

不只義大利、美海軍...數發部列 DeepSeek「危害國家資安產品」，宣告公部門禁用

中國新創公司開發的人工智慧（AI）大型語言模型（LLM）DeepSeek（深度探索），近日引發多國提出資安、隱私等方面的疑慮。我國數位發展部周五（1/31）提出公告，特別警示公務機關與關鍵基礎設施等，應限制使用 DeepSeek AI 產品，以避免造成危害國家資通安全的疑慮。

DeepSeek 引多國擔憂資安 數發部宣布公部門禁用

中國開發的 AI LLM「DeepSeek」不但衝擊輝達（NVDA）等美國 AI 相關科技股股價，也引發多國擔憂其有資安、隱私疑慮。其中，美國白宮正在評估其國安風險，美國海軍則直接下令禁用，而義大利數據保護局更是要求將其 APP 下架，韓國當局則出手調查是否有數據隱私疑慮。

台灣的數發部則是在周五發布新聞稿指出，基於國家資通安全考量，該部特別警示公務機關與關鍵基礎設施等應限制使用 DeepSeek AI 產品，以避免使用者相關數據或資訊被這類有資安疑慮的產品傳送，造成危害國家資通安全的疑慮。

來自中國且涉資安疑慮 數發部列入危害國家資通安全產品

數發部表示，依行政院及所屬機關（構）使用生成式 AI 參考指引，業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關、機構同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。

數發部也發現，DeepSeek AI 服務為中國產品，其運行涉跨境傳輸及資訊外洩等資安疑慮，屬危害國家資通安全產品，為防範公務機關內部資訊在無法有效監管的情況下外流並構成危害風險，我國從 2019 年行政院公布實施「各機關對危害國家資通安全產品限制使用原則」。

引用「危害資安產品使用原則」 數發部禁公部門使用 DeepSeek

數發部接著說，該原則已明確要求中央與地方機關、機構、公立學校、公營事業、行政法人以及自行或委外營運提供公眾活動或使用之場地，限制使用危害國家資通安全產品。此外，中央目的事業主管機關應督導資通安全管理法所定關鍵基礎設施提供者及政府捐助之財團法人，參考辦理。

數發部強調，上班時間內不得利用電腦及網路設備從事與公務無關之行為，各機關資通安全防護至關重要，數發部也將持續掌握相關技術發展，並適時調整資安政策，以保障國家資訊安全。

(資料來源：今周刊 114 年 1 月 31 日報導)

避免機密從口出，公務機密始維護

廉政檢舉專線 0800-286-586

法務部矯正署雲林監獄政風室關心您