主題	**生成式人工智慧時代的資料主權：法令遵循新戰場** **Data Sovereignty in the Age of Generative AI: A New Compliance Frontier**
類別	訊息新知 (Nov 2025)
內容	生成式人工智慧的崛起，正讓「資料主權」成為企業合規治理的全新焦點。當 AI 模型橫跨全球資料集進行訓練與推論，資料不再受限於伺服器所在地，而可能在無形間穿越多重司法邊界。這對金融、科技與政府單位而言，都是前所未見的挑戰。 本篇專文指出，生成式 AI 的不透明性與「Shadow AI（影子 AI）」現象，正在削弱組織對資料流向的掌控力。員工可能在無意間輸入含有個資或商業機密的提示語，導致資料外洩或違反跨境法規。要在創新與合規間取得平衡，企業必須重新定義資料治理策略──從導入主權雲與私有 AI 模型，到運用聯邦學習與差分隱私等技術，確保資料留在合法邊界內。 更關鍵的是，企業應將 AI 納入 ISO 27001、NIST AI RMF 與 EU AI Act 等既有治理框架中，建立跨部門 AI 合規委員會，落實資料分級、追蹤與員工教育。唯有將資料主權視為生成式 AI 治理的核心，組織才能在這場全球 AI 浪潮中兼顧創新與信任。 全文詳閱: https://www.isaca.org/resources/isaca-journal/issues/2025/volume-5/data-sovereignty-in-the-age-of-generative-ai