[Unofficial Translation]

Personal Information Protection Commission

Press Release

The PIPC Announces Status Examination Results of DeepSeek Service

- Recommendation for correction: Having robust legal bases for cross-border data transfer; destructing user-entered data transferred to Volcano; and enhancing transparency in providing services
- Recommendation for improvement: Implementing stronger safeguards recommended by the PIPC; checking whether children's personal data is collected and destructing such data; overhauling overall personal data processing systems and upgrading safety measures; and designating a domestic agent

April 24, 2025
(This is an unofficial translation of a press release, originally prepared in Korean.)

The Personal Information Protection Commission (PIPC) held its ninth plenary meeting of 2025 and concluded deliberations on status examination results of Hangzhou DeepSeek Artificial Intelligence Co., Ltd. (DeepSeek) on April 23, 2025.

Developments in Response to DeepSeek

Amid the privacy concerns over DeepSeek after the launch of its R1 Large Language Model (LLM) AI chatbot, the Personal Information Protection Commission (PIPC) sent an inquiry to DeepSeek on January 31, 2025, and initiated a technical analysis with the Korea Internet & Security Agency (KISA) on how this chatbot functions. The technical analysis found out traffic generated by third-party data transfer and insufficient transparency in DeepSeek's privacy policy.

In this regard, the PIPC started conducting a status examination on DeepSeek. The status examination scheme aims to proactively identify privacy vulnerabilities to prevent potential breaches and issue recommendations if breaches are found. At the early stage of the status examination, DeepSeek said that it failed to consider the legal requirements pursuant to the Personal Information Protection Act (PIPA) before launching its service in Korea and showed its willingness to comply with the PIPA. Meanwhile, DeepSeek temporarily suspended new downloads of its chatbot service on Apple's App Store and Google Play until necessary updates are implemented to ease privacy concerns raised among the Korean people.

The PIPC closely examined the company's data processing practices and compliance efforts, and the following explains the status examination results of DeepSeek.

1. Privacy Policy

When launching its services in Korea on January 15, 2025, DeepSeek only provided its privacy policy in Chinese and English. Before the status examination, its privacy policy was found to have insufficient transparency as required by the PIPA as follows:

i) Lack of information on procedures and methods regarding personal data destruction;
ii) Lack of the details of safeguards put in place; and
iii) The details of a chief privacy officer (CPO), such as name and contact information.

Additionally, the privacy policy also referenced the collection of a wide range of information, including keystroke patterns and rhythms.

During the status examination, DeepSeek submitted a Korean version of its privacy policy by specifying the legal requirements pursuant to the PIPA, such as legal bases for data processing, the retention period, destruction procedures and methods, the details of a CPO, among others, on March 28, 2025. The company clarified that the collection of users' keystroke patterns was listed in the privacy policy, but it did not collect such patterns. DeepSeek revised its privacy policy to specify what kind of personal information is collected and the PIPC confirmed such claims during the status examination. A Korean version of DeepSeek's privacy policy, and jurisdiction-specific clauses, will be disclosed via its website and application when resuming new downloads of its R1 LLM chatbot services.

2. Cross-border Transfer of Personal Data

DeepSeek transferred users' personal data to servers located in China and the U.S. to improve service functionality, security, and customer support. Still, it failed to obtain separate consent from users regarding cross-border data transfer and disclose the fact in its privacy policy with the launch of its services in Korea. Moreover, DeepSeek transferred the details of device information, user networks, applications, and user input to Beijing Volcano Engine Technology Co., Ltd. (Volcano).

Throughout the status examination, DeepSeek added the legal requirements associated with cross-border data transfer in its privacy policy and submitted to the PIPC. Regarding data transferred to Volcano, the company explained that it used Volcano's cloud service to improve security vulnerabilities, user interface (UI), and user experience (UX). As the PIPC pointed out, the transfer of user input is not necessary; DeepSeek has blocked the transfer of user input since April 10, 2025. DeepSeek claimed that Volcano is a subsidiary of ByteDance, but it is an independent corporation. The data entrusted for processing is used for service operation and improvement, not marketing. The company expressed willingness to meet the legal requirements and comply with due process under the PIPA to safeguard personal information.

3. User Input for AI Model Development and Training

DeepSeek used publicly available data, such as open-source data, and data collected by webscraping, and user-entered data for its AI development and training as other AI service providers do, but failed to provide users with features to opt-out of providing user input for AI development and training. Its privacy policy also failed to provide sufficient information and user notification regarding user input for AI development and training.

During the status examination, DeepSeek has added opt-out features associated with providing user-entered data for AI development and training since March 17, 2025, and notified the PIPC. Last year, the PIPC conducted a status examination of a few major generative AI services and made some recommendations for improving their services. Recommendations include:

- Privacy redaction by considering the list of URLs published by KISA and the PIPC when preparing AI training data. The URLs are deemed to be high-risk websites with possibilities of containing illegitimate personal data that includes resident registration numbers (RRNs), mobile numbers, and account numbers;
- Clear user notification to inform that its AI models will be trained on user-entered data, and providing users with opt-out features to respect their right to choose; and
- Specific details regarding data processing flows associated with AI.

Following the PIPC's recommendation, DeepSeek has agreed to implement stronger safeguards.

4. Age Verification and Other Safeguards for Children

DeepSeek claimed that it does not collect children (those aged below 14), but it lacked an age verification procedure to check whether a user is a child when joining the services. However, the company established an age verification procedure during the status examination. The PIPC found out that DeepSeek has taken necessary measures to address security vulnerabilities identified, such as complacency in access control to the developer servers' database, insufficient prevention of directory listing, among others, during the status examination.

Administrative Disposition and Future Plans

The PIPC decided to issue recommendations for correction on DeepSeek to enhance transparency in providing services on an ongoing basis as follows:

- Having robust legal bases for cross-border data transfer;
- Destructing user-entered data transferred to Volcano's server immediately, and
- Disclosing its privacy policy in Korean.

Moreover, the PIPC decided to issue recommendations on DeepSeek to improve its data practices as follows:

- Complying with stronger safeguards recommended by the PIPC based on last year's

status examination on major generative AI services;
- Checking whether children's data is collected and destructing such data;
- Upgrading overall safety measures for its data processing system; and
- Designating a domestic agent.

When DeepSeek accepts the PIPC's recommendations for correction within 10 days, it is deemed to have received them. DeepSeek is required to inform the PIPC of its implementation results within 60 days. The PIPC will monitor DeepSeek's implementation status at least twice and keep an eye on its compliance status to align with the PIPA.

Meanwhile, the PIPC provides "Compliance Checklists for Foreign Business Operators," based on "Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators," released in April 2024, on the occasion of the status examination of DeepSeek. The compliance checklists help foreign business operators respect the Korean data subjects' rights and promote data protection by looking into the legal requirements to be met before launching and operating their services.

[Unofficial Translation]

Compliance Checklists for Foreign Business Operators

Preface

- As global service roll-outs have become commonplace, more and more foreign businesses are operating in Korea, leading to an increase in data breaches. In this regard, the Personal Information Protection Commission (PIPC) provides compliance checklists to meet the legal requirements of the Personal Information Protection Act (PIPA) for foreign business operators.

  For more information, please refer to "Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators", released in April 2024.
  (How to access: www.pipc.go.kr > Law & Guidelines > Guidelines)

- Privacy laws and compliance requirements vary from jurisdiction to jurisdiction; however, foreign business operators are required to conduct a prior review to respect the Korean data subjects and uphold their privacy rights.

- Where a service has a significant impact on the Korean data subjects, the PIPA may apply to foreign business operators. They can rely on a "Prior Adequacy Review Mechanism" before they launch their services in Korea to comply with the PIPA.

  Application Criteria: Whether a foreign business operator provides goods or services to the Korean data subjects, its processing has an impact on the Korean data subjects, or a foreign business operator has an establishment in the Korean territory.
  Contact: adequacy@korea.kr

1. Writing and Disclosing a Privacy Policy

	Items to be Checked	Tick
1	Writing and disclosing a privacy policy in Korean	☐
2	Clarifying a personal data processor that processes the personal information of the Korean data subjects	☐
3	When processing personal information outside of Korea, clarifying that fact, the name of the country, and the entity ● The personal data to be processed ● The purposes of the processing ● The processing and retention periods ● The details of third-party provision ● When and how to destruct personal information ● Potential disclosure of sensitive data or how to choose not to be disclosed ● The details of entrustment ● The details of pseudonymization ● How to exercise rights and duties as a data subject and legal representative ● The name and contact details of a Chief Privacy Officer (CPO) and the relevant department for lodging a complaint ● The lawful basis for cross-border transfer ● The name of a country when personal information is collected outside of Korea ● The details of safeguards ● The details of the installation and operation of automatic devices to collect personal information ● The details of changes to the privacy policy	☐
4	Writing and disclosing a privacy policy that covers all the legal requirements pursuant to the PIPA * Not literally translating the existing privacy policy with a focus on other jurisdictions' legal frameworks (ensuring compliance with the PIPA is required) * Clearly distinguishing between the 'entrustment of processing' and 'third-party provision'	☐
5	Using the term "Privacy Policy" to place it on the website, among others	☐
6	Stipulating the categories of personal information processed without consent and the relevant legal basis	☐

2. Cross-border Data Transfer

	Items to be Checked	Tick
1	Meeting the legal requirements regarding whether cross-border data transfer takes place * The provision, entrustment of processing, or storage of personal information to an entity outside of Korea falls under the purview of cross-border data transfer ● Obtaining separate consent needed when providing personal information ● Stipulating the fact of entrustment of processing or storage of personal information in a privacy policy	☐
2	Putting safeguards in place, lodging a complaint, or applying for dispute settlement, or other privacy-safeguarding measures	☐

3. Domestic Agent

	Items to be Checked	Tick
1	Designating a domestic agent in cases where a business has no address or establishment in Korea, and its sales revenues or amount of personal data held exceeds a certain extent	☐
2	Designating a domestic agent in cases where the PIPC requests the submission of required data, on-site examination, or statements of officials	☐
3	Disclosing the details of a domestic agent, e.g., the name, address, phone number, and email, in a privacy policy	☐

4. Entrustment of Personal Data Processing

	Items to be Checked	Tick
1	Including the legal requirements when you entrust the processing of personal data to another entity ● Prohibiting personal data processing beyond the purposes of entrustment ● The purposes and scope of the entrustment ● Restriction on re-entrustment ● Access control and other safeguards ● Overhauling of the management of entrustment and other supervisory affairs ● Compensation when an entrustee fails to comply with legal obligations	☐
2	Providing compliance training to an entrustee, overhauling the status of data processing, and other supervisory affairs	☐

5. Special Category Data

	Items to be Checked	Tick
1	Obtaining consent of a legal representative when processing a child's personal information (a child aged below 14 under the PIPA)	☐
2	Verifying the age information of a data subject to see whether the data subject is a child * In a way that the data subject enters birth dates, or using a self-authentication service	☐
3	Prohibition on the processing of sensitive data in principle (Notifying statutory information and obtaining separate consent for the collection)	☐
4	Prohibition on the collection of resident registration numbers (RRNs) without a legal basis * RRNs should be redacted for the collection of ID cards (resident registration certificate, passport, and others)	☐
5	Notifying statutory information and obtaining separate consent for the collection of passport, driver's license, or foreign resident registration numbers	☐

6. Respecting the Rights of Data Subjects

	Items to be Checked	Tick
1	Preparing a channel for the data subjects to exercise their rights (via the websites, apps, email, or phone number)	☐
2	Processing a request of the data subjects regarding their right to access, rectification,	☐

	erasure, and restrict processing, and notifying the results within 10 days	
3	Notifying a reason when rejecting the request for access or others, and rendering the provision or access after the reason no longer applies	☐

7. Safeguards

	Items to be Checked	Tick
1	Implementing technical, organizational, and physical safeguards ● Establishing internal management plans and overhauling ● Restriction on access authority ● Access control measures ● Encryption-at-rest and encryption-in-transit ● Storage and overhauls of access logs ● Anti-malware software	☐

8. Notifying and Reporting a Data Breach

	Items to be Checked	Tick
1	Notifying the data breach of the affected data subjects within 72 hours	☐
2	Reporting a data breach affecting 1,000 individuals or more, revealing sensitive data or personally identifiable information, or caused by hacking and other illegal access, within 72 hours * The PIPC or the Korea Internet & Security Agency (KISA) and the link is available here	☐
3	Taking measures after becoming aware of a data breach and implementing countermeasures to mitigate damages	☐

9. Development and Deployment of AI Services (Recommendation)

	Items to be Checked	Tick
1	Implementing technical and organizational measures when processing publicly available data for the development and deployment of AI services ● Verification and management of training data provenance ● Prevention of personal data leaks and exposure ● Safe storage and management of personal information ● Adding safeguards through fine-tuning ● Applying prompt and output filtering ● Specific data redaction from the training results ● Establishing processing standards for training data and disclosing them in a privacy policy ● Considering to carry out a data protection impact assessment (DPIA) ● Safeguards tailored to the development and deployment of AI, such as open-source models, application programming interface (API), etc.	☐
2	Ensuring users' rights to choose, such as providing features to delete user-entered data and opt-out of AI model training	☐
3	Redacting identifiers, data, or personal information of users in training datasets when utilizing user-entered data for AI model training, and notifying the fact of human intervention to users	☐