LAW

In the past, South Korea did not have a comprehensive law governing data privacy. However, a law relating to protection of personal information (Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011.

Moreover, there is sector specific legislation such as:

- the Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator

- the Use and Protection of Credit Information Act ('UPCIA') which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, etc. of an individual person. The UPCIA primarily applies to Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, and

- the Act on Real Name Financial Transactions and Guarantee of Secrecy ('ARNFTGS') which applies to information obtained by financial or financial services institutions.

Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.

DEFINITIONS

Definition of personal data

Under PIPA, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with other information).

Under the IT Network Act, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables such person to be identified.
Definition of sensitive personal data

Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual’s:

- thoughts or creed
- history regarding membership in a political party or labour union
- political views
- health care and sexual life,
- other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person.

The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. The IT Network Act also has a similar definition.

NATIONAL DATA PROTECTION AUTHORITY

The Ministry of the Interior ("MOI") is in charge of the execution of PIPA. The Korea Communications Commission ("KCC") is in charge of the execution of the IT Network Act.

REGISTRATION

Under PIPA, a public institution which manages a Personal Data file (collection of Personal Data) shall register the following with the MOI:

- name of the Personal Data file
- basis and purpose of operation of the Personal Data file
- items of Personal Data which are recorded in the Personal Data file
- the method to process Personal Data
- period to retain Personal Data
- person who receives Personal Data generally or repeatedly, and
- other matters prescribed by Presidential Decree. A ‘public institution’ in this context refers to any government agency or institution.

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

- the name of the institution which operates the Personal Data file
- the number of subjects of the Personal Data included in the Personal Data file
- the department of the institution in charge of Personal Data processing
the department of the institution handling the Personal Data subjects’ request for inspection of Personal Data, and

the scope of Personal Data inspection of which can be restricted or rejected and the grounds therefore.

Only ‘public institutions’ are required to register with the MOI.

DATA PROTECTION OFFICERS

Under PIPA, every Data Handler (which means any person, any government entity, company, individual or other person that, directly or through a third party, handles Personal Data in order to manage Personal Data files for work purposes) must designate a data protection officer.

Under the IT Network Act, every IT Service Provider must designate a director or chief officer of the department in charge of handling Personal Data as a data protection officer. Pursuant to Presidential Decree of the IT Network Act where, an IT Service Provider has less than 5 employees, the owner or representative director shall be the person in charge.

There are no nationality or residency requirements for the data protection officer. In the event that a data protection officer is not designated, the Data Handler may be subject to a maximum administrative fine of KRW 10 million under the PIPA or KRW 20 million under the IT Network Act.

COLLECTION & PROCESSING

If a Data Handler under PIPA or an IT Service Provider under the IT Network Act intends to collect Personal Data from the data subject or IT service user, it must:

- first notify the data subject or IT service user of the vital information stipulated under the law, and
- obtain the data subject’s or IT service user’s prior consent to such collection other than some exceptional cases stipulated under the law.

If a Data Handler under PIPA intends to collect Sensitive Personal Information, the consent must be separately obtained.

Under the amended IT Network Act, which became effective as of 18 August 2012, an IT Service Provider shall not collect a Resident Registration number (equivalent to Social Security number in the United States), unless:

- the IT Service Provider is designated as an identification institution by the KCC, or
- there exist special provisions under any other laws or Notification of the KCC.

Under the PIPA, prior to obtaining the prerequisite consent for collecting Personal Data from a data subject, a Data Handler must notify the data subject of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected
- time period for possession and use of Personal Data, and
- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, prior to obtaining prerequisite consent for collecting Personal Data from an IT service user, an IT Service Provider must notify the IT service user of:

- the purpose of collection and use of Personal Data
- items of Personal Data to be collected, and
• time period for possession and use of Personal Data.

Under the newly amended PIPA, effective as of 7 August 2014, an Data Handler shall not handle a Resident Registration number, unless:

• there exists special provisions requiring or permitting the handling of the Resident Registration number under other laws

• there is clear evidence of some urgent need to handle the data, for the sake of the safety or property of the data subject or of a third party, or

• the handling of the Resident Registration number is unavoidable and there exist special provisions under ordinance of the MOI.

When a certain business transfer occurs, the Data Handler or IT service provider must provide its data subjects or IT service users a chance to opt out by providing a notice, including items of:

• the expected occurrence of Personal Data transfers

• the contact information of the recipient of the Personal Data, including the name, address, telephone number and other contact details of the recipient, and

• the means and process by which the data subject or IT service user may refuse to consent to the transfer of Personal Data.

If the data subject or IT service user is under 14, the consent of his/her legal guardian must be obtained.

As a general rule, a Data Handler under PIPA or an IT Service Provider under the IT Network Act may not handle Personal Data without obtaining the prior consent of the data subject or IT service user, beyond the scope necessary for the achievement of the Purpose of Use. This general rule also applies where a Data Handler or IT Service Provider acquires Personal Data as a result of a merger or acquisition.

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

• where there exist special provisions in any Act or it is inevitable to fulfil an obligation imposed by or under any Act and subordinate statute

• where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute

• where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data

• where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, and

• where it is necessary for a Data Handler to realise his/her legitimate interests and this obviously takes precedence over the rights of a subject of Personal Data. In such cases, this shall be limited to cases where such data is substantially relevant to a Data Handler’s legitimate interests and reasonable scope is not exceeded.

Exceptions to the general rule above apply in the following cases under the IT Network Act:

• if the Personal Data is necessary in performing the contract for provision of IT services, but it is obviously difficult to get consent in an ordinary way due to any economic or technical reason.

• if it is necessary in settling the payment for charges on the IT services rendered, and
• if a specific provision exists in this Act or any other Act.

Under the ARNFTGS, financial institutions must obtain written consent for the disclosure of an individual’s information relating to his/her financial transactions.

TRANSFER

As a general rule, a Data Handler or an IT Service Provider may not provide Personal Data to a third party without obtaining the prior opt in consent of the data subject or IT service user.

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

• where there exist 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, and

• where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Exceptions to the general rule above apply under the IT Network Act if a specific provision exists in this Act or any other act otherwise.

Under PIPA, a Data Handler must obtain consent after it notifies the data subject of:

• the person (entity) to whom the Personal Data is furnished

• purpose of use of the Personal Data by the person (entity)

• types of Personal Data furnished

• period of time during which the person (entity) will possess and use the Personal Data, and

• the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, an IT Service Provider must notify the IT service user of:

• the person (entity) to whom the Personal Data is furnished

• purpose of use of the Personal Data by the person (entity)

• types of Personal Data furnished, and

• period of time during which the person (entity) will possess and use the Personal Data, and then obtain consent from the IT service user.

The UPCIA stipulates that prior to obtaining prerequisite consent for providing personal credit information to any other person, a Credit Information Provider/User must notify the credit information subject of:

• the person (entity) to whom the credit information will be furnished

• the purpose of use of the Personal Credit Information by the person (entity)

• the types of Personal Credit Information to be furnished, and
• the period of time during which the person (entity) will possess and use the Personal Credit Information.

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

• where a Credit Information Company as defined under Article 2.5 of the UPCIA provides such information for the purpose of performing central management and utilisation thereof with another Credit Information Company or Credit Information Collection Agency as defined under Article 2.6 of the UPCIA

• where such provision is required to perform a contract, and to entrust the processing of credit information under Article 17.2 of the UPCIA

• where the relevant Personal Credit Information is provided as part of rights and obligations that are transferred by way of business transfer, division, merger, etc

• where Personal Credit Information is provided for a person who uses the information for purposes prescribed by Presidential Decree, including claims collection (applicable only to the credit which is an object of collection), license and authorisation, determination of a company’s credit worthiness, and transfer of securities

• where Personal Credit Information is provided in accordance with a court order for submission thereof or a warrant issued by a judicial officer

• where such information is provided upon the request of a prosecutor or judicial police officer, in the event of occurrence of an emergency where a victim’s life is in danger or he/she is expected to suffer bodily injury, etc., so that no time is available to issue a judicial warrant

• where such information is provided as the head of a competent government office requests, in writing, for the purpose of inquiry and examination in accordance with any laws pertaining to taxes or demands the taxation data required to be provided in accordance with such laws pertaining to taxes

• where Personal Credit Information held by a financial institution is provided to a foreign financial supervisory body in accordance with international conventions, etc

• where information by which the credit worthiness of related persons, such as a violator of credit order prescribed by Presidential Decree, and an oligopolistic stockholder and the largest investor of an enterprise, can be determined, is provided; and

• where such information is otherwise provided in accordance with other laws.

Under the ARNFTGS, financial institutions must obtain written consent for the transfer of an individual’s information relating to his/her financial transactions to a third party.

Under PIPA, when processing Personal Data acquired indirectly by way of a third party transfer, transferees who meet a certain threshold as provided by the Presidential Decree will be obligated to notify the data subject of (i) the third party source (transferor) from which the Personal Data was acquired, (ii) the intended use of the received Personal Data, and (iii) the fact that the data subject has the right to request for suspension from processing Personal Data.

SECURITY

Under PIPA and IT Network Act, every Data Handler or IT Service Provider must, when it handles Personal Data or Sensitive Personal Data of a data subject or IT service user, take the following technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of Personal Data:

• establishment and implementation of an internal control plan for handling Personal Data 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 Data

• measures for preventing fabrication and alteration of access records

• measures for security including encryption technology and other methods for safe storage and transmission of Personal Data

• 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 Data.

**BREACH NOTIFICATION**

Under PIPA, if a breach of Personal Data occurs the Data Handler must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects exceeds 10,000, the Data Handler shall immediately report the notification to data subjects and the result of measures taken to MOI, KISA or the National Information Security Agency ('NIA').

Under the IT Network Act, an IT Service Provider must, if it discovers an occurrence of intrusion:

• report it to the KCC or the Korea Internet & Security Agency (KISA) within twenty four (24) hours of knowledge of the intrusion, and

• analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The KCC may, if deemed necessary for analysing causes of an intrusion, order an IT Service Provider to preserve relevant data, such as access records of the relevant information and communications network.

Under the newly amended IT Network Act, which became effective as of 29 November 2014, if a loss, theft or leakage of Personal Data occurs, the IT Service Provider must notify the IT Service user immediately and report to the KCC within twenty four (24) hours of the details and circumstances, and the remedial steps planned.

**ENFORCEMENT**

The competent authorities may request reports on the handling of Personal Data, and also may issue recommendations or orders if a Data Handler or IT Service Provider violates PIPA or the IT Network Act. Non compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, MOI, the supervising authority for Data Handlers, can issue a corrective order in response to any breach of an obligation not to provide Personal Data 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, MOI may take an incremental approach and instruct, advise and make recommendations to the Data Handler.

Under the IT Network Act, an IT Service Provider who collected Personal Data without consent of the relevant user shall be subject to the penalty of imprisonment for not more than 5 years or a fine not exceeding KRW 50 million.

Under the UPCIA, a Credit Information Provider/User who has provided Personal Credit Information without consent of the relevant credit information subject shall be subject to the penalty of imprisonment of up to 5 years or a fine not exceeding KRW 50 million.

Under the ARNFTGS, a person who discloses information or data concerning financial transactions shall be punished by imprisonment not exceeding 5 years or by a fine not exceeding KRW 30 million.

**Punitive damages**
In the event that a Credit Information Provider/User suffers any damages resulting from the Data Handler’s conduct, the Credit Information Provider/User may bring a claim against the Data Handler for such damages. In such cases, a Data Handler may not be discharged from liability unless it can prove that there was no intentional act nor negligence on its part.

As of July 25, 2016, as a result of an amendment to PIPA, in instances Personal Data breaches caused by the Data Handler’s intentional act or negligence, the Data Handler may be liable for three times the damages suffered.

**ELECTRONIC MARKETING**

Under the IT Network Act, anyone who intends to transmit an advertisement by information and communication network must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement with commercial purposes may not be transmitted.

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

- 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, log, IP information, etc. are also regulated by the IT Network Act as personal data, which if combined with other information enable the identification of a specific individual person easily. Under the IT Network Act, using cookies (or web beacons) must be done with the opt-out consent of the user and the privacy policy must publicise the matters concerning installation, operation and opt-out process for automated means of collecting personal information, such as cookies, logs and web beacons.

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 (the ‘Location-based Service Provider’) shall report to the KCC. Further, any person (entity) who intends to collect location information and provide
the collected location information to location-based service providers (the ‘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 utilising personal location information provided from 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

Daniel Lee
Partner
T +82 2 6270 8899
daniel.lee@dlapiper.com

DATA PRIVACY TOOL

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

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.