

企业人工智能合同：价值、控制与责任的真正归属

作者：苏振国、张浩然

我们在先前发表的文章《[企业人工智能中的隐性所有权问题](#)》中探讨了保留对数据权利与控制未必等于能保留由数据所创造的价值。

这项观察有着重要的实务影响。

企业人工智能所衍生的许多重大问题，并非取决于技术本身，而是取决于机构内部如何通过合同安排采购、部署及管理人工智能系统。随着人工智能从实验阶段迈向关键业务部署（**business-critical deployment**）阶段，这些合同安排将日渐决定价值归属何处、谁控制由此产生的能力，以及谁须为其后果承担责任。

“**人工智能合同往往充当将治理期望转化为运营义务的机制。**

数据所有权仅是起点

大多数关于人工智能合同的讨论，往往从基础数据的所有权开始。这固然重要，但鲜少是分析的终点。

在许多商业安排中，各方都能确定在该安排中提供或控制的资料。然而，更具商业意义的问题往往在于在该安排中提供的资料在日后可如何被使用。为了提供特定服务而获得处理资料的权利是一回事。但是否拥有权利将同一资料用于测试、基准比较、分析、模型开发或未来服务改进，则是截然不同的另一回事。

因此，有效的合同审查应同时考量资料的允许使用范围、所有权和控制权。问题的关键不仅在于服务提供者能否存取资料，更在于其能否，以及基于何种目的，从该资料中获取超出当前可预见合作范围的价值。

未来价值取决于数据的使用与改进的权利

人工智能合同中最重要的一环在于客户资料可被如何使用。两份都规定客户保留其为合作目的所提供的资料的权利的协议，可以产生实质上截然不同的商业结果。

一份协议可能允许将提示词、输出内容、反馈或使用资料用于评估、训练、微调或改进供应商自身更为广泛的系统；另一份则可能将其使用范围限制于提供、保障及支持合同范围的服务。即使合同明文禁止资料用于模型训练，独立的权利条款仍可能允许供应商进行分析、基准测试、安全监控或产品开发。

这些活动在技术与商业层面上均属不同范畴。因此，合同应明确界定相关资料类别、各项资料可被使用的目的、可能受惠的系统，以及合作关系终止后合同方是否仍受合同条文限制。这些都是协商与草拟合同时的重点，但它们往往被人忽略。

许多以人工智能作为基础的服务可通过累积反馈、评估及工作流程改善而提升价值。此等价值最终究竟归属于客户、服务供应商，抑或由双方共享，将取决于技术架构、合同中的权利分配，以及各方如何分配未来收益。

知识产权日趋复杂

人工智能不仅使知识产权的传统假设更趋复杂，更为其带来了革命性的改变。

许多机构假设数据的所有权将自然延伸为由该数据所创造的一切成果的所有权。实际上，人工智能项目往往包含专有资料、授权内容、第三方模型，以及在实施过程中产生的新资产。

针对特定客户的知识库、提示词库、检索配置、评估框架、智能代理工作流程（**agent workflow**）及整合方案本身可能具备商业价值。相关权利可能由客户、服务提供者及其他独立技术供应商共同持有。

关于由人工智能辅助或生成的内容是否存在知识产权、谁有权行使此类权利、定制化模型的处理方式，以及对特定项目改进的再利用等问题，正变得日渐重要。上述问题的答案将取决于适用法律、人类所作出的贡献的程度与性质，以及相关的合同安排。

在某些人工智能项目中，具有商业价值的知识产权与专有技术，可能在项目初期并未存在，而是通过过程中的实施方式、定制化及操作逐步产生。

控制可能比所有权更为重要

企业人工智能带来了一项在采购过程中未必显而易见的挑战：依赖性。

许多机构围绕第三方供应或控制的技术，建构出具有战略重要性的能力，却往往未能充分认识由此产生的依赖性。这未必会造成问题。但这意味着若机构的底层能力存取权限发生变化，周边资产（**surrounding assets**）的所有权所提供的保护可能相当有限。无论支持该系统的数据归谁所有，定价、功能、服务可用性及战略方向皆可能影响人工智能系统的实际效用。

因此，正在审查人工智能合同安排的机构应考量可迁移性、退出权、过渡协助以及供应商集中风险。采购人工智能已不再仅仅是为取得技术，它更关乎维护战略灵活性，并避免过度依赖单一供应商。

人工智能合同正逐渐成为治理文件

许多机构仍将人工智能合同视为单纯的采购文件。然而，这些合同也日渐成为机构的人工智能治理框架的一部分。它们虽无法取代内部治理，但能将治理要求转化为涉及资料、数据管理、测试、监控、安全、审查支持、事件应变、变更管理及人类监督等方面的义务。

人工智能治理框架通常强调问责制度、人类监督、透明度、可审查性、适当监控以及在人工智能生命周期中明确的责任划分。在香港，私隐专员公署的《[人工智能\(AI\)：个人资料保障模范框架](#)》为采购、实施及使用任何类型人工智能系统的机构在人工智能治理中，就个人信息保护方面，提供建议及最佳行事常规。这些期望会产生实际的合同后果。诸如由谁监控系统效能、评估重大变更或效能下降、调查事件、维护相关记录、支持人工审查以及回应监管机构查询等问题，仅凭治理政策是无法解决的。

因此，人工智能采购与人工智能治理之间的界线正逐渐模糊。人工智能合同往往充当将治理期望转化为运营义务的机制。

“ 采购人工智能已不再仅仅是为取得技术，它更关乎维护战略灵活性，并避免过度依赖单一供应商。”

责任未必伴随所有权

其中一项最重要的观察是：所有权与责任往往朝着不同的方向发展。

某供应商可能控制底层模型或服务的存取权限；另一供应商则可能负责运营基础设施；系统整合商则可能开发针对客户的特定工作流程或整合方案。然而，当问题浮现时，尽管有第三方供应商的存在，监管机构、客户及其他利益相关方仍可能将目光投向使用该系统并依赖其输出内容的机构。

对于在受监管环境中运作的机构而言，技术的所有权仅能反映部分情况。即使系统、模型或基础设施由第三方提供，使用该系统的机构仍可能保留重大的治理、监督及运营责任。合同上的责任分配可规范各方关系，并可在法律允许的情况下改变适用法律或法规下的预设立场。因此，在采用人工智能服务时，审慎的规划、合同草拟及风险分配至关重要。

这正是为什么人工智能治理与采购日益超越传统软件授权的概念，延伸至可解释性（**explainability**）、测试、安全性、可审查性及人类监督等议题的原因之一。

实务观点

有效的人工智能合同审查不应局限于所有权条款。

更实用的做法是考虑三个更广泛的主题：

- **价值：**系统所创造的价值最终归属何处？
- **控制：**若技术、商业关系或战略优先事项发生变化，谁将控制该能力？
- **责任：**当系统产生意外结果时，谁应承担 responsibility？

这些考量往往比任何单一合同条款更能揭示风险与机遇的真实分配状况。

我们能够如何提供协助

人工智能采购正处于技术、知识产权、数据隐私、治理、合规和商业策略的交汇处。

我们在知识产权（包括但不限于著作权、商标及专利）、技术合同、治理和监管风险方面有着丰富的经验，能够协助机构评估或审查人工智能相关的安排。相关的议题可能包括数据的允许使用范围、模型改进权（**model improvement rights**）、所有权和授权、技术依赖性、监管机制，以及参与者之间的责任分配。

如果您的机构正在采购、部署或审查人工智能能力（**AI capabilities**），针对性的审查有助于厘清现有安排是否妥善处理价值、控制与责任的议题，以及这些安排是否与贵机构更广泛的商业和治理目标一致。

我们很乐意与您探讨上述议题将如何影响您现有或拟议的人工智能安排。

作者

苏振国是铭德有限法律责任合伙律师事务所的合伙人。他为企业治理、监管和风险管理相关的法律意见，包括因采用新技术而产生的问责、监督和技术风险。

张浩然是铭德有限法律责任合伙律师事务所的律师。他协助客户处理具争议和无争议的知识产权事宜（包括但不限于著作权、商标、设计、专利、机密资料等）、技术合同和数据相关事项，包括技术项目所衍生的所有权、授权和权利分配等问题。

苏律师和张律师从治理、技术风险、知识产权及技术合同等角度，为企业人工智能的采用及部署带来不同观点和见解。



苏振国

合伙人，香港

T: 2841 6879

E: eddy.so@minterellison.com



张浩然

律师，香港

T: 2841 6805

E: kennis.cheung@minterellison.com

铭德及有关办事处：

阿德莱德 奥克兰 布里斯班 堪培拉 达尔文 黄金海岸 香港 伦敦 墨尔本 珀斯 悉尼 乌兰巴托 惠灵顿

本通讯由铭德有限法律责任合伙律师事务所编写，用于略举相关时期的某些事项，仅供参考，并不旨在提供全部内容。本通讯并非用于提供法律意见，其内容也不构成法律意见，任何人亦不应出于任何一般目的或就特定交易及/或情况依赖本通讯的内容。您应在将本通讯的信息应用在特定情况之前寻求专业意见。如果您对本通讯有任何疑问或意见，请联络您在铭德有限法律责任合伙律师事务所的日常联系人。铭德有限法律责任合伙律师事务所对于基于依赖本通讯的信息而造成的任何损失不承担任何责任。