

AI ベンダーと企業データを共有することに伴う潜在的リスク **The Hidden Risks of Sharing Company Data with AI Vendors**

文書の分析、ワークフローの自動化、ビジネス上の知見の生成などを目的として、第三者である AI プラットフォームを利用する企業が増えるにつれ、多くの企業が自社の最も重要な資産である自社独自のデータをベンダーに提供することが見受けられるようになりました。こうしたツールは業務効率を大幅に向上させる可能性があります、企業はアップロードされた情報がその後どう扱われるのかを理解しておく必要があります。ベンダーの利用規約によっては、企業データが保持され、AI モデルの改善に使用されたり、下請け業者と共有されたり、あるいは複数の法域にまたがって保存されたりする可能性があります。たとえベンダーが秘密保持を約束していたとしても、適切な契約上の保護措置が講じられていなければ、企業は営業秘密、機密性の高い事業情報、顧客データ、知的財産などを流出させるリスクにさらされることになります。

特に知的財産への影響は重大なものとなり得ます。営業秘密の保護は、一般的に、秘密を維持するための合理的な措置を講じているかどうか重要です。もし適切な制限を設けず機密情報を第三者である AI プロバイダーに広く共有した場合、営業秘密としての保護が損なわれたのではないという疑義が生じる可能性があります。さらに企業は、AI が生成した成果物の所有権は誰にあるのか、アップロードされたデータについてベンダーが何らかの権利を取得するのか、そして顧客情報を将来のモデルの学習に使用しないことにベンダーが合意しているか、といった点も慎重に検討すべきです。規制業種に属する事業を行う企業は、AI システムを通じて機密情報が処理される際に適用される、プライバシー、サイバーセキュリティ、データガバナンスに関する義務についても考慮する必要があります。

AI を活用したサービスを導入する前に、企業はデータの所有権、利用許諾範囲、データ保持に関する施策、セキュリティ管理体制、補償条項、秘密保持義務などに重点を置いて、ベンダーとの契約内容を慎重に精査すべきです。導入段階で十分に検討を行うことで、AI のメリットを享受しつつ、意図しない情報開示、知的財産権の喪失、あるいはデータやモデルの成果物をめぐる将来的な紛争のリスクを最小限に抑えることができます。AI 技術やそれを取り巻く法的リスクは絶えず変化しているため、近時、AI ベンダーとの契約の見直しを実施していない企業は、改めて確認を行うことをお勧めします。

本記事の内容についてご質問がございましたら、著者、または増田・舟井・アイファート・ミッチェル法律事務所の知的財産テクノロジー・部門のメンバーまでお問い合わせください。

The Hidden Risks of Sharing Company Data with AI Vendors

As companies increasingly rely on third-party artificial intelligence platforms to analyze documents, automate workflows, and generate business insights, many are providing vendors with some of their most valuable assets: proprietary data. While these tools can offer significant efficiencies, businesses should understand what happens to their information once it is uploaded. Depending on the vendor's terms of service, company data may be retained, used to improve AI models, shared with subcontractors, or stored across multiple jurisdictions. Even where a vendor promises confidentiality, organizations risk exposing trade secrets, sensitive business information, customer data, or intellectual property if appropriate contractual safeguards are not in place.

The intellectual property implications can be particularly significant. Trade secret protection generally depends on maintaining reasonable measures to preserve secrecy. If confidential information is broadly shared with third-party AI providers without adequate restrictions, questions may arise regarding whether trade secret protections have been compromised. In addition, companies should carefully examine who owns AI-generated outputs, whether the vendor receives any rights in the uploaded data, and whether the vendor has agreed not to use customer information to train future models. Businesses operating in regulated industries should also consider privacy, cybersecurity, and data governance obligations that may apply when sensitive information is processed through AI systems.

Before adopting an AI-enabled service, companies should carefully review vendor agreements with a focus on data ownership, permitted uses, retention practices, security controls, indemnification provisions, and confidentiality obligations. A thoughtful assessment at the outset can help organizations capture the benefits of AI while minimizing the risk of unintended disclosure, loss of intellectual property rights, or future disputes over data and model outputs. Companies that have not recently evaluated their AI vendor contracts may wish to do so as AI technologies—and the legal risks surrounding them—continue to evolve.

If you have any questions regarding the content of this article, please contact the author or any member of Masuda Funai's Intellectual Property and Technology Practice Group.