因應使用「生成式AI（Generative AI）」工具的營業秘密管理強化建議

2024年7月1日，美國實務界律師撰文針對使用生成式AI（Generative AI）工具可能導致的營業秘密外洩風險提出營業秘密保護管理的強化建議，其表示有研究指出約56%的工作者已經嘗試將生成式AI工具用於工作中，而員工輸入該工具的資訊中約有11%可能包含公司具有競爭力的敏感性資訊或客戶的敏感資訊，以Chat GPT為例，原始碼（Source Code）可能是第二多被提供給Chat GPT的機密資訊類型。系爭機密資訊可能被生成式AI工具提供者（AI Provider）用於訓練生成式AI模型等，進而導致洩漏；或生成式AI工具提供者可能會監控和存取公司輸入之資訊以檢查是否有不當使用，此時營業秘密可能在人工審查階段洩漏。

該篇文章提到，以法律要件而論，生成式AI有產生營業秘密之可能，因為營業秘密與著作權和專利不同之處在於「發明者不必是人類」；因此，由生成式 AI 工具協助產出的內容可能被視為營業秘密，其範圍可能包括：公司的內部 AI 平台、基礎的訓練算法和模型、輸入參數和輸出結果等。惟基於目前實務上尚未有相關案例，故生成式AI輸出結果在法律上受保護的範圍與條件仍需待後續的判例來加以明確。

實務專家提出，即使訴訟上尚未明確，企業仍可透過事前的管理措施來保護或避免營業秘密洩露，以下綜整成「人員」與「技術」兩個面向分述之：

一、人員面：

1.員工（教育訓練、合約）

在員工管理上，建議透過教育訓練使員工了解到營業秘密之定義及保護措施，並告知向生成式AI工具提供敏感資訊的風險與潛在後果；培訓後，亦可進一步限制能夠使用AI工具的員工範圍，如只有經過培訓及授權之員工才能夠存取這些AI工具。

在合約方面，建議公司可與員工簽訂或更新保密契約，納入使用生成式AI的指導方針，例如：明確規定禁止向生成式AI工具輸入公司營業秘密、客戶數據、財務信息、未公開的產品計劃等機密資訊；亦可增加相關限制或聲明條款，如「在生成式AI工具中揭露之資訊只屬於公司」、「限制公司資訊僅能存儲於公司的私有雲上」等條款。

2.生成式AI工具提供者（合約）

針對外部管理時，公司亦可透過「終端使用者授權合約（End User License Agreement，簡稱EULA）」來限制生成式AI工具提供者對於公司在該工具上「輸入內容」之使用，如輸入內容不可以被用於訓練基礎模型，或者該訓練之模型只能用在資訊提供的公司。

二、技術方面：

建議公司購買或開發自有的生成式AI工具，並將一切使用行為限縮在公司的私有雲或私有伺服器中；或透過加密、防火牆或多種編碼指令（Programmed）來避免揭露特定類型的資訊或限制上傳文件的大小或類型，防止機密資訊被誤輸入，其舉出三星公司（Samsung）公司為例，三星已限制使用Chat GPT的用戶的上傳容量為1024位元組（Bytes），以防止輸入大型文件。

綜上所述，實務界對於使用生成式AI工具可能的營業秘密風險，相對於尚未可知的訴訟攻防，律師更推薦企業透過訴訟前積極的管理來避免風險。本文建議企業可將前述建議之作法融入資策會科法所創意智財中心於2023年發布「營業秘密保護管理規範」中，換言之，企業可透過「營業秘密保護管理規範」十個單元（包括從最高管理階層角色開始的整體規劃建議、營業秘密範圍確定、營業秘密使用行為管理、員工管理、網路與環境設備管理、外部活動管理，甚至是後端的爭議處理機制，如何監督與改善等）的PDCA管理循環建立基礎的營業秘密管理，更可以透過上述建議的做法（對單元5.使用管理、單元6.1保密約定、單元6.4教育訓練、單元7.網路與環境設備管理等單元）加強針對生成式AI工具之管理。

本文同步刊登於TIPS網站（https://www.tips.org.tw）

相關連結

Diana H. Leiden & Helen Winters, Harnessing Generative AI: Best Practices For Trade Secret Protection, Mondaq, Jul. 1, 2024

你可能會想參加

→ 【線上場】113年「新創採購機制及鼓勵照護機構參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 新創必知的商標保護與申請
→ 113年新創採購-照護機構獎勵說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【中部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【臺北場】113年度新創採購-招標作業廠商說明會
→ 【臺中場】113年度新創採購-招標作業廠商說明會
→ 【高雄場】113年度新創採購-招標作業廠商說明會
→ 品牌企業商標管理實務課程
→ 【北部場】營業秘密保護實務座談會
→ （實體-上午場）2024科技專案成果管理之法制與實務課程
→ （直播-上午場）2024科技專案成果管理之法制與實務課程
→ （實體-下午場）2024科技專案成果管理之法制與實務課程
→ （直播-下午場）2024科技專案成果管理之法制與實務課程

徐婕伊
研究助理 編譯整理

上稿時間：2024年08月

資料來源：
Diana H. Leiden & Helen Winters, *Harnessing Generative AI: Best Practices For Trade Secret Protection*, Mondaq, Jul. 1, 2024, https://www.mondaq.com/unitedstates/new-technology/1485314/harnessing-generative-ai-best-practices-for-trade-secret-protection#authors (last visited Jul. 26, 2024).

延伸閱讀：
<營業秘密保護管理規範>，財團法人資訊工業策進會科技法律研究所網站，https://stli.iii.org.tw/publish-detail.aspx?no=72&d=7212（最後瀏覽日：2024/07/30）。

文章標籤

智財訴訟 | 智財授權 | 人工智慧 | 智財風險 | 智財管理 | 營業秘密 | 技術保護 | 智財治理 | 人工智慧風險管理

推薦文章