



PIPC Clarifies the Applicability of PIPA for Foreign Companies

2024.05.03

Background

On April 4, 2024, the Personal Information Protection Commission (**PIPC**) published a *Handbook on the Applicability of the Personal Information Protection Act to Foreign Business Operators (Handbook)*. The Handbook establishes clear standards to help foreign companies understand when and how they become subject to the Personal Information Protection Act (**PIPA**) requirements. Read on to find out more about the specific obligations the Handbook outlines for covered businesses.

Key Aspects

1. Businesses subject to the PIPA.

The Handbook explains that foreign companies may find themselves subject to the PIPA in the following circumstances: (i) where a company provides goods or services to Korean data subjects, (ii) where a company's data processing activities (involving Korean data subjects) have a direct and significant impact on Korean data subjects, or (iii) where a company maintains a place of business within the state borders of Korea.

a) Provision of goods or services to Korean data subjects

A foreign company deemed to target Korean consumers, taking into account various factors such as the language and the currency supported and the manner in which the company's service(s) is provided, can expect a higher likelihood that the PIPA will govern their business practices.

As state borders are becoming more blurred in today's economy, the Handbook provides some concrete examples to help foreign companies assess whether their business models would trigger the PIPA:

PIPA <u>applies</u> if a company:	PIPA <u>does not apply</u> if a company:
•holds itself out as a service provider for Korean data subjects	•provides accommodation services abroad and collects/uses personal data of Korean guests
•operates a website with a country-code domain (.kr) or local code (ko-kr) for Korea	•operates a business operating system hit with a cyberattack, which results in a data breach that affects its Korean employees based overseas
•launches in the app market goods/services targeted at Korean consumers	•does not provide delivery services to Korea, requiring Korean data subjects to receive products purchased on the company's online mall through international parcel forwarding service providers
•supports only Korean in the course of providing its services (irrespective of its terms stating that the laws of another jurisdiction shall govern)	•explicitly limits the use of its services by Korean data subjects by, for instance, blocking Korean IP addresses for its shopping mall(s) or refusing to launch its services in Korean app markets (irrespective of whether Korean data subjects are able to bypass such restrictions)

b) Data processing activities with a direct and significant impact on Korean data subjects

Even where a foreign company does not target Korean data subjects, the company may still be governed by the PIPA if the company can reasonably foresee that its processing of Korean data subjects' personal information will have a direct and significant impact on Korean data subjects.

According to the Handbook, such impact can be anticipated where a company (i) provides a service based on its collection of personal information of Korean data subjects which the company discloses on its website or (ii) processes personal information of Korean data subjects (a) in the course of servicing Korean companies, (b) based upon an agreement entered into with a Korean company to process the personal information, or (c) in order to further its business interests upon receipt of Korean data subjects' personal information from Korean companies (e.g. for AI model development).

c) A place of business maintained in Korea

The Handbook also states that the PIPA can also come into play where a foreign company maintains a place of business in Korea where data processing activities take place, although a case-by-case analysis would be required in such instances to confirm the relevance between the foreign company's data processing activities and the operations undertaken by the local entity. For instance, where a foreign company forms a local entity in Korea for software sales and maintenance while operating an online mall outside Korea that does not target Korean consumers, the Handbook clarifies that the PIPA may not extend to the foreign company's operations of the online shopping mall outside Korea.

Meanwhile, in cases where a foreign company designates its local entity in Korea as the personal information controller for Korean data subjects, the Handbook provides that the local entity so designated will become subject to the PIPA.

2. PIPA requirements that foreign companies should closely observe.

As a rule, each entity subject to the PIPA, whether domestic or foreign, must ensure compliance with all applicable PIPA requirements. Noting the unique circumstances of foreign companies, however, the Handbook outlines several requirements that foreign companies must satisfy but often overlook.

Issue	Description
Data breach	<ul style="list-style-type: none"> • Notice to affected data subjects and reporting to the competent authority must be made within 72 hours of becoming aware of a data breach. • A company is deemed to have constructive awareness of a data breach with implications for Korean data subjects even where the extent of the incident is not fully ascertained if the company (i) is aware of a data breach incident and (ii) does not manage its personal information system by classifying data/data subjects for each county in which they operate.
Privacy policy	<ul style="list-style-type: none"> • A privacy policy written in Korean must be set in place. A mere translation of a privacy policy originally prepared under the laws of another country will not suffice. • Among others, the privacy policy must specify the personal information controller processing the personal information of Korean data subjects, the fact that data processing occurs overseas (where applicable), and the country in which the processing takes place.
Data subjects' rights	<ul style="list-style-type: none"> • There must be specific methods and procedures that allow Korean data subjects to easily exercise their rights over their personal information. Information about such methods should be available in Korean. • If foreign laws limit the disclosure of personal information requested by Korean data subjects, a company should evaluate whether: (i) it is subject to such non-disclosure requirement, (ii) the non-disclosure obligations under such foreign laws align with the Constitution and related laws of Korea, and (iii) the need to adhere to the foreign law overrides the data subject's rights.
Consent from legal guardians (applicable when dealing with data subjects under 14 years of age)	<ul style="list-style-type: none"> • Personal information of children under the age of 14 must not be collected without the consent of their legal representatives.
Damage Relief	<ul style="list-style-type: none"> • A foreign company's headquarters and its Korean entity must each assess whether it is required to purchase insurance or accumulate reserves to cover potential liabilities for damage compensation.
Domestic agent	<ul style="list-style-type: none"> • Foreign companies required to designate a domestic agent are advised to appoint an entity they have founded in Korea or one over which they have significant control. • Note that if the domestic representative uses recorded audio to direct consumers to email or online forms or is unable to address consumers' complaints or claims for damages, the foreign company may be deemed to not have appointed a domestic

	representative.
Personal information processing	<ul style="list-style-type: none"> •Foreign companies must carefully assess whether their activities constitute a “third party provision” or “outsourcing of the processing” of personal information and ensure they meet applicable requirements.
Regulatory investigations	<ul style="list-style-type: none"> •The PIPC has the authority to issue RFIs to investigate (non)compliance with data privacy laws. The PIPC can also cause government officials to enter foreign companies’ business premises to obtain statements from relevant individuals and examine books or records. • If necessary, the PIPC may further demand appearance or statements from the foreign company’s personnel.
Corrective order and sanctions	<ul style="list-style-type: none"> •Upon a finding of a legal violation, a foreign company may be ordered to cease infringing activities, suspend its data processing activities, or take required actions to prevent subsequent violations. • A company deemed non-compliant may also face an administrative penalty of up to 3% of its global revenue, a criminal referral to investigative authorities, disciplinary actions, and/or a public announcement of its non-compliance and resulting regulatory sanctions.

Key Takeaways

The increasing number of global services offered to Korean data subjects has prompted hotly debated discussion on whether and how the PIPA should apply to foreign companies.

With detailed examples, the Handbook aims to guide foreign companies through their PIPA obligations. However, there are unresolved ambiguities. For instance, there is no guidance on how the level of “direct and significant impact” on Korean data subjects is to be determined. The Handbook also states that a determination of whether a company provides goods or services to Korean data subjects will be made based on consideration of various factors, suggesting that the PIPA’s reach may go far beyond the stakeholders’ expectations.

Since a finding of non-compliance with the PIPA can have serious implications for foreign companies operating across the globe, companies conducting operations in Korea or otherwise servicing Korean data subjects should review and amend their business practices to ensure compliance with the PIPA.

Key Contacts

Sinook Kang

Hyein Lee

Senior Partner

+82-2-316-4059
sokang@shinkim.com

Senior Foreign Attorney

+82-2-316-1641
hilee@shinkim.com

Jihyun Kang

Partner

+82-2-316-1518
jhykang@shinkim.com