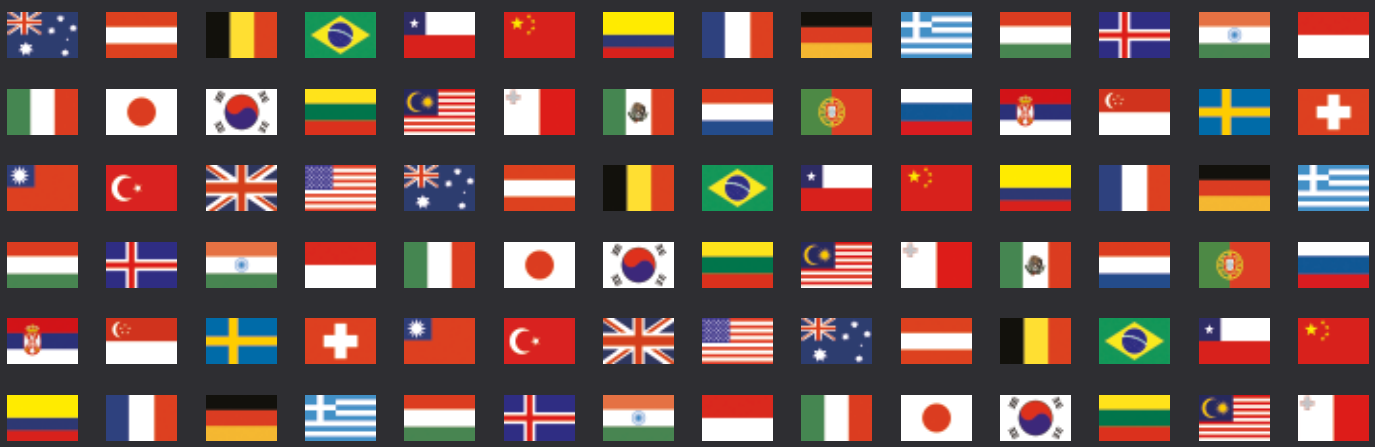
Data Protection & Privacy 2020

Contributing editors
Aaron P Simpson and Lisa J Sotto



LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Eighth edition
ISBN 978-1-83862-146-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2020

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Hungary, Iceland, Indonesia and Malaysia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Korea

Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim
LAB Partners

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of PII in Korea consists of the Personal Information Protection Act (the PIPA) and various sector-specific laws. The PIPA is the overarching statute regarding the protection of PII and was enacted with reference to the OECD guidelines and similar foreign precedents. Regarding information communication technology (ICT) and online privacy, the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) applies. Additionally, Korea has the following sector-specific laws that regulate the protection of PII:

- the Credit Information Use and Protection Act (the Credit Information Act) governs the protection of credit information in the finance sector;
- the Framework Act on Consumers applies to consumer data;
- the Act on the Consumer Protection in Electronic Commerce, etc. (the Electronic Commerce Act) governs privacy in the context of electronic commerce;
- the Act on the Protection, Use, etc, of Location Information (the Location Information Act) governs location information;
- the Medical Service Act applies to dated related to healthcare;
- the Act on the Promotion of Workers' Participation and Cooperation applies to data in the context of labour and employment; and
- the Framework Act on Education applies to data in the context of education.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

In Korea, multiple governmental authorities deal with data protection. The Personal Information Protection Commission, which is under the direct supervision of the President, is a governmental commission established pursuant to the PIPA with the authority to review and determine PII protection policies, to enhance systems and laws and to interpret and implement laws related to PII. The Ministry of the Interior and Safety has the authority to oversee compliance with the PIPA and has the power to demand information, investigate, impose monetary fines, issue corrective orders, charge and recommend sanctions. The Korea Communications Commission (the KCC) has the authority to oversee compliance with the Network Act and has the power to regulate, demand information, investigate, impose monetary fines and issue corrective orders. The KCC also has authority to oversee the compliance with the Location Information Act and has the power to demand information, investigate and impose monetary fines. The Financial Services Commission has the authority to oversee the Credit Information Act and has the power to investigate any violation of the Credit Information Act and impose monetary fines. The Korea Internet and Security Agency (the KISA) has been delegated authority from the Ministry of the Interior and Safety and the Korea Communications Commission and functions as the enforcement body with regards to the PIPA and the Network Act. The Fair Trade Commission has the power to order corrective measures regarding unfair terms and conditions relating to PII.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches??

The controlling authority of the PIPA is the Ministry of the Interior and Safety. Because the PIPA explicitly states that 'unless specifically provided in other laws, the regulation of PII protection shall comply with the PIPA', it is inevitable for sector-specific authorities such as the Financial Services Commission or the Korea Communications Commission to cooperate with the Ministry of the Interior and Safety. Although there are no statutory legal obligations, the relevant authorities all cooperate with each other in practice.

Recently, there is a movement to amend the PIPA to elevate the status of the Personal Information Protection Commission as the control tower of data protection to facilitate consistent and cooperative regulation by the relevant governmental agencies.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The PIPA, the Network Act and other sector-specific laws provide for administrative sanctions or criminal penalties that apply upon occurrence of breaches.

In the case of PIPA, a company that violates the PIPA can be subject to both administrative sanctions and criminal penalties. The Ministry of the Interior and Safety can issue corrective orders such as the termination of any activities that infringe on PII, the temporary suspension of PII processing and the implementation of necessary measures to protect, and prevent any infringement of, PII. Additionally, if the company is determined to have violated any laws related to PII protection, a recommendation for disciplinary measures against the responsible individual (including the representative director and the officer in charge) may be issued. Further, a monetary fine up to 500 million won can be

imposed for the loss, theft, leakage, alteration and impairment of a resident registration number. PII collection, or obtaining consent for PII collection, through false pretences or improper means, disclosing or providing unauthorised access to PII acquired in the course of business, or impairing, destroying, modifying, falsifying or impairing another person's PII without proper authorisation or beyond the scope of his or her authorisation can be subject to imprisonment for up to five years or a monetary penalty up to 50 million won under the PIPA. Further, a party that fails to adopt necessary measures to procure security pursuant to the PIPA and, as a result, incurs loss, theft, leakage, alteration or impairment of PII can be subject to imprisonment for up to two years or a monetary penalty up to 10 million won.

In the case of the Network Act, if the ICT service provider collects PII without consent, uses PII for a purpose beyond the agreed scope, provides PII to a third party, delegates PII processing without consent, fails to supervise or train the delegatee PII processor resulting in the delegatee's breach of privacy laws, incurs loss, theft, leakage, falsification, alteration and impairment of PII due to the lack of data protection measures, or transfers PII overseas without consent, the KCC may impose a monetary fine of up to 3 per cent of the revenue in relation to such violation.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The PIPA is the overarching law and applies to all private sectors and government sectors, individuals and companies. There is no organisation that is exempt from the PIPA. However, the PIPA provides that when a governmental agency requires PII to conduct its duties prescribed by law for the purpose of public interest, PII may be collected, used and provided without consent.

The Network Act and sector-specific laws such as the Credit Information Act, the Location Information Act, the Medical Service Act and the Framework Act on Education only apply to the relevant sector.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The PIPA and the Network Act both restrict the unauthorised interception of communications or electronic commerce. The PIPA focuses on implementing measures that would prevent unauthorised interception while the Network Act provides for protection of PII processed by ICT networks and penalises interception by unauthorised persons.

Such activities could also be subject to the Protection of Communications Secrets Act or the Criminal Act. Under the Protection of Communications Secrets Act, mail censorship, interception of ICT communications, providing communication records, or recording of or listening to confidential conversations of third parties are prohibited unless they fall under statutory exceptions.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

There are several laws that provide for specific data protection rules by sector. The ICT sector is subject to the Network Act, the Framework Act on Electronic Documents and Transactions, the Location Information Act, and the Protection of Communications Secrets Act. Employee monitoring is governed by the Act on the Promotion of Workers' Participation and Cooperation. Information in the healthcare sector is subject to the Medical Service Act, National Health Insurance Act, Public Health and Medical Services Act and Emergency Medical Service Act. Data protection in the finance sector is governed by the Credit Information Act whereas the education sector is governed by the Framework Act on Education.

PII formats

8 | What forms of PII are covered by the law?

Under the PIPA, PII means information regarding a living person such as the name, resident registration number or image that can identify such living person. Even if a certain piece of information cannot, by itself, identify a person, if the information can be easily combined with other information to identify a person, such information is also deemed to be PII. There is no limit as to the format or formality of the PII.

Under the Network Act, the definition of PII is the same. However, the parties who are regulated by the Network Act are limited to those who intermediate communication using telecommunication systems or provide telecommunication systems or those who use services provided by ICT service providers to provide information or intermediate information provision for profit.

Under the sector-specific laws, the scope of PII that is covered differs. For example, under the Credit Information Act, personal credit information means data that is necessary to determine the creditworthiness and credit transaction capacity of an individual. Under the Location Information Act, the personal location information means the location of a certain individual (including information, when combined with other information, can identify the location of an individual).

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The PII protection laws of Korea do not explicitly deal with extra-territorial application. The position of the Korean government, however, is that foreigners or foreign corporations that process PII of Koreans should implement PII protection measures that commensurate to the level of PII protection under Korean law under the principle of reciprocity.

The recent amendments to the Network Act and its Enforcement Decree adopt such principle of reciprocity for foreign ICT service providers and also imposes new obligations on foreign ICT service providers companies as follows: First, an ICT service provider who does not have a domicile or place of business in Korea and whose (i) total revenue for the preceding year is not less than 1 trillion won or (ii) revenue relating to ICT services for the preceding year is not less than 10 billion won must designate a representative in Korea to act as the Chief Information Protection Officer under the Network Act. The representative must perform the duties of the Chief Information Protection Officer under the Network Act and in the event of any data leakage, file reports to the regulatory authorities, to notify the data subjects and to submit material for investigation. Second, the rules that previously applied to overseas transfer of PII also apply to onward transfer of PII (that has already been transferred overseas) to a third country. Accordingly, in such case of onward transfer, the data subject's consent is required and the PII protective measures under the Network Act should be implemented. Third, by adopting the principle of reciprocity, any foreign ICT service provider who is domiciled in a country that restricts overseas transfer of PII can be subject to the same level of restriction for overseas transfer of PII from Korea.

Covered uses of PII

10 Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Under the PIPA, 'processing' means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, output, correction, recovery, use, provision, disclosure and destruction of PII and other similar activities. The PIPA does not particularly distinguish between those that control or own PII and those that provide PII processing services to owners. Under the PIPA, a single concept or term of 'PII processor' is used for a party (such as a public institution, legal person, organisation or individual) that processes personal information directly or indirectly to operate personal information files for official or business purposes.

Rather, a similar distinction under the PIPA to that between data controller and data processor would be the concept of delegator and delegatee of processing. When a PII processor delegates PII processing to a third party (ie, delegatee), the delegator needs to conduct training of the delegatee to prevent loss, theft, leakage, falsification, alteration or destruction of PII and supervise the delegatee's processing activities to ensure secure processing of PII in accordance with the Enforcement Decree of the PIPA. In the event any liability arises in the context of PII processing by the delegatee due to the violation of the PIPA, the delegatee would be treated as an employee of the delegator vis-à-vis the data subject. The delegatee is prohibited from using PII beyond the scope of delegation and from providing the PII to third parties.

The PIPA also imposes a higher level of PII protection to certain types of PII processors. Governmental agencies have heightened obligations for PII protection compared with the private sector. Such obligations include the duties to:

- disclose the registration of PII files;
- conduct privacy impact assessments;
- establish and disclose privacy policies that include policies regarding PII files that are subject to registration;
- grant the data subject the right to access PII; and
- participate in dispute resolution procedures.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

As a matter of principle, PII processing is permitted only with the consent of the data subject. However, PII processing without consent is possible in the following exceptional or inevitable cases under the applicable law.

Under the PIPA, PII processing without the data subject's consent is permitted in the following cases:

- statutory exceptions;
- inevitable for compliance with law;
- inevitable for governmental agencies to conduct their statutory duties;
- inevitable for executing and performing contracts with the data subject;
- necessary to protect the life, physical safety or property interest of the data subject or a third party and the data subject is not available to provide consent; or
- necessary to achieve the legitimate interest of the data processor and such interest overrides the interest of the data subject.

Under the Network Act, PII processing without the data subject's consent is permitted in the following cases:

- necessary to provide the ICT services under the contract with the data subject and obtaining customary consent is not feasible due to economic or technical difficulties;
- necessary to process payment for the ICT services that have been provided to the data subject; or
- statutory exceptions under other laws.

Further, under the recent amendments to the Network Act, the additional obligations are imposed if the data subject is under 14. Such additional obligations include ensuring that (i) the consent uses an easily understandable format and clear and straightforward language; and (ii) the consent of the legal representative is also obtained.

Under the Credit Information Act, PII processing without the data subject's consent is permitted in the following cases:

- statutory exceptions;
- inevitable for compliance with the law;
- inevitable for executing and performing contracts, such as financial transactions, with the data subject;
- necessary to protect the life, physical safety or property interest of the data subject or a third party and the data subject is not available to provide consent; or
- necessary to achieve the legitimate interest of the data processor and such interest overrides the interest of the data subject.

Under the Location Information Act, PII processing without the data subject's consent is permitted in the following cases:

- upon the request of an emergency rescue agency or the police for the purpose of emergency rescue;
- upon the request of an emergency rescue agency for the purpose of sending warnings;
- inevitable for executing and performing contracts with the data subject;
- necessary to process payment for the location information services or location-based services that have been provided to the data subject; or
- statutory exceptions under other laws.

Legitimate processing – types of PII

12 Does the law impose more stringent rules for specific types of PII?

Under the PIPA, more stringent rules (such as obtaining a separate consent) apply to:

- sensitive information (such as ideology, beliefs, trade union or political party membership, political opinion, health, sexual life or other type of information that could substantially impair the data subject's privacy); and
- personal identification information (such as resident registration number, passport number, driver's licence number or foreigner registration number).

In particular, the processing of resident registration numbers (which is a type of personal identification information) is prohibited in principle and only allowed if specifically permitted under law or explicitly required to protect the life, physical safety or property interest of the data subject or a third party.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The PIPA and the Network Act requires data processors to notify the data subject as set forth below.

PIPA

First, when the data processor obtains consent from the data subject for PII collection, the data processor must notify the data subject of the following information:

- the purpose of the collection and use of PII;
- the type of PII being collected;
- the retention period of PII; and
- the right to refuse consent and the disadvantages resulting from refusing consent.

If there are any changes to the above, such changes also need to be notified to the data subject.

Second, if the PII being processed by the PII processor is collected from someone other than the data subject, the PII processor must notify the data subject of the following information immediately upon the request of the data subject:

- the source of the PII collection;
- the purpose of the PII processing; and
- the right of the data subject to request the PII processor to suspend processing of the data subject's PII.

Third, if the PII processing is being delegated to a third party, the following information needs to be published on the relevant website or otherwise disclosed in a manner easily accessible to the data subject:

- the processing activity that is being delegated; and
- the identity of the delegatee.

Fourth, in the case of PII transfer due to corporate events such as business transfer, the transferor must notify the data subject in writing or by posting on the transferor's website.

Network Act

First, when obtaining consent from the data subject for PII collection, the data processor must notify the data subject of the following information:

- the purpose of the collection and use of PII;
- the type of PII being collected; and
- the retention period of PII.

If there are any changes to the above, such changes also need to be notified to the data subject.

Second, in the case of PII transfer due to corporate events such as business transfer, the transferor must notify the data subject by email or by posting on the transferor's website.

Third, ICT service providers whose revenue for ICT related services is 10 billion won or more in the preceding year or whose number of daily average users is one million or above for the last three months of the preceding year must notify the data subjects of the use of PII at least once a year by email, mail, text or telephone.

Exemption from notification

14 | When is notice not required?

Notice is not required for exceptional circumstances, such as a threat to life, the risk of bodily harm or the substantial impairment of rights regarding another person's property or other interest.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Under the PIPA and the Network Act, the consent for collection of PII and the consent for sharing PII with a third party (or, in the case of the Network Act, delegation of processing to a third party) should be clearly distinguished so that the data subject is aware of the scope of each consent. Also, when collecting PII, the data processor needs to clearly distinguish between mandatory PII and optional PII thereby providing a degree of control to the data subject.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Under the PIPA, a PII processor must ensure the accuracy, completeness and currency of the PII to the extent required for the purpose of the PII processing by implementing the following procedures:

- pre-verification of PII being inputted;
- data subject's right to access and correct PII; and
- correction or deletion of inaccurate information.

Further, the PII processor should exercise due care when processing PII to prevent any intentional or negligent alteration or destruction of PII.

Under the Network Act, ICT service providers are required to implement technical and organisational measures to ensure the security of PII and to prevent the falsification, alteration or destruction of PII. Like the PIPA, the Network Act requires procedures for granting the data subject access to PII and the right to request correction of PII to ensure the input of accurate data and for rectifying or deleting any incorrect information.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Under the PIPA, the PII must be destroyed when it becomes no longer necessary to retain PII due to the expiry of the PII holding period or the expiry or completion of the purpose of the PII processing.

The specific holding period for PII is determined by the sector-specific laws. For example, the Act on the Consumer Protection in Electronic Commerce, etc, states that information on:

- expression and advertising should be stored for six months;
- contracts and retraction of applications should be stored for five years;
- payment and provision of goods should be stored for five years; and
- consumer complaints and dispute resolution should be stored for three years.

Additionally, under the Credit Information Act, credit information should be deleted by the date which is the earlier of (i) five years from the termination of the financial transaction and (ii) three months from the date on which the purpose for collecting and providing PII has been achieved. Please note that certain records (as set forth in question 23) require retention for three years under the Credit Information Act.

Finality principle

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

A PII processor can only use PII for the purpose for which the PII was collected. It is illegal for a PII processor to use the PII beyond the purpose of collection unless the consent of the data subject has been obtained or there are exceptions in other statutes. Accordingly, it can be viewed that the finality principle has been adopted.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

In principle, a PII processor can only use PII for the purpose for which the PII was collected unless the exceptions that allow PII processing without consent (as described in question 11). Accordingly, unless the new purpose falls under these exceptions, additional consent from the data subject would be required to use PII for a new purpose.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Under the PIPA, a PII processor is required to implement physical, technical and organisational measures to procure security, including internal controls, access records, access controls, security software, encryption, lock system, safety measures for accidents and disasters. Details of such measures are set forth in the Standards for Procuring Safety Measures regarding Personal Information issued by the Ministry of the Interior and Safety.

Under Network Act, a PII processor is required to implement physical, technical and organisational measures to procure security, including internal controls, access records, access controls, security software, encryption, lock system, security measures for printing and copying and restricted PII display. Details of such measures are set forth in the Standards for Technical and Organisational Protective Measures regarding Personal Information issued by the KCC. Also, the recent amendments to the Network Act empowers the KCC to audit the ICT service providers to confirm whether sufficient access control procedures for information protection are in place.

Notification of data breach

21 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the PIPA, once the PII processor finds out that PII has been leaked, the PII processor must notify, without delay, the data subject of the following:

- the type of PII that has been leaked;
- the timing and background of the leakage;
- the actions that the data subject can take to minimise the damages resulting from the PII leakage;
- the remedial measures being taken by the PII processor and the procedures for compensation for damages; and
- the contact information of the division where the data subject can file for damages.

In the event the PII processer takes emergency action to prevent any additional leakage such as suspending connection, inspecting and supplementing defects and deleting leaked PII, the PII can notify the data subject after such action has been taken. If the data leakage involves not less than 1,000 data subjects, the PII processor must notify the data subject in writing and also post such information on its website for seven days or more (or if there is no website, in its place of business or other easily accessible place).

Further, in the event the PII leakage exceeds the scale prescribed under the Enforcement Decree of the PIPA, the PII processor must notify, without delay, the result of the remedial measures and data subject notification to the Minister of the Ministry of Interior and Safety or the KISA.

INTERNAL CONTROLS

Data protection officer

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Under the PIPA, a PII processor has the obligation to designate a data protection officer (DPO) who is in charge of PII processing activities. The duties of the DPO include the following:

- the establishment and implementation of PII protection plans;
- the periodical review and improvement of PII processing status and practice;
- the handling of complaints and compensation for damages arising from PII processing;
- the establishment of internal control systems to prevent leakage, misuse and abuse of PII;
- the establishment and implementation of PII protection education plans;
- the protection, control and supervision of PII files;
- the establishment, amendment and implementation of privacy policies;
- the organisation of PII files; and
- the destruction of PII whose purpose has been achieved or whose retention period has expired.

Further, the DPO must take immediate remedial action once the DPO becomes aware of any breach of privacy laws.

Under the Network Act, a Chief Information Protection Officer should be appointed in relation to the security of ICT systems and security of PII. The duties of the Chief Information Protection Officer include the following:

- the establishment, management and operation of an information protection system;
- the analysis, assessment and improvement of defects in PII protection;
- the prevention and remedy of infringement accidents;
- the establishment of preemptive data protection measures and the design and implementation of security measures;
- the pre-assessment of information security;
- the review of encryption of material information and the adequacy of security servers; and
- any other activities prescribed under the relevant laws to procure information protection.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The obligation to maintain internal records is set out in sector-specific PII protection laws. For example, under the Credit Information Act, credit information companies are required to maintain the following information for three years:

- the name and address of the customer and the name and address of the entity whom the PII was provided to or exchanged with;
- the details of the workscope requested by the customer and the date thereof; and
- the processing details of the requested workscope and the date and details of the credit information provided.

While the above retention period applies to the aforementioned information, the Credit Information Act requires that all credit information be deleted by the date that is the earlier of (i) five years from the termination of the financial transaction and (ii) three months from the date on which the purpose for collecting and providing PII has been achieved.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Under the PIPA, heads of governmental agencies have the obligation to conduct a privacy impact assessment that analyses the causes and suggests improvements if there is a risk of infringement of PII arising from the management of PII files pursuant to the standards prescribed under the Enforcement Decree of the PIPA.

The Network Act requires electronic communication business operators and information providers or intermediaries using electronic communication services to obtain certification of their overall systems (including physical, technical and organisational measures) to ensure the security and reliability of the information communication network.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

There are no general obligations that require PII processors to register with the supervisory authorities. However, certain sectors require registration with, or permits from, the relevant supervisory authority as follows:

- PIPA: governmental agencies that operate PII files must register certain matters regarding the PII files with the Minister of the Ministry of Interior and Safety.
- Location Information Act: a permit from the KCC is required to provide location-based services; provided that any location-based service that does not deal with PII can simply file a report with the KCC.
- Credit Information Act: a permit from the Financial Services Commission is required to conduct a credit information business that deals with credit information, such as a credit rating business, credit investigation business or debt collection business.
- Network Act: to conduct identity verification business, an application to and designation by the KCC is required.

Formalities

26 | What are the formalities for registration?

Each registration is subject to the formalities prescribed under the sector-specific law. For example, with respect to location-based services, the requisite documents for obtaining a permit or filing a report should be submitted to the KCC in accordance with the Enforcement Decree to the Location Information Act. No fees are required to be paid to the Korea Communications Commission with respect to the permit or filing. Recently, the Location Information Act has been amended to simply the filing requirements for one person companies or small companies conducting location-based services. Periodical renewal is not required but an amendment filing should be made when there is a change in the information submitted to the KCC.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Any location-based service that has not obtained the requisite permit or filed the relevant report will be subject to criminal penalties. Likewise, conducting any credit information business without the requisite permit will be subject to criminal penalties. Anyone conducting identity verification business without designation by the applicable regulatory authority will be subject to a monetary penalty of 10 million won.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

The supervisory authority may refuse to issue permits if the relevant criteria under the sector-specific law is not satisfied. As an example, with respect to a location-based service that deals with personal location information, the following criteria will be comprehensively reviewed in determining the issuance of the permit:

- the feasibility of the location-based service plan;
- technical and organisational measures for the protection of personal location information;
- adequacy of the size of facilities regarding the location-based service;
- financial and technical capacity; and
- other matters necessary for conducting a location-based service.

Public access

29 | Is the register publicly available? How can it be accessed?

The KCC website provides information on location-based service with permits, the Financial Services Commission website provides information on credit information business with a permit and the KCC website provides information on businesses that are designated as an identity verification agency.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

As registration or filings are not required in general for PII processors in Korea, specific legal effects do not exist.

Other transparency duties

31 | Are there any other public transparency duties?

Under the PIPA, a PII processor has the obligation to disclose its PII processing policy which includes the purpose of PII processing,

retention period, third party sharing, delegation of processing, data subject's rights, the DPO and the operation of any devices that automatically collect PII (such as internet connection information files) and the refusal thereof. The PII processor must also grant the data subject access to his or her PII.

Under the Network Act, the ICT service provider has the obligation to disclose its PII processing policy which must include information similar to those required under the PIPA. Also, the data subject has the right to access his or her PII and request provision of the PII.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the PIPA, the date subject's consent is required for the PII processor to disclose PII to a third party. In contrast, the data subject's consent is not required to delegate PII processing to a third party as long as such delegation is posted on PII processor's website. The rationale behind this dichotomy is that the provision of PII to third parties is for the benefit of the third-party recipient, whereas the delegation of PII processing is for the benefit of the PII processor.

On the other hand, under the Network Act, an information communication service provider is required to notify, and obtain the consent of, the data subject for both the provision of PII to third parties and the delegation of PII processing. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied.

Restrictions on disclosure

33 Describe any specific restrictions on the disclosure of PII to other recipients.

Under the PIPA and the Network Act, when PII is being disclosed to another recipient due to a merger or business transfer, the PII processor is required to notify the data subject prior to such disclosure. In the case where PII is disclosed to the delegatee in the context of delegation of PII processing, the data subject's consent is required for ICT service providers under the Network Act whereas only notice is required for PII processors under the PIPA.

Cross-border transfer

34 Is the transfer of PII outside the jurisdiction restricted?

Under the PIPA, to provide PII to a third party outside Korea, the following information needs to be notified to the data subject and consent must be obtained for such transfer:

- the recipient of PII;
- the recipient's purpose for using PII;
- the type of PII being provided;
- the period of storage and use of PII by the recipient; and
- the right of the data subject to refuse consent to transfer and, in the event there are any disadvantages arising from such refusal, the details of such disadvantage.

A PII processor cannot enter into a contract for overseas transfer of PII in violation of these restrictions under the PIPA. Note, however, that no consent is required when PII is being provided to a third party outside of Korea for the purpose of delegating PII processing.

Under the Network Act, an information communication service provider must obtain consent both for the provision of information to a third party and for the delegation of PII processing to a third party. Exceptions to the consent requirement are available where the delegation by the information communication network provider is necessary for the performance of the contract on the provision of information communication services and the furtherance of the user's convenience, as long as the other relevant conditions under the Network Act have been satisfied. The recent amendments to the Network Act require the data subject's consent in the case of onward transfer of PII (that has already been transferred outside Korea) to a third country.

Notification of cross-border transfer

35 Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Approval or authorisation from a supervisory authority is not required for cross-border transfer of PII.

Notwithstanding, the government can require an information communication service provider to adopt the following measures with respect to the processing of information related to national security and policies or information regarding advanced technology or devices developed in Korea:

- the establishment of systematic and technical measures to prevent the illegitimate use of the information communication network;
- systematic and technical measures to prevent the unlawful destruction or manipulation of information; and
- measures to prevent the leakage of material information acquired during the information communication service provider's processing of information.

Further transfer

36 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The recent amendments to the Network Act require the data subject's consent in the case of onward transfer of PII (that has already been transferred outside Korea) to a third country.

RIGHTS OF INDIVIDUALS

Access

37 Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Under the PIPA, a data subject can request a PII processor for access to the PII being processed and the PII processor must allow the data subject to access his or her PII within the time frame set forth in the Enforcement Decree of the PIPA. If there is any justifiable reason for delay in granting access, the PII processor can extend the time frame by notifying the data subject of such extension and the relevant cause. Once the cause no longer exists, the PII processor must grant access to the data subject without delay.

The PII processor can refuse or limit the data subject's access in the event there are:

- statutory prohibitions or restrictions on access;
- potential threat to life or risk of bodily harm; or
- potential impairment of property or other rights of another person.

In such cases, the PII processor must notify the data subject of the reason for the refusal or limitation of access.

Under the Network Act, the data subject may request the ICT service provider for access or provision of his or her PII being processed and the ICT service provider must take the necessary measures upon such request.

Other rights

38 | Do individuals have other substantive rights?

Under the PIPA, an individual can require a PII processor to correct or delete his or her PII once the data subject has accessed and reviewed his or her PII. Further, the data subject can require the PII processor to suspend processing of his or her PII.

Under the Network Act, the data subject has the right to cancel his or her consent for PII processing and the right to request correction of any inaccuracies.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under the PIPA, a data subject can seek monetary damages or compensation if the damages incurred by the data subject were due to the violation of the PIPA by the PII processor. In such cases, the PII processor will be liable unless it can prove that there was no intentional misconduct or negligence on the part of the PII processor. If the data subject incurred damages caused by the loss, theft, leakage, falsification, alteration or impairment of PII arising from the intentional misconduct or negligence of the PII processor, the court can order payment of damages up to three times the amount of the damages incurred.

The Network Act contains similar provisions and the recent amendments to the Network Act require ICT service providers above a certain size to take measures such as setting aside reserves or purchasing insurance to ensure payment of damages.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Both. The rights of data subjects under the PIPA can be exercised through litigation in court or by filing a request for corrective orders with regards to a PII processor's infringement of the data subject's legitimate rights.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No further provisions.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects can appeal against unlawful orders of the supervisory authorities to the courts.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

There are no specific statutory provisions that deal with cookies or equivalent technology. Nonetheless, cookies can be viewed as PII in certain circumstances.

Under the Network Act, an information communication service provider is required to include in its PII processing policy terms regarding the installation, operation and rejection of devices that automatically collect PII, such as internet connection record files. Such a PII processing policy should be disclosed to its users in an easily accessible manner according to the requirements of the Enforcement Decree to the Network Act.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Under the Network Act, in order to distribute marketing information for commercial purposes through electronic transmission, the express prior consent of the recipient is required. In the following cases, however, such consent requirement is waived:

- a party that has collected the recipient's contact information through transactions regarding certain goods sends the recipient marketing information for commercial purposes regarding the same type of goods; and
- a telemarketer under the Act on Door-to-Door Sales, etc, verbally notifies the recipient where his or her PII was collected and makes solicitations over the telephone.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The Act on the Development of Cloud Computing and Protection of Its Users (the Cloud Computing Act) was enacted in 2015 and is currently in effect. The principles of the PIPA and the Network Act as well as sector-specific laws may also apply to cloud computing service providers.

Under the Cloud Computing Act, a cloud computing service provider must endeavour to enhance the quality, performance and data protection levels of its cloud computing service. The Minister of the Ministry of Science and ICT has the authority to set out the standards for quality, performance and data protection (including physical, technical and organisational measures) and issue a recommendation to cloud service providers to comply with such standards. Also, under the Cloud Computing Act, a cloud service provider cannot disclose a user's information to a third party nor use the user's information for purposes other than providing cloud computing services without the user's consent, unless a court order or subpoena has been issued by a judge. The user can require the cloud computing service provider to inform the user of the country in which the user's information is stored.

Recently, the Electronic Finance Supervisory Regulations have been amended to allow the use of cloud for PII such as credit information and personal identification information to promote the adoption of cloud to further innovation and development of fintech business.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The issue of whether Korean privacy laws should apply to global companies and how Korean privacy laws can effectively been enforced against companies without a physical presence in Korea has been the subject of a long-standing debate, often resulting in the argument of reverse discrimination against Korean companies that are subject to the stringent requirements under Korean privacy laws. To counter such problems, the Network Act has been amended recently to enhance the protection of Koreans against foreign companies that process PII of Korean data subjects but do not have a physical presence in Korea and to adopt the principle of reciprocity. Specifically, the amendments to the Network Act include the following:

- an ICT service provider that does not have a domicile or place of business in Korea and whose (i) total revenue for the preceding year is not less than 1 trillion won or (ii) revenue relating to ICT services for the preceding year is not less than 10 billion won must designate a representative in Korea to act as the Chief Information Protection Officer; or (iii) by adopting the principle of reciprocity, any foreign ICT service provider that is domiciled in a country that restricts overseas transfer of PII can be subject to the same level of restriction for overseas transfer of PII from Korea; and
- to protect the cross-border circulation of PII of Koreans, consent will be required for onward transfer of PII (that has already been transferred overseas) to a third country.

LAB PARTNERS

Young-Hee Jo
yhjo@labpartners.co.kr

Seungmin Jasmine Jung
smjung@labpartners.co.kr

Kwangbok Kim
kbkim@labpartners.co.kr

8F, VPLEX, 501 Teheran-ro
Gangnam-gu
Seoul 06168
Republic of Korea
Tel: +82 2 6956 0250
http://labpartners.co.kr

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-146-9