DATA PROTECTION LAWS OF THE WORLD

South Korea

SOUTH KOREA

Last modified 19 January 2024

LAW

The main laws that apply to the handling of data about individuals are the Personal Information Protection Act (“**PIPA** ”) (amended in September 2023) and the Act on the Use and Protection of Credit Information (“**CIA**”).

Prior to 5 August 2020, the Act on Promotion of Information and Communications Network Utilization and Data Protection (“**Network Act**”) contained data protection-related provisions applicable to Online Service Providers (OSPs), which are (i) telecommunications service providers registered under the Telecommunications Business Act or (ii) a person who provides information or mediates the provision of information for profit by using services provided by a telecommunications service provider. Most organisations that operate websites / apps (except for non-profit organisations) as well as network operators are OSPs. However, most of these provisions were moved to the PIPA (Chapter 6, Special Rules on Processing of Personal Information by Online Service Providers), pursuant to an amendment to the Network Act and the PIPA that went into effect on 5 August 2020.

In 2023, the PIPA was further amended in keeping up with the principle of “same conduct – same regulation” for all personal data controllers by repealing special provisions that previously only applied to OSPs. The Amended PIPA has become effective from 15 September 2023, with certain exceptions such as the right of portability, where the effective date is yet to be determined. On 23 November 2023, the Personal Information Protection Commission (“**PIPC** ”) which is tasked with enforcing the PIPA proposed an amendment to the Enforcement Decree of the PIPA to provide the subordinate details of the PIPA amendments.

DEFINITIONS

Definition of personal data

Under PIPA, “personal information” means information relating to a living individual that constitutes any of the following:

a. Information that identifies a particular individual by his / her full name, resident registration number, image, etc.
b. Information which, even if by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in this case, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured)
c. Information under items (a) or (b) above that is pseudonymised in accordance with the relevant provisions and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (referred to as “pseudonymised information”).

Definition of sensitive personal data

Under the PIPA, “sensitive information” is defined as personal information concerning an individual’s ideology, faith, labor union

membership, political views or membership in a political party, health or medical treatment information, sexual orientation, genetic information, criminal records and biometric data for the purpose of uniquely identifying a natural person and race / ethnic information. Sensitive information can be processed if (a) such processing is required or permitted by a statute, or (b) the consent of the data subject is separately obtained.

Definition of Unique Identification personal data

Under the PIPA, “unique identification information” is defined to be Resident registration number (“**RRN** ”), driver’s license number, passport number, and foreigner registration number. Other information, apart from RRNs, can be processed if (a) such processing is required or permitted by statute, or (b) the consent of the data subject is separately obtained. RRN can only be processed based on a legal basis, irrespective of whether consent to the processing is obtained from the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The PIPC is in charge of the enforcement of PIPA.

The PIPC shall perform the following work:

1. Matters concerning the improvement of law relating to personal information protection;
2. Matters concerning the establishment or execution of policies, systems or plans relating to personal information protection;
3. Matters concerning investigation into infringement upon the rights of data subjects and the ensuing dispositions;
4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;
5. Exchange and cooperation with international organizations and foreign personal information protection agencies to protect personal information;
6. Matters concerning the investigation and study, education and promotion of law, policies, systems and status relating to personal information protection;
7. Matters concerning the support of technological development and dissemination relating to personal information protection and nurturing of experts; and
8. Matters specified as the work of the PIPC by the PIPA or other statutes.

REGISTRATION

Under PIPA, there is no general rule regarding the registration of personal data controller, however, a public institution which manages a personal information file (i.e. collection of personal information) shall register the following with the PIPC. A “ public institution” in this context refers to any government agency or institution.

- name of the personal information file;
- basis and purpose of operation of the personal information file;
- items of personal information which are recorded in the personal information file;
- the method to process personal information;
- period to retain personal information file;
- person who receives personal information generally or repeatedly; and
- other matters prescribed by the Presidential Decree.

The Presidential Decree of PIPA stipulates that the followings also shall be registered with the PIPC:

- the name of the institution which operates the personal information file;
- the number of subjects of the personal information included in the personal information file;
- the department of the institution in charge of personal information processing;

- the department of the institution handling the data subjects’ request for inspection of personal information; and
- the scope of personal information inspection of which can be restricted or rejected and the grounds therefore only “public institutions” are required to register with the PIPC.

DATA PROTECTION OFFICERS

Under PIPA, every personal data controller (which means any person, any government entity, company, individual or other person that, directly or through a third party, controls and / or processes personal information in order to operate personal information files as part of its activities) must designate a chief privacy officer (“**CPO**”) who must be an employee or executive of the company.

The CPO’s obligations under the PIPA are as follows:

- establishing and implementing plans for the protection of personal information;
- performing periodic investigations and improving the status and practices of the processing of personal information;
- handling complaints and dealing with damage pertaining to the processing of personal information;
- establishing internal control systems for preventing leakage, misuse and abuse of personal information;
- establishing and implementing training sessions for the protection of personal information;
- protecting, managing, and monitoring personal information files;
- establishing, amending, and implementing a personal information processing policy;
- managing materials concerning the protection of personal information; and
- destroying personal information for which the purpose of processing has been achieved or for which the retention period has expired.

The Proposed Enforcement Decree of the PIPA lays the grounds for the CPO to independently perform his / her duties. Under the Proposed Enforcement Decree, a personal data controller must (i) guarantee the CPO’s access to all information in relation to the processing of personal information, (ii) establish a system for the CPO’s direct reporting to the representative and the board of directors at least once a year, (iii) provide the CPO with human and material resources by creating an organizational structure suitable for the performance of duties, and (iv) prohibit a situation where the CPO is placed at a disadvantage by reason of non-compliance with unreasonable instructions.

Personal data controllers that meet certain criteria are required to designate a CPO with (i) at least three years of experience in personal information protection, and (ii) a combined career of at least six years in personal information protection, data protection, and information technology. More specifically, the obligation to designate a CPO with the foregoing qualifications is applicable to an entity whose annual sales revenue or income amounts to at least KRW 150 billion, and (i) processes sensitive information or unique identification information of at least 50,000 data subjects, or processes personal information of at least 1 million data subjects; (ii) is a school under the Higher Education Act with at least 10,000 enrolled students as of December 31 of the immediately preceding year; (iii) is a tertiary hospital under the Medical Service Act; or (iv) is a public institution operating a personal information processing system which meets the standards set by the PIPC.

There are no nationality or residency requirements for the CPO. In the event that a CPO is not designated, the personal information processing entity may be subject to a maximum administrative fine of KRW 10 million under the PIPA.

COLLECTION & PROCESSING

Under the PIPA, there must be a specific legitimate basis for collection and use of personal information, with the most representative basis being the data subject's consent. As a result, in principle, the explicit consent of data subjects must be obtained before processing their personal information. However, the data subjects' consent is not required in cases where the processing of personal information is prescribed by a statute or where it is necessary for an entity to process personal information in order to comply with its legal obligations.

Exceptions to the general rule above which are applicable to personal data controller are as follows:

- where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations;

- where it is unavoidable for a public institution’s performance of work under its jurisdiction as prescribed by statutes or regulations, etc;
- where it is necessary to perform an agreement entered into with a data subject or to take measures as requested by a data subject in the course of executing such agreement;
- where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;
- where it is necessary to attain the legitimate interests of a personal data controller, the interest of which is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope.
- where it is urgently necessary for public safety and security, public health, etc.

While one consent form may be used, separate consents must be obtained respectively for each type of processing activity (e.g. collection and use, third party provision) and for different types of personal information (e.g. unique identification information and sensitive information).

Under the PIPA, data subjects must be informed of, and provide their consent to, the following matters before their personal information is collected and / or used:

- the purpose of the collection and use;
- the items of personal information that will be collected;
- the duration of the possession and use of the personal information; and
- the fact that the data subject has a right to refuse to give consent and the negative consequences or disadvantages that may result due to any such refusal.

The processing of the RRN (which is a type of unique identification information) is prohibited even with the consent of the data subject unless the processing is explicitly required or permitted under a statute.

If the data subject is under the age of 14, the consent of their legal guardian must be obtained.

TRANSFER

As a general rule, a personal data controller may not provide personal information to a third party without obtaining the prior opt in consent of the data subject.

Exceptions to the general rule above apply in the following cases:

- where there exists special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute;
- where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc;
- where it is deemed manifestly necessary for the protection of life, bodily and property interests of a data subject or a third party where imminently endangered; and
- where it is urgently necessary for the public safety and security, public health, etc.

Under the PIPA, a personal data controller must obtain consent after it notifies the data subject of:

- recipient of personal information;
- purposes for which the recipient of personal information uses such information;
- particulars of personal information to be provided;
- period during which the recipient retains and uses personal information;
- the fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

When a business transfer occurs, the personal data controller may transfer personal information without consent; provided that it must provide its data subjects a chance to opt out by providing a notice of:

- expected personal information transfer;

- contact information of the recipient of the personal information, including the name, address, telephone number and other contact details of the recipient; and
- means and process by which the data subjects may refuse to consent to the transfer of personal information.

In addition to the restrictions set out above, consent must be received as a general rule for the cross-border transfer of personal information under the PIPA, however, consent need not be received in the following cases:

- where there are special provisions on cross-border transfers under laws, treaties or other international agreements;
- where delegation of processing or storage is necessary for the execution and performance of agreements with data subjects and such details are disclosed in the privacy policy or notified to the data subjects via email, etc;
- where the recipient of personal information has taken all necessary measures, such as authentication and safety measures required by the PIPC, such as ISMS-P; or
- where the countries or international organizations that personal information is transferred to are recognized by the PIPC as having an adequate level of protection.

While this exemption from the overseas consent requirement was only applicable to OSPs, the amended PIPA now applies this exemption to all personal data controllers.

When obtaining consent for cross-border transfers, personal data controllers must notify the following:

- specific information to be transferred overseas;
- destination country;
- date, time, and method of transmission;
- name and the contact information of the third party;
- third party's purpose of use of the personal information and the period of retention and usage; and
- method and procedure for rejecting the cross-border transfer and the consequences thereof.

SECURITY

Under the PIPA, every personal data controller must, when it processes personal information of a data subject, take the following technical and administrative measures in accordance with the guidelines prescribed by the Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of personal information:

- establishment and implementation of an internal control plan for handling personal information in a safe way;
- installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to personal information;
- measures for preventing fabrication and alteration of access / log records;
- measures for security including encryption technology and other methods for safe storage and transmission of personal information; and
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software, and other protective measures necessary for securing the safety of personal information.

The PIPA provides detailed measures to be taken by the personal data controller in its subordinate regulations.

BREACH NOTIFICATION

In the event of a personal information leakage, the personal data controller must notify the affected data subjects within 72 hours of becoming aware of the leakage. The data controller must also report to the regulator within 72 hours if: (i) personal information of 1,000 or more data subjects has been leaked, (ii) sensitive information or unique identification information has been leaked, or (iii) personal information has been leaked through unauthorized access from the outside. However, no regulatory reporting is needed if the data controller is able to take measures to significantly reduce the possibility of infringement of the rights and interests of the affected data subjects, such as retrieving or deleting the compromised personal information.

ENFORCEMENT

The competent authorities may request reports on the handling of personal information, and also may issue recommendations or orders if a personal data controller violates the PIPA. Non-compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, PIPC, the supervising authority, can issue a corrective order in response to any breach of an obligation not to provide personal information to a third party. Breach of a corrective order leads to an administrative fine of not more than KRW 30 million. Prior to issuing a corrective order, PIPC may take an incremental approach and instruct, advise and make recommendations to the personal data controller. On the other hand, where personal information has been transferred to a third party without the consent of the data subject and in the absence of exceptional circumstances, both the transferor and the transferee (if it received the personal information knowing that the data subject had not given consent) can be subject to criminal sanctions (imprisonment of up to 5 years or a criminal fine of up to KRW 50 million).

Punitive damages

In instances of data breaches caused by the personal data controller's intentional act or negligence, the personal data controller may be liable for up to five times the damages suffered.

ELECTRONIC MARKETING

Under the Network Act, anyone who intends to transmit an advertisement by electronic transmission media must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement for profit may not be transmitted.

In addition, the transmitter of advertisement information for profit must disclose the following information specifically within the advertisement:

- the identity and contact information of the transmitter; and
- instructions on how to consent or withdraw consent for receipt of the advertisement information.

A person who transmits an advertisement shall not take any of the following technical measures:

- a measure to avoid or impede the addressee's denial of reception of the advertising information or the revocation of his consent to receive such information;
- a measure to generate an addressee's contact information, such as telephone number and electronic mail address, automatically by combining figures, codes, or letters;
- a measure to register electronic mail addresses automatically with intent to transmit advertising information for profit, and various measures to hide the identity of the sender of advertising information or the source of transmission of an advertisement.

ONLINE PRIVACY

Cookie, logs, IP information, etc. may also be regulated by the PIPA as personal information, if combined with other information may enable the identification of a specific individual person easily.

The protection of location information is governed by the provisions of the Act on the Protection, Use, etc. of Location Information (“**LBS Act**”).

Under the LBS Act, any person who intends to collect, use, or provide location information of a person or mobile object shall obtain the prior consent of the person or the owner of the object, unless:

- there is a request for emergency relief or the issuance of a warning by an emergency rescue and relief agency;
- there is a request by the police for the rescue of the person whose life or physical safety is in immediate danger, or there exist special provisions in any Act.

Under the LBS Act, any person (entity) who intends to provide services based on location information (“Location-based Service Provider”) shall report to the Korea Communications Commission (“**KCC**”). Further, any person

(entity) who intends to collect location information and provide the collected location information to Location-based Service Providers (“Location Information Provider”) shall obtain a license from the KCC.

If a Location Information Provider intends to collect personal location information, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location Information Provider;
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- details of the services the Location Information Provider intends to provide to Location-based Service Providers;
- grounds for and period of retaining data confirming the collection of location information; and
- methods of collecting location information.

If a Location-based Service Provider intends to provide location-based services by utilizing personal location information provided by a Location Information Provider, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location-based Service Provider;
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- details of the location-based services;
- grounds for and period of retaining data confirming the use and provision of location information; and
- matters concerning notifying the personal location information subject of the provision of location information to a third party as below.

If a Location-based Service Provider intends to provide location information to a third party, in addition to the above, it must notify the subjects of personal location information of the third party who will receive the location information and the purpose of this provision.

KEY CONTACTS

Kim and Chang
www.kimchang.com/

Michael Kim
Senior Foreign Attorney
Kim & Chang
T +82-2-3703-1732
michael.kim@kimchang.com

Ari Yoon
senior Korean Attorney
Kim and Chang
T +82 2 3703 4568
ari.yoon@kimchang.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.