개인정보보호위원회	Press Releases	다시 대한민국! 새로운 국민의 나라

At press time	**Thursday, April 24, 2025, 12:00 PM**	**Deployment**	**Wed, Apr 23, 2025, 18:00**
	(Thursday, April 24, 2025, three hours)		

Personal Information Protection Commission releases results of preliminary inspection of DeepSeek service

■(Corrective Recommendation) Ensure legal basis when transferring personal information overseas and immediately destroy personal information already transferred, and continue to enhance service transparency by disclosing and specifying Korean processing policies

■ (Recommendation for Improvement) Compliance with the enhanced safeguards recommended by the Personal Information Protection Commissioner in relation to artificial intelligence (AI), and overall review of processing systems and enhancement of safety measures

■Plan to manage compliance through in-country agents and follow-up inspections

The Personal Information Protection Commission (Chairman Ko Hak-soo, hereinafter referred to as the "Commission") held its 9th plenary meeting on Wednesday, April 23, and **deliberated** and resolved the results of the preliminary inspection of Hangzhou DeepSeek Artificial Intelligence Co.

☐ **What's happened since then**

In January of this year, shortly after the launch of the DeepSeek service, concerns were raised about domestic and international privacy violations, and the Personal Information Commissioner's Office immediately sent DeepSeek a letter of inquiry regarding the way it collects and processes personal information (Jan. 31)and conducted technical analysis the Korea Internet & Security Agency (Director Sangjoong Lee) to identify some of the deficiencies in its communication capabilities with other operators and personal information processing policy (hereinafter referred to as the 'Processing Policy').

In response, the Personal Information Protection Commission launched a preliminary fact-finding inspection[(*) of] DeepSeek, and in the process, acknowledged that it had partially neglected to consider the Personal Information Protection Act (the "Protection Act") and expressed its intention to actively cooperate with the Personal Information Protection Commission, and temporarily suspended new downloads from the domestic app market (2.15.).

* Proactive reality check: A system introduced to prevent the risk of infringement by proactively checking vulnerabilities in personal information protection and recommending corrections when violations are found (Article 63(2) of the Protection Act)

The Personal Information Commissioner's Office confirmed the following points during the preliminary inspection.

☐ **Preliminary findings**

(1) Overall processing policy

(When Deepseek launched on the Korean app market on January 15, 25, it disclosed its processing policy only in Chinese and English, and in the processing policy, it omitted the requirements of Korean protection laws, such as procedures and methods for destroying personal information, safety measures, and the name and contact information of the person in charge of personal information protection, and stated it collects a wide range of information such as keystroke patterns and rhythms.

(Inspection process) Deepseek <u>submitted</u> (3.28.)<u>a processing policy in Korean,</u> including statutory matters under the Protection Act, <u>and a separate Korean jurisdiction clause</u> (legal basis for processing, retention period, destruction procedure and method, personal information protection officer, etc. In addition, the company confirmed that the keystroke pattern in question described when the information to be collected was not finalized at the time of service preparation, and that it did not actually collect it, and that it has revised its processing policy with the correct collection items.

* The full text of the Korean processing policy and jurisdiction clause will be disclosed through the web and app when the DeepSeek service resumes.

International transfer of personal information

(Initially), DeepSeek transferred personal information to multiple companies in China and the United States (for purposes such as service improvement, security, and customer service response), without obtaining consent from users at the time of service initiation or disclosing the transfer in its processing policy. In particular, DeepSeek device information, network information, app information, and user input to artificial intelligence (AI) Beijing Volcano Engine Technology Co

(Inspection process) Deepseek submitted the <u>statutory matters related to offshore transfer</u> (consignment) in <u>its Korean language processing policy.</u> Regarding the transfer to Volcano, the company explained that it used cloud services to improve security vulnerabilities and user interface (UI) and user experience (UX), and confirmed that it <u>blocked new transfers</u> (4.10.~) <u>response to the Commission's pointing out that it was unnecessary to transfer the contents entered by users at prompts.</u>

③ Related to AI (artificial intelligence) development and learning

(Initially) DeepSeek was using publicly available data (such as open source data and web collection data) and user input to prompts for AI development and learning similar to other AI providers, but in the case of AI prompt input, there was no function for users to reject the use of AI development and learning, and the processing policy and terms of use were only labeled as 'service provision and improvement', so it could not be considered that sufficient explanation or notice.

(Inspection process) Deepseek has informed and that it has prepared a function (3.17.that allows users to opt-out of AI (artificial) development and learning utilization of AI (intelligence) prompt input contents, and in particular, it has decided to with all the 'enhanced protection measures' * recommended by Information Commissioner's Office after the preliminary of major AI services last year ('24.).

> * Reflect deletion and blocking of pages (URLs) exposing personal information (resident registration numbers, mobile phone numbers, account numbers, etc.) provided by the Korea Internet & Security Agency during pre-learning, clearly informing users of the purpose of using user-entered data and ensuring their right to choose whether or not to use it, and providing specific guidance on the overall personal information processing flow related to AI (artificial intelligence).

④ Other: related to children's personal information and safety measures

Although DeepSeek does not collect personal information of children under the age of 14, it did not have a procedure for checking the age of children when signing up for the service, but during the inspection process, it established a procedure for age verification. In addition, it was confirmed that measures were completed during the inspection process for some identified security vulnerabilities (such as failure to restrict access to the development server database and failure to prevent directory listings).

☐ Disposition and future plans

(Disposition) Based on the results of the above inspection, the Personal Information Commissioner decided to issue a recommendation Deepseek to faithfully prepare the legal basis for transferring personal information overseas, immediately destroy the prompted input of users who have already transferred to Volcano, and continue to secure transparency of the service, including disclosing the Korean processing policy.

In addition, was decided to recommend [1] compliance with the 'Enhanced Privacy Measures Plan' prepared based on the results of the preliminary inspection of major AI services last year, [2] checking whether children's personal information is collected and destroying it, [3] improving safety measures across the personal information processing system, and [4] improving the designation of domestic agents.

(Future Plans) If DeepSeek accepts the Personal Information Protection Commissioner's remediation recommendation within 10 days, it is considered to have received a remediation order (Article 63(2) of the Protection Act), and the results of the implementation of the remediation and improvement recommendations must be reported to the Personal Information Protection Commissioner within 60 days. In the future, the Personal Information Commissioner continue to monitor DeepSeek's implementation of the corrective and improvement recommendations at least twice a year.

On the occasion of the DeepSeek inspection, the Personal Information Commissioner's Office decided to provide the key points of the "Guide for Overseasto Apply the Personal Information Protection Act" published last year in the form of a checklist. Overseas operators are required to use it to check the basics in advance to ensure that they faithfully guarantee the rights of Korean information subjects and safely protect personal information before launching and operating their services.

[Attachment 1 Basic checklist for compliance with the Foreign Operator Protection Act (Korean and English)

Attachment 2] Excerpt of the South Korea Jurisdiction Clause from the DeepSeek Privacy Policy (Provided by the

Attachment 3] Opt-out of learning and age verification of user input data (provided by the provider)

Responsible for	Privacy Commissioner	Responsible for	and chapter	Hae Sook Kim (02-2100-3111)
<General	Investigations1	Representative	Investigator	Myungseok Ko (02-2100-3119)
		Representative	Investigator	Hye Won Do (02-2100-3117)
<Co	Korea Internet & Security Agency Research	Responsible for	Teams Chapter	Dae Sik Park (061-820-2830)
		Representative	Line λ	Minjun Shin (061-820-2836)

Note	Recommendations for corrections and improvements *State the relevant provisions

Separation	Corrections and recommendations for improvement	Related articles	Corrective action (proposed)
Processing policies	• Disclose Korean language processing policies, including items under protection laws, and continue to ensure transparency of services	§30①②	•Remediation §632②
International transfers	• Have a lawful basis for international transfers of personal information and destroy personal information that is no longer needed	§28.8①	
Privacy learning and AI development	• Enhanced privacy measures such as excluding URLs containing personal information such as social security numbers from training data	§3④ §15	•Recommendations for improvement §61②
Child information	• Determine whether children's personal information is collected and take appropriate action, such as destroying it	§3④·⑧ §22.2	
Safety measures	• Strengthen safety measures by reviewing the entire personal information processing system and remediating vulnerabilities.	§3④ §29	
Domestic Agent	• Designate a domestic agent to implement corrective and improvement recommendations, comply with other protection laws, and protect the rights of Korean data subjects	§312①	

Attach 1	Basic checklist for compliance with the Foreign Operator Protection Act (Korean and English)

Basic checklist for compliance with the Foreign Operator Protection Act

> Not mine

○ As global services become more common and the number of overseas companies operating in Korea increases, the number of cases of personal information infringement by overseas companies is also increasing, so it is recommended that overseas companies launch their services in Korea before launching their services in Korea.
"The Personal Information Protection Act and guide you through the requirements of the "Personal Information Protection Act

For more information, refer to the 'Guide on Application of the Personal Information Protection Act for Overseas Businesses (April 24)' (Location: Personal Information Protection Commissioner's website (pipc.go.kr)> Act> Guide)

○ laws and related to the protection of personal information may differ by country and compliance requirements may vary, following   of basic information that is the protection personal information and the rights of Korean data should be in advance.

○ In the event of a   substantial   impact on a Korean data subject, the overseas business entity shall be deemed to have a
"The Personal Information Protection Act may apply, and "qualitative review" system may be utilized to ensure compliance with the Personal Information Protection Act prior to the launch of service in Korea.

Criteria: Provision of goods or services to Korean data subjects, impact on Korean data subjects, presence of business operations in the territory of Korea, etc.

For related inquiries adequacy@korea.kr

① Establishing and disclosing a privacy policy

What to check	Check results
Prepare and publish a Korean-language privacy policy	☐
② Clearly describe the personal information processor that processes the personal information of Korean data subjects	☐
③ If personal information is processed outside of Korea, clearly state the fact, the country where the personal information is processed, and the name of the business entity. ○ What personal information we process ○ Purposes of processing personal data ○ Processing and retention periods ○ Third-party offerings ○ Destruction Procedures and Methods ○ Potential disclosure of sensitive information and How to choose private ○ About outsourcing ○ Handling of pseudonymized information ○ Data Subject and Legal Representative Rights How to exercise your obligation ○ CPO Statements and Grievances Processing department name and contact information ○ International relocation grounds, etc. ○ Personal information directly from abroad The name of the country at the time of collection ○ Safety precautions ○ Automated Personal Information Collection Devices ○ Processing policy changes ○ Installation and Operation Denials	☐
④ Create and disclose all of the information required by the protection laws. Do not simply translate a processing policy that was established under the laws of another country. * Disclose separately for "outsourced processing" and "provided by third parties	☐
⑤ Use the name "Privacy Policy" when disclosing it on your internet homepage, etc.	☐
⑥ Specify the items of personal information that can be processed without consent and the legal basis for such processing	☐

② International transfers of personal information

What to check	Check results
① Check whether the transfer is international and meet the legal basis If personal information is provided, processed, entrusted, or stored to a business located outside of Korea, it is transferred overseas. ○ Separate consent when providing personal information ○ Disclosure of processing policy in case of consignment and storage, etc.	☐
To take measures to ensure safety, handle grievances and resolve disputes about personal information infringement and other measures necessary to protect your privacy.	☐

③ Domestic agent

What to check	Check results
① Does not have an address or business office in Korea and retains sales or personal information Designate a domestic agent for overseas businesses over a certain size	☐
The Privacy Commissioner requests the submission of documents, access to the site, or statements of relevant persons, Coordinate the appointment of a domestic agent	☐
Disclose the name, address, phone number, and email of the domestic agent in the processing policy	☐

4️⃣ Delegation of processing of personal information

What to check	Check results
(1) Include protection law content in documents when outsourcing personal information processing tasks ◯ Prohibit processing personal information outside the scope of the outsourcing　　◯ Purpose and scope of the engagement ◯ Redelegation restrictions　　◯ Safety measures, such as access restrictions ◯ Oversight, including checking the status of management　　◯ Damages for breach of fiduciary duty, etc.	☐
Oversight, including training fiduciaries and checking on the status of processing related to outsourced work	☐

5️⃣ Special types of personal information

What to check	Check results
Obtaining consent of legal representative when processing personal information of children (under 14 years of age under the Korean Protection Act)	☐
Check the age information of the data subject to determine if he/she is a child Requiring the data subject to enter their date of birth or using an identity verification service.	☐
③ Prohibition of processing sensitive information in principle (notice of legal matters and separate consent when collecting)	☐
④ No collection of social security numbers without legal basis Remove social security numbers even when collecting IDs (social security cards, passports, driver's licenses, etc.)	☐
⑤ Obtain legal notice and separate consent when collecting passports, driver's licenses, and alien registration numbers	☐

6️⃣ Data Subjects Rights

What to check	Check results
Provide a window to exercise information subject rights (, app, email, phone, etc.)	☐
Processing and notification of results within 10 days for requests for access, **correction**, deletion, and suspension of processing	☐
③ Notify the reason for refusal of access, etc. and provide access once the reason for refusal is over	☐

7️⃣ Safeguards

What to check	Check results
Implementing technical, administrative, and physical measures necessary to ensure safety ◯ Establish and review internal management plans　　◯ Restrict access　　◯ Access control measures ◯ Encryption at rest and in transit　　◯ Keeping and checking access records　　◯ Malware protection	☐

8️⃣ Breach notification and reporting

What to check	Check results
Notify the data subject within 72 hours of a personal information breach	☐
In principle, if personal information is leaked through illegal access such as hacking, sensitive or uniquely identifiable information, or illegal access by more than 1,000 people, it should be reported within 72 hours. Personal Information Protection Commission or Korea Internet & Security Agency (https://www.privacy.go.kr)	☐
③ Take immediate action upon confirmation of damage such as leakage and implement measures to minimize damage	☐

⑨ AI Development — Service Delivery (Recommendations)

What to check	Check results
Implement technical and administrative safeguards when processing disclosed personal information for AI development and services <table><tr><td>○ Sources of training data collection Validation-Management</td><td>○ Preventing the leakage and disclosure of personal information</td><td>○ Secure storage of personal information and management</td></tr><tr><td>○ Safety through fine-tuning Add a device</td><td>○ Filtering and output Apply</td><td>○ Learning In the results, click specific Delete data</td></tr><tr><td>○ Learning Data Privacy and data processing Disclosure in policies</td><td>○ Consider conducting a privacy impact assessment</td><td>○ AI development and deployment characteristics such as open source, API, etc. Safety measures</td></tr></table>	☐
Allow users to delete their data and opt out of AI learning. 　　Ensuring user choice, such as having an opt-out feature	☐
Remove user identifiers when using user input to train AI, Notice to users of data redaction and personal information removal and human review	☐

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 Korean territory.

* Contactadequacy@korea.kr

☐ 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 destroy 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 transfers	◯ 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

Items to be Checked	Tick
④ Writing and disclosing a privacy policy that covers all 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	☐

A Cross-border Data Transfers

Items to be Checked	Tick
① Meeting the legal requirements regarding whether cross-border data transfers take 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 transfers	☐

◯ Obtaining separate consent needed personal information	◯ Stipulating the fact of entrustment when providing of processing or storage of personal information in a privacy policy

Items to be Checked	Tick
Putting safeguards in place, lodging a complaint, or applying for dispute settlement, or other privacy-safeguarding measures	☐

□ 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	☐
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 <table><tr><td>◯ Prohibiting personal data processing beyond the purposes of entrustment</td><td>◯ The purposes and scope of the entrustment</td></tr><tr><td>◯ Restriction on re-entrustment</td><td>◯ Access control and other safeguards</td></tr><tr><td>◯ Overhauling of the management of entrustment and other supervisory affairs</td><td>◯ Compensation when an entrustee fails to comply with legal obligations</td></tr></table>	☐
Providing compliance training to an entrustee, overhauling the status of data processing, and other supervisory affairs	☐

A Special Category Data

Items to be Checked	Tick
Obtaining consent of a legal representative when processing a child's personal information (a child ages below 14 under the PIPA)	☐
Verifying the age information of a data subject to see whether the data subject is a child 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
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 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	☐

A Safeguards

Items to be Checked	Tick
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	☐

☐ 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: https://www.privacy.go.kr	☐
③ Taking measures after becoming aware of a data breach and implementing countermeasures to mitigate damages	☐

☐ Development and Deployment of AI Services (recommendation)

Items to be Checked	Tick
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.	☐
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	☐

<u>Daehan Min Guk</u>

If you the Services from the People's Republic of China, the following additional apply. order to Services to you, we collect and process directly of China.

Legal basis for processing personal information

We process the personal described in this Privacy Policy in to fulfill the contract we have you for the provision of our or to process your requests the course of creating account in accordance with Article 15, 1, subparagraph 4 of the Personal Protection Act. (redacted)

Handling pseudonymous information

We may, in some cases, aggregate or anonymize the information we collect about you and it   way that does not you or other purposes, the extent by applicable . (redacted)

How we share your information Outsourcing the processing of
your personal information

We personal in to provide our services in accordance with Article 28 (8) (1) (3) of the Personal Data Protection Act (entrustment of the processing and storage of personal for the conclusion and performance of a contract with a data controller).

How long we hold your information

We will promptly destroy your personal data when it is no longer required, such as when the retention period expires or when we have fulfilled the purposes for which processed it. However, if , we keep your personal for the periods, including for the following reasons (emphasis added)

Procedures and methods for destroying personal information

The procedures and methods for the destruction of personal information are as follows: (emphasis added)

Your Rights

You may exercise your rights as a data subject through a legal representative or an authorized representative. (emphasis added)
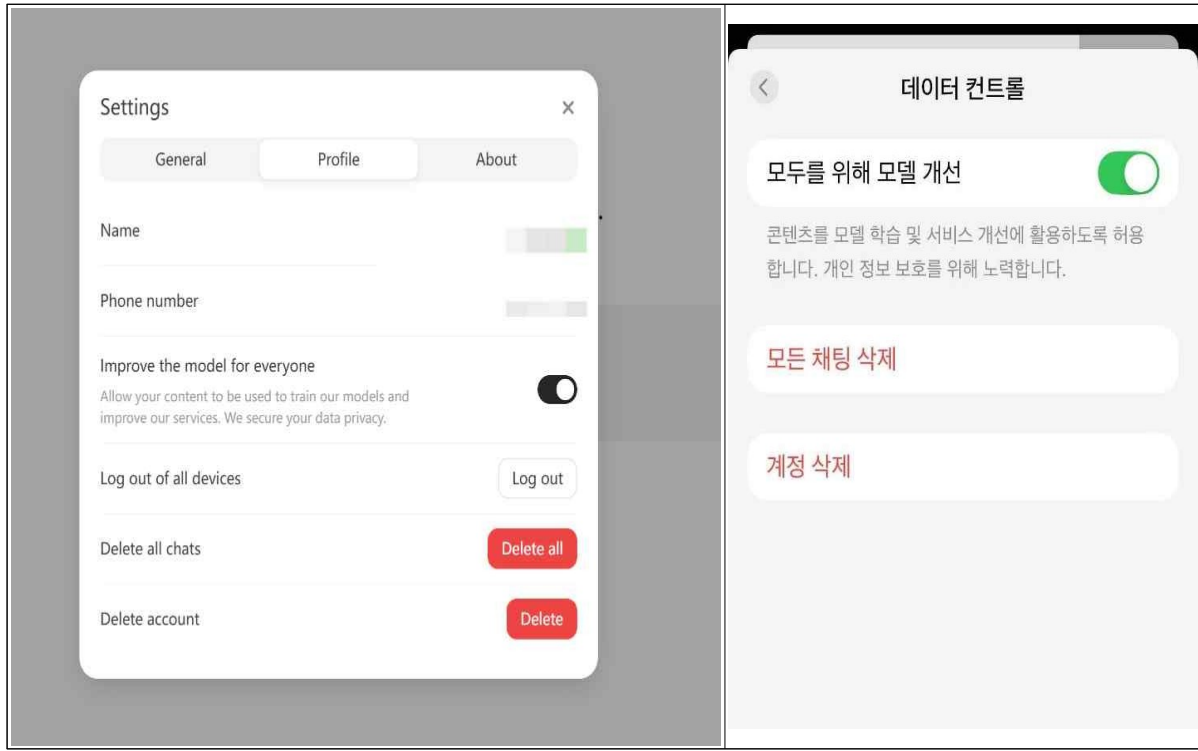
Who's responsible for privacy

 are responsible for the overall processing of personal information and have designated a person responsible for the protection of personal information as follows to handle complaints and remedy any harm caused. (Italics added)

Attach 3	Ability to opt-out of learning from user input data and age verification process (provided by provider)

☐ Ability to opt out of AI learning

☐ Age verification process