

South Korea's privacy regulator suspends new downloads of the DeepSeek app

Source copy kept by wheresthe.ai for the story "South Korea's privacy regulator suspends new downloads of the DeepSeek app" (<https://wheresthe.ai/d/kr-pipc-deepseek-downloads-suspended-2025-02/>).

Source: <https://thehackernews.com/2025/02/south-korea-suspends-deepseek-ai.html>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: 68ab6abbdf0c40c0aaf811d8c2fba23bd26442d8b21320a170ddc918ad55ac

South Korea Suspends DeepSeek AI Downloads Over Privacy Violations

Ravie Lakshmanan Feb 17, 2025 Artificial Intelligence / Data Protection

South Korea has formally suspended new downloads of Chinese artificial intelligence (AI) chatbot DeepSeek in the country until the service makes changes to its mobile apps to comply with data protection regulations.

Downloads have been paused as of February 15, 2025, 6:00 p.m. local time, the Personal Information Protection Commission (PIPC) said in a statement. The web service remains accessible.

The agency said it commenced its own analysis of DeepSeek right after its launch and that it "identified some shortcomings in communication functions and personal information processing policies with third-party service providers."

DeepSeek is said to have recently appointed a local representative, per PIPC, with the company also acknowledging it had failed to take into consideration domestic privacy laws when launching the service.

To that end, downloads of DeepSeek are being paused until the company implements the necessary improvements that bring the service in compliance with the Personal Information Protection Act.

"This temporary suspension of the DeepSeek app restricts new app downloads from the app market, and we ask existing users to use it cautiously, such as not entering personal information in the DeepSeek input window (prompt) until the final results are announced," the agency noted.

Furthermore, PIPC intends to ensure compliance and improve guidance so as to prevent similar lapses from occurring in the future.

The development comes shortly after South Korea's National Intelligence Service (NIS) called out the service for "excessively" collecting personal data and using the information to train its AI systems.

In recent weeks, DeepSeek's Android and iOS apps have also been found to contain security weaknesses that allow certain data to be sent to its servers in unencrypted format.

Beijing has previously said it allows internet companies across the world to operate in the country as long as they follow local laws and regulations, and that it would never ask any company or individual to collect or store data in breach of laws..

Found this article interesting? Follow us on Google News , Twitter and LinkedIn to read more exclusive content we post.

SHARE

Tweet

Share

Share

Share

SHARE

AI Ethics , artificial intelligence , Compliance , cybersecurity , data protection , national security , Privacy , South Korea , technology

✂ Top Stories This Week

Researchers Demonstrate OpenBSD Root Exploit Chaining 37-Year-Old Shared-Memory Bug
Critical PwnEscape Linux Kernel Vulnerability Lets Guest VMs Read Host Memory
ThreatsDay: Adobe RCE, DNS Wallet Theft, NVIDIA Container Escape, Self-Healing Backdoor + 23 More
Citizen Lab Traces Zero-Click Candiru Spyware Infections at Al Jazeera to Targeted Online Ads
NGINX Fixes 5 Flaws, Including Possible RCE and a TLS Bug That May Skip Client-Cert Checks
Next.js Ships Out-of-Band Patch for Two Critical RCE Flaws in Caching and SVG Processing
Palo Alto Networks Patches PAN-OS Authenticated RCE Flaw Amid Active Exploitation
GhostAction Compromises About 1,900 GitHub Accounts, Targets Over 30,000 Repositories
Cisco Warns of Active Attacks Exploiting New Critical Secure Email Gateway Vulnerability
Langflow's Critical Authenticated RCE Flaw Targeted in 1,423 Honeypot Exploit Attempts
Hackers Backdoor Nextcloud Servers Through Critical Flaw in Collabora's Built-in CODE App
U.S. Shuts Down Over 40 Laptop Farms, Charges 14 in North Korean IT Worker Fraud
curl Patches HTTP/2 Upload Flaw After PoC Demonstrates Client-Side Code Execution
Researchers Used a Public OpenAI Model to Build a \$250,000 Chrome Full-Chain Exploit in Six Days
AI-Found Linux Kernel Flaw Gives Local Users Root, and Can Break a Guest Out to the Host
Microsoft Patches Record 1,413 Flaws, Including Exploited Windows Shell Bug
OpenAI Employee Arrested for Allegedly Planting Hidden Recorder in Executive Conference Room
Anthropic Warns Small AI Models Could Soon Form Self-Propagating IoT Botnets
Docker Fixes Critical Two-Year-Old Hub Flaw That Let One User Push Images as Another
SAP Discloses Critical CVSS 10 Flaw in Cloud SDK for Python Allowing OAuth2 Credential Theft
LG Smart TVs Vulnerable to Pre-Auth Root Takeover From Local Network
Attackers Heat French Supermarket Fridges Up to 50°C by Hijacking Danfoss Controllers
GitLab Patches CVSS 10.0 Flaw That Could Let Unauthenticated Users Run Server Code
✂ Weekly Recap: Helpdesk 0-Days, Rogue Certs, ShinyHunters Arrest, AI-Fooling Malware and More
Researchers Publish Working Exploit for Pre-Auth AnyDesk Linux Flaw That Gives Root Access

★ Featured Resources

Download the 2026 Agent Security Report for a Five-Step Risk Reduction Framework
Get the Five-Stage Identity Maturity Roadmap for Governing AI Agents
Benchmark Your AI Risk Priorities Against 1,600 CISOs—Download the 2026 Report
No Exploit Yet? Preview the Summit Demo on Validating CVE Exposure