DATA PROTECTION LAWS OF THE WORLD

Japan vs South Korea

DLA PIPER

JAPAN

Last modified 1 January 2024

LAW

The Act on the Protection of Personal Information ("**APPI**") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("**PPC** "), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted in 2003 but was amended and the amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI ("**Amended APPI**"). The Amended APPI came into force on April 1, 2022. Also, there was a separate data protection law for public sector. However, the data protection law for public sector was integrated into the APPI and became effective on April 1, 2022 (the data protection law for local governments became effective after April 1, 2023).

DEFINITIONS

Definition of Personal Information

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

Personal Information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information. According to the guidelines issued by the PPC, "easy reference to other information" means that a business operator can easily reference other information by a method taken in the ordinary course of business. If a business operator needs to make an inquiry of another business operator to obtain the "other information" and it is difficult for the business operator to do so, such a situation would not be considered an "easy reference to other information".

Personal Information includes any "Personal Identifier Code". A Personal Identifier Code refers to certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual. Typical examples of such code would be passport numbers or driver's license numbers.

Definition of Sensitive Personal Information

Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for third party transfer for sensitive information- prior consent is basically required from the data subject to transfer the sensitive information to a third party.

Definition of Anonymously Processed Information

"Anonymously Processed Information" refers to any information about individuals from which all personal information (i.e. the information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restored by taking appropriate measures specified in the enforcement rules and the relevant PPC guidelines. As noted above, Personal Information includes personal identifier codes, so these must also be removed before information is considered anonymized.

If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use

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.

notified to the data subjects or disclosed to third parties without requiring the consent of the data subjects. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of Personal Information. Additionally, before disclosing the Anonymously Processed Information to a third party, a business operator must publicly state (likely in its privacy policy) the items of information (for example, gender, birth year and purchase history) included among the Anonymously Processed Information, and the means by which it shares the Anonymously Processed Information.

Definition of Pseudonymously Processed Information

Given the high hurdle of utilizing Anonymously Processed Information, such information has been less utilized than originally expected. The Amended APPI introduces the concept of "Pseudonymously Processed Information", which is the information that is processed so that such information is (i) not able to be used to identify a specific individual; but (ii) is able to be de-crypted by referencing other information. For example, Pseudonymously Processed Information is information in which names, addresses, and other similar such information are replaced with a random string of characters. Unlike normal Personal Information, a business operator can change the utilization purpose of Pseudonymously Processed Information at its own discretion (i.e. a business operator does not need to obtain consents from data subjects to change the utilization purpose). It is expected that business operators may utilize Pseudonymously Processed Information for internal data analytics purposes.

Definition of Personally Referable Information

The Amended APPI defines information which is related to personal matters, but that does not fall under the definition of Personal Information as "Personally Referable Information". The definition of Personally Referable Information is quite vague, but based on the guidelines issued by the PPC, it includes, among other things, a web browsing history collected through the terminal identifier such as cookie information, a person’s age, gender or family makeup that are linked to his / her email address, a person’s purchase history of goods and / or services, a person’s location data, or a person’s area of interest. The handling of Personally Referable Information is not regulated as Personal Information, but prior consent from data

subjects would be required to transfer Personally Referable Information in certain circumstances as discussed below.

NATIONAL DATA PROTECTION AUTHORITY

The PPC has been tasked with providing many of the details necessary to interpret and enforce the APPI. The PPC issues guidelines for general rules for handling Personal Information, offshore transfer, confirmation and record requirements upon provision of Personal Information to third parties and creation and handling Anonymously or Pseudonymously Processed Information. The PPC is neutral and independent, and it has the power to enforce the APPI. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines and criminal penalties.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower
32nd Floor
3-2-1 Kasumigaseki
Chiyoda-ku Tokyo 100-0013
Japan

Telephone

+81-(0)3-6457-9680

Website

ppc.go.jp

REGISTRATION

Japan does not have a central registration system.

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

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific directors or employees should be assigned to control Personal Information (e.g. Chief Privacy Officer).

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

Specifying the Purpose of Use

COLLECTION & PROCESSING

Under the PIPA, there must be a specific legitimate basis for collection and use of personal information, with the

When handling Personal Information, a business operator must specify to the fullest extent possible the purpose of use of the Personal Information ("Purpose of Use"). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling Personal Information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the data subjects when Personal Information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When Personal Information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognizable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must 'publicly announce or 'expressly show the Purpose of Use in a reasonable and appropriate way. According to the guidelines issued by the PPC, the appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage so that the data subject can easily find the Purpose of Use before submitting the Personal Information.

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

Disclosing / Sharing Personal Information

Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the Personal Information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger / business transfer or entrusting the handling of Personal Information to third party service providers.

Even disclosing the Personal Information within group companies is considered disclosing the Personal Information to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose Personal Information to third parties, unless individuals opt out of allowing the business operator to do so. The Amended APPI stipulates that Personal Information that has been transferred from others through the opt out measure or that has obtained by illegal manners, and Sensitive Personal Information cannot be transferred through the opt out measure. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out.

- the name, address and representative person of the business operator;
- the fact that the purpose of use includes the provision of such information to third parties;
- the nature of the Personal Information being provided to third parties;
- the method by which Personal Information has been 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;

- the method by which Personal Information will be provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject;
- the method for an individual to submit an opt out request to the business operator;
- the method to update Personal Information which has been provided to their parties; and
- the schedule date of provision of Personal Information.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Information. Generally, written consent should be obtained whenever possible. When obtaining consents, it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Information will be disclosed, the contents of the Personal Information and how the third party will use the provided Personal Information.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Information from the data subject:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject;
- receipt of a consent email from data subjects;
- the data subject's check of the confirmation box concerning the consent;
- the data subject's click of a button on the website concerning the consent; and
- the data subject's audio input, or touch of a touch panel concerning the consents.

If Personal Information is to be used jointly, the business operator could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Information will be used jointly;
- the item of the Personal Information to be disclosed;
- the scope of the joint users;
- the purpose for which the Personal Information will be used by them; and
- 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.

- the name, address and representative person of the business operator responsible for the management of the Personal Information.

Transfer of Personally Referable Information

The Amended APPI stipulates that prior consent from data subjects is necessary if Personally Referable Information is transferred to a third party and the receiving party can identify a specific individual by way of referencing such Personally Referable Information with any information that the receiving party already has in its possession. In general, such consents are to be obtained by the receiving party and therefore, the transferor needs to, in advance to transferring Personally Referable Information to a third party, confirm if the receiving party has already obtained consents. That being said, it is possible that the transferor collects data subjects’ consents on behalf of the receiving party.

Cross-border Transfer

Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the enforcement rules of the APPI or the third party receiving Personal Information has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, UK and EU countries are specified as white-listed countries based on the adequacy decision on January 23, 2019.

According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Information are at least equal with the requirements for protection of Personal Information under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Information.

According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. With regard to data subject's consents to transfer their Personal Information to foreign countries, the Amended APPI stipulates that the business operator shall provide the following information to the data subject when obtaining consents therefrom: (i) name of the country where the receiving party resides, (ii) data protection law system in the country and (iii) the data

protection measures that the receiving party implements. In addition, the business operator needs to take necessary measures to ensure that the receiving party of such Personal Information continuously takes proper measures to process the Personal Information in a manners equivalent to the requirements of the APPI.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Information. The APPI does not set forth specific steps that must be taken. The PPC guidelines suggest recommended steps that business operators should take to ensure that Personal Information is secure. These necessary and appropriate measures generally include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures".

Guidelines often contain several specific steps or examples that entities subject to the guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to Personal Information, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

Under the Amended APPI, business operators shall report data breach incidents to the PPC and affected data subjects if the data breach incidents could harm the rights and interests of individuals. The PPC set the concrete threshold for reporting obligations and in the case of any of the below (i)-(iv), the business operator needs to report it to the PPC and notify the affected individuals: (i) Sensitive Personal Information is or likely to have been leaked, (ii) Personal Information that would cause financial damage by unauthorized use is or likely to have been leaked, (iii) data leakage by wrongful purpose is or likely to have been occurred, and (iv) data leakage incident that involves more than 1,000 data subjects is or likely to have been occurred.

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.

In addition, the PPC guidelines suggest that business operators (i) make necessary investigations and take any necessary preventive measures, and / or (ii) make public the nature of the breach and steps taken to rectify the problem, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Information which has been disclosed was immediately collected before being seen by any third party or not actually disclosed, (such as the case where the company has encrypted the data or otherwise secured the data in such a way that it has become useless to third parties being in possession of such data), the notice to the PPC or any other relevant authority is not necessary.

ENFORCEMENT

If the PPC finds any violation or potential violation of the APPI, the PPC may request the business operator to submit a report, conduct on-site inspection and request or order the business operator to take remedial actions. If a business operator does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 500,000.

If a business operator does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 1,000,000. If the party that fails to follow such order is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

An unauthorized disclosure of Personal Information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000. If the party that discloses Personal Information is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

ELECTRONIC MARKETING

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

The Act on Specified Commercial Transactions ("**ASCT**") and the Act on the Regulation of Transmission of Specified Electronic Mail ("**Anti-Spam Act**") regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (i.e. an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email or fax advertisements for 3 years for email advertisements and 1 year for fax advertisements after the last transmission date of an email or fax advertisement to the consumer.

If a seller has breached any of these obligations regarding email advertisements, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (e.g. an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient;
- for-profit entities or individuals engaged in business sending any email to advertise their own or another’s business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (e.g. there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act;
- an email is required to include a sender’s email address or a URL so that recipients can send opt-out notices to the sender; and
- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to

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.

imprisonment for up to 1 year or a fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 1,000,000 if an officer or an employee of the entity commits the violation mentioned above.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies, but it is generally considered that cookies fall under the definition of the Personally Referable Information and thus the transfer of such data would be regulated by the APPI in certain circumstances. In addition, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (e.g. member registration) and it is utilized (e.g. for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the **APPI**.

Moreover, under the Telecommunications Business Act, when providing telecommunications services to users as specified in the applicable Ministry of Internal Affairs and Communications ordinance and sending a telecommunication to the user’s device that gives a command to activate the device's information transmission function which transfers the information to third parties (such as third-party cookie), the service provider must take one of the following measures: (i) notify users of the content of information to be sent, Purpose of Use and the destination of information to be sent, or put these information in a condition where users can easily learn about it, (ii) obtain users consent, or (iii) take opt-out measures.

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;

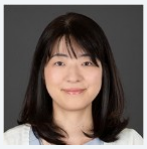
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- details of the services the Location Information Provider intends to provide to Location-based Service Providers;
- grounds for and period of retaining data confirming the collection 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



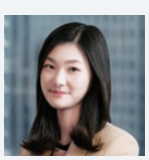
Tomomi Fujikouge
Of Counsel
T +81 3 4550 2817
tomomi.fujikouge@dlapiper.com

DATA PRIVACY TOOL

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

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

DATA PRIVACY TOOL

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