal data of users who sign up for membership. To the extent that there is a "relationship between the OSP and the users whereby the user uses the online services provided by the OSP,"[8] the Network Act's requirements for protecting personal data take precedence over the requirements of the PIPA.

In addition to Chapter 4 on the protection of personal data, the Network Act prescribes requirements for matter such as the sending of commercial messages (i.e., spam),[9] the protection of juveniles in an online setting, and the prevention of infringement of other individuals' rights.[10]

3) Other

Besides the PIPA and the Network Act, there are other laws that impose requirements concerning personal data protection. For example, the Use and Protection of Credit Information Act includes provisions on protecting credit information. The Act on Real Name Financial Transactions and Guarantee of Secrecy includes provisions on protecting information and materials relating to financial transactions, and the Electronic Financial Transactions Act includes provisions that protect information relating to electronic financial transactions. In particular, financial institutions must

---

6) Network Act, Art. 2(1)(3).

7) Network Act, Art. 2(1)(4).

8) The Korean Supreme Court has also reached a decision implying that, for data to be considered the personal data of a user protected under the Network Act, there must be a relationship between the user and the OSP whereby the user is provided with and uses the services of the OSP (Judgment of Oct. 17, 2013, 2012Do4387 (Supreme Court of Korea)).

9) Network Act, Art. 50 to 50-8.

10) Network Act, Chapter 5.

strictly comply with these laws in addition to the PIPA and the Network Act, as well as the requirements prescribed in their subordinate regulations.[11)]

2. Difference between the third-party provision of personal data and the delegation of personal data processing

For all transfers of personal data to third parties, the PIPA and the Network Act distinguish between the provision of personal data to a third party ("third-party provision") and the delegation of personal data processing ("delegation"), for which they impose different requirements and corresponding penalties.

However, the PIPA and the Network Act do not explicitly address the standards for distinguishing between a third-party provision and a delegation, and there have been numerous debates on the exact difference between the two concepts. In a recent decision, the Supreme Court explicitly addressed this issue by distinguishing the two as follows:[12)]

> [omitted] … The "third-party provision" of personal data under Article 17 of PIPA and Article 24-2 of the Network Act is referring to a transfer of personal data that goes beyond the scope of the original purpose for collecting and using personal data and is intended to further the third-party recipient's business purposes. The "delegation of personal data processing" under Article 26 of PIPA and Article 25 of the Network Act is referring to a transfer of personal data that is intended to further the delegator's own business purposes in relation to its original purpose for collecting and using the personal data. The delegatee entity of a delegation of personal data processing does not independently benefit from the processing of personal data other than receiving remuneration for providing the delegated services for the delegator entity, processes personal data pursuant to the supervision and management of the

11) For example, the Financial Services Commission has issued a notification entitled Regulation on the Outsourcing of Data Processing by Financial Institutions.

12) Judgment of April 7, 2017, 2016Do13263 (Supreme Court of Korea).

> transferor of personal data and only within the scope of the delegation, and does not constitute a "third party" under Article 17 of PIPA and Article 24-2 of the Network Act. A determination on whether a specific act constitutes the provision of personal data versus the delegation of personal data processing must be based on a consideration of a totality of factors such as the purpose and method of collecting the personal data, whether remuneration was provided, whether the delegatee was actually managed/supervised, the impact on the need to protect the personal data of data subjects or users, and which entity has a practical need to use the personal data at issue.

Specifically, the Supreme Court held that whether a transfer of personal data constitutes a third-party provision or a delegation will depend on whether the transfer is intended to further the business purposes of the transferee—in which case, the transfer will constitute a third-party provision—or the transferor—in which case, the transfer will constitute a delegation. This holding is interpreted as being consistent with earlier precedents and the position of regulatory agencies on this issue.

In practice, whether a data transfer constitutes a third-party provision versus a delegation will require a case-by-case analysis based on the guidance provided in the above Supreme Court case. However, the transfer of personal data for purposes such as delivering products, handling customer complaints, and engaging in telemarketing are considered representative examples of delegations of personal data processing.[13)]

13) See the Manual on Personal Information Protection Laws, Guidelines, and Notifications issued by the Ministry of the Interior (currently known as the Ministry of the Interior and Safety) in December 2016 (p. 182); see also the Manual on Personal Information Protection Laws for OSPs issued by the Korea Communications Commission in September 2012 (p. 46).

III. Key issues regarding the cross-border transfer of personal data

1. Definitions and requirements for cross-border transfers of personal data

1) The PIPA

While the PIPA explains that the "provision" of personal data includes the concept of "sharing,"[14] the PIPA does not include a separate provision for the meaning of "provision." However, Article 7, paragraph 1, of the Standard Guidelines on Personal Information Protection issued by the Ministry of the Interior and Safety ("MOIS")[15] explains that the provision of personal data includes "all conduct that brings about the transfer or joint use of personal data such as physically transferring a personal data storage device or printed materials, books, etc. containing personal data, transmitting personal data through a network, providing a third party with access rights to personal data, and a Personal Data Controller's sharing of personal data with a third party."

Respecting international data transfers, Article 17(3) of PIPA states, "[W]hen a Personal Data Controller provides personal data to a third party located overseas, the Personal Data Controller shall first inform the Data Subjects of any of the subparagraphs of paragraph (2), and obtain consent from them. The Personal Data Controller shall not enter into a contract for the cross-border transfer of personal data in violation of this Act." Article 17(2) further states the following:

> **Article 17 (Provision of Personal Data)** ② The Personal Data Controller shall inform Data Subjects of the following when it obtains consent under subparagraph 1 of paragraph (1). The same shall apply when any of the following is changed:
> 1. The name of the third party

14) PIPA, Art. 17(1).

15) As these "Standard Guidelines" were issued pursuant to Article 12(1) of the PIPA, it constitutes a "Notification" of the MOIS.

2. The third party's purpose of use of the personal data
3. The types of personal data to be provided
4. The third party's period of retention and use
5. The fact that the data subject has the right to refuse to give consent and the negative consequences or disadvantages that may result due to any such refusal

2) Network Act

Previously, the Network Act required OSPs wanting to transfer users' personal data overseas to obtain the users' consent without considering the type or purpose of the transfer (i.e., there was no exception to the consent requirement for overseas data transfers). However, the effectiveness of this requirement was questionable because the Network Act did not include provisions that imposed a penalty for failing to meet this consent requirement. In response, the National Assembly of Korea amended the provisions of the Network Act concerning overseas data transfers on March 22, 2016.

Because of the amendment, the current version of Article 63(2) of the Network Act imposes requirements depending on the type of overseas data transfer. Specifically, Article 63(2) states that the users' consent must be obtained to transfer their personal data overseas, and Article 63(3) comments that the following information must be disclosed to users prior to obtaining their consent:[16] (i) the types of data to be transferred overseas; (ii) the destination country; (iii) the date, time, and method of transmission; (iv) the name of the third party (if the third party is a legal entity, the name of the legal entity, and the contact information of the person in charge of personal data protection within that legal entity); and (v) the third party's purpose of use for the personal data and the period of retention and use.

Additionally, under the Network Act and its sub-regulations, if users' personal data are transferred overseas, OSPs must also take measures to protect personal data, including (i) technical and managerial measures to protect personal data; (ii) measures for processing complaints and dispute

16) Providing a user's personal data overseas without his/her consent can result in the imposition of an administrative surcharge of up to 3% of revenues related to the violation (Network Act; Art. 64-3(1)(8)).

resolutions for any infringement of personal data; and (iii) other measures necessary for the protection of personal data. All the foregoing items must also be reflected in an agreement between the OSP and the overseas entity.[17)]

2. Requirement to specify each third-party recipient

Overseas transfers to third parties can occur for a variety of reasons. For example, a multinational company's headquarters may request the provision of employees' personal data from the Korean subsidiary for the purpose of human resource management, and customer information can be shared among companies for joint marketing/promotional activities. While these types of data sharing can occur among a minority of entities, it is not uncommon for large multinational companies to engage in such types of data sharing on a regular basis.

However, the PIPA and the Network Act's requirement to obtain prior consent for the provision of personal data overseas after specifying the name of each recipient can pose a challenge for companies who are more familiar with the requirements of jurisdictions whose privacy regulations permit consent to be obtained on a categorical basis (e.g., obtain consent for business partners rather than each specific business partner). Moreover, as the PIPA and the Network Act do not recognize an exception or a separate set of requirements for data transfers among affiliate entities, the above consent requirement requires companies that wish to transfer personal data overseas to obtain consent after disclosing each recipient of personal data in all circumstances, which can be difficult on a practical level.

Another requirement under the PIPA and the Network Act that can be even more challenging to meet on a practical level is to obtain new consent every time there is a change to matters disclosed prior to obtaining the data subject or users' consent, including cases where a recipient of personal data is added.[18)] In practice, decisions to provide personal data (e.g., a decision to share customer information with a business partner) can occur even after obtaining the data subject/user's consent. However, because the PIPA and

17) Network Act, Art. 63(4); Enforcement Decree of the Network Act, Art. 67.

18) PIPA, Art. 17(2); Network Act, Art. 24-2(1).

the Network Act require consent to be obtained for a third-party provision after disclosing the name of each third-party recipient and prohibits providing personal data to additional third-party recipients without obtaining new consent, it can be difficult for companies to share personal data after obtaining the initial consent for a third-party provision.

It is unclear whether these types of requirements under the PIPA and the Network Act balance the need to protect personal data with the facilitation of the sharing of personal data or, going further, actually accomplish the statutes' stated purpose of protecting personal data. While a more flexible approach may be difficult under current requirements, one possible means to accommodate the practical realities of data sharing may be to permit companies to include a link to a reference that identifies all third-party recipients (e.g., a website that lists all affiliate entities that will be provided with personal data) instead of disclosing all third-party recipients on a consent form before obtaining consent.

From a long-term perspective, another possible means is for Korea to follow the approach taken in jurisdictions that permit the disclosure of third-party recipients on a categorical basis before obtaining the data subjects' consent.[19] While the current requirement to disclose all third-party recipients on an individual basis can be viewed as guaranteeing informed consent and preserving data subjects' right to know how their personal data are shared, listing the name of each third-party recipient may not be effective in accomplishing these aims. Rather, clearly identifying the types or categories of third parties that will receive the data subjects' personal data before obtaining their consent and providing more details to data subjects seeking additional information may be more effective and would be more likely to balance the respective needs of companies and data subjects.

19) For example, the EU's General Data Protection Regulation, which will be enforced on May 25, 2018, provides in Article 13 ("Information to Be Provided Where Personal Data Are Collected from the Data Subject") that it is sufficient to disclose "the recipients or categories of recipients of the personal data" in connection with the disclosure of personal data.

3. The provision of personal data pursuant to foreign laws or requests from foreign government authorities

There are instances where Korean companies receive requests for the submission of materials that include personal data pursuant to foreign laws or requests made by foreign government authorities (e.g., discovery requests from U.S. courts).

In such cases, while it is permissible to provide the requested materials after obtaining the data subject/user's consent for a third-party provision, it can be practically difficult for companies to obtain the requisite consent. There have been discussions on whether it is possible for companies to cite the PIPA and the Network Act's exception to the consent requirement for a third-party provision pursuant to "requirements under other laws."[20)]

However, the phrase "other laws" from the above exception is currently understood as referring to the laws of Korea, not foreign jurisdictions. Accordingly, if a Korean company submits personal data to foreign government authorities pursuant to foreign laws without the data subject/user's consent, there is a significant risk of the submission being deemed a violation of the PIPA and the Network Act, and the company may be subject to various penalties, including civil liability for damages incurred by the data subjects, under both laws.[21)]

Alternatively, in limited circumstances, a data transfer for which the data subject/user's consent was not obtained can nonetheless be considered valid if it is deemed a "justifiable act that is not against socially accepted norms" under Article 20 of the Korean Criminal Act.

More specifically, Article 20 of the Korean Criminal Act articulates the general principle that "justifiable acts not against socially accepted norms" should not be considered violations of law, and the Supreme Court has held that the following five factors must be met for an act to be deemed "justifiable": (i) the motive or purpose of the act is justifiable, (ii) the means/method of accomplishing the act is material to the underlying motive or purpose, (iii) there is a balance between the need for protection

---

20) PIPA art. 18(2)(2); Network Act Art. 24-2(1) and 22(2)(3).

21) PIPA, Art. 39(1); Network Act, Art. 32(1).

and the need for infringement (minimization of the violation), (iv) there is an urgency, and (v) there are no other means other than the act in question (subsidiarity).[22)]

In the context of a provision of personal data to a foreign government authority without the requisite consent, which would otherwise violate the PIPA and/or the Network Act, these five factors may be described as follows: (i) the provision provides the Personal Data Controller with a "justifiable benefit"; (ii) the provision is necessary to protect the justifiable benefit to the Personal Data Controller; (iii) the provision is conducted to minimize any violations of privacy or right to personal autonomy; (iv) there is an urgent need to provide the personal data, e.g., to avoid the destruction of evidence or to avoid the loss of time against an expiry period; and (v) there are no alternative means for transferring the personal data without consent.

If the above factors are met, it may be possible to argue that the provision of personal data to foreign government authorities is possible without the data subject/user's consent. However, in light of the growing social awareness of personal data-related issues and increasingly strict penalties under the PIPA and the Network Act, it is unclear whether such an argument will be accepted by Korean courts and regulators.

IV. Key issues concerning the overseas delegation of personal data processing[23)]

1. Definitions and requirements for the delegation of personal data processing

1) The PIPA

As the PIPA does not include separate requirements for the overseas

22) Judgment of Dec. 26, 2002, 2002Do5077 (Supreme Court of Korea), etc.

23) If a financial institution delegates the processing of personal data that includes an individual's financial transaction data overseas, it may need to comply not only with the regulations described in Section II.1.(3) of this article, but also with sector-specific laws specific to the financial sector, which may take precedence over the PIPA and the Network Act.

delegation of personal data processing, it is interpreted as permitting an overseas delegation of personal data if the following major requirements for a delegation under Article 26 are met[24]:

- Execution of a delegation document[25]: A delegation must be based on a document that addresses certain prescribed issues.[26] This requirement is typically met through a delegation agreement. However, other types of documents can also be used.
- Disclosure of the delegation status[27]: the (i) names of the delegatees and (ii) descriptions of the delegated services must be disclosed so data subjects can easily confirm them. The PIPA prescribes the specific method of disclosure,[28] and this requirement is typically met by disclosing the above information on the company's website.[29]
- Notification of delegation status[30]: if the marketing or promotion of goods or services is delegated, a notice including the (i) names of the delegatees and (ii) descriptions of the delegated tasks must be provided to the data subjects via letter, email, fax, telephone, text message, or similar means.

---

24) Article 2.2 of the PIPA broadly defines "processing" as including "collection, production, association, connection, recording, storing, possession, treating, editing, searching, output, correction, restoration, use, provision, disclosure, destruction, and other similar acts." Therefore, simply delegating the storage of personal data may constitute the "delegation of personal data processing," in addition to tasks such as personal data analysis.

25) PIPA, Art. 26(1).

26) The issues that must be addressed are: (i) the purpose and scope of the delegation; (ii) the limitations on the scope of delegation (e.g., the prohibition against processing personal data for any purpose other than the delegated purpose and the limitations on sub-delegation); (iii) technical and managerial protective measures; (iv) measures to ensure security such as access restrictions to personal data; (v) matters regarding supervision, such as check-ups of the current status of personal data management in connection with the delegation; and (vi) provisions for the compensation of damages in cases where the delegatee company breaches its duties. (PIPA Art. 26(1); Enforcement Decree of the PIPA Art. 28(1).)

27) PIPA, Art. 26(2).

28) PIPA, Art. 26(2); Enforcement Decree of the PIPA, Art. 28(2) and (3).

29) More specifically, a common approach is to disclose a privacy policy that includes information on the current status of delegation on the company's website.

30) PIPA, Art. 26(3); Enforcement Decree of the PIPA, Art. 28(4).

Notably, under the PIPA, the data subject's consent is not required for a delegation of personal data processing, even though the data subject's consent is required for a third-party provision.

2) Network Act

Under the Network Act, in principle, the data subject's consent is required for the overseas delegation of personal data processing and the overseas storage of personal data, similar to a third-party provision.

However, the data subject's consent is not required if the overseas delegation or storage is deemed necessary for the purpose of fulfilling the terms of an agreement regarding the provision of online services to users and improving their convenience, in which case, it is sufficient to disclose all of the information required under Article 63(3)[31] (i) in a privacy policy or (ii) via email, letter, fax, telephone, or similar means.[32]

In practice, there have been numerous debates on exactly which types of overseas delegations and/or storage would be "deemed necessary for the purpose of fulfilling the terms of an agreement on the provision of online services to users and improving their convenience" and be subject to the exception to the consent requirement, as discussed in the following section.

2. The Network Act's exception to the consent requirement

As noted above, Article 63(3) of the Network Act provides an exception to the consent requirement for an overseas delegation of personal data processing if the delegation is "deemed necessary for the purpose of fulfilling the terms of an agreement on the provision of online services to users and improving their convenience." This exception is often discussed in connection with cloud service providers, because the use of a cloud service provider to manage personal data involves transferring personal

31) Article 63(3) requires the disclosure of the following: (i) the types of information to be transferred overseas; (ii) the destination country; (iii) the date, time, and method of transmission; (iv) the name of the third party (if the third party is a legal entity, the name of the legal entity and the contact information of the person in charge of the personal information protected within that legal entity); and (v) the third party's purpose of use of the personal information and the period of retention and use.

32) Network Act, Art. 63(2).

data to the service provider's data centers, which are typically located overseas.[33)]

As for the meaning of the phrase "if deemed necessary for the purpose of fulfilling the terms of an agreement on the provision of online services to users and improving their convenience" under Article 63(3), to date, the Korea Communications Commission ("KCC"), which is the regulator tasked with enforcing the Network Act, has not expressed its views on the scope of this exception. In addition, there are no relevant precedents, although the wording of this exception is identical to the wording of the exception to the prior consent requirement for a domestic delegation.

In fact, Article 25 of the Network Act on the domestic delegation of personal data processing states that an OSP must notify users of (i) the name of the delegatee and (ii) the delegated task before obtaining their express consent unless the delegation is "deemed necessary for the purpose of fulfilling the terms of an agreement on the provision of online services to users and improving their convenience," in which case, it is sufficient to disclose certain information concerning the delegation through the privacy policy or notify users of that information via email or other such methods. However, it appears that the KCC is currently interpreting this exception very narrowly, as the KCC's guidelines on the Network Act explain that the exception under Article 25 applies in cases where the delegation is required for the OSP to fulfill its agreement with the user.[34)] Specifically, the guidelines state that the exception would apply to an online shopping mall operator's transfer of customer information to a logistics provider (for the purpose of delivering the goods ordered by the customer) and a call center that it operates (for the purpose of handling customer complaints and inquiries), while the exception would not apply where an OSP transfers customer information to a PR firm (for the purpose of arranging a

33) Recently, the issue of whether the use of a cloud service provider constitutes a delegation of personal data processing has been subject to debate. Those supporting the view that the use of a cloud service provider does not constitute a delegation of personal data processing argue that cloud service providers merely provide equipment (e.g., servers) for processing information without reviewing the information or confirming whether such information contains personal data.

34) See the *Manual on Personal Information Protection Laws for OSPs* issued by the Korea Communications Commission in September 2012 (p. 46–48).

promotional event or sweepstakes) and where a website operator transfers customer information to a service provider (for the purpose of providing online ads).[35]

From a company's perspective, the issue of whether consent must be obtained for a delegation of personal data processing is very important. Given the current uncertainties, it would be helpful for courts and the KCC to provide additional guidance about when the exception to the consent requirement applies to an overseas delegation of personal data processing. Thus, companies should closely analyze the interpretation of such guidance and regulatory enforcement trends.

On a more fundamental level, it would also be helpful to have public discussions on whether the Network Act should be amended so it does not require consent for the delegation of personal data processing, similar to the approach taken under the PIPA. As discussed above, the delegation of personal data processing occurs in the context of the transferor's original purposes for collecting and using personal data, for which the data subjects' consent must be separately obtained. Consequently, data subjects who consented to the transferor's collection and use of their personal data to further their original purposes are aware of, or can easily anticipate, how their personal data will be processed by delegatees, and disclosing certain details on the delegation should be sufficient for informing them about how their personal data are processed. In addition, respecting the collection and use of personal data for purposes that are not directly related to the execution of an agreement between the data subjects and the transferor, data subjects can decide whether they will consent to such a collection and use of their personal data. It may not be necessary to subsequently check whether they will consent to a related delegation of their personal data. Therefore, it may be more reasonable for the Network Act to permit a delegation of personal data processing without the data subjects' consent, while requiring the delegator to properly maintain and supervise the

35) Although the *Manual on Personal Information Protection Laws for OSPs* was issued when the exception did not include the phrase "and improving their convenience," which was subsequently added per an amendment to the Network Act, the Manual nonetheless appears to be applicable because the added language further narrowed the scope of the exception, and the KCC has not expressed a different view of its interpretation of the exception since the amendment.

delegatee's processing of personal data.

3. Requirement to take security measures to ensure the protection of personal data

Korean privacy laws prescribe specific security measures that companies must take to ensure the safe management of personal data. Information regarding such measures is provided in notifications issued by the MOIS and the KCC pursuant to the PIPA and the Network Act, respectively. For example, the KCC has issued *Guidelines for Technical and Administrative Measures for the Protection of Personal Information*, which includes provisions on the following[36]:

- Article 1 Purpose
- Article 2 Definition
- Article 3 Establishment and Enforcement of the Internal Management Plan
- Article 4 Access Control
- Article 5 Prevention of Fabrication or Alteration of the Access Record
- Article 6 Encryption of the Personal Information
- Article 7 Prevention of Malicious Programs
- Article 8 Prevention of Physical Access
- Article 9 Protective Measures When Printing and Copying
- Article 10 Protective Measures of Restrictively Indicating the Personal Information
- Article 11 Re-examination of Regulation

The failure to take the measures prescribed in these guidelines can, on its own, result in the imposition of administrative fines.[37] In addition, the loss or leakage of personal data caused by the failure to take these measures

36) Similarly, the MOIS has issued *Guidelines for Measures to Ensure Security of Personal Information* pursuant to PIPA, which includes similar requirements.

37) PIPA, Art. 75(2)(6); Network Act, Art. 76(1)(3).

can result in an administrative surcharge or criminal penalties.[38] Last, damage incurred by the data subjects can result in civil liability for damages.[39] As such, it is important for companies to comply with these measures to the greatest extent possible.

If the processing of personal data is delegated to a third party, the delegator may be held liable if the third party fails to take the above security measures.[40] Therefore, it is often the case that delegators require third-party delegatees to follow the above security measures. If the third-party delegatee is a foreign service provider that is not familiar with Korean privacy laws, it may be difficult for that service provider to comply with the detailed security requirements of the guidelines. To prevent this, it is advisable for a Korean company to inspect the foreign service provider's facilities and security measures prior to delegating the processing of personal data overseas.

Under the PIPA, once the personal data become unnecessary because the purpose of collecting the personal data has been fulfilled or the retention period has expired, the personal data must be permanently destroyed so they cannot be recovered or restored unless there is a statutory basis for further retaining the personal data.[41] The Network Act includes a similar requirement.[42] Therefore, a delegator should confirm that a delegatee has the technical means to permanently destroy personal information subject to the above destruction requirement.

---

38) PIPA, Art. 34-2(1) and 73.1; Network Act, Art. 64-3(1)(6) and 73.1.

39) PIPA, Art. 39(1); Network Act, Art. 32(1).

40) Article 26(6) of the PIPA comments, "[W]ith respect to damages that are incurred because the delegatee violates this law in the course of processing personal data in connection with the delegated task, the delegatee will be considered an employee of the Personal Data Controller." Article 25(5) of the Network Act includes similar language.

41) PIPA, Art. 21(1) and (2).

42) Network Act, Art. 29. Under the current version of the Network Act and pursuant to an amendment effective May 28, 2014, a violation of the destruction requirement under Article 29 can result in the imposition of a criminal penalty (i.e., imprisonment for up to two years or a criminal fine of up to KRW 20 million). The previous version of the Network Act, which was in place prior to the abovementioned amendment, imposed an administrative penalty for the same violation, and it is unclear whether imposing a criminal penalty for the sole reason that personal information (which was properly collected, used, and stored) was not destroyed pursuant to Article 29 is appropriate under the principles of subsidiarity and proportionality.

V. Recent international developments

1. Participation in the APEC CBPR System

In June 2017, Korea's application to join the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPRs) was accepted. The CBPRs is a global certification program for protecting personal data that was developed in 2011 as part of APEC's efforts to further electronic commerce and corresponding cross-border transfers of personal information. To date, other participating economies include the United States, Mexico, Japan, and Canada, and approximately 20 companies including Apple and IBM have obtained CBPR certification.[43)]

Korea is currently in the early stages of implementing the CBPR system, as its application for an Accountability Agent has not yet been filed. Once the CBPR system is fully implemented, with corresponding amendments being made to the PIPA and the Network Act, the requirements for international data transfers among CBPR-certified companies are expected to become less burdensome.

2. Efforts to obtain an adequacy decision pursuant to the GDPR

The EU's General Data Protection Regulation ("GDPR") is expected to become effective on May 28, 2018. The GDPR restricts the transfer of personal data from the EU to third countries that have not obtained an adequacy decision from the European Commission to cases where the transfer is made pursuant to mechanisms such as Commission-approved standard data protection clauses, Binding Corporate Rules, or specific authorization by the competent supervisory authority. In this regard, the Korean government is currently aiming to obtain an adequacy decision from the Commission pursuant to Article 45 of the GDPR, which would greatly assist Korean companies subject to the GDPR.

---

43) Joint Press Release issued on June 13, 2017, by the Related Agencies (*The MOI and the KCC Participate in APEC's Personal Information Protection Certification System*); for more detailed information on the CBPRs, please refer to the official website (http://www.cbprs.org).

VI. Conclusion

This article discussed Korea's privacy regime for protecting personal data and how the PIPA and the Network Act distinguish between data transfers that constitute a third-party provision versus a data transfer that constitutes a delegation of personal data processing. This article also explained that, although there are some differences in how overseas data transfers are regulated under the PIPA and the Network Act, both laws impose a consent requirement for a third-party provision, which can be challenging for companies to meet due to the need for disclosing each third-party recipient prior to obtaining consent. In addition, the lack of regulatory guidance on how to respond to requests for personal data from foreign government authorities pursuant to foreign laws also poses a challenge to companies receiving such requests. As for the overseas delegation of personal data processing, this article explained the requirements under the Network Act and the issues to consider when selecting a delegatee. Last, this article discussed recent international developments involving Korea and cross-border data transfers, which are expected to facilitate cross-border data transfers for CBPR-certified companies and companies subject to the GDPR.

As noted in the introduction, there is a need to ensure both the free flow of information across borders and the data subjects' rights concerning their personal data. As cross-border transfers of personal data become increasingly prevalent, it remains to be seen how these interests will be balanced under Korea's regulations as well as the regulations of foreign jurisdictions.