# Korea


Iris Hyejin Hwang


Hye In Lee

D'Light Law Group



## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The Personal Information Protection Act ("**PIPA**") regulates data protection, from the establishment of national policies on Personal Information protection to detailed procedures and methods of Personal Information Processing and protection.

### 1.2 Is there any other general legislation that impacts data protection?

Apart from PIPA, there is no other general legislation that governs data protection in particular.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The Credit Information Use and Protection Act ("**Credit Information Act**") regulates "Credit Information", meaning information relating to a person's credit that can identify such person, or information that can determine the transaction details, creditworthiness, or credit transaction capacity of such person.

The Act on the Protection, Use, Etc. of Location Information ("**Location Information Act**") regulates the location information of a person.

The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. ("**Network Act**") used to have provisions regulating personal data processing by providers of information and communications services, before most of such provisions were moved to the revised PIPA, which will be effective from August 5, 2020.

### 1.4 What authority(ies) are responsible for data protection?

The Personal Information Protection Commission ("**PIPC**") under the Prime Minister's office oversees the protection of Personal Information (defined below) by: i) improving laws relating to Personal Information protection; ii) establishing or executing policies, systems, or plans relating to Personal Information protection; iii) investigating infringements of the rights of Data Subjects (defined below), and any ensuing dispositions; and iv) managing complaints or remedial procedures about Personal Information Processing and mediation of disputes over Personal Information. PIPC has jurisdiction over the interpretation and operation of law related to Personal Information protection.

The Financial Services Commission ("**FSC**") oversees credit information businesses and their compliance with Credit Information Act, with the power to order any violating company to take corrective measures.

The Korea Communications Commission ("**KCC**") oversees businesses handling personal location information, and their compliance with the Location Information Act. In case of non-compliance, KCC may revoke the permission granted to a location information provider or a location-based service provider through a cease-and-desist order on operations, from a certain duration up to a permanent basis.

The Korea Internet & Security Agency ("**KISA**") performs works delegated by PIPC including, without limitation, receiving reports of Personal Information leaks and collecting relevant materials from a Personal Information Controller in case of a reported violation of PIPA.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  PIPA takes "Personal Information" to mean any of the following information relating to a living individual:
  (a) information that identifies an individual by his or her full name, resident registration number, image, etc.;
  (b) information which, by itself, does not identify an individual, but may be easily combined with other information to identify an individual. The ease of combination is determined by reasonably considering the time, cost, technology, etc. used to identify the individual and the likelihood that the other information can be procured; or
  (c) information under items (a) or (b) that is pseudonymised, and thereby becomes incapable of identifying an individual without the use or combination of information that restores the information to its original state ("**Pseudonymised Information**");
- "**Processing**"
  "Processing" means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of Personal Information, and other similar activities.

- "**Controller**"
  "Personal Information Controller" ("Controller") in PIPA means a public institution, legal person, organisation, individual, etc. that processes Personal Information directly or indirectly to operate Personal Information Files as part of its activities. The term "Personal Information File" means a set or sets of Personal Information arranged or organised in a systematic manner based on a certain rule for easy search of the Personal Information.
- "**Processor**"
  "Processor" is unused in PIPA. Instead, PIPA uses "Outsourcee" for an entity that processes Personal Information under an outsourcing contract, in its provision that regulates the outsourcing of Personal Information Processing.
- "**Data Subject**"
  "Data Subject" means an individual who is identifiable through the information processed and is the subject of that information.
- "**Sensitive Personal Data**"
  *In lieu* of Sensitive Personal Data, PIPA uses "Sensitive Information" to mean ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other Personal Information that is likely to markedly threaten the privacy of the Data Subject.
  It is also prescribed by Presidential Decree of PIPA ("**PIPA Presidential Decree**") which, as of April 22, 2020, includes bio-data and criminal records, although the government is further revising the PIPA Presidential Decree to include in "Sensitive Information" information about: i) an individual's physical, physiological and behavioural characteristics, which is generated through certain technical means for the purpose of identifying a specific individual; and ii) race or ethnicity, that may unfairly discriminate against individuals in light of the purpose or situation of processing the information.
- "**Data Breach**"
  Rather than "Data Breach", PIPA uses "Leak, Etc." in one provision to mean loss, theft, or leak of Personal Information. In other provisions, PIPA lists loss, theft, leak, forgery alteration, or damage, instead of using "Leak, Etc.".

*Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

- "**Pseudonymisation**"
  "Pseudonymisation" means a procedure to process Personal Information by deleting in part, or replacing, in whole or in part, certain information so that the Personal Information cannot identify an individual without additional information.
- "**Personally Identifiable Information**"
  "Personally Identifiable Information" means information that can be used to uniquely identify an individual in order to comply with statutes. Only the resident registration number, driver's licence number, passport number, and alien registration number are prescribed as Personally Identifiable Information under the PIPA Presidential Decree.
- "**Information and Communications Service Provider**" ("**ICSP**")
  An ICSP is any person who: i) allows other parties to communicate with each other through the use of machinery, lines, or other facilities/equipment necessary to transmit or receive codes, speech, sound, or images by wire, wireless connection, light, or other electronic methods; ii) provides the facilities to communicate with others; or iii) conducts business to provide information or allow the provision of information using those facilities.

## 3 Territorial Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

PIPA has extraterritorial reach. For example, it specifies that a) any ICSP (person or corporation) with no address or office in Korea, who b) receives Personal Information of Korean users ("**ICSP, Etc.**"), must designate an agent with an address or office in Korea to act on its behalf in case any of the following criteria applies:

1. a person whose global sales for the preceding year (or preceding business year for a corporation) reach or exceed KRW 1 trillion;
2. a person whose sales in Korea from information and telecommunications services for the preceding year (or preceding business year for a corporation) reach or exceed KRW 10 billion;
3. a person who stored or maintained at least one million domestic users' Personal Information on an average daily basis over the three months immediately before the end of the preceding year; or
4. a person who caused or is likely to have caused a Personal Information breach or Leak, Etc. incident under PIPA, and was consequently required by KCC to submit relevant materials, documents, etc.

For the other provisions under PIPA, which does not explicitly state its extraterritorial reach, it is understood that they may still apply to foreign persons or corporations. The understanding is based on KCC's actions under the Network Act's Personal Information protection and oversight of ICSP before the Network Act's revision and the absorption of certain provisions into the revised PIPA. In 2014, KCC imposed administrative surcharges on both Google Korea LLC and Google Inc. for collecting Personal Information of users without the users' consent. The administrative surcharge imposed on Google Inc. itself was KRW 212,300,000.

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Controllers must make their privacy policy and other matters related to Personal Information Processing public, and guarantee the Data Subject's rights, e.g., the right to access one's Personal Information.
- **Lawful basis for processing**
  Controllers must collect any Personal Information lawfully and fairly, and endeavour to obtain the trust of Data Subjects by observing and performing the duties and responsibilities required in PIPA and other related statutes.
- **Purpose limitation**
  Controllers must explicitly state the purposes of the Personal Information Processing, and ensure that this is carried out in an appropriate manner within the scope of the stated purposes.

- **Data minimisation**
  Controllers must collect the minimum required Personal Information necessary for the stated purposes.
- **Proportionality**
  Please see above.
- **Retention**
  The Controller must manage Personal Information safely according to the processing methods, types, etc. of Personal Information, accounting for the possibility of infringement on the Data Subject's rights and the severity of the relevant risks. Accordingly, the Controller must destroy Personal Information without delay when the Personal Information becomes unnecessary owing to the expiry of the retention period or the fulfilment of the purpose of processing the Personal Information, unless another statute requires retention of such Personal Information.

*Other key principles – please specify*

- The Controller must ensure Personal Information is accurate, complete, and up to date to the extent necessary for the purposes for which the Personal Information is processed. Additionally, if it is possible to fulfil the purposes of collecting Personal Information by processing anonymised or Pseudonymised Information, the Controller must endeavour to process Personal Information through anonymisation where possible, but at least through Pseudonymisation.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  The Data Subject may request access to his/her Personal Information from the Controller processing it. Unless there is a reason to limit such access stated under PIPA, the Controller must enable access to the Personal Information within 10 days of its receipt of a request.
- **Right to rectification of errors**
  The Data Subject may send a request to the Controller for the correction of his/her Personal Information. The Controller must correct the Personal Information and notify the Data Subject of the change within 10 days of its receipt of the request.
- **Right to deletion/right to be forgotten**
  Unless the collection of certain Personal Information is required by another statute, the Data Subject may request that the Controller delete certain Personal Information. The Controller must delete the requested Personal Information and notify the Data Subject within 10 days of its receipt of the request.
- **Right to object to processing**
  The Data Subject may request the relevant Controller to suspend processing of his/her Personal Information. Unless there are exceptions under PIPA, the Controller must suspend the processing of such Personal Information, and notify Data Subject of the status within 10 days of its receipt of the request.
- **Right to restrict processing**
  Nothing under Korean law grants Data Subjects the right to restrict processing.
- **Right to data portability**
  PIPA does not grant Data Subjects the right to data portability. However, under the Credit Information Act, Data Subjects of credit information may request their credit information to be transmitted to themselves or to a certain third party regulated by the Credit Information Act.
- **Right to withdraw consent**
  PIPA lacks any provisions that apply to all Controllers, but it specifically provides that a Data Subject may withdraw his/her consent provided to an ICSP, Etc. Once Data Subject withdraws his/her consent, the ICSP, Etc. must take the necessary measures, such as destroying the information to such an extent that it is not recoverable or revivable, without delay.
  According to the Credit Information Act, when the Data Subject of personal credit information consents to allow a credit information provider/user to provide his/her Credit Information to a third party for purposes other than assessing the individual's creditworthiness, the Data Subject may exercise the right to withdraw such consent.
  When the Data Subject withdraws his/her consent to a third-party transfer, and the credit information provider/user faces difficulty in the performance of a contract with such Data Subject (*i.e.*, the credit information provider/user becomes unable to provide services promised to such Data Subject) before transferring the Data Subject's Credit Information to a third party, the Data Subject must clarify his/her intention not to be provided with the goods or service of the underlying contract when withdrawing such consent.
- **Right to object to marketing**
  When obtaining consent to process Personal Information for the purpose of marketing, the Controller must clearly notify such purpose to Data Subjects, and the Controller may not refuse to provide its goods or services even if a Data Subject refuses to provide consent to use for marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Anyone who suffers an infringement of rights or interests over one's Personal Information during Personal Information Processing by a Controller may report such infringement to government authorities, and KISA is the designated special agency for receiving and processing such reports.

*Other key rights – please specify*

- **Notification of the Use History of Personal Information**
  ICSP, Etc. meeting the requirements prescribed by PIPA Presidential Decree must notify users of the use history of their Personal Information on a regular basis. This does not apply where the collected information does not include contact information that enables notification to users.

## 6 Registration Formalities and Prior Approval

### 6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

In general, businesses have no legal obligation to register with nor notify the data protection authorities in respect of processing activities. However, businesses who collect a certain type of information may need to register with or notify a relevant protection authority.

For example, anyone intending to engage in the business of collecting personal location information and providing such information to location-based service providers must obtain permission from KCC. Also, anyone intending to engage in the business of providing services based on personal location information must file a report to KCC.

**6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

When applying for permission from KCC for the business of collecting personal location information and providing such information to location-based service providers, applicants must submit a business plan containing the company's financial statement, the business plan, the location information protection plan, and the system composition and operation plan, etc.

When filing a report to KCC regarding the business of providing services based on personal location information, the reporter must submit its business plan, including the status of the service provider and the details of its business, the details and location of the main facilities for its business, and the measures for protecting location information required by the Location Information Act.

**6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

Each registration/notification is made per legal entity.

**6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

Any legal entity, foreign or local, intending to engage in the businesses outlined in question 6.1 must either apply for permission or file a report as set out in question 6.2.

**6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

Please refer to the answer to question 6.2.

**6.6 What are the sanctions for failure to register/notify where required?**

Anyone who engages in the business of collecting personal location information without obtaining KCC's permission may be punished by imprisonment with labour for not more than five years or by a fine not exceeding KRW 50 million.

Anyone who engages in the business of providing services based on personal location information without filing a report to KCC may be punished by imprisonment with labour for not more than three years or by a fine not exceeding KRW 30 million.

**6.7 What is the fee per registration/notification (if applicable)?**

No fee is required for such registration or report.

**6.8 How frequently must registrations/notifications be renewed (if applicable)?**

A renewal procedure is not required for such registration or report. However, when there is any change in the legal entity's trade name, principal place of business or location information system, the legal entity must report the change to KCC.

**6.9 Is any prior approval required from the data protection regulator?**

Please refer to the answer to question 6.2.

**6.10 Can the registration/notification be completed online?**

Yes, registration/notification may be completed at https://www.emsit.go.kr/ (only available in Korean).

**6.11 Is there a publicly available list of completed registrations/notifications?**

Yes, the list may be viewed at https://kcc.go.kr/user.do?boardId=1030&page=A02060400&dc=K02060400 (only available in Korean). However, KCC does not update the list frequently.

**6.12 How long does a typical registration/notification process take?**

It normally takes about two months to obtain permission from KCC for the business of collecting personal location information and providing such information to location-based service providers. It takes about two weeks to receive the decision from KCC about the report for the business of providing services based on personal location information.

## 7 Appointment of a Data Protection Officer

**7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Anyone who processes Personal Information directly or indirectly to operate one or more Personal Information Files as part of its activities must appoint a Data Protection Officer ("**DPO**").

**7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Anyone required to appoint a DPO (as defined under question 7.1) that fails to do so could be administratively fined up to KRW 10,000,000.

**7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The DPO may not be subject to disadvantages without justifiable grounds by its employer for performing the functions of the role required by PIPA.

**7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

The DPO of a legal entity must be the owner of the business, its representative, or its executive officer. In the case that a legal entity lacks an executive officer, the head of a department in charge of the affairs related to Personal Information Processing may become DPO. In theory, if a person holds a position in two different entities that meet the requirement, he/she could become the DPO of both legal entities.

**7.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Please refer to the answer to question 7.4.

**7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The DPO must: i) establish and implement a Personal Information protection plan; ii) conduct a regular survey of the status and practices of Personal Information Processing, and improve shortcomings; iii) handle complaints and remedial compensation in relation to Personal Information Processing; iv) build the internal control system to prevent the leak, abuse, and misuse of Personal Information; v) prepare and implement an education programme about Personal Information protection; vi) protect, control, and manage the Personal Information Files; vii) establish, modify, and implement a privacy policy pursuant to PIPA; viii) manage materials related to the protection of Personal Information; and ix) destroy Personal Information whose purpose of processing has been attained or whose retention period has expired.

**7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, such registration/notification is not required.

**7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

Every Controller must prepare and disclose a privacy policy that contains contact information such as the name of the DPO or the name, telephone number, etc. of the department which performs the duties related to Personal Information protection and manages complaints.

## 8 Appointment of Processors

**8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

An agreement is required in order to outsource Personal Information Processing.

**8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

According to PIPA and the PIPA Presidential Decree, an agreement to outsource Processing must include: i) a requirement that the Personal Information Processing must solely be for the outsourced purpose; ii) technical and managerial safeguards of Personal Information; iii) purpose and scope of outsourced work; iv) a restriction against the subcontracting of the outsourced tasks; v) measures to ensure the safety of Personal Information; vi) measures for the supervision of the Outsourcee's management of Personal Information gained in relation to outsourcing; and vii) measures concerning the liability for damages in case of breach of the Outsourcee's obligation.

## 9 Marketing

**9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Under the Network Act, the transmission of marketing information for a commercial purpose through electronic transmission requires express and prior consent from recipients. Consent is not required if someone who has directly collected contact details from a recipient and sold goods or a service to the recipient sends electronic direct marketing for the same kind of goods or service sold within six months of the previous sale. Any transmission of marketing information for a commercial purpose through an electronic transmission other than email between 9 p.m. and 8 a.m. of the following day (Korea Standard Time) must obtain separate, prior consent from the intended recipient.

**9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

Such restrictions apply to both business-to-business and business-to-consumer marketing.

**9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The restrictions described in the answer to the question 9.1 apply to the transmission of marketing information for a commercial purpose by using any electronic transmission, including telephone, mobile phone, fax, PC, etc. However, registered telemarketing business entities and persons who engage in telemarketing on behalf of such business entities may give marketing information for a commercial purpose and recommend a purchase by phone or mobile phone when such entities or persons notify the recipient of where the recipient's Personal Information was collected.

**9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Such restrictions also apply to marketing sent from other jurisdictions to recipients in Korea.

**9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

KCC may order corrective action and impose administrative fines on those who have failed to comply with such restrictions, and KISA manages complaints and advises recipients in relation to the transmission of marketing information.

**9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

A person can only receive a marketing list when all Data Subjects on a list have given prior consent to provide their Personal Information after being notified of the recipient of such Information, the purpose for which the recipient of Personal Information will use such information, particulars of the Personal Information to be provided, and the period for which the recipient will retain and use the Personal Information.

**9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Anyone who sends marketing information for a commercial purpose through electronic transmission without express, prior consent from recipients may be subject to an administrative fine of up to KRW 30,000,000.

## 10 Cookies

**10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

Under PIPA, the Controller must disclose its privacy policy, including information about the use of cookies to automatically collect Personal Information, and the means to opt out.

**10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

No such distinction is made.

**10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

No enforcement action has yet been taken specifically regarding cookies.

**10.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

The disclosure of a privacy policy, including information on cookies in accordance with PIPA, is important and non-compliance with this requirement will likely result in an administrative fine of up to KRW 10,000,000.

## 11 Restrictions on International Data Transfers

**11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Korean laws distinguish the transfer of Personal Information from the outsourcing of Personal Information Processing. When a Controller transfers Personal Information of Data Subjects to a recipient for the benefit of such recipient, and such Personal Information is to be used by the recipient for the recipient's business, the Controller is supplying Personal Information. When supplying Personal Information of Data Subjects to a recipient in another jurisdiction, Controllers must notify Data Subjects about the recipient of the Personal Information and obtain their prior consent. To obtain proper consent, the Data Subjects must be notified of: i) the recipient's purpose for the Personal Information; ii) the details of the Personal Information to be supplied; iii) the period for which the recipient will retain and use the Personal Information; and iv) the right of Data Subjects to refuse to give consent, and disadvantages, if any, that may result from the refusal.

On the other hand, when a Controller provides Personal Information of Data Subjects to a recipient for its benefit, and Personal Information is to be used by the recipient for the Controller's business, the transfer of Personal Information will be considered to constitute outsourcing of Personal Information Processing. Regardless of the Outsourcee's jurisdiction, the Controller who outsources Personal Information Processing must post the scope of the outsourced work and the Outsourcee on its homepage. If the Controller is not an ICSP, Etc., no additional notification procedure or consent from the Data Subjects is required for the outsourcing of Personal Information Processing.

If the Controller is an ICSP, Etc., and wants to outsource Personal Information Processing to an Outsourcee in another jurisdiction, then it must notify Data Subjects of certain information related to the outsourcing and obtain their consent. The information must include: i) the particulars of the Personal Information to be transferred; ii) the country to which the Personal Information is to be transferred, transfer date and method; iii) the name of the Outsourcee (if the Outsourcee is a corporation, the contact information of the person responsible for the management of information must be provided); iv) the Outsourcee's purpose for the Personal Information; and iv) the period for which the Outsourcee will retain and use the Personal Information. In case of outsourcing of Personal Information Processing, the ICSP, Etc. may elect to include the required information within its privacy policy, send an email, or provide a written form, instead of obtaining separate notice and consent.

Notwithstanding the foregoing, an ICSP, Etc. in a country that restricts cross-border transfer may be subject to an equivalent level of restrictions. However, this will not apply where cross-border transfer is necessary to implement a treaty or other international arrangements.

**11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

As described in question 11.1, any transfer of Personal Information abroad will require some form of notice to Data Subjects, and consents where necessary. In case of outsourcing Personal Information Processing, the notice and consent may be replaced by the posting of the required notice in the Controllers' privacy policies.

**11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No such registration/notification is required.

## 12 Whistle-blower Hotlines

**12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

PIPA lacks provisions concerning corporate whistle-blowers. However, according to the Protection of Public Interest Reporters Act ("**PPIRA**"), anyone with knowledge that a company has violated or is likely to violate certain laws, including PIPA, the Credit Information Act and the Network Act, may report such wrongdoing to the representatives or employees of the company, an administrative agency, an oversight authority with the power to direct, supervise, regulate, or investigate such violation, or an investigative agency, etc.

PPIRA only applies when a company has violated or is likely to violate one or more provisions, the violation of which may result in: i) criminal punishment; ii) disposition to withdraw or cancellation of permits, authorisations, or licences granted by a governmental agency; iii) suspension of business; iv) corrective orders; or v) administrative fines, etc.

In the case that a report is made, the Personal Information of the reporter must be kept confidential, and no disadvantage may be given to the reporter.

**12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is generally permitted. Pursuant to PPIRA, however, the reporter must provide: i) his/her Personal Information such as name, resident registration number, address, and contact information; and ii) the identity of the violator of the laws covered by PPIRA, information about the violation, and purpose and reasons for the report.

## 13 CCTV

**13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The installation of CCTV in a public place is permitted only when necessary to: prevent and investigate crime; protect facilities and prevent fire; control traffic; collect, analyse, and provide traffic information; or when specifically permitted by law and no registration, notification, or prior approval from an authority is required for such use of CCTV.

In general, the installer must post a notice detailing: the purpose and place of installation; the range of the cameras' coverage and times of operation; and the name and contact information of the manager in charge.

**13.2 Are there limits on the purposes for which CCTV data may be used?**

Regarding the installation of CCTV in a public place, please refer to the answer to the question 13.1.

Regarding the installation of CCTV in a private area, this will be regarded as a means of collecting Personal Information and will usually require the prior consent of Data Subjects.

## 14 Employee Monitoring

**14.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

In general, any employee monitoring that must process Personal Information of an employee requires the employee's prior consent as a Data Subject under PIPA. Businesses typically obtain the employee's prior written consent when the employment contract with a new employee is executed.

Notwithstanding the practice, the Act on the Promotion of Workers' Participation and Cooperation provides that in a workplace with 30 or more employees, the company must establish a labour-management council which has the authority to determine the scope of employee monitoring tools in the workplace.

Even with such restrictions on monitoring, and despite the provisions in the Criminal Act that ban the reading of the contents of another person's sealed or secretly designed letter, document, or records in all media, the courts have ruled in favour of companies who have monitored employees without consent; for example, where a company had removed the hard disk of the personal computer of an employee on which the employee had set a password, to verify a rumour that the employee was embezzling the company's funds. The hard disk was connected to another computer, and searched using certain keywords, which resulted in the discovery of messenger conversations and emails that confirmed the suspicions.

In the criminal case against the company for the violation of the employee's privacy, the Supreme Court concluded that, under the circumstances – which required urgent and discreet action by the company where: i) it could specifically and rationally

suspect that the employee had engaged in a crime; ii) the scope of the access to the hard disk was limited to that related to the crime; iii) the employee agreed when joining the company not to use the company's computer without permission and to return all work-related results to the company; and iv) various materials that confirmed the employee's criminal activity were found as a result of the search – the company's act was justifiable and acceptable in accordance with social norms that were not punishable pursuant to the Criminal Act.

**14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Please see question 14.1.

**14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Please see question 14.1.

## 15 Data Security and Data Breach

**15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Controllers must take the technical, administrative, and physical measures necessary to secure the safety of Personal Information as prescribed by the PIPA Presidential Decree. The Outsourcee must also take similar measures, although Controllers also remain liable if damages arise due to an Outsourcee's failure to comply.

**15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Under PIPA, when Personal Information of 1,000 or more Data Subjects has been leaked, the Controller must notify the Data Subjects without delay, prepare and take measures to minimise the damage, and report the leak to PIPC or KISA with regard to such notifications and measures. When an ICSP, Etc. becomes aware of a leak, such ICSP, Etc. must, regardless of the number of Data Subjects affected, identify in its report the types of Personal Information leaked, the time of the leak, the measures that can be taken by the users, the countermeasures taken by it, and the contact information of its department managing the leak with which the users may consult. The report must be filed within 24 hours after the ICSP, Etc. becomes aware of such leak.

**15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

When Personal Information of Data Subjects has been leaked, the Controller must, without delay and regardless of the number of the Data Subjects affected, notify the Data Subjects of: the types of Personal Information leaked; the time of the leak; the reason for the leak; the measures that can be taken by the Data Subjects to minimise damages; the countermeasures taken by it and its procedures to remedy the damages to the Data Subjects; and the contact information of its department to which Data Subjects may report any damages incurred by them. If the Controller is an ICSP, Etc., it must notify the users as set forth in question 15.2 within 24 hours after becoming aware of such leak.

**15.4 What are the maximum penalties for data security breaches?**

The maximum penalties that may be imposed on each entity for a data security breach are as follows:

- A Controller that fails to implement technical, administrative measures may be administratively fined up to KRW 30,000,000.
- Where a Controller fails to take the necessary measures for data security required by PIPA, and Personal Information processed by such Controller has been lost, stolen, leaked, forged, altered or damaged, such Controller may be imprisoned for up to two years or criminally fined up to KRW 20,000,000.
- Where an ICSP, Etc. fails to take the necessary measures for data security discussed in the answer to question 15.1, and users' Personal Information processed by such Controller has been lost, stolen, leaked, forged, altered, or damaged, such ICSP, Etc. may be administratively fined up to 3% of its revenue relating to such violation.
- PIPC may impose and collect fines of up to KRW 500,000,000 if the resident registration number processed by the Controller is lost, stolen, leaked, forged, altered, or damaged.

## 16 Enforcement and Sanctions

**16.1 Describe the enforcement powers of the data protection authority(ies).**

| Investigatory/ Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| PIPC | PIPC may impose administrative fines or issue corrective orders to the violator of certain provisions of PIPA or other laws relevant to Personal Information protection. | PIPC may refer the violator of certain provisions of PIPA to the public prosecutor. |
| FSC | FSC may impose administrative fines or order the stoppage of business operations for a certain period to the violator of certain provisions of the Credit Information Act. | N/A |

| Investigatory/ Enforcement Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| KCC | KCC may impose administrative fines or revoke the permission or authorisation granted to a location information provider or a location-based service provider, or order the stoppage of business operations, for a certain period or permanently, if KCC finds non-compliance with certain provisions of the Location Information Act. | N/A |
| Public Prosecutors | None. | They may prosecute violators of certain provisions of PIPA or other laws related to Personal Information. |

**16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

PIPC, FSC and KCC may issue bans to violators of certain provisions related to Personal Information protection, and these bans do not require a court order.

**16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

In Korea, the data protection authorities tend to actively exercise their powers.

For example, in 2019, prior to the revision of the Network Act of 2020, KCC imposed a fine of more than KRW 1,800,000,000 on an e-commerce company for leaking the Personal Information of only 20 users in 2018, because the company had previously leaked Personal Information of its users in 2017.

During the three months from January to March 2019, the Ministry of Public Administration and Security, pursuant to PIPA (before its revision in 2020), imposed administrative measures on 91 entities due to violations of PIPA.

**16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

As previously mentioned, KCC administratively fined Google Inc. more than KRW 200,000,000 in 2014, because it had collected Personal Information of Data Subjects without their prior consent while developing its Street View service. According to KCC's report, KCC personnel visited Google's headquarters in the USA to verify that Google had destroyed the storage disk with the illegally collected data.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Korean laws do not provide any relevant rules on foreign e-discovery requests.

**17.2 What guidance has/have the data protection authority(ies) issued?**

There is no relevant guidance issued by any data protection authority.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

When a leak of Personal Information is confirmed, the data protection authorities check whether the Personal Information has been legally collected, the collected data were properly destroyed, and whether the Personal Information protection measures have been properly implemented pursuant to the applicable law. The amounts of administrative fines will depend on the types and numbers of violations of the legal requirements.

**18.2 What "hot topics" are currently a focus for the data protection regulator?**

As discussed in question 1.3, PIPA has been revised in 2020. Pursuant to the revised PIPA, Controllers may provide to another entity or use Personal Information without the consent of Data Subjects within the scope reasonably related to the initial purpose of the collection, considering whether the Data Subjects would be disadvantaged and whether the requisite measures have been taken to secure the Personal Information, such as encryption, etc.

The revised PIPA has special provisions concerning Pseudonymous Information. A Controller may process Pseudonymised Information without the consent of Data Subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc. The combination of Pseudonymised Information processed by different Controllers for statistical purposes, scientific research and preservation of records for the public interest, etc. may only be conducted by a specialised institution designated by PIPC or the head of the related central administrative agency. A Controller who intends to release the combined information outside the organisation that combined the information must obtain approval from the head of the specialised institution after processing the information into Pseudonymised Information. When processing any Pseudonymised Information, a Controller must take technical, organisational, and physical measures, such as separately storing and managing additional information needed for restoration to its original state, as may be necessary to ensure the safety of Personal Information from loss, theft, leak, forgery alteration, or damage. Finally, the processing of Pseudonymised Information for the purpose of identifying a certain individual is prohibited.

**Iris Hyejin Hwang** is an associate at D'LIGHT, where she specialises in litigation, local and international dispute resolution related to ICT & new technology, intellectual property, and entertainment & media. Prior to joining D'LIGHT, Ms. Hwang served as a corporate counsel at Neowiz Corporation where she advised on personal information protection, domestic and international IP licensing, content sourcing, distribution and investment matters relating to PC online/mobile games. Prior to Neowiz, Ms. Hwang was a corporate counsel at the Korea Creative Content Agency. She is a dispute resolution expert, having worked on a wide array of local and international litigation and dispute resolution matters involving PC online/mobile game, music and movie industry players in Korea and abroad. Ms. Hwang continues to serve as a mediator at the Korean Commercial Arbitration Board.

**D'Light Law Group**
5F, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: hjh@dlightlaw.com
URL: eng.dlightlaw.com

**Hye In Lee** is an associate at D'LIGHT, where she focuses on advising and assisting on litigation and legal issues in the ICT and FinTech industries, including blockchain systems. Ms. Lee also has extensive field experience in both international legal cases, such as global investment, M&A and international arbitrations, and local legal cases, including IP litigation, financing, investigations by the public prosecutor and/or the Korean Free Trade Commission, from her time as corporate counsel at Samsung C&T Corporation and Netmarble Corporation.

**D'Light Law Group**
5F, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: hil@dlightlaw.com
URL: eng.dlightlaw.com