Strelia M&A Series

April 2023

M&A in the AI Market – Addressing the Unique Challenges Ahead

AI is influencing and transforming every aspect of the economy. As the number of AI companies continues to grow, we are also seeing a hike in M&A activity in this industry. While AI potential and benefits are significant, it comes with unique and evolving legal challenges. In this Strelia M&A Series, we look at some of the legal implications of AI M&A, including the need for heightened due diligence, the importance of AI-specific representations and warranties, and regulatory risks that are specific to the AI industry, including FDI-related risks.

AI Due Diligence - Concentrating in Key Areas

Conducting due diligence on AI companies requires a buyer to focus specifically on key areas like IP ownership, data protection, cybersecurity, and ethics.

Assessing IP ownership of AI technologies and systems is a challenging task for any buyer because there is no single type of IP right that can safeguard the entire technology system. However, a combination of various IP rights may apply to different components of the AI system. Patents and copyrights are not always available or may be insufficient. Trade secrets protection can shield confidential information, hence numerous elements of an AI system. To evaluate the target's IP ownership, the buyer must consider a holistic approach, and in addition to patents and copyright protection, concentrate on assessing the measures that the target took to keep its AI system confidential. These could include NDAs, employment contract terms, cybersecurity measures, internal policies, and other relevant aspects.

Data are crucial assets for any AI company. They are also a major consideration in M&A transactions. However, data are regulated extensively, particularly in industries like healthcare and finance. Buyers must therefore thoroughly evaluate the data regulatory framework that applies to the specific industry in which the AI target operates. Buyers should also assess whether the target's data collection and processing comply with relevant laws and regulations and determine who bears the risk in third-party arrangements concerning data processing.

Cybersecurity risks in the context of AI are higher, so buyers must conduct cybersecurity-focused due diligence investigations. This is because the AI-generated output depends on the data input. If the data input is compromised, the results may be affected. AI systems that rely heavily on machine-learning algorithms or AI Systems that are connected through the internet are particularly vulnerable to cyber-attacks. Therefore, buyers should analyze the target's cybersecurity risk profile in depth, ensuring that the target is compliant by assessing any past incidents and how they were managed, and reviewing the target's response plan.

Buyers should also bear in mind ethical concerns in AI technologies and systems. To address these, buyers should identify the risks, check the target's policies and procedures, assess the target's corporate culture, identify regulatory requirements, review the impact on stakeholders, and consider potential AI bias.

AI Representations and Warranties - Revisiting Standard Risk Allocation

With AI technologies and systems being so distinct, this means that standard IP representations and warranties no longer suffice. Representations and warranties in AI transactions are certainly more intricate and nuanced because of its unique nature and its reliance on data and algorithms. And because representations and warranties serve as the foundation in risk allocation between a buyer and a seller, customizing them to cover

each feature of the AI technology at stake also affects the risk allocation.

AI-specific Regulatory Risk - Giving Appropriate Attention

A range of regulations already govern the AI industry. The draft EU AI Regulation aims to put requirements in place on AI systems, with a focus on high-risk AI applications. Buyers should expect the regulatory burden on AI businesses to become heavier and should give appropriate attention to how the target embeds existing and anticipated legal and regulatory standards in its business.

FDI (foreign direct investment) and national security regulations may also be relevant, depending on the nature of the AI technology and system. Several jurisdictions already have national security and FDI rules and regulations in place that specifically address AI, among other technologies.

Gisèle Rosselle
Partner
gisele.rosselle@strelia.com

Céderic Devroey
Senior Associate
cederic.devroey@strelia.com

Marie-Elisabeth Dubois
Associate
marie-elisabeth.dubois@strelia.com