Securing Sensitive Data: Contract Clauses for AI Integration

May 27, 2025

Artificial Intelligence (AI) is no longer confined to specialized platforms like ChatGPT or other large language models. Everyday business software—including common suites from Microsoft and Adobe—has begun integrating AI-driven features that may process, store, or learn from user input. This evolving landscape creates unique risk considerations regarding how confidential and sensitive data is handled.

Organizations must remain vigilant about the risk that confidential data could be inadvertently retained, analyzed, or shared outside intended boundaries. For example, if a user inadvertently inputs trade secrets into an AI-powered software tool, there is no absolute guarantee that the tool will not use, store, or train on that data, potentially making it accessible for other purposes. Such incidents raise legal and compliance concerns, especially when sensitive or proprietary information is involved.

In response to these concerns, many companies are adopting contract language that addresses the use of AI systems. These clauses aim to prevent the unintentional disclosure of private data and ensure that neither party uses the other's confidential information to develop or enhance any AI models. By including clear guardrails and usage parameters, parties can leverage the benefits of AI tools while maintaining strong confidentiality standards.

Although every contract should be tailored to the specific

circumstances of the parties involved, clauses that are appearing in modern contracts generally read somewhat along the following lines:

> *"AI System" refers to any Artificial Intelligence software or functionality, whether generative or otherwise, including but not limited to machine learning models, large language models, or embedded tools within third-party platforms. Each Party agrees that no Party shall disclose or provide Confidential Information to an AI System that can be accessed by individuals or entities other than the disclosing Party and the receiving Party, unless expressly authorized in writing. Confidential Information shall not be used to train, develop, fine-tune, or otherwise enhance any AI System, algorithm, or related dataset without prior written consent of the other Party. Furthermore, any AI System utilized must be configured or managed so it does not retain, learn from, or generate future outputs based on the disclosing Party's Confidential Information unless expressly permitted. Each Party shall implement appropriate technical and organizational measures to ensure that any AI System used in the course of performance under this Agreement cannot inadvertently store, transmit, or share Confidential Information in contravention of this provision.*

Such contract language underscores the importance of transparency and proactive protection of sensitive data in an AI-driven environment. As AI technologies become increasingly pervasive, it is prudent to adopt contractual safeguards that help all parties preserve the confidentiality and integrity of proprietary information.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com