

企業人工智能合約：價值、控制與責任的真正歸屬

作者：蘇振國、張浩然

我們在先前發表的文章《[企業人工智能中的隱性擁有權問題](#)》中探討了保留對數據的權利與控制未必等於能保留由數據所創造的價值。

這項觀察有著重要的實務影響。

企業人工智能所衍生的許多重大問題，並非取決於技術本身，而是取決於機構內部如何透過合約安排採購、部署及管理人工智能系統。隨著人工智能從實驗階段邁向關鍵業務部署（business-critical deployment）階段，這些合約安排將日益決定價值歸屬何處、誰控制由此產生的能力，以及誰須為其後果承擔責任。



人工智能合約往往充當將管治期望轉化為營運義務的機制。

數據擁有權僅只是起點

大多數關於人工智能合約的討論，往往從基礎數據的擁有權開始。這固然重要，但鮮少是分析的終點。

在許多商業安排中，各方都能確定在該安排中提供或控制的資料。然而，更具商業意義的問題往往在於在該安排中提供的資料在日後可如何被使用。為了提供特定服務而獲得處理資料的權利是一回事。但是否擁有權利將同一資料用於測試、基準比較、分析、模型開發或未來服務改進，則是截然不同的另一回事。

因此，有效的合約審查應同時考量資料的允許使用範圍、擁有權和控制權。問題的關鍵不僅在於服務提供者能否存取資料，更在於其能否，以及基於何種目的，從該資料中獲取超出當前可預見合作範圍的價值。

未來價值取決於數據的使用與改進的權利

人工智能合約中最重要的一環在於客戶資料可被如何使用。兩份都規定客戶保留其為合作目的所提供的資料的權利的協議，可以產生實質上截然不同的商業結果。

一份協議可能允許將提示詞、輸出內容、反饋或使用資料用於評估、訓練、微調或改進供應商自身更為廣泛的系統；另一份則可能將其使用範圍限制於提供、保障及支援合約範圍的服務。即使合約明文禁止資料用於模型訓練，獨立的權利條款仍可能允許供應商進行分析、基準測試、安全監控或產品開發。

這些活動在技術與商業層面上均屬不同範疇。因此，合約應明確界定相關資料類別、各項資料可被使用的目的、可能受惠的系統，以及合作關係終止後合約方是否仍受合約條文限制。這些都是協商與起草合約時的重點，但它們往往被人忽略。

許多以人工智能作為基礎的服務可透過累積反饋、評估及工作流程改善而提升價值。此等價值最終究竟歸屬於客戶、服務供應商，抑或由雙方共享，將取決於技術架構、合約中的權利分配，以及各方如何分配未來收益。

知識產權日趨複雜

人工智能不僅使知識產權的傳統假設更趨複雜，更為其帶來了革命性的改變。

許多機構假設數據的擁有權將自然延伸為由該數據所創造的一切成果的擁有權。實際上，人工智能項目往往包含專有資料、授權內容、第三方模型，以及在實施過程中產生的新資產。

針對特定客戶的知識庫、提示詞庫、檢索配置、評估框架、智能代理工作流程（agent workflow）及整合方案本身可能具備商業價值。相關權利可能由客戶、服務提供者及其他獨立技術供應商共同持有。

關於由人工智能輔助或生成的內容是否存在知識產權、誰有權行使此類權利、客製化模型的處理方式，以及對特定項目改進的再利用等問題，正變得日益重要。上述問題的答案將取決於適用法律、人類所作出的貢獻的程度與性質，以及相關的合約安排。

在某些人工智能項目中，具有商業價值的知識產權與專有技術，可能在項目初期並未存在，而是透過過程中的實施方式、客製化及操作逐步產生。

控制可能比所有權更為重要

企業人工智能帶來了一項在採購過程中未必顯而易見的挑戰：依賴性。

許多機構圍繞第三方供應或控制的技術，建構出具有戰略重要性的能力，卻往往未能充分認知由此產生的依賴性。這未必會造成問題。但這意味著若機構的底層能力存取權限發生變化，周邊資產（**surrounding assets**）的擁有權所提供的保護可能相當有限。無論支援該系統的數據歸誰所有，定價、功能、服務可用性及戰略方向皆可能影響人工智能系統的實際效用。

因此，正在審查人工智能合約安排的機構應考量可攜性、退出權、過渡協助以及供應商集中風險。採購人工智能已不再僅僅是為取得技術，它更關乎維護戰略靈活性，並避免過度依賴單一供應商。

人工智能合約正逐漸成為管治文件

許多機構仍將人工智能合約視為單純的採購文件。然而，這些合約也日益成為機構的人工智能管治框架的一部分。它們雖無法取代內部管治，但能將管治要求轉化為涉及資料、數據管理、測試、監控、安全、審查支援、事件應變、變更管理及人類監督等方面的義務。

人工智能管治框架通常強調問責制度、人類監督、透明度、可審查性、適當監控以及在人工智能生命週期中明確的責任劃分。在香港，私隱專員公署的《[人工智能\(AI\)：個人資料保障模範框架](#)》為採購、實施及使用任何類型人工智能系統的機構在人工智能管治中，就保障個人資料私隱方面，提供建議及最佳行事常規。這些期望會產生實際的合約後果。諸如由誰監控系統效能、評估重大變更或效能下降、調查事件、維護相關紀錄、支援人工審查以及回應監管機構查詢等問題，僅憑管治政策是無法解決的。

因此，人工智能採購與人工智能管治之間的界線正逐漸模糊。人工智能合約往往充當將管治期望轉化為營運義務的機制。



採購人工智能已不再僅僅是為取得技術，它更關乎維護戰略靈活性，並避免過度依賴單一供應商。

責任未必伴隨擁有權

其中一項最重要的觀察是：擁有權與責任往往朝著不同的方向發展。

某供應商可能控制底層模型或服務的存取權限；另一供應商則可能負責營運基礎設施；系統整合商則可能開發針對客戶的特定工作流程或整合方案。然而，當問題浮現時，儘管有第三方供應商的存在，監管機構、客戶及其他持份者仍可能將目光投向使用該系統並依賴其輸出內容的機構。

對於在受監管環境中運作的機構而言，技術的擁有權僅能反映部分情況。即使系統、模型或基礎設施由第三方提供，使用該系統的機構仍可能保留重大的管治、監督及營運責任。合約上的責任分配可規範各方關係，並可在法律允許的情況下改變適用法律或法規下的預設立場。因此，在採用人工智能服務時，審慎的規劃、合約起草及風險分配至關重要。

這正是為什麼人工智能管治與採購日益超越傳統軟件授權的概念，延伸至可解釋性（**explainability**）、測試、安全性、可審查性及人類監督等議題的原因之一。

實務觀點

有效的人工智能合約審查不應局限於擁有權條款。

更實用的做法是考慮三個更廣泛的主題：

- **價值：**系統所創造的價值最終歸屬何處？
- **控制：**若技術、商業關係或戰略優先事項發生變化，誰將控制該能力？
- **責任：**當系統產生意外結果時，誰應承擔責任？

這些考量往往比任何單一合約條款更能揭示風險與機遇的真實分配狀況。

我們能夠如何提供協助

人工智能採購正處於技術、知識產權、資料私隱、管治、合規和商業策略的交匯處。

我們在知識產權（包括但不限於版權、商標及專利）、技術合約、管治和監管風險方面有著豐富的經驗，能夠協助機構評估或審查人工智能相關的安排。相關的議題可能包括數據的允許使用範圍、模型改進權（**model improvement rights**）、擁有權和授權、技術依賴性、監管機制，以及參與者之間的責任分配。

如果您的機構正在採購、部署或審查人工智能能力（**AI capabilities**），針對性的審查有助於釐清現有安排是否妥善處理價值、控制與責任的議題，以及這些安排是否與貴機構更廣泛的商業和管治目標一致。

我們很樂意與您探討上述議題將如何影響您現有或擬議的人工智能安排。

作者

蘇振國是銘德有限法律責任合夥律師事務所的合夥人。他為企業提供管治、監管和風險管理相關的法律意見，包括因採用新技術而產生的問責、監督和技術風險。

張浩然是銘德有限法律責任合夥律師事務所的律師。他協助客戶處理具爭議和無爭議的知識產權事宜（包括但不限於版權、商標、設計、專利、機密資料等）、技術合約和數據相關事項，包括技術項目所衍生的擁有權、授權和權利分配等問題。

蘇律師和張律師從管治、技術風險、知識產權及技術合約等角度，為企業人工智能的採用及部署帶來不同觀點和見解。



蘇振國

合夥人，香港

T: 2841 6879

E: eddy.so@minterellison.com



張浩然

律師，香港

T: 2841 6805

E: kennis.cheung@minterellison.com

銘德及有關辦事處：

阿德萊德 奧克蘭 布里斯班 坎培拉 達爾文 黃金海岸 香港 倫敦 墨爾本 珀斯 悉尼 烏蘭巴托 威靈頓

本通訊由銘德有限法律責任合夥律師事務所編寫，用於略舉相關時期的某些事項，僅供參考，並不旨在提供全面內容。本通訊並非用於提供法律意見，其內容也不構成法律意見，任何人亦不應出於任何一般目的或就特定交易及/或情況依賴本通訊的內容。您應在將本通訊的資訊應用在特定情況之前尋求專業意見。如果您對本通訊有任何疑問或意見，請聯絡您在銘德有限法律責任合夥律師事務所的日常連絡人。銘德有限法律責任合夥律師事務所對於基於依賴本通訊的資訊而造成的任何損失不承擔任何責任。

© 2026 銘德有限法律責任合夥律師事務所