Lexis+ AI™

Lexis+AI™ 資訊安全說明書

LexisNexis®將安全放在所有工作的首位。我們的產品從一開始就秉持優先保護客戶資料的開發理念。

我們全方位的資料保護計畫可保障您寶貴資訊的安全。為了確保在整個產品生命週期中實施全面的安全管控，我們組建了一個應用和安全專家團隊。他們與我們優秀的產品開發和營運團隊攜手合作， 確保每個產品都符合嚴格、經審核的標準。

安全、隱私和可信：我們的承諾

透過 LexisNexis®解決方案體驗無與倫比的安全性和尖端技術。相信我們能在提供一流性能的同時保護您的寶貴資產。

請使用下面的導航連結簡要了解我們對您的資料所做的承諾。

數據

您的提示詞

- 您的對話將在 90 天後或使用者刪除之時清除（以先發生者為準）。
- 您的對話歷史儲存在安全的環境中，並使用 AES-256 進行靜態加密。
- LexisNexis®大型語言模型合作夥伴受我們協議的約束，「不得根據您的資料訓練」我們的客製化模型。
- 我們的雲端提供者有用於支援和故障排除的日誌，無法存取使用者提示詞。

您上傳的文件

- 您的文件由您掌控。您可以透過刪除對話留言來刪除文件，或者我們的系統會在您閒置 10 分鐘後清除文件。
- 您的文件將在正在進行的對話期間保留。
- 您與上傳檔案有關的對話將在 90 天後或使用者刪除之時（以先發生者為準）清除。

隱私設計

隱私設計原則被整合到開發流程中，並進行合規性監督，以確保 LexisNexis 解決方案符合所有適用的隱私和資料保護法律。 作為公司培訓流程的一部分，所有員工都必須接受資料保護培訓。 除此以外，公司每年定期進行有關資料保護和資料安全的強制性合規培訓。 LexisNexis 在僱用/服務合約中包含資料保護和保密條款。

加密

所有 Lexis+ AI™ 使用者資料（提示字詞/檔案）均使用 AWS 的金鑰管理服務和 AES-256 加密技術進行靜態加密。 傳輸中的網路流量使用 TLS 1.2。每個使用者請求都被單獨處理，並在隨後產生具有生成功能的單獨事項。

審查與政策

LexisNexis®聘請獨立的第三方審查專員，根據「 安全、可用性、處理完整性、保密性和隱私 」的信任服務原則， 對 Lexis®和 Lexis+®進行 SOC 2 類型 2 年度檢查。 Lexis+ AI™ 則於 2024 年第一季進行 SOC2 檢查。

LexisNexis®擁有一套健全的資訊安全政策。 這使我們能夠有效地應對針對系統的潛在威脅。我們的事件回應計劃包括技術、行政、業務和執行升級流程，並定期更新和測試。公司還聘請了外部公司，在必要時提供專業知識和指導。

安全與存取控制

網路安全控制是根據最低權限原則實施的。 這些控制措施還可防止未經授權的存取和流量截獲。 這些保護措施可限制系統的入站和出站訪問，以及進出系統的內部流量。在可能和必要的情況下，使用專用端點安全存取雲端服務，以確保相關交易的安全。

對公司網路的存取僅限於公司管理的設備，並使用多因素身份驗證。授權基於最小特權原則。根據履行工作職能的需要提供特權帳戶，由管理層批准，並定期進行訪問審查。 存取權限在終止時自動刪除。

LexisNexis®供應商管理方案在採購過程中對供應商進行安全和背景檢查與評估。我們採用基於風險的方法對供應商進行評估，評估因素包括對資料（使用者 / 公司）的存取權限、系統存取權限以及代表公司履行關鍵職能的權限。

我們使用內部工具和第三方公司進行滲透測試，以驗證我們的防禦能力。自動化的內部和外部漏洞掃描提供了對新風險的持續可見性。對發現的任何項目進行集中跟蹤，以確保適當的風險優先度排序。 以風險優先的方式與支援團隊協調補救工作。

架構

Lexis+ AI™ 將採用與 Lexis+®和我們其他產品相同的安全架構、審查、審計和驗證方式進行部署和維護。
生成式人工智慧功能的設計和部署符合我們的高等級安全標準，重點是保護和細分用戶活動。
我們的安全團隊將繼續積極參與 Lexis+ AI™ 工程設計和部署的各個方面。

高階架構流程：

1. 使用者的提示詞/請求/檔案透過 TLS 1.2 安全性傳送到 Lexis+® 伺服器。
2. 嵌入模型會對提示詞進行意圖解析，並將其分解為單獨的查詢，以便從我們的內容中檢索資訊。
3. 然後，提示字和內容回應將使用 TLS 1.2 傳送到我們在 AWS Bedrock (Claude2)/Azure(OpenAIGPT4) 中託管的私有大型語言模型中。
4. 然後在 Lexis+ AI™ 中向使用者展示生成式的、有根據的應答。
5. 使用者的指令和回覆作為對話歷史的一部分，將在安全加密的資料庫（AES-256）中保留長達90天。而文件則會在10 分鐘對話閒置後清除。
6. Anthropic和 Open AI 無法存取我們的模型或服務端。 我們的架構排除了這兩家機構根據用戶對話記錄或訓練模型的可能性。
7. AWS Bedrock和 Microsoft Azure 雲端服務都有日誌記錄，用於支援和故障排除，但無法存取使用者的提示詞。

Q&A

我在該工具的輸入內容是否會被用於訓練 Lexis+ AI™ 模型?
LexisNexis®不會使用客戶資料來調整或訓練我們的大型語言模型。使用者亦可單獨控制提示詞歷史記錄，並可選擇從我們的服務端刪除提示詞歷史記錄。欲了解更多資訊，請訪問我們的隱私權政策 https://www.lexisnexis.com/en-us/terms/privacy-policy.page-policy.page

Lexis+ AI™ 會利用第三方系統處理我的資料嗎?
LexisNexis®利用人工智慧技術的第三方供應商來確保我們的人工智慧解決方案能夠利用新生成式人工智慧中最好的功能。所有人工智慧技術的第三方提供者都通過了我們的安全審查流程。

Lexis+ AI™中使用的第三方模型僅部署在 AWS Bedrock 和 Microsoft Azure 受保護的私有雲環境中，這些環境是安全的 LexisNexis®雲端環境的一部分，並受適用於我們整個平台的 LexisNexis®安全 管控的約束。這些模型僅供 LexisNexis®使用，公眾或其他公司不得使用。

LexisNexis® 部署的所有模型均採用專用的加密認證連接，符合或超過我們的高安全標準。所有數據都經過加密，並且始終處於 LexisNexis®的控制之下。

你們的加密標準是什麼?
所有 Lexis+ AI™客戶資料（提示詞/檔案）都經過靜態加密（AES-256）和傳輸加密（TLS 1.2）。

LexisNexis®員工可以查看我的查詢對話嗎?
擁有適當存取權限的產品支援專家將能夠審查客戶使用數據，以便提供產品支援和排除技術故障。存取權限僅限於授權人員，客戶關聯資訊將被化名。

我上傳的檔案怎麼辦 – 你們會保留它們嗎?
上傳的檔案會在對話期間安全地儲存在 AWS 的暫存快取中。所有文件都會在閒置 10 分鐘後清除，使用者也可以透過刪除對話留言來清除檔案。

公司管理員能否將 Lexis+ AI™ 的使用限制在某些功能或公司某些使用者範圍內?
如果出現任何明顯的資訊安全問題或疑慮，管理員可以選擇暫時停用其企業的文件上傳和文書起草任務。

在哪裡可以找到與你們的審查和政策相關的文件和報告?
所有報告和文件均依預先要求提供。更多資訊，請聯絡您的客戶經理團隊。

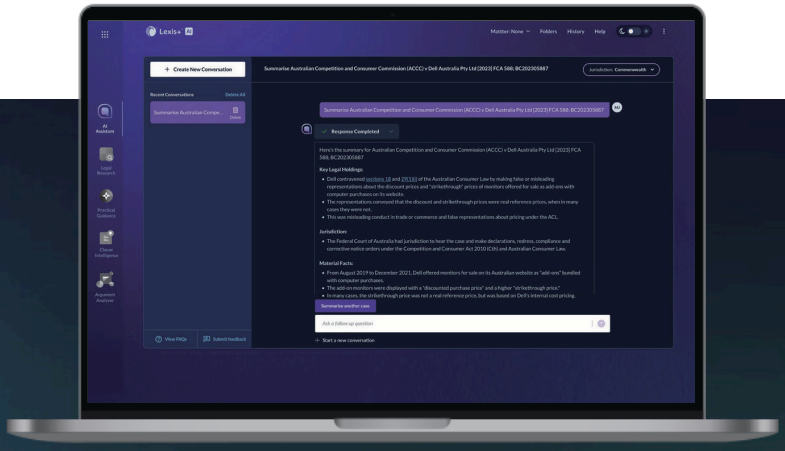
我的 Lexis+ AI™ 資料是否可用於 LexisNexis®內的其他 Lexis®服務?
客戶資料只能在輸入該資料的產品的上下文中使用，不得與其他產品共享，除非得到明確許可和通知。

聯絡我們

security@lexisnexis.com
privacy.inquiries@lexisnexis.com
support.tw@lexisnexis.com

其他資料

LexisNexis®法律與專業資料隱私行為準則
RELX 負責任的人工智慧原則
您的安心是我們的首要任務
深度資訊安全文件—根據要求提供
詳細架構圖 – 根據要求提供



每個律師的世界都將發生變化

公司網站：www.lexisnexis.com/zh-tw
產品網站：www.lexisnexis.com/zh-tw/products/lexis-ai
電郵地址：support.tw@lexisnexis.com

如需進一步瞭解詳情，歡迎聯繫我們銷售的代表。

LexisNexis®