Lee & Ko 법무법인(유) 광장

Understanding Data Privacy Law of Korea in International Air Transport

April 17, 2024

Partner(Attorney at Law) Young Joo Cho

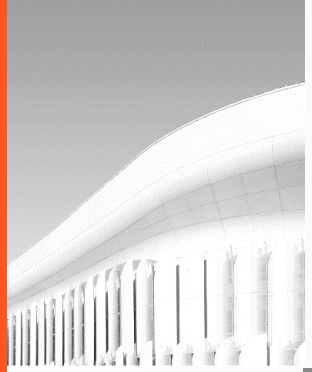
Mobile: +82.10.7484.3118

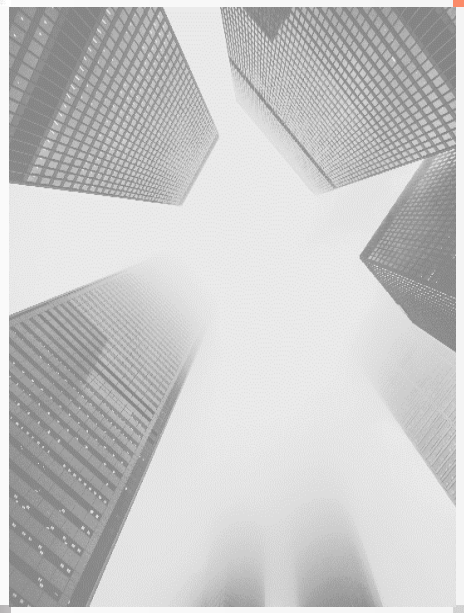
youngjoo.cho@leeko.com

Background

Why should we study data privacy law?

- Amidst the global emphasis for enhanced personal data protection, the aviation sector faces challenges due to conflicting regulations across countries. This complexity arises due to the sector's unique feature, wherein individuals from various nations are information principals subject to diverse data protection frameworks. The surge in regulations, particularly concerning air transport security and pandemic control, further complicates these matters.
- Accordingly, the significance of safeguarding data and personal information cannot be overstated. However, the current landscape is marked by inconsistent and contradictory laws of each States, often blending personal data protection regulations from different States. These regulations frequently do not align with the specificities of international civil aviation, causing difficulties for governments and airlines in the adoption and implementation of such laws.
- Therefore, this presentation will try to explain the main issues regarding data privacy law of Korea in international air transport.





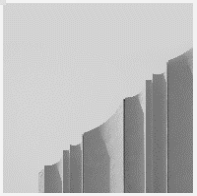


Table of Contents

I. Major Concepts in the Personal Information Protection Act

1. Personal Information

"Information relating to a living individual", "personal information" means the following:

- Information that **identifies a particular individual** by his or her full name, resident registration number, pictures, etc.
- Information which, even if it by itself does not uniquely identify an individual, may be **easily combined with other information to uniquely identify an individual**.
  - ✓ In such cases, whether or not there is **ease of combination** shall be determined by **reasonably considering the time, cost, technology**, etc. **used to identify the individual** such as likelihood that the other information can be procured.
- "**Pseudonymized information**", which is any of the above information that is pseudonymized.
  - ✓ Information that is incapable of uniquely identifying an individual **without the use or combination of information for restoration** to the original state
  - ✓ In some legislations such as the California Consumer Privacy Act does not regard "Pseudonymized information" as "personal information"
    - ❖ "**Anonymized information**" if any such information is **no longer capable of identifying an individual** even if additional information is used – no longer a "personal information" - EU, U.S. China also do not regard "Anonymized information" as "personal information"

Relevant Issues

- Information relating to a living individual
  - ✓ Not personal information if certain information is about a **deceased person, a corporate entity**, or an **organization**, or a **corporation**.
- Information that may be easily combined with other information to uniquely identify an individual
  - ✓ Behavioral information, and AD-ID: Although the **Personal Information Protection Committee ("PIPC") has yet to announce its conclusive opinion**, they may be deemed "personal information" depending on specific circumstances.

2. Personal Information Controller

A legal entity that processes personal information to operate the personal information files for the purpose of its work

- "**For the purpose of its work**"
  - ✓ Excludes personal activities, private relationships, etc.
  - ✓ Does not matter whether any compensation or personal benefit is involved
  - ✓ Requires an intent to continue and/or repeat (whether or not the processing was, in fact, done single time)
- "**Personal information files**"
  - ✓ A set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy search of the personal information (in forms of not only electronic database but also written materials)
  - ✓ Not "processing of personal information" if one-time notetaking or documentation

Distinguished concepts

- Personal information handler: An individual who processes personal information under command and supervision of a personal information controller, including any employees of a personal information controller.
- Personal information processing entrustee: An individual who processes personal information based on business entrustment by a personal information controller.

3. Major Laws & Regulations Other Than Personal Information Protection Act

Credit Information Use And Protection Act

- The term "credit information" means the information which is necessary to determine the creditworthiness of the counterparty
- also constitutes credit information if certain information can identify a specific data subject when combined with other credit information
- Personal credit information also constitutes personal information, but it is governed by the Credit Information Use And Protection Act and is **subject to stricter laws and regulations than personal information generally is**.

Act On The Protection And Use Of Location Information

- The term "location information" means information about a place whose position is located by using telecommunications equipment facilities, etc.
  - ✓ GPS information is one example, and information simply stating when and where a person visited is not location information.
- Where a person intends to conduct a business using location information, such person needs to obtain a location information business or location-based service **business license** depending on the specific details of the intended business.

II. Step-by-Step Issues in Personal Information Processing

1. Collection and Use of Personal Information

Principle – Consent of the Data Subject (Information Provider)

- Statutory Notification Items
  - ✓ Must **notify** "i) the **purpose** of the collection and use of personal information; ii) **particulars** of personal information to be collected; iii) the **period** for retaining and using personal information; and iv) the fact that the data subject is **entitled to deny consent**, and disadvantages, if any, resulting from the denial of consent".
  - ✓ If any of the notified information is changed, must notify again and **obtain consent again**.
  - ✓ Use outside the scope of the purpose for which certain information was collected is **prohibited as 'outside-purpose use'**.
- Must **notify in advance** whether to collect or user the information

Exceptions

- Where there is a **special provision** in the **law** or it is **necessary to comply with a legal obligation**.
  - ✓ E.g., medical record keeping under the Medical Service Act and age verification obligations under the Youth Protection Act
- Where **necessary to fulfill a contract** or to take steps at the request of the data subject in the course of entering into a contract
  - ✓ Applicable to **employment relationships** (e.g., collection of bank account information for wage payment)
- Other exceptions do exist on an extremely limited basis

2. Third-Party Provision and Processing Entrustment of Personal Information

Third-Party Provision of Personal Information

- Principle – **Consent** of data subject
  - ✓ Must **notify** "i) person who will be receiving the personal information; ii) use purpose(s) of the person who will be receiving and using the personal information; iii) retention and use period for the received personal information; and iv) the fact that the data subject has a right to deny consent, and disadvantages, if any, resulting from the denial of consent".
  - ✓ Must obtain consent **separately from the consent to use and collection** of personal information

- Exception – where provided to a third-party within the scope of the collected purpose in accordance with the exceptions applicable to the use and collection of personal information
  - ✓ Where there is a **special provision in the law or it is necessary to comply with a legal obligation**.
  - ✓ In the case of international air transportation, the collection of personal information for immigration inspection under the **Immigration Control Act** (Articles 6, 12, 12-2 of the Immigration Control Act), quarantine inspection under the Quarantine Act (Article 12 of the Quarantine Act), request for **passenger reservation data** (Article 29-4 of the Quarantine Act), and confirmation of identity under the **Aviation Security Act** (Article 14-2 of the Aviation Security Act) may serve as legal grounds for the processing of personal information. As such, processing of Personal Information without the consent of the Data Subject may occur within the scope of such regulations.

- Providing personal information to third-party for **purposes other than** those for which it was collected **requires separate consent** or an exception, such as special provisions in other laws and regulations is needed.

2. Third-Party Provision and Processing Entrustment of Personal Information

Processing Entrustment of Personal Information

- Does **not require prior consent** of data subject

- It is similar to third-party provision in a sense that personal information is transferred to a third-party, but third-party provision is for the business processing and interests of the recipient, whereas **processing entrustment is for the business processing and interests of the personal information controller**.

  ✓ E.g., - business association, and sales of personal information = third-party provision of personal information/ entrument of the operation of call-center and website = processing entrustment of personal information

- Must meet certain requirements, such as **entering into a personal information processing entrustment agreement**, **disclose** the entrusted tasks and the entrustee in the privacy policy, etc.

- Entrustor must manage and supervise the enstrustee, and the entrustor may be held liable if a data subject claims damages due to the enstrustee's violation of the Personal Information Protection Act.

3. Cross-Border Transfer of Personal Information

Meaning of Cross-Border Transfer

- Includes provision to third parties outside of the country, access outside of the country, entrustment of personal information processing outside of the country, and storage of personal information outside of the country.
- Since the cross-border transfer includes mere 'storage', it may constitute cross-border transfer if a foreign entity directly collects personal information. cross-border collection of personal data directly by a foreign entity may also constitute a cross-border transfer.

Requirements for Cross-Border Transfer of Personal Information

- Principle – **separate consent of data subject**
  - ✓ Must notify "i) particulars of the personal information to be transferred; ii) the country to which the personal information is transferred, transfer date, and method; iii) name of the recipient of personal information (referring to the name of a corporation and the contact information of the corporation, if the recipient is a corporation); iv) the purpose of using personal information by the recipient of personal information and the period of retention and use of personal information; and v) the method and procedure for refusing the transfer of personal information and the effect of such refusal."
- Exception applies in the cases of overseas processing entrustment or overseas storage of personal information.
  - ✓ Exception applies where certain cross-border transfer is **necessary for execution or performance of contracts**, on the premise that the above notification items have been disclosed in the privacy policy.
- Cross-border transfer is permitted where it is recognized that **the personal information protection system of the country or international organization to which the personal information is to be transferred is substantially equivalent to the Personal Information Protection Act of Korea**.
  - ✓ Adopted with reference to the relevant provisions in the European General Data Protection Regulation (GDPR). However, **no country/international organization has yet to be recognized** as such since the amendment is still in its early stages.

Personal Information Protection Commission to issue a cease order in the event of cross-border transfer in violation of the Personal Information Protection Act

4. Destroying Personal Information

When to Destroy Personal Information

- Upon the **expiry of the retention period** notified at the time of collection
- When the personal information becomes unnecessary, such as achieving of the purpose of processing the collected personal information
  - ✓ E.g., **cancellation of membership, termination of business**, etc.

Where Necessary to Preserve Personal Information Pursuant to Other Laws and Regulations

- Where there is a document retention obligation under certain laws and regulations
  - ✓ Material documents under the Labor Standards Act– must preserve for three (3) years (e.g.,– employment agreement shall be preserved for a period of three (3) years after resignation)
  - ✓ Must be stored and handled apart from other personal information

To be completely destroyed in a form that cannot be restored or reproduced again

III. Issues and Cases of Personal Information Leakage

1. Issues Related to Personal Information Leakage

Concept of 'Leakage'

- Allowing **access to unauthorized persons** due to a loss of control by the personal information controller, other than by applicable law or the personal information controller's free will.

How to react to Incidents of Personal Information Leakage

- **Notification to Data Subject**
  - ✓ Must notify within **72 hours** of becoming aware of the incident
  - ✓ Must notify personal information items leaked, when and how they were leaked, what the data subject can do to minimize the damage, the personal information controller's responses taken or to be taken and damage remediation procedures, and the department and contact person in charge.
  - ✓ If there are data subjects whose **contact information is unknown, must post on the website for at least 30 days** (usually both individual notification and website notification are made)
- **Report to the Personal Information Protection Committee or the Korea Internet & Security Agency**
  - ✓ Must report when more than 1,000 people are leaked / sensitive or uniquely identifiable information is leaked / leakage due to Illegal access from outside (hacking, etc.).
  - ✓ Must report within **72 hours** of becoming aware of the incident

2. Legal Responsibilities (Relevant Cases)

Sanctions Imposed of Incidents of Personal Information Leakage

- Investigate whether the **security technology and policies taken by the personal information controller were appropriate**
  - ✓ "Standards for Measures to Secure the Safety of Personal Information", promulgated by the Personal Information Protection Commission, applies
  - ✓ Investigation involves **comprehensive consideration** of the level of **generally known information security technology**, the degree of economic cost and utility required for information security, the **level of hacking technology actually used**, etc.

> In an appeal against a regulator's imposition of a fine, the court ruled that it is difficult to conclude that the personal information controller's safeguards taken were insufficient.

- **Fines and penalties may be imposed for violations of safeguards standards or insufficient measures**.
  - ✓ Penalties are calculated at no more than **3% of "(total revenue - revenue not related to the violation)"** – where violation is of **minor importance, penalties can range from 0.03% to 1%, but can be 2% or more in very serious cases**.

> There was a case where a penalty of **KRW 1 billion (around 750,000 USD) was imposed** where the leakage of personal information occurred due to credential stuffing (a method of stealing personal information when logging in by entering an already stolen ID or PW), which resulted in about 800,000 cases of personal information being leaked

  - ✓ Amendments to the Personal Information Protection Act have changed the threshold for penalties, which could result in higher fines under current standards.

2. Legal Responsibilities (Relevant Cases)

Damages Claim From Data Subjects

- Only requires proof of the personal information controller's violation of the law and the damages incurred to the data subject.
- Damages may be awarded **even if a causal link between the violation of the law and the personal information leakage is not established**, or if the data subject fails to demonstrate specific damages.

Damages of KRW 50,000 to 200,000 won per data subject who suffered leakage are being imposed, but the current trend is to find greater responsibility in personal information controllers

Criminal Punishment Imposed on Those who Leaked Personal Information (Hackers, Employees, etc.).

2. Legal Responsibilities (Relevant Cases)

No cases yet confirmed in which the Korean authority imposed penalties on airlines

- Personal Information Protection Committee ("PIPC") did discuss with the **aviation industry officials on ways how to strengthen the level of personal information protection around November 2023**. Given the characteristics of the aviation industry, particularly emphasis was placed on restrictions on the processing of sensitive information and unique identification information and compliance with the PIPA regarding the provision of personal information to third parties and overseas transfers.
- In this regard, any airline operating in Korea which does not comply with PIPA, such as without consent processes sensitive information and personally identifiable information or provide personal information to a third party, then the airline or a person in charge of business **may be subject to imprisonment of five (5) years or less or a fine of up to KRW 50 million**. Also the airline may be imposed a penalty surcharge of up to **3% of its total sales** (excluding sales that are not related to the violation). In addition, the airline may be subject to a **fine of KRW 30 million or less** if the airline breaches its obligation to take safety measures, such as encrypting sensitive information and personally identifiable information.
- Further, if an airline fails to comply with any legal requirements, such as the disclosure of its privacy policy on matters related to separate consent for **overseas transfer or entrustment of processing and storage**, the airline may be ordered to suspend overseas transfer from the Personal Information Commission and may be imposed with a **penalty of up to 3% of total sales**. In case the airline breaches of its obligation to take safety measures for overseas transfers, the airline may be subject to a **fine of up to KRW 30 million**.

2. Legal Responsibilities (Relevant Cases)

A prison term for the unauthorized sale of personal information (November 25, 2020, Korean Press)

- Daegu District Court sentenced a defendant who **sold personal information** in exchange for money to **one year and six month imprisonment** and **payment of approximately KRW 301,000,000** (around USD 224,000) penalty. The defendant sold personal information (including phone number) of 32,000 persons in exchange for KRW 301,000,000. The judge explained that prison sentence was necessary because substantial amount of personal information was sold and there is high possibility that such information would be used for fraud.

Police had a raid on gambling place of Person X based on a phone call. Person X asked the police for the identity of the caller and police told Person X of the last four digit of the caller's mobile phone number

- Even if it is not possible to make identification just with the **last four digits of mobile phone number**, such information can be **easily combined with other relevant information** (e.g., birthday, home phone number, phone number of family members, etc.) to identify an individual and such possibility is even greater if such information is provided to a person who has personal connection with the owner of the phone number. l (Nonsan Branch, Daejeon District Court, 2013godan17, August, 9, 2013)

2. Legal Responsibilities (Relevant Cases)

Data breach of an online job searching website resulted in unlawful access to a cover letter with a photograph of an applicant

- A **portrait or likeness of a person** is one of the oldest and definite way of identifying a person and is information identifying a particular person, same as a name or resident registration number (Seoul High Court, 2008na25888, November 25, 2008)

Phone call records acquired during police investigation

- The Supreme Court held that **phone call records** are personal information (Supreme Court, 2008do5526, October, 23, 2008)

IV. Major Contents of the Amended Personal Information Protection Act

III. Major Contents of the Amended Personal Information Protection Act

Major Contents of the Amendment Dated September 15, 2023 (Currently in Effect)

- **Online-offline consolidated regulations**
  - ✓ Consolidated previously separate regulations for processing personal information through online services and offline processing of personal information

- **Expanded imposition of penalties**
  - ✓ Expanded penalties from being imposed only on violations of laws related to the processing of personal information through online services **to cover all forms of personal information processing**
  - ✓ Changed the basis for calculating penalties from '**revenue related to the violation' to 'total revenue'**

> As compared to the past, **much higher penalties may be imposed** for violation of the Personal Information Protection Act

Major Contents of the Amendment to be Effective as of March 15, 2024

- Ensure data subjects' right to object to and request an explanation of decisions made by processing personal data with "automated systems (including AI)'

III. Major Contents of the Amended Personal Information Protection Act

Major Contents of the Amendment to be Effective as of September 15, 2024

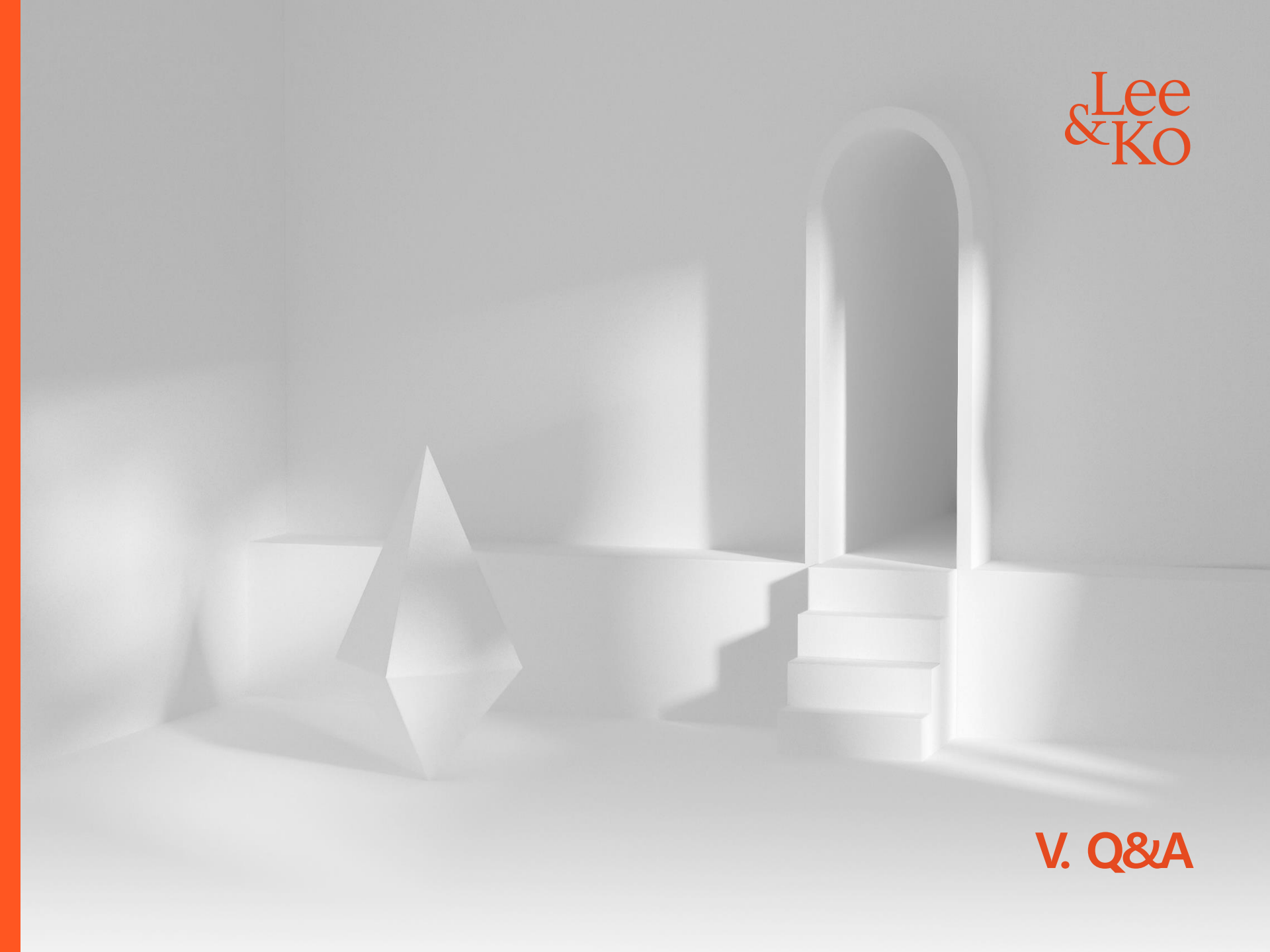
- When obtaining consent to the processing of personal information, one must allow the data subject to freely decide whether to consent or not.

The Personal Information Protection Commission intends to **reform the current practices of 'mandating consent to data subjects'**

Major Contents of Other Amendments (Effective Dates Unknown)

- Create a right of data subjects to request to personal information controllers over a certain size to transfer personal information.

Subject personal information controllers, criteria for personal information subject to such transfer request, etc. have not been determined.



V. Q&A

Young Joo Cho
Mobile: +82.10.7484.3118
youngjoo.cho@leeko.com

Thank you

Lee & Ko