Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Chinese AI under scrutiny: How DeepSeek neglected the protection of user data

The South Korean Personal Information Protection Commission (PIPC) announced that the Chinese company Hangzhou DeepSeek Artificial Intelligence transferred personal data and the content of user requests (prompts) without the explicit consent of users when it launched its application on the South Korean market at the beginning of the year.

The PIPC's statement said that data, including personally identifiable information and information about devices, networks and the app itself, was transferred to companies in China and the United States without this being specified in the data processing policy or users having the opportunity to accept these practices.

This move led to a temporary halt in new downloads of the application in February but also to deeper doubts about the practices of Chinese AI start-ups in the global market.

DeepSeek launched its service on the Korean market on 15 January 2025, promising advanced generative AI features tailored to local needs.

However, as early as 31 January, the PIPC initiated a preliminary request for information on how user data is managed and reminded the company of the strict legal requirements for transferring data abroad.

In February, after DeepSeek partially admitted that it had not fully complied with local regulations on personal data protection, the agency suspended new downloads of the application until it had fulfilled its legal obligations. However, the web service remains available to users in the country, further complicating regulatory oversight.

Detection of irregularities

Details released on 24 April show that in addition to basic user data, the content that users entered into DeepSeek prompts — from questions to quotes — was also transferred to Beijing Volcano Engine Technology, which is affiliated with ByteDance.

In addition, metadata about network parameters and the application versions installed on the devices were also transferred, allowing detailed profiling of user behaviour.

Subsequently, DeepSeek claimed that this practice aimed to enhance user experience and eliminate security vulnerabilities. However, the fact that such transfers were not announced in advance or properly documented in the privacy policy indicates an obvious failure to apply the basic principle—that only the data necessary to provide the service was collected.

> The company must revise the data processing policy and include precise procedures for data destruction, security compliance measures and mechanisms for informing users about the rights to consent and withdraw consent

In response to the irregularities identified, the PIPC issued a formal recommendation requesting DeepSeek to immediately remove all previously transferred prompt content from the Beijing Volcano Engine infrastructure and to create a clear and legally sound plan for any future international transfers of personal data.

In addition, the company must revise the data processing policy and include precise procedures for data destruction, security compliance measures and mechanisms for informing users about the rights to consent and withdraw consent.

Attacks on the trust of users

If DeepSeek does not comply with these corrective measures, the company will face financial and reputational consequences based on the European General Data Protection Regulation (GDPR), as well as stricter requirements resulting from the recently adopted EU Artificial Intelligence Act.

According to the provisions of this law, violating prohibited practices can be penalised with fines of up to USD 35 million, or 7% of annual global turnover, and up to EUR 15 million, or 3% of annual global turnover, for other violations.

The EU adopted its regulation on 21 May 2024, and it entered into force on 1 August of the same year. It provides for additional monitoring and reporting measures for AI service providers from third countries if they have users in the EU.

> DeepSeek has already suffered a serious blow to user trust

Regulatory challenges aside, DeepSeek has already suffered a serious blow to user trust.

In January 2025, a group of experts from Wiz Research discovered a flaw in the configuration of the company's cloud storage that allowed open online access to a database with more than a million sensitive entries, including chat histories, API keys, and system logs.

While the company's swift response prevented immediate misuse, it fuelled fears that similar security incidents could have far-reaching consequences, particularly if the data was misused for hybrid cyber operations directed against democratic societies.

Initiating investigations

The global context further complicates the situation: European and American regulators, along with Italy, Canada, Australia, Taiwan, and several other countries, have launched investigations or banned DeepSeek in their territories due to potential risks.

Italy's Garante temporarily blocked the chatbot at the end of January 2025 until the company adjusts its privacy policy, while the US National Security Council has launched a national security impact assessment. The governments of Canada and Australia have banned the use of the application on official (government) devices, and Taiwan has advised government organisations to avoid using DeepSeek services to reduce the risk of confidential information being leaked.

For DeepSeek, a startup that attracted significant investment at the beginning of the year due to its rapid rise in popularity, these events are a major blow.

> Investors are questioning the long-term viability of a business model based on processing user data

Investors are questioning the long-term viability of a business model based on processing user data, while negotiations to re-enter the South Korean market have stalled.

The company must not only introduce strict compliance mechanisms but also invest in building trust with regulators and users around the world.

Among the technical changes DeepSeek has made are blocking the transfer of prompt content to Beijing-based Volcano Engine Cloud Services on 10 April; appointing legal representatives in South Korea; and beginning a review of its data retention and deletion policies.

However, PIPC points out that the blocking itself is not sufficient without a documented legal basis for future transfers and clear procedures to ensure user privacy in accordance with relevant laws. The entire process requires additional revisions to security measures and the introduction of risk management standards.

Global consequences

Regulators around the world are expected to tighten controls on AI providers from third countries. On 2 August 2026, the EU will implement some provisions of the AI Act that prohibit manipulative practices of AI tools in

the commercial and public sectors, while the rest of the rules will apply until 2030.

The EU will implement some provisions of the AI Act that prohibit manipulative practices of AI tools in the commercial and public sectors, while the rest of the rules will apply until 2030

In South Korea, the PIPC announces possible updates to the law to increase the level of sanctions and extend jurisdiction to additional categories of data, including user input when interacting with AI models. This trend points towards the gradual harmonisation of data protection rules in the age of artificial intelligence.

Ultimately, DeepSeek is at a turning point: either it quickly adapts its practices and regains the trust of users and regulators, or it risks permanent exclusion from key markets on which the further development of Chinese AI startups in the global economy depends.

Companies developing AI solutions need to understand that security and transparency are inseparable pillars of success, while regulators and users are becoming increasingly demanding when it comes to protecting their rights.