

# *Can Korea's Highly 'Consent-Oriented Approach' Survive the 4th Industrial Revolution Era?*

*Kwang Bae Park*



# Can Korea's Highly "Consent-Oriented Approach" Survive the 4<sup>th</sup> Industrial Revolution Era?

KWANG BAE PARK<sup>1</sup>

## I. INTRODUCTION

Korea is generally known to have one of the strictest data protection regulatory regimes in the world for its complicated regulations and active enforcement by regulators, even after the European Union's General Data Protection Regulation ("GDPR") has become effective on May 25, 2018. Especially, the requirement for obtaining the consent of the data subject in various stages of processing the personal information ("**Consent-Oriented Approach**") is one of the most distinctive features demonstrating the complexity of Korea's data protection laws and regulations.

The Consent-Oriented Approach is established by various Acts in Korea, including the Act on Promotion of Information Communication Network Usage and Information Protection ("**Network Act**"), the first data protection and privacy law in Korea concerning the private sectors relating to, in particular, the private sectors' communications and online services. Since its enactment in 2001, the Network Act has been amended more than 20 times and gradually expanded its scope to cover the processing of personal information "offline" (e.g., processing of personal information by department stores and travel agencies). A decade later, Korea enacted the Personal Information Protection Act ("**PIPA**") in 2011, which then started to govern the processing of personal information offline, instead of the Network Act. In fact, the PIPA regulates all aspects of personal information processing by private and public sectors, requiring the data subjects' consent in various stages of processing personal information from the collection and use of personal information to the destruction of personal information by the data handler ("**Data Controller**").<sup>2</sup>

In addition, there are several other sector-specific laws regulating the processing of personal information in Korea, which generally take precedence over the PIPA. For example, the Act on the Use and Protection of Credit Information ("**Credit Information Act**") applies to the activities in the financial sector, while the Medical Service Act and the Protection and Use of Location Information ("**Location Information Act**") applies to the medical sector and location information industry sector, respectively. In this respect, the Network Act is also a sector-specific law, which applies to businesses in the communications, broadcasting and online sectors.

---

<sup>1</sup> Partner, Lee & Ko, South Korea

<sup>2</sup> Under the PIPA, the data handler refers to a public agency, corporation, organisation, or individual that processes personal information on its own or through a third party in order to operate a personal information file for business purposes. In most cases, a data handler corresponds to a data controller under the EU Data Protection Directive 95/46/EC or the GDPR, and the relationship between the data controller and the data processor are similar under EU and Korean data protection laws."

Each sector-specific law provides its own consent requirements with respect to the processing of personal information. While some of the consent requirements set forth in the sector specific laws overlap with those provided in the PIPA, there are many additional requirements for the consent stipulated in each sector-specific law, which makes it further complicated for the businesses to comply with Korea's personal information protection laws.

This paper will provide the background of Korea's implementation of the Consent-Oriented Approach, complexity of the consent requirements under Korean laws, and practical impact of the Consent-Oriented Approach in the practice. The paper will then examine the implications of the Consent-Oriented Approach in relation to the key industries of the 4<sup>th</sup> Industrial Revolution, including big data, IoT, AI and blockchain.

## II. STRICT CONSENT REQUIREMENTS IN KOREA

### 1. Right to privacy as a constitutional right under the Constitution of Korea

Article 10 of the Constitution of Korea provides that “[a]ll citizens shall be assured of human worth and dignity and have the right to pursue happiness,” and paragraph 2 of Article 17 provides that “[t]he privacy of the citizen shall not be breached.”<sup>3</sup>

Several judicial decisions have read privacy or data protection principles into the Korean Constitution.<sup>4</sup> In a landmark decision handed down on 26 May 2005,<sup>5</sup> the Constitutional Court acknowledged for the first time that Korean citizens have a right to “self-determination of personal information,” a concept closely related to the idea of informational self-determination developed by the German Constitutional Court. The court ruled:

*The right to control one's own personal information is the right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, designed to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology.*

Several rights are derived from this right to control personal information:

- (a) the right to prevent the collection and usage of personal information in the absence of the data subject's prior consent;

---

<sup>3</sup> For a detailed presentation, see Graham Greenleaf, *Data privacy laws in Asia – Trade and Human Rights Perspective* (Oxford University Press, 2014) at p 127ff.

<sup>4</sup> For a detailed presentation, see Kwang Bae Park, *Regulation of Cross-Border Transfers of Personal Data*, (Asian Business Law Institute, 2018) at p349 to 352

<sup>5</sup> Case 17-1 KCCR 668, 99Hun-Ma513 and 2004Hun-Ma190 (26 May 2005) (“Resident Registration Act Case” or “Collecting and Computerizing Fingerprints and Using Them for Investigation Purposes Case”).

- (b) the right to access and request correction of collected personal information;
- (c) the right to request suspension of the collection and usage of personal information; and
- (d) the right to request destruction of stored personal information.

## **2. Importance of consent of data subject**

Under the PIPA, the data subject's consent is one of the legal bases that allow a Data Controller to lawfully process the data subject's personal information. For example, Article 15(1) of the PIPA provides that personal information may be collected/used in the following cases:

- i. the data subject's consent is obtained;
- ii. the collection/use is specifically required or permissible under applicable laws and regulations or is inevitable to comply with the Data Controller's obligations under applicable laws and regulations;
- iii. the collection/use is inevitable for a public agency to carry out its business in the field under its jurisdiction, as provided in the applicable laws and regulations;
- iv. the collection/use is necessary to enter into and perform a contract with the data subject;
- v. there exist clear and urgent needs to protect the life, bodily and economic interest of the data subject or a third party, but where the prior consent to the collection/use cannot be obtained, either because the data subject or his/her legal guardian cannot express his/her intent, or because his/her address is unknown; or
- vi. the collection/use is necessary to achieve the legitimate interest of the data user and 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 user and not exceed a reasonable scope.

However, the above legal grounds for processing personal information are widely considered to be much narrower in scope than what is provided under Article 6 of the GDPR. Additional consent is also often required from the data subject, as further explained in section 3 below, depending on the type of the processing involved (e.g., provision of personal information to third parties, cross-border transfer of personal information), the purpose of the processing, and the items of personal information to be processed. Therefore, in practice, the data subject's consent is the most important and fundamental legal basis for processing personal information in Korea. As such, the Data Controllers in Korea in most cases have no choice but to obtain the data subject's consent in order to process his/her personal information.

## **3. Consent requirements under Korean data protection law**

Under the PIPA and other sector-specific data protection laws, the consent from one data subject are required for various stages of his/her data processing. The consent needs to be separate and specific to each stage of the data processing and must be obtained at the time the information is first collected. When the risk associated with the data processing changes (e.g., provision of personal information to third parties, outsourcing of the processing to a third party, cross-border transfer of personal information), a separate consent is also required. If the personal information processed by the Data Controller includes particular identification data such as the data subject's resident registration number and passport number, or sensitive personal information<sup>6</sup> such as health information, separate consent is required. Also, if the Data Controller intends on using the personal information for marketing purposes, separate consent must once again be obtained from the data subject. Other instances that require separate consent from the data subject is when a child's personal information is processed, or personal location information is collected/used.

Generally, when the law requires the consent of the data subject, it means that explicit, opt-in consent of the data subject must be obtained, and such consent needs to be obtained before or (at least) at the time of the collection and use of the personal information. When obtaining consent, Data Controllers must indicate whether the consent being sought is "mandatory" or "optional." Mandatory consent is consent that is required if the data subject wishes to have access to the agreed-upon service that he/she has signed up for, while optional consent means the data subject is allowed to choose whether he/she will give consent to the collection of his/her personal information for the described purpose, even though not providing the optional consent may limit his/her ability to access certain services provided by the Data Controller.

Due to the complicated consent requirements mentioned above, data subjects and Data Controllers in Korea are used to giving and requesting, respectively, various consents for the processing of personal information. It is not uncommon in Korea for a data subject to be asked to provide 10 or more consents before he/she may use a certain service. This is probably why the consent requirements under Korea's data protection and privacy regime are likely viewed as the most stringent in the world.

Korea's current consent requirements under the data protection laws are the product of several amendments and new legislation that were adopted by legislators following an increasing frequent mass data breach incidents since 2008. Through legislation, Korean legislators have taken the position that the Data Controller's failure to obtain a data subject's consent is an infringement upon the data subject's constitutional "right to informational self-determination," and have worked towards shaping the relevant laws and regulations to prevent such infringement.

However, these requirements often seem to operate as serious impediments to business activities or industries that rely on extensive processing of personal information, e.g., online target marketing or

---

<sup>6</sup> Defined by Article 23 of the PIPA as "information on the ideology, creed, membership of a labor union or political party, political views, health, sexual preferences, bio-data, and criminal records."

the big data industry. Due to these circumstances, there has been considerable criticism from affected industries and practitioners regarding the strict regulation of the processing of personal information.

#### **4. Enforcement activities of regulators on the consent requirement**

If a Data Controller processes personal information (in particular, providing the personal information to a third party) without the data subject's consent even though consent is required, the Data Controller may be subject to (i) civil liability against the data subject, (ii) administrative sanctions by the regulators (e.g., the Ministry of Interior and Safety, Korea Communications Commission, Financial Services Commission), and/or (iii) criminal penalties. In practice, Data Controllers who provide personal information of an individual to a third party without the individual's consent, or use the personal information for purposes other than those that were consented to by the data subject are often subject to criminal penalties. As such, the risk associated with processing personal information without the consent of the data subject is very high, and the Data Controllers in Korea are well aware of this.

### **III. 4<sup>th</sup> INDUSTRIAL REVOLUTIN AND CONSENT MECHANISM IN KOREA**

As is the case in several other countries, the Korean Government has also been contemplating ways to develop industries that are at the core of the Fourth Industrial Revolution, including big data, IoT, AI, and blockchain. Over the past 5-6 years, industry experts and privacy specialists have repeatedly voiced the need for more flexible consent requirements, limiting an unnecessarily broad interpretation of the definition of personal information, and less risk of criminal penalties for Data Controllers who fail to obtain a data subject's consent in order to promote the growth of Korea's IT-driven industries and keep up with the changes taking place as part of the Fourth Industrial Revolution. These discussions have not gone unnoticed by the Korean authorities, and the Guidelines on Personal Information De-identification Measures ("De-Identification Guidelines") that were issued in 2016 reflect some of the efforts made by the authorities towards creating a regulatory environment that fosters the development of IT and use of big data.

On 30 June 2016, the Korean authorities responsible for enforcing data protection and privacy laws and regulations (i.e., MOIS, KCC, FSC, Ministry of Science and ICT, Ministry of Health and Welfare, and Office for Government Policy Coordination) jointly issued the De-Identification Guidelines stating their official position on the de-identification of personal information, with the objective to support the big data industry and related companies.<sup>7</sup> While not legally binding, the De-Identification Guidelines are significant given the number and quality of its signatories.

---

<sup>7</sup> Kwang-Bae Park & Hwan-Kyoung Ko, "Highlights of the 'Big Data Guidelines for Data Protection'" *Lee&Ko Newsletter* (January 2015). See also Graham Greenleaf, "2014–2017 Update to Asian Data Privacy Laws – Trade and Human Rights Perspectives" (12 July 2017) UNSW Law Research Paper No 47, 2017, at pp 13–14.

The De-Identification Guidelines specifies that while information which is presumed “de-identified” in accordance with the guidelines may be used and provided to third parties without obtaining the data subject’s further consent, the Data Controller must still implement certain safeguards in order to prevent re-identification.

By adopting these guidelines, the above-mentioned authorities have sought to reduce much of the existing ambiguity associated with the concepts of “personal information” and “de-identification,” and to lay the foundation for utilizing big data while promoting the security of personal information in Korea.

However, two years of the efforts to relax the consent requirements under the De-Identification Guidelines turned out to be not so successful and ended up being used by only around 20 companies and institutions which processed the data pursuant to the De-Identification Guidelines. After various discussions among the Korean government, relevant industries and civil society organizations, Korea is now preparing to revise the law itself by amending the PIPA, Network Act, Location Information Act, the Credit Information Act. The amendments to the above Acts are currently being reviewed by the National Assembly after their proposal in November 2018.

#### IV. CONCLUSION

In Korea, the legal framework for data protection includes the PIPA, which was enacted based on the OECD’s 8 Privacy Principles, and various other sector-specific laws and regulations. The Supreme Court of Korea has acknowledged that the right to self-determination of personal information is a constitutional right, and upon this principle, Korea has developed strict consent requirements to protect personal information. However, this Consent-Oriented Approach is often viewed as excessively stringent, exceeding the purpose of upholding the right to self-determination of personal information, and to the extent, preventing the necessary developments to be achieved in the era of the 4th Industrial Revolution in Korea.

The rights of the data subjects should remain important in the 4<sup>th</sup> Industrial Revolution era, and the sufficient safeguards for preventing unauthorized data processing should remain in place as needed. However, Korea’s experience with the Consent-Oriented Approach suggests that in the 4th Industrial Revolution which inevitably requires mass collection and processing of data, it is more desirable for countries to focus on the accountability of the data controller/processor, instead of consent requirements, to efficiently protect personal information and at the same time, achieve the necessary developments in the 4<sup>th</sup> Industrial Revolution era. The details of the specific legal framework to be established to achieve this balance will need to be developed by each country considering various factors such as the existing laws and regulations, culture, institutions and perception of data protection in the particular country.

