Journal of Korean Law | Vol. 17, 53-77, December 2017

Main Issues in Korea Regarding Consent for the Processing of Personal Information, with Emphasis on Recent Supreme Court Cases

Kwang Bae Park, Sunghee Chae, Jaeyoung Chang

Abstract

* Kwang Bae Park (partner and leader), Sunghee Chae (partner), and Jaeyoung Chang (associate) are attorneys working in the technology, media, and telecommunications (TMT) practice group at Lee & Ko.

I. Introduction

Under South Korean data protection laws, consent is accorded the highest status as a legitimizing ground for the processing of personal information. Therefore, determining the circumstances under which consent should be obtained, as well as the conditions and methods for obtaining consent, can be regarded as some of the most important issues under Korea's Personal Information Protection Act ("**PIPA**"). In relation to the foregoing, two influential Supreme Court decisions were rendered in 2016 and 2017, respectively. The purpose of this paper is to provide an overview of how the issues of consent are being resolved in Korea by focusing on the two influential Supreme Court decisions mentioned above.

II. Topic of discussion–Regulation of consent for the processing of personal information under Korean law

1. Concept and meaning of "consent"

Notwithstanding the significance of consent under Korean data protection laws, such laws do not actually define the concept of consent. This is in contrast to the EU's General Data Protection Regulation ("**GDPR**"), even though this definition is provided in the Recitals and not the main body of the statute, which stipulates that consent should be "a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data."[1)]

Instead, a guide to interpreting the PIPA, the general data protection law and the most important of Korean data protection laws, published by the Ministry of the Interior and Safety ("**MOIS**") based on the PIPA, provides that "it should be clearly evident that the data subject has

1) Recital 32 of the GDPR.

provided his/her voluntary consent to the data handler[2] for the collection and use of personal information" and that "the consent of the data subject under the PIPA means express consent."[3] In any event, although there is no provision under Korean law that expressly states the requirements for consent, there are provisions prescribing the methods for obtaining consent. For example, under Article 15.2 of the PIPA, prior to obtaining consent, data subjects must be notified of matters such as:

1. The purpose of the collection and use of personal information,
2. Items of personal information to be collected,
3. The period for retaining and using personal information, and
4. The fact that the data subject is entitled to refuse consent, as well as any disadvantages that the data subject will face in case he/she refuses to provide consent (Article 15.2 of the PIPA).

2. Consent to the collection of personal information

Article 15.1 of the PIPA provides the following legitimizing grounds for the collection of personal information:

1. If consent is obtained from the data subject;
2. If collection is specifically required or permissible under applicable laws or necessary to comply with the data handler's obligations under applicable law;
3. If collection is unavoidable for a public institution to perform its official duties pursuant to relevant laws;
4. If it is unavoidably necessary to execute and perform a contract with the data subject;
5. If there exists a clear and urgent need to protect the life, physical,

---

2) Under the PIPA, a "data handler" is defined as any person (including public agency, legal entity, organization, and natural person) who processes personal information to operate a personal information file for a business purpose on his/her own or through a third party (Article 2.5). This concept is quite similar to that of a data controller under the GDPR, with a few minor differences on which we do not elaborate further in this paper.

3) MOIS, "Comprehensive Guide to Data Protection Laws and Regulations," 2017, pp.71–72.

> or economic interest of the data subject or a third party, and the consent to the collection of personal information cannot be obtained in an ordinary manner because the data subject (or his/her legal guardian) cannot express his/her intent, his/her address is unknown; or
>
> 6. Where the collection is necessary to achieve the legitimate interest of the data handler where such interest clearly overrides the rights of the data subject, provided that the collection/use will be substantially relevant to the legitimate interest of the data handler, and that such collection/use is performed only to a reasonable extent.

Although the above provision appears to be similar to Article 6.1 of the GDPR,[4] in actuality, the status of consent as a legitimizing ground under Korean data protection laws is different from that under the GDPR. In Korea, consent is considered, in principle, to take precedence over other legitimizing grounds, rather than having equivalent status.[5]

In particular, the legitimizing grounds such as the above subparagraph 6 require that the legitimate interest of the data handler *clearly* overrides the

---

4) Article 6.1. Processing shall be lawful only if and to the extent that at least one of the following applies:

> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5) Young-Joon Kwon, *Thoughts on the Self-Determination Right to Personal Information and the Consent Regime*, 2015 Naver Privacy Whitepaper, p.89.

rights of the data subject and, thus, can be characterized as being much stricter than the equivalent requirement under Article 6.1.(f) of the GDPR[6] and are not invoked very often. Furthermore, Article 22.2 of the Act on the Promotion of Information and Communications Network Utilization and Information Protection, Etc. (the "**Network Act**"), which regulates information and communications service providers ("**ICSPs**") that process the personal information of users, expressly requires consent, in principal, for the collection of personal information, except in the following cases:

> 1. If it is seriously difficult to obtain consent from the data subject in an ordinary manner for an economic or technical reason, yet the collection/use of the personal information is necessary to perform a contract with the data subject concerning the provision of information and communications services;
> 2. If the collection/use is necessary for the settlement of payment regarding the provision of information and communications services to the data subject; or
> 3. If the collection/use is specifically required or permissible under the Network Act or any other applicable law or regulation.

Therefore, the consent of a data subject can be viewed as being the main legitimizing ground for the collection and use of personal information under Korean law. Thus, it is legally impermissible in many cases to collect and use personal information without consent unless personal information is collected from a source other than the data subject.[7]

3. Consent to the provision of personal information

One important characteristic of Korean data protection laws is that there is no singular legitimizing ground for all types of "processing" of personal information. Rather, Korean data protection laws require different legitimizing grounds for each type of processing, i.e., the "collection and

---

6) MOIS, op. cit., p.81 (Footnote 3)

7) In such cases, Article 20 of the PIPA applies, which only requires ex-post-facto notification of certain matters instead of the data subject's prior consent.

use," "provision," and, where applicable, even "outsourcing of the processing" of personal information. In other words, Korean data protection laws provide separate legitimizing grounds for each type of processing, whereas under Article 6 of the GDPR, a singular legitimizing ground exists for all types of processing.

For example, under the PIPA, a private company's provision of personal information to a third party is only permissible under the following circumstances:

> 1. If consent is obtained from the data subject;
> 2. If the provision is specifically required under other applicable laws and regulations, or necessary to comply with the data handler's obligations under other applicable laws and regulations; or
> 3. If there exists a clear and urgent need to protect the life, physical, or economic interest of the data subject or a third party, and the consent to the provision of personal information cannot be obtained in an ordinary manner because the data subject (or his/her legal guardian) cannot express his/her intent, or his/her address is unknown.

These are quite distinctive legitimizing grounds from those we have reviewed in relation to the collection and use of personal information in Section 2.(2), above. In addition, similar restrictions in cases where the Network Act is applicable. In practice, the above exceptions to the consent requirement under Korean data protection laws are only recognized in certain limited circumstances.

4. Sub-conclusion

Accordingly, consent holds a key position among legitimizing grounds for the processing of personal information under Korean law. Therefore, determining what is required for consent to be legitimate and valid becomes a critical issue. For example, an important question is how to treat consent that has been obtained in accordance with formalities prescribed by law but from which it is difficult to conclude that the data subject has genuinely expressed his/her actual consent. Is this consent valid? A different question involves a situation in which the data processing at issue is conducted without any express consent or any other legitimizing grounds under the relevant laws, but it would be quite unfair if such processing is deemed illegal. Meanwhile, as discussed above, because the legitimizing grounds for processing will be recognized in only certain limited circumstances, consent will need to be obtained in the majority of cases to process personal information. However, it may be unreasonable to regard all processing of personal information that lacks consent, even in cases where obtaining consent is not recommendable or even impossible, as being illegal. The following Supreme Court decisions address this issue in further detail.

III. Database Information Case (Supreme Court Decision in Case No. 2014Da235080 rendered on August 17, 2016) — Whether consent needs to be obtained for the collection and provision of publicly available personal information

1. Background

The plaintiff, a professor at a law school, claimed KRW 3 million (approx. USD 2,700) in damages against the defendant, a legal information service firm that operated a database of legal professionals, for collecting personal information without his consent, including his date of birth, occupation, job title, educational background, and photographs (collectively, the "**Subject Information**") from his law school's website and for disclosing the Subject Information to the defendant's users in exchange for a fee.[8] The act of providing the Subject Information was partially conducted prior to September 30, 2011, when the PIPA first entered into force, while the remaining Subject Information was provided thereafter.

8) Originally, the plaintiff also claimed damages against both domestic and global search engines for their widespread dissemination of the Subject Information received from the defendant. This claim was dismissed by the court of first instance, and the plaintiff did not appeal this decision thereafter.

The decisions rendered by the first and second instance courts ordered the defendant to pay compensation to the plaintiff on the grounds that it was illegal to provide personal information to third parties for profit without obtaining the consent of the data subject, regardless of whether such provisions occurred prior to or after the PIPA took effect. However, the Supreme Court reversed the lower court decisions and dismissed the plaintiff's claim.

This case addressed the issue of whether consent was legally necessary for the collection and provision of publicly available personal information. Specifically, after the PIPA took effect, the aforementioned legitimizing grounds under Article 17 for the provision of personal information became applicable. As such, the provision of the Subject Information in this case without obtaining consent from the data subject would be a violation of Article 17.1 based on a strict interpretation of the text.

2. Rationale for Decision rendered by the Court of First Instance (Seoul Central District Court Decision in Case No. 2013Na49885 rendered on November 4, 2014)

1) Before the PIPA took effect

Before the PIPA entered into force, there were no applicable legal provisions for the provision of personal information such as those prescribed in articles 15.1 and 17.1 of the PIPA. As such, it was necessary to determine whether the defendant's collection and use of personal information constituted a tortious act under Article 750 of the Civil Code.

In this connection, the decision rendered by the court of first instance found that, because the data subject was entitled to the right to informational self-determination, the acts of collecting and providing the Subject Information to third parties without consent prior to when the PIPA took effect constituted tortious acts under the Civil Code, in the absence of exceptional circumstances, as long as they were conducted for the purpose of obtaining a profit.

Specifically, the court of first instance reasoned that using personal information for a commercial purpose without obtaining the consent of data subjects represented an archetypal example of the misuse/abuse of personal information and, furthermore, infringed upon the proprietary interest of such data subjects. As such, even though the Subject Information was publicly available, this does not necessarily lead to the conclusion that: i) the data subject had consented to the use of the Subject Information for the purpose of obtaining a profit, and ii) that there was a legitimate interest of the data handler that took precedence over those of the data subject when collecting and providing the Subject Information to third parties for the purpose of obtaining a profit. Notably, the court viewed personal information as having proprietary characteristics, as well as being a subject of moral right, by regarding the profit motive associated with the provision of personal information as an important factor for consideration.

2) After the PIPA took effect

After the PIPA entered into force, it was necessary to determine whether the defendant's collection and provision of Subject Information to third parties was compliant with articles 15.1 and 17.1 of the PIPA. Regarding this connection, the decision rendered by the court of first instance found that the defendant failed to meet the requirements for the provision of personal information to third parties and that the defendant provided the Subject Information illegally because it was difficult to conclude that the plaintiff implicitly agreed to such provision for the purpose of obtaining a profit. Once again, the profit motive associated with the provision of personal information was regarded as an important issue for consideration.

3. Supreme Court's Decision

1) Whether the existence of the profit motive affected the determination of illegality regarding the collection and provision of the Subject Information

The Supreme Court found that the existence of the profit motive emphasized by the court of first instance was not a decisive factor in determining the illegality of the provision of personal information. Specifically, although the Supreme Court did not deny the right to informational self-determination of personal information, it found that the extent to which this right should be protected must be decided after weighing other competing legitimate interests and that the profit motive was but one of many such competing legitimate interests.

2) Whether the data subject consented to the defendant's act of collecting and providing Subject Information

The Supreme Court determined that the data subject provided consent because the Subject Information had already been disclosed on public websites, including the website of the law school where the plaintiff worked.

First, the Supreme Court reasoned that if there was no express consent by the data subject, the totality of the circumstances needed to be considered to ascertain whether the data subject's consent had actually been provided. Specifically, the Supreme Court stated that certain circumstances should be considered, such as:

> Whether the acts falls under the scope of consent that was given by the data subject should be judged in an objective manner by examining the nature of the disclosed personal information, the form and scope of the disclosure, the inferred intention or purpose of the data subject's disclosure, the form of information processing such as the data subject's provision of personal information, whether the scope of the disclosure changed due to the provision of information, and whether the provision of the information has considerable relevance with the original purpose of the disclosure.

Notably, the Supreme Court also considered whether the interest gained by the defendant through processing the Subject Information outweighed the legitimate interests of the data subject as an important consideration. Specifically, the Supreme Court stated that there should be a consideration of the following:

> [T]he status of the plaintiff as a public figure, the public nature and public interest of publicly disclosed information, the purpose or intention of the plaintiff to publicly disclose such information, the nature and value of the publicly disclosed personal information and the socio-economic need to use such information, the amount of interest gained by the defendant through the processing of the information, and degree of concern that the interest of the plaintiff could be infringed.

In summary, the Supreme Court found that the defendant did not process the Subject Information against the explicit wishes of the plaintiff and further concluded that the defendant collected and provided the Subject Information with the consent of the data subject. Specifically, the Supreme Court held that, when viewed objectively, there was consent by the plaintiff for the defendant's collection and provision of the Subject Information when considering…

> …the nature of the information already disclosed to the public, the methods and scope of disclosure, the inferred intent or purpose of disclosure by the plaintiff, the fact that the Subject Information, which had been provided by the defendant to third-parties through its website, is not different from the personal information, which had been disclosed by the Plaintiff, the purpose of the provision of the Subject Information by the defendant was to provide job-related information of the plaintiff, which is closely related with the plaintiff's original intent of disclosure, and that the acts conducted by the defendant did not alter the perception of the plaintiff regarding his personal information.

Therefore, the plaintiff's consent can be inferred for the acts conducted by the defendant prior to when the PIPA took effect and, thus, were not unlawful. In addition, the acts committed by the defendant after the PIPA took effect did not violate articles 15 and 17 of the PIPA, which require the consent of the data subject in connection with the collection and provision of personal information.

4. Assessment

As discussed earlier, the Supreme Court determined the illegality of the information processing by weighing the respective interests of the data subject and the data handler after taking into account the totality of the circumstances. This approach was applied regardless of whether the information processing occurred prior to or after the PIPA took effect. Specifically, the Supreme Court considered circumstances such as the nature (the plaintiff's status as a public figure, the public nature, and the public interest of the disclosed information) of the personal information already disclosed by the data subject, the inferred purpose and intent of the plaintiff from the methods and scope of disclosure (publicly available to anyone on the internet home page), the socioeconomic need for the data handler and the general public to use such information, the amount of interest gained by the defendant through processing, and the infringement of the plaintiff's interest due to the processing.

This decision appears to be valid in terms of its conclusion. Particularly regarding the collection and provision of Subject Information that occurred prior to when the PIPA took effect, the approach of weighing competing legitimate interests based on specific circumstances appears to be valid because the decision concerns the determination of whether a tortious act under the Civil Code can be recognized rather than violations of specific provisions of the PIPA. This is because in Korea, the constitutional basis for the protection of personal information is the right to informational self-determination, which is treated as a "moral right" encompassing all rights to moral interests under the Civil Code, excluding proprietary interests, while the methodology for determining the infringement of moral rights is based on the weighing of competing interests in each specific circumstance.[9)]

However, we would like to raise questions regarding the soundness of this decision for the collection and provision of Subject Information that occurred after the PIPA took effect. As mentioned previously, Article 15.2 of the PIPA requires data handlers to notify data subjects of the following matters when obtaining consent for the collection of personal information under Article 15.1:

> 1. The purpose of the collection and use of personal information;
> 2. Items of personal information to be collected;
> 3. The period for retaining and using personal information; and
> 4. The fact that the data subject is entitled to refuse consent and any disadvantages that the data subject will face in case he/she refuses to provide consent.

9) Supreme Court, 2008Da42430, September 2, 2011; Sunghee Chae, *The Concept of the Right to Informational Self-Determination,* Vol.20, No.3, J. Korean Information L., pp.301~302 (2016).

Likewise, under Article 17.2. of the PIPA, when providing personal information, data handlers are required to notify data subjects of matters such as:

1. The recipients to whom the personal information will be provided;
2. The recipients' purpose for using the personal information;
3. The items of personal information to be provided; and
4. The periods of use/retention for the personal information.

However, once again, there is no evidence in the case record to suggest that the defendant provided such notice to the plaintiff.

Additionally, Article 17.1 of the Enforcement Decree of the PIPA provides that consent shall be obtained by any of the following methods:

1. To provide a consent form stating the matters requiring consent, either directly, by mail, or by facsimile, to the data subject, and obtain the data subject's written consent thereto via his/her signature or seal;
2. To inform the data subject of the matters requiring consent, and confirm his/her intent of consent by telephone;
3. To inform the data subject of the matters requiring consent by telephone, have the data subject confirm such information posted on the designated website, etc., and contact the data subject again by telephone to confirm his/her consent to the information posted thereon;
4. To post the matters requiring consent on the designated website, etc., and have the data subject express his/her consent to it;
5. To send an electronic mail to the data subject containing the matters requiring his/her consent, and receive a return e-mail containing his/her consent thereto; and
6. Other methods to inform the data subject of the matters requiring consent by a method similar to those referred to in subparagraphs 1 through 5, and to confirm his/her consent thereto."

In summary, the consent required under the PIPA pertains to the data subject's explicit consent that has been obtained through methods prescribed thereunder. In this regard, even though the defendant's acts of collecting and providing the Subject Information might have been conducted within the scope of what the plaintiff would have consented to, it may be argued that there was no consent of the kind specified in articles 15 and 17 of the PIPA.

Nonetheless, the Supreme Court held that valid consent existed in this case. This appears to be partially in line with the stance of the MOIS, the relevant regulator.[10] Apart from the practical adequacy of the conclusion reached by the Supreme Court, we believe that this decision contradicts the express language of the aforementioned provisions of the PIPA. It seems that there was no explicit consent, as required under the PIPA, but only implied consent as determined by the Supreme Court after reviewing the circumstances of the case. Could we, nevertheless, still recognize the existence of valid consent in this case, at least from the perspective of the PIPA? Maybe not.

In this regard and in our opinion, the legitimizing grounds for the defendant's collection of the Subject Information in this case should have been, instead of consent, the legitimate interests of the defendant, i.e., "where the collection is necessary to achieve a legitimate interest of the data handler where such interest clearly overrides the rights of the data subject; provided that the collection/use will be substantially relevant to the legitimate interest of the data handler, and that such collection/use is performed only to a reasonable extent," as set forth in Article 15.1(vi) of the PIPA.

However, this inevitably raises an unresolvable problem, which is that there is no way to legitimize the provision of personal information to third parties in this case. Unlike Article 15.1, Article 17.1 of the PIPA does not provide the "legitimate interest of data handler" as a legitimizing ground

---

10) Standard Guidance for the Protection of Personal Information, officially announced by the Ministry of Public Administration and Security, art. 6.4 states as follows: "Where a data handler collects any personal information through publicly disclosed media or online addresses (hereinafter, "internet websites") such as internet homepages, such data handler may only use the personal information within the scope of consent expressly indicated by the data subject or within the scope of consent that is imputable based on socially accepted norms after considering the contents existing on the relevant internet homepage."

for the provision of personal information. Thus, under current laws, it seems almost impossible to avoid the conclusion that there was neither valid consent nor any other legitimizing ground under the applicable provisions of the PIPA in connection with the provision/disclosure of personal information. This conclusion—that the provision of personal information in this case is illegal—may seem unreasonable. We believe this is why the Supreme Court chose to rely on "consent" as a legitimizing ground for the defendants' acts despite the questionable rationale of this approach.

We believe that one of the ways to avoid this discrepancy is to argue that the current provisions of the PIPA, which do not give legitimizing grounds for the providing of personal information such as Article 15.1(vi), may be unconstitutional because they unduly restrict the data handler's right to choose an occupation (i.e., freedom of commerce), a fundamental right under Korea's Constitution, in relation to data processing. Eventually, legislative amendments may need to be introduced that permit the provision of personal information in cases where a legitimate interest exists instead of giving separate legitimizing grounds for the collection and provision of personal information, respectively.

IV. Homeplus Case (Supreme Court Decision in Case No. 2016Do13263 rendered on April 7, 2017)—Regarding consent that satisfies formalities prescribed by law but which may not actually constitute informed consent

1. Background

The database information case discussed above recognized the existence of consent even though such consent did not satisfy formalities prescribed by law. In this case, the issue was the other way around. What was at stake in this case was whether there was a violation of the PIPA even though a consent that satisfied formalities prescribed by law had been obtained.

Because this is a criminal case and the factual background is quite detailed, we intend to focus only on the following aspects for the purpose of this paper:

Homeplus is a retailer that operates large discount stores in Korea. Homeplus entered into business partnership contracts with insurance companies whereby Homeplus would sell items of personal information obtained through promotional giveaway events to such insurance companies for KRW 1,980 per item. Thereafter, Homeplus conducted promotional giveaway events on 11 separate occasions from December 2011 until June 2014. Through these events, Homeplus collected a total of around 7.12 million items of personal information (e.g., name, date of birth or resident registration number,[11] cell phone number, number of children, whether living in the same household as parents, etc., that will collectively be known as the "**Subject Information**") after obtaining consent to the provision of such personal information to third parties. Homeplus sold about 6 million items of the Subject Information to insurance companies and received about KRW 11.9 billion in payments.

The following coupon was used in the above giveaway events.

11) A national identifier assigned to each Korean citizen pursuant to the Resident Registration Act. For your reference, resident registration numbers are widely used in Korea as a means for identity authentication and as a result, the processing of resident registration numbers is strictly regulated.

This coupon was comprised of a notice informing customers that Homeplus would be offering free gifts (the large rectangular boxes in the top section that contain Korean letters in bold type on the left side and pictures of prizes such as cars on the right side); blocks in the middle section for filling in the Subject Information, and the consents to the collection of the Subject Information and to the provision of the Subject Information to third parties in the bottom section. The texts within the two bold rectangles in black merely state, "to verify each participant's identity in the event a gift is awarded" and "to contact winning participants by mobile phone in the event a gift is awarded," respectively, as the reasons why the collection of the Subject Information is necessary. There is no mention of the business partnership between Homeplus and the insurance companies in this section. However, the following information is provided in the section that is highlighted within the grey oval, adjacent to the small box where participants are asked to indicate their consent to the provision of the Subject Information to third parties (highlighted in yellow) in a 1-mm font size.

> [Consent to the collection, outsourcing of the processing, and use of personal information] "The purpose of collection and use" is to draw prizes and deliver them to participants, to supply information for insurance marketing, introduce products of Homeplus partners, provide information on such partners, etc.
> [Consent to the Provision of personal information to third parties] "The recipients of personal information" was specified as insurance companies (the actual company names were indicated therein) and "the purpose of using personal information" as "to use as marketing materials for telemarketing of insurance products, etc."

In short, although there was notice that personal information would be provided to insurance companies in the coupon, such notice was not easily noticeable and there was no mention that this personal information was being sold to the insurance companies. The coupon places emphasis on highlighting the details of the promotional giveaway rather than the provision of personal information to the insurance companies.

These facts brought into question whether PIPA's Article 72.2 would be applicable. It stipulates: "any person who acquires personal information or obtains consent to the processing of personal information by fraud or other unlawful means, and any person who knowingly receives such personal information for a profit-seeking or unlawful purpose." Any violation of the foregoing provision would be subject to imprisonment of up to three years or a fine of up to KRW 30 million.

2. First Instance Court's Decision

The decision rendered by the court of first instance (Seoul Central District Court 2015Godan510) and affirmed by the court of second instance (Seoul Central District Court in Case No. 2016No223 rendered on August 12, 2016) found that Homeplus was not guilty based on the above information.

According to the first instance court's decision, Homeplus could not be deemed a "person who acquires personal information or obtains consent to the processing of personal information by fraud or other unlawful means" because it provided notice of all legally prescribed matters (articles 15.2 and 17.2 of the PIPA) in its coupon, including the fact that it would be providing the Subject Information to insurance companies and the purposes for such provision (for use as marketing material by the insurance companies) when obtaining consent for the collection and use of personal information. Moreover, Homeplus was under no obligation to disclose that it would be paid for providing the Subject Information to third parties, and such disclosure was not a key factor in influencing a participant's decision to give his/her consent.

Notably, regarding the fact that Homeplus specified matters related to the provision of the Subject Information to third parties in a 1-mm font size,[12] the first-instance court determined the following:

> [A] font size of 1mm is widely used in lottery tickets, instructions for medicines, and for other applications and this font size appears to have been readable for participants of the promotional giveaway

12) This part of the judgment caused much controversy in Korean society. See the newspaper article at: http://www.ytn.co.kr/_ln/0103_201608122211425507, etc.

> event, and when considering that Homeplus provided an enlarged photo of the coupon beside the coupon submission box, it is difficult to conclude that Homeplus deliberately reduced the font size in order to render the contents unreadable, and that it was reasonable to assume that participants willingly provided consent while fully recognizing the fact that their personal information could be provided to insurance companies for marketing purposes.

In other words, because Homeplus generally satisfied the formalities prescribed by law when obtaining consent for the collection and use of personal information, it did not "acquire personal information or obtain consent to the processing of personal information by fraud or other unlawful means," irrespective of the readability of the consent matters.

3. Supreme Court's Decision

The Supreme Court overturned the lower courts' decisions as below.

1) Criteria for its decision

Regarding the test for determining the existence of "fraud or other unlawful means," the Supreme Court stated:

> [T]he data handler's act of obtaining the consent at question should not be viewed in isolation but the entire process for obtaining such consent should be examined and a determination should be made based on socially accepted norms after considering the motives and purposes for collecting personal information, the relevance between the purpose for collection and the personal information that is to be collected, specific methods used for collection, compliance with the PIPA and other relevant laws and regulations, the contents and volume of the obtained personal information, and whether any sensitive information or particular identification information was also collected.

2) Application of criteria

Based on the foregoing criteria, the Supreme Court found that

Homeplus had "acquired personal information or obtained consent to the processing of personal information by fraud or other unlawful means" because it misled customers into believing they were participating in a promotional giveaway and collected personal information that was unrelated to the event and provided it to third parties. In addition, customers would have had difficulty clearly understanding the contents of the consent considering the small font size of the text within the coupon and when considering the volume of personal information collected by Homeplus and the profits it earned by selling the personal information to third parties. Respecting the small font size (i.e., 1 mm) of the text in the coupon, in contrast to the first instance court's decision, the Supreme Court commented:

> [C]ustomers could not easily read the information in the coupon relating to consent because the font size of the text was about 1mm and because it must have been difficult for any customers who actually participated in the event to fully comprehend the contents therein[; thus,] the data handler violated its obligation under the PIPA to provide separate notice for each consent matter so that data subjects can clearly understand such matters when providing their consent thereto.

4. Assessment and Comparison with Similar Cases

This Supreme Court decision is expected to widely influence the actual processing of personal information in Korea going forward. Because of this decision, a clear precedent was established enabling the punishment of any data handlers who utilized personal information collected under circumstances in which it was difficult for data subjects to clearly understand what they had consented to, even if the consent they had provided satisfied formalities prescribed by law.

In this connection, there are lingering questions regarding whether the consent obtained by Homeplus can be deemed null and void because it was not informed consent and whether it could have been punished for violating Article 17.1 of the PIPA, which requires data handlers to provide personal information only with the consent of data subjects.

This question is important because the provision of personal information without consent is punishable by imprisonment of up to five years or a fine of up to KRW 50 million, which is more serious than the maximum three years or KRW 30 million prescribed for acquiring personal information or obtaining consent to the processing of personal information by fraud or other unlawful means.

However, as discussed previously, although the PIPA prescribes the specific matters and methods of notification as precedents for obtaining consent, it does not expressly provide that only genuine informed consent might legitimize the processing of personal information. As such, it remained possible for consent to be deemed valid as long as the formalities prescribed by law were satisfied, even though the text of the notice was in a font size as small as 1mm, it may have been practically difficult for data subjects to understand the information in the notice, or it was difficult for data subjects to know the exact scope of the consent they were providing when reading the information on the form. In other words, as long as the consent satisfied the formalities prescribed by law, the PIPA and other Korean laws did not explicitly address whether the validity of such consent could be questioned in cases in which such consent may not constitute informed consent.

Meanwhile, in another case, an ICSP, as defined under the Network Act, conducted a promotional giveaway and provided the personal information it had collected to insurance companies and other third parties after obtaining consent from participants online. The Supreme Court found that the ICSP failed to obtain consent for the provision of personal information as required under the Network Act (Supreme Court Decision in Case No. 2014Du2638 rendered on June 28, 2016). The notification of matters related to consent was provided on the bottom of the screen below the section where users were asked to indicate their intent to participate in the event. Furthermore, the actual box users could check to indicate their consent to the collection of personal information appeared in a separate pop-up window. The Supreme Court decided that the consent obtained by the ICSP was null and void because it violated Article 17.1 of the PIPA, remarking:

> [W]hen considering the language, framework, and purpose of relevant legal provisions [on the methods for obtaining consent and

> the matters that must be notified when obtaining consent], an ICSP should provide prior notice of all matters prescribed by law on its website in a manner that is clearly noticeable by regular users of the website so that they may easily understand specific contents therein in order for such ICSP to be deemed to have duly obtained consent from its users for the collection and provision of personal information under the Network Act. Additionally, the sections describing the notification matters for consent and the checkbox where users can actually indicate their consent should be placed in close proximity to one another so that users may be fully aware of the notification matters when deciding whether to consent to the collection and provision of personal information. Finally, consent methods should be provided which allow users to clearly recognize that they are providing their consent to the collection and provision of their personal information.

In light of the foregoing decision, it may be possible to argue that consent should be deemed null and void in cases where there was no genuine informed consent, even though such consent satisfied formalities prescribed by law.

5. Aftermath of this case

This Supreme Court decision had far-reaching social repercussions in Korea, as proposed amendments to the PIPA were submitted before the National Assembly shortly thereafter that aimed to prohibit the provision of personal information to third parties for the purpose of obtaining profit. Although none of the above amendment proposals have yet to pass the National Assembly, certain provisions of the PIPA relating to the methods for obtaining consent were amended recently.

Specifically, Article 22.2 of the PIPA was amended [effective October 19, 2017] and now stipulates that "where a data handler . . . obtains consent through writing [including through 'electronic documents' as defined under the Framework Act on Electronic Documents and Transactions], the data handler shall clearly indicate the purpose for collecting/using personal information, the items of personal information to be collected/

used and other important matters prescribed by Enforcement Decree in accordance with methods prescribed by Enforcement Rule so that such information can be easily noticeable." Accordingly, related amendments to the Enforcement Decree and Enforcement Rule of the PIPA, which both entered into effect on the same day as the effective date of the above amendment to the PIPA, now provide that the following information should be clearly indicated, among others, through the use of colored letters, bold letters, or different sized fonts:

> 1. The fact that the personal information of data subjects may be used for promoting goods or services, soliciting the purchase of goods or services, and any other related purpose, and that data subjects may be contacted directly as a result;
> 2. Any of the following categories of personal information;
> a. Sensitive information as defined under Article 23(1) of the Act; or
> b. A passport number, driver's license number, or alien registration number as defined under Articles 19(2)~(4) of the Enforcement Decree;
> 3. Information on the recipient(s) of personal information and the purpose for receiving personal information;
> 4. The periods of retention/use of personal information.
> The above amendments were widely criticized for being overly formalistic, and their actual scope of application has yet to be clearly established in terms of the relationship between the PIPA and the Network Act. As such, it may be necessary to monitor how these provisions are actually enforced in practice and whether any related changes to the Enforcement Decree and Enforcement Rule of the PIPA occur in the future.

V. Conclusion

We have reviewed two recent Supreme Court decisions addressing the concept of consent under the PIPA in the previous sections. The two decisions appear to contradict one another in certain aspects but also appear to share certain similarities. Specifically, in our view, the two decisions do not rely solely upon a formalistic approach (i.e., whether legal formalities prescribed by Korean data protection laws have been satisfied) when determining whether the consent at issue is valid. The Database Information Case found that the processing of data at issue was lawful despite the fact that the consent obtained failed to meet the requirements for valid consent. Conversely, the Homeplus Case found that the processing of data at issue was unlawful despite the fact that the consent obtained met the requirements for valid consent. In each case, the Supreme Court tried to devise a conclusion that appears fair and appropriate for each specific situation after considering various factors and weighing the respective positions of the data handler and data subjects and their competing legitimate interests.

However, as evidenced in the foregoing cases, current legal provisions are inadequate to provide a clear and coherent set of rules to determine the validity of consent. Hence, we have doubts about the desirability of the current situation. In other words, if the requirements for valid consent have been legally prescribed, they should not be easily ignorable when subsequently interpreting the law. Conversely, if the requirements for valid consent have been met, then the consent obtained in such cases, in addition to the lawfulness of the processing of data pursuant thereto, should be presumed to be valid. Yet, as the contrasting decisions rendered by the Supreme Court in the Database Information Case and Homeplus Case seemingly illustrate, current legal provisions regarding consent are inadequate to effectively adjudicate disputes and appear to require further adjustment through interpretation. In our view, this inadequacy results from the fact that the practical usefulness of consent provisions in the PIPA are undermined by their excessive rigidity. Therefore, serious debate must take place regarding the possible amendment of such provisions.

In any case, regardless of the aforementioned legislative approach, when considering the importance placed on consent under Korean data protection laws as a legitimizing ground for the processing of personal information, these recent Supreme Court decisions are expected to significantly influence the processing of personal information in the future, both in theory and in practice. As such, we believe it will be noteworthy to monitor both theoretical and practical changes surrounding the processing of personal information and any relevant court decisions going forward.

References

Sunghee Chae, *The Concept of the Right to Informational Self-Determination,* Vol.20, No.3, J. Korean Information L., pp.301~302 (2016).

Young-Joon Kwon, *Thoughts on the Self-Determination Right to Personal Information and the Consent Regime*, 2015 Naver Privacy Whitepaper, p.89.

Ministry of the Interior and Safety, Comprehensive Guide to Data Protection Laws and Regulations, 2017.

YTN News Article (in Korean), *Homeplus, Found Not Guilty on Appeal for Providing Notice in 1mm Size Letters* (August 12, 2016), http://www.ytn.co.kr/_ln/0103_201608122211425507