AI, Machine Learning & Big Data 2026

Eighth Edition

Contributing Editor:
Charles Kerrigan
CMS LLP

glg Global Legal Group

TABLE OF CONTENTS

Hungary

Endre Várady
János Tamás Varga
Andrea Belényi

VJT & Partners

Trends

The Hungarian artificial intelligence (AI) landscape is characterised by the rapid expansion of practical use cases across industries, combined with growing regulatory pressure and strategic repositioning by both businesses and policymakers.

From a business perspective, AI adoption is no longer experimental. A wide variety of use cases has emerged across sectors including workflow optimisation, predictive analytics, fraud detection, customer interaction and decision-support systems. In manufacturing and logistics, AI is primarily used for predictive maintenance and supply chain optimisation, while in financial services it plays a key role in risk assessment, compliance (particularly transaction monitoring) and fraud detection.

Across sectors, a notable technological shift is underway: the transition from generative AI to more agentic AI systems, where technology not only supports decision-making but increasingly executes tasks autonomously. As AI systems move beyond supporting decisions to actively executing tasks, they create new legal and operational challenges, driven by their autonomy, access to sensitive data and direct impact on real-world outcomes.

From a regulatory perspective, the implementation of the EU AI Act marks a significant structural development. Hungary has begun establishing its institutional framework by designating two key authorities: the National Accreditation Authority, responsible for the registration and conformity assessment of high-risk AI systems; and a market surveillance authority tasked with ongoing oversight, enforcement and the operation of a regulatory sandbox. Beyond these institutional steps, Hungary has so far largely aligned with the EU framework without introducing significant local deviations.

The competitive landscape is defined by intensifying pressure on companies to accelerate AI adoption. Businesses face a dual challenge: keeping pace with technological developments while managing legal and operational risks. In practice, many organisations are still at an early stage in building internal governance frameworks, which creates a "move fast and break things" dynamic, potentially leading to significant legal, financial and reputational exposure.

The key legal issues arising from AI adoption do not stem solely from AI-specific regulation. Instead, a broad range of existing horizontal legal frameworks apply, including civil liability, consumer protection,

competition law, employment law, data protection, cybersecurity and intellectual property (IP). This creates a complex and fragmented compliance environment where AI-related risks must be assessed holistically rather than in isolation.

At the same time, companies are increasingly seeking to maximise the value of data as a strategic asset. As in other jurisdictions, business models are shifting towards more data-driven approaches, but this transition requires a higher level of data governance maturity. In Hungary, this is closely linked to broader policy developments, including the government's National AI Strategy for 2025–2030 (AI Strategy) and the anticipated implementation of the EU Data Act. While the strategy outlines an ambitious framework for data governance, its practical impact will ultimately depend on how this framework is translated into concrete legal and institutional arrangements and implemented in practice.

From a policy standpoint, the government maintains a supportive but structured approach to AI adoption. The updated AI Strategy reflects a holistic vision, focusing on data governance, the development of ethical and legal frameworks, the creation of data platforms and testing environments, and the clarification of responsibilities across the AI value chain. At the same time, increasing attention is being paid to AI safety, trust and ethical considerations, although practical implementation remains at an early stage.

State support for AI development is primarily channelled through strategic initiatives and ecosystem-building measures outlined in the AI Strategy, including support for innovation, data infrastructure and cooperation between public and private actors.

In terms of sectoral leadership, financial services remain at the forefront of AI adoption, driven by strong regulatory incentives and data availability. Other leading sectors include manufacturing and telecommunications. Across these sectors, demand for AI-related advisory is increasing, particularly in the area of AI risk management, where businesses are seeking integrated guidance covering legal, technical and organisational aspects.

Overall, the defining trend in Hungary is that AI is becoming a core business capability while simultaneously evolving into a highly regulated and risk-sensitive domain. The key challenge for businesses is not only technological adoption, but the ability to embed AI into operations in a compliant, controlled and strategically aligned manner.

Ownership/protection

The ownership and protection of AI systems in Hungary is governed not by AI-specific rules, but by a combination of IP, contractual arrangements and data-related frameworks, which together create a layered and fragmented regime.

Ownership of AI algorithms

Under Hungarian law, ownership of AI-related software and algorithms depends primarily on the employment relationship or contractual framework. As a general rule, software and inventions created by employees within the scope of their employment duties vest in the employer in terms of economic rights, while the author remains the natural person and retains moral rights.

A key condition is that the work must be created as part of the employee's job responsibilities. In practice, this makes internal documentation and role definition critical in determining ownership.

From an IP perspective, copyright protects only the expression of the software – such as the source code or its specific implementation – but not the underlying ideas, principles or algorithms as such. As a result, competitors may independently develop similar solutions, provided they do not infringe copyright or misuse trade secrets or protected know-how under Hungarian trade secret rules.

Key IP issues arising in practice

Several practical challenges arise in relation to AI development and deployment.

First, authorship and ownership may become unclear, particularly in multi-developer environments or where AI-assisted coding tools are used. Second, the use of third-party training data raises significant legal risks, especially where the origin or licensing of datasets is uncertain. Ensuring a "clean dataset" is increasingly becoming a central compliance issue.

Third, traditional IP frameworks are not always well suited to AI systems. Since abstract algorithms are not protected as such, companies often face difficulties in securing exclusive rights over their core technological solutions. In this context, know-how and trade secrets frequently become more effective protection tools than formal IP rights.

In addition, contractual issues are becoming more complex. AI-related licence agreements often differ from traditional software licences, particularly because the concept of "use" becomes more fluid, encompassing activities such as model modification, fine-tuning and integration with other systems, which may extend beyond the originally authorised scope. These issues require more detailed and forward-looking contractual structuring.

AI-generated content and inventions

Hungarian copyright law is based on the principle of human creative activity. As such, purely AI-generated content is unlikely to qualify for copyright protection unless there is sufficient human input to meet the originality threshold.

From a patent perspective, AI-related inventions may be protected if they meet the requirements of novelty, inventive step and industrial applicability. However, abstract methods or algorithms in themselves are not patentable as such, which limits the scope of protection for certain types of AI innovation.

Protection of technology and data

In practice, companies rely on a combination of protection mechanisms. Patents may be used for technical solutions, copyright for software, and contractual arrangements – such as non-disclosure and licensing agreements – for controlling use and access.

However, in the AI context, trade secret protection plays a particularly central role, especially where patent protection is not available or would require disclosure of sensitive information. The Hungarian Trade Secret Act provides a framework for protecting algorithms, datasets and other confidential business information, provided that appropriate internal safeguards are in place.

Additional ownership challenges

Beyond core IP issues, several additional ownership-related questions arise.

These include the ownership of training data and databases, the allocation of rights between employers and independent contractors, and the treatment of contributions from multiple parties in collaborative development environments. Cross-border development further complicates these issues, raising questions of applicable law and jurisdiction.

Liability for infringing outputs also represents an emerging concern, particularly where AI systems generate content that may violate third-party rights.

Data ownership, security and privacy

Hungarian and EU law do not recognise "ownership" of data in a traditional property sense. Instead, data is regulated through a combination of data protection, trade secret and cybersecurity rules.

Personal data is governed primarily by the General Data Protection Regulation (GDPR) and its Hungarian implementation framework, while business-related data may be protected through trade secret law and contractual arrangements. This creates a functional rather than proprietary approach to data control.

Balancing IP protection and regulatory requirements

A key challenge for businesses is to strike a balance between protecting IP and complying with increasing regulatory obligations, particularly under the EU AI Act.

While companies seek to preserve trade secrets and proprietary technologies, they are also required to ensure transparency, documentation and auditability, especially for high-risk AI systems. Importantly, the "black box" nature of AI does not eliminate the need for explainability – legal frameworks increasingly require that systems be explainable, even if not fully interpretable at a technical level.

Overall, Hungarian and EU regulation follow a risk-based approach, imposing stricter requirements on high-risk AI systems while maintaining a degree of flexibility to support innovation.

The practical challenge for businesses lies in designing protection and compliance strategies that can operate effectively within this dual framework.

Antitrust/competition laws

The application of Hungarian competition law to AI and big data raises a number of novel and evolving challenges, particularly in relation to algorithmic decision-making and data-driven market power.

Algorithmic collusion

Under Hungarian competition law, algorithmic collusion may still qualify as a prohibited agreement or concerted practice even in the absence of explicit human coordination. Where companies knowingly deploy algorithms that result in coordinated market behaviour – such as price alignment – competition authorities are likely to attribute responsibility to the undertaking.

In this context, liability does not depend on direct human interaction, but rather on whether the undertaking could reasonably foresee or control the outcome of the algorithmic system. This reflects a broader enforcement approach, under which companies cannot avoid competition law liability by delegating decision-making to automated systems.

At the same time, purely autonomous and genuinely unforeseeable algorithmic collusion remains a theoretical grey area. However, in practice, authorities tend to interpret responsibility broadly, placing the burden on companies to ensure that their AI systems do not produce anti-competitive outcomes.

Big data and market power

The increasing importance of data as a strategic asset also raises significant competition law concerns. The accumulation and control of large datasets can reinforce market power and create barriers to entry, particularly where access to data becomes a key competitive parameter.

In certain cases, data may function as an essential input, and restrictions on access may raise dominance-related concerns under Hungarian and EU competition law. Beyond dominance, big data can also facilitate collusive behaviour, for example, by increasing the ability of competitors to monitor each other's behaviour or enabling real-time algorithmic pricing that automatically reacts to competitors' prices, potentially leading to coordinated outcomes.

Finally, data accumulation may enable various forms of exclusionary conduct, including tying, bundling or self-preferencing practices in digital ecosystems. These concerns are particularly relevant in platform-based business models, where control over data, users and infrastructure can reinforce competitive advantages.

Board of directors/governance

Effective governance is a critical component of AI adoption. In practice, implementing AI without proper

governance is comparable to driving a car without a steering wheel: movement is possible, but direction and control are fundamentally lacking.

In the absence of detailed local guidance, Hungarian businesses should align with international best practices and emerging EU expectations. This typically includes the mapping of AI systems, stakeholder identification with clearly defined roles and responsibilities, structured use case authorisation processes, vendor due diligence, and role-based training and awareness programmes.

Similarly to the "privacy by design" approach under GDPR, organisations should aim to embed key principles – such as transparency, fairness, human oversight and accountability – into AI systems from the outset. Governance should not be a one-off exercise, but rather a continuous process, supported by ongoing risk monitoring, testing and improvement.

Impact on due diligence

AI and big data significantly expand the scope of legal and technical due diligence. In addition to traditional IT and data protection reviews, companies must assess AI-specific elements such as training data, model architecture, technical documentation, data governance frameworks and compliance with emerging regulatory standards.

In this context, evolving market practice – such as emerging AI-related contractual clauses – can provide useful guidance on how diligence processes should be structured. Increasingly, due diligence must also address how AI systems are integrated into broader business operations and decision-making processes.

Impact on fiduciary duties

The use of AI has direct implications for directors' fiduciary duties under Hungarian law. Directors are required to act with the care generally expected from persons in such positions, which in an AI context means that they cannot rely blindly on automated systems.

Instead, directors are expected to understand the key risks associated with AI deployment – including data use, bias, regulatory compliance and operational risks – and to ensure that appropriate governance and control mechanisms are in place.

Liability will typically be assessed based on whether directors acted on an informed basis, in good faith and in the best interests of the company. The use of AI systems without adequate validation, oversight or risk assessment may fall short of this standard.

Setting the right governance framework, including proper documentation, internal approvals and oversight mechanisms, is therefore essential – not only to ensure trustworthy AI and maintain stakeholder confidence, but also to mitigate potential management liability under the Hungarian Civil Code.

Impact on communication

AI also affects how companies communicate with both internal and external stakeholders.

From an internal perspective, Hungarian law does not impose specific AI-related disclosure obligations on shareholders beyond general corporate governance rules. However, given the increasing relevance and risk profile of AI, regular and structured reporting to shareholders is advisable in order to support informed decision-making and reduce liability exposure.

From an external perspective, transparency requirements are increasing under EU frameworks, including the AI Act and GDPR. Companies must ensure that their communications regarding AI use, capabilities and risks are accurate and not misleading.

This is particularly relevant in the context of so-called "AI washing", where companies overstate the capabilities or reliability of AI systems. While Hungarian enforcement practice has so far focused on areas such as greenwashing, it is reasonable to expect that similar scrutiny may emerge in relation to AI-related claims.

In addition, contractual communication with vendors and partners must address key issues such as data use, liability allocation and audit rights.

Regulations/government intervention

Applicable laws and regulatory framework

Hungary does not currently have a standalone AI statute. Instead, AI-related issues are addressed through a combination of horizontal legal frameworks – including data protection, copyright, contract and tort law – and sector-specific regulation.

However, this landscape is undergoing a fundamental shift with the entry into force of the EU AI Act, which introduces directly applicable, risk-based obligations across Member States. In response, Hungary has begun establishing its national implementation framework, including the designation of competent authorities and the creation of a regulatory sandbox to support compliant innovation.

As a result, Hungary is transitioning from a fragmented, technology-neutral regulatory approach towards a more structured and harmonised AI-specific regime driven at the EU level.

Law reform and upcoming regulation

Beyond the EU AI Act, several additional regulatory developments will significantly shape the Hungarian AI landscape in the coming years.

One of the most important is the implementation of the EU Data Act, which places data governance at the centre of the digital economy. As AI systems are inherently data-driven, the practical impact of the Data Act on data access, sharing and monetisation is expected to be substantial, requiring businesses to rethink their data strategies and contractual frameworks.

Another key development is the revised Product Liability Directive, already implemented in Hungary (coming into force in December 2026). The new framework expands liability beyond traditional physical products to include software and AI systems, effectively extending responsibility across the entire lifecycle of digital and intelligent products.

This represents a significant shift in risk allocation. Hungarian businesses will need to proactively adapt by strengthening internal risk management, revisiting contractual frameworks and preparing for a more complex liability landscape, while maintaining customer trust in increasingly automated systems.

Overall, Hungary is not pursuing an independent AI legislative path but is actively aligning with and implementing EU-level reforms, complemented by national strategic initiatives such as the updated AI Strategy.

Regulatory authorities

While the AI market surveillance authority serves as the central authority under the EU AI Act framework, oversight continues to be fragmented across multiple regulators depending on the legal and sectoral context. Key regulators include:

- the Hungarian Data Protection Authority, which plays a central role in AI-related data processing and profiling under GDPR;
- the Hungarian Competition Authority, responsible for competition and consumer protection issues in digital markets;
- the National Media and Infocommunications Authority, overseeing media and certain digital platform activities; and
- sector-specific regulators, such as the Central Bank of Hungary, which has issued guidance on the use of AI in the financial sector, covering areas such as governance, data management, risk controls, procurement and AI literacy.

Government approach and policy direction

Hungary's regulatory approach to AI closely follows the EU's risk-based model, which imposes stricter obligations on high-risk systems while maintaining flexibility for innovation in lower-risk use cases.

At a policy level, the government seeks to strike a balance between promoting competitiveness and ensuring trust and compliance. This is reflected in the updated AI Strategy, which emphasises the development of a comprehensive legal and ethical framework aligned with EU standards, while also supporting innovation, data-driven growth and the protection of fundamental rights.

In practical terms, this approach requires continued investment not only in technological infrastructure, but also in regulatory capacity, institutional coordination and market awareness. The effectiveness of the framework will ultimately depend on how these elements evolve in parallel.

AI in the workplace

The use of AI in the workplace is no longer a future concept but an emerging operational reality. In practice, AI is already being used in areas such as recruitment screening, CV filtering, performance evaluation and workflow optimisation. However, many employers do not yet perceive these tools as "AI systems" in a regulatory sense and therefore tend to underestimate the associated legal and compliance risks.

From a legal perspective, the most sensitive area is the use of AI in employment-related decision-making. Under the EU AI Act, certain HR applications – such as systems used for recruitment, promotion or employee evaluation – are likely to qualify as high-risk AI systems, triggering enhanced compliance obligations. At the same time, existing Hungarian legal frameworks already impose strict limits. In particular, the principle of equal treatment – covering both direct and indirect discrimination – applies to AI-driven decisions, meaning that biased datasets or outcomes may give rise to liability.

Hungarian labour law also sets clear boundaries on the use of AI in the workplace. Employers may only apply such tools where this is necessary and proportionate, and data processing must be limited to what is required for employment purposes or the enforcement of legal claims. Monitoring of employees may not interfere with private life, and the use of biometric systems is restricted to exceptional, high-risk cases (for example, where necessary to protect life, health or significant financial interests). In addition, where AI systems materially affect working conditions or employee rights, employers are required to consult the works council in advance, reinforcing the importance of transparency and procedural safeguards.

Another practical challenge arises in the employment context, where organisations are increasingly facing the use of so-called "shadow AI". Employees may rely on AI tools – such as generative AI solutions – without formal authorisation or internal guidelines, often to improve efficiency or automate tasks. This creates significant risks, including uncontrolled data use, confidentiality breaches and a lack of oversight, highlighting the need for clear internal employment policies and governance frameworks.

Looking ahead, the role of AI in the workplace is expected to expand significantly, particularly as more advanced and autonomous systems are introduced. As this trend accelerates, Hungarian employers will need to shift from *ad hoc* adoption to a more structured and compliant approach, integrating AI governance into HR processes and ensuring alignment with both regulatory expectations and broader organisational risk management.

Implementation of AI/big data/machine learning into businesses

The implementation of AI within organisations requires a structured and lifecycle-based approach rather than *ad hoc* deployment.

Before introducing AI systems, companies should carry out comprehensive risk assessments and ensure that systems are tested and monitored throughout their lifecycle. In practice, this often follows a continuous improvement model, where systems are regularly reviewed, adjusted and validated.

A key element is the development of "AI by design" frameworks, ensuring that core principles – such as fairness, transparency, non-discrimination, human oversight and robustness – are embedded from the outset rather than addressed retrospectively.

Beyond technical considerations, organisations should adopt a holistic governance approach. This includes, in particular, maintaining an inventory of AI systems, clearly defining roles and responsibilities across stakeholders, and establishing cross-functional processes that integrate legal, technical, business and ethical considerations throughout the AI lifecycle. Internal review mechanisms and ethics functions may support the ongoing identification and mitigation of AI-related risks.

Data governance is another critical success factor. Since AI performance is directly linked to data quality, companies must ensure that datasets are properly selected, documented and controlled.

When relying on third-party AI solutions, contractual structuring becomes particularly important. Agreements should address issues such as liability, indemnification, permitted use and compliance with applicable regulatory requirements. Careful vendor selection is essential to ensure that external solutions meet both technical and legal expectations.

Finally, companies must remain mindful that even prior to the full application of the EU AI Act, existing Hungarian legal frameworks already apply to AI systems. As a result, implementation must be approached with a compliance-first mindset, rather than assuming that regulation is still "future-facing".

Civil liability

The liability framework for AI systems in Hungary is still evolving, and, to date, there is limited case law specifically addressing AI-related damage. As a result, liability is currently assessed primarily under existing legal regimes, applied by analogy to AI systems.

From a Hungarian law perspective, two main liability regimes are particularly relevant.

First, strict liability for hazardous activities may apply where the operation of an AI system involves increased risk. In such cases, the operator – i.e. the party controlling the risks associated with the system – may be held liable irrespective of fault. Exemption from liability is only possible if the damage was caused by an unavoidable external event beyond the operator's control.

Second, product liability may arise where AI systems qualify as products. Under the current framework (based on Directive 85/374/EEC), manufacturers may be subject to no-fault liability for defective products. However, applying traditional product liability concepts to AI raises significant challenges. AI systems are not static but continuously evolving, making it difficult to determine the relevant point in time for assessing defects. In addition, the interconnected nature of AI systems complicates the identification of responsibility, while the "black box" effect may create evidentiary difficulties for claimants.

These structural challenges are addressed, at least in part, by the new EU Product Liability Directive (2024/2853), which will significantly reshape the liability landscape.

Under the revised framework, the concept of a product is expanded to include software and other digital elements, and liability may extend beyond the moment a product is placed on the market, covering its entire lifecycle, including updates and modifications. The Directive also introduces mechanisms to alleviate the claimant's burden of proof, including disclosure obligations and rebuttable presumptions in certain cases.

The Hungarian implementation (coming into force in December 2026) closely follows the EU model, while also adapting certain elements to the domestic legal system. Notably, the definition of a defect is broadened to include not only safety expectations in a physical sense, but also factors such as cybersecurity requirements, user expectations and functional reliability.

Liability is also extended across the supply chain, potentially encompassing manufacturers, component suppliers, importers, distributors and even certain digital service providers. Importantly, any party that

substantially modifies a product and places it back into circulation may be treated as a manufacturer. In the AI context, this could raise questions as to whether users engaging in activities such as model fine-tuning or system integration may fall within the scope of product liability, although the precise boundaries will need to be clarified in practice.

From a procedural perspective, the new regime introduces a more structured limitation framework, including a three-year limitation period from the date the damage becomes known and a long-stop period, with extended timelines for latent personal injuries up to 25 years.

From a business perspective, these developments represent a fundamental shift. Product liability is no longer confined to tangible goods or static risks – it increasingly follows the dynamic lifecycle of AI-driven products and services.

As a result, companies should begin preparing at an early stage. Risk management must be embedded throughout the lifecycle of AI systems, from design and development to deployment, updates and integration. This includes reviewing supply chain arrangements, clearly allocating responsibilities in contracts, and ensuring that insurance coverage adequately reflects AI-related risks.

In addition, technical documentation and traceability – already relevant under the EU AI Act – will become critical from a liability perspective as well. Businesses that go beyond using "off-the-shelf" solutions, for example, by modifying or fine-tuning AI systems, should carefully assess whether they may assume a quasi-manufacturer role under the new framework.

Overall, the direction of travel is clear: liability rules are evolving to reflect the realities of AI, placing greater emphasis on control, lifecycle responsibility and risk management. Hungarian businesses will need to adapt accordingly in order to mitigate exposure and maintain trust in increasingly autonomous systems.

Conclusion

AI in Hungary is no longer a future-facing concept, but a present and increasingly central business capability, shaped by both rapid technological adoption and an accelerating EU-driven regulatory environment. As this chapter has shown, the key challenge is not whether AI will be used, but how it can be deployed in a way that is legally compliant, operationally sound and strategically aligned.

Across all areas – from ownership and competition to governance and liability – a common pattern emerges: existing legal frameworks continue to apply, but are being stretched and reinterpreted in light of AI's unique characteristics.

At the same time, new EU instruments, most notably the AI Act, the Data Act and the revised Product Liability Directive, are gradually building a more structured and lifecycle-based regulatory system. This creates a dual reality for businesses, where innovation must go hand in hand with increasing expectations around transparency, accountability and risk management.

From a practical perspective, the key lesson is that AI cannot be treated as a purely technological issue. It requires a holistic governance approach, combining legal, technical and business considerations as well as integrated risk management from the outset.

Companies that invest early in AI governance, including data management and risk frameworks, will be better positioned not only to ensure compliance, but also to turn compliance into a competitive advantage. In this sense, the core message is clear: in the age of AI, those who manage risk well will be the ones who innovate successfully.

Endre Várady

Tel: +361 501 9900 / Email: varadye@vjt-partners.com

Endre Várady advises on data protection, digital transformation and broader ICT matters, with a particular focus on the legal implications of emerging technologies, including AI. His work centres on supporting clients in the implementation and governance of AI-driven solutions, combining regulatory, contractual and operational perspectives.

He regularly assists with the localisation and deployment of cross-border digital products and serves as a key contact for international law firms on complex TMT and AI-related matters. His practice covers data governance, cloud services, platform regulation and the integration of generative AI into business processes.

Endre leads the firm's award-winning Data Protection practice and has been involved in the development of GDPR compliance tools, including Adatsólyom. He also has extensive experience in structuring and negotiating technology transactions, particularly in relation to cloud-based and data-driven services.

János Tamás Varga

Tel: +361 501 9900 / Email: vargajt@vjt-partners.com

János Tamás Varga is the founder and managing partner of VJT & Partners. Over the past 25 years, he has built extensive experience advising on complex cross-border transactions, high-stakes legal matters and regulatory challenges across a wide range of industries.

In addition to his recognised M&A practice – covering international private equity, venture capital and strategic investments into Hungarian companies – János plays a leading role in the firm's TMT practice. He has a strong track record in technology-driven transactions, including tech-related M&A and investments, and regularly advises on the structuring and negotiation of IT and digital contracts, including those involving emerging technologies such as AI.

Andrea Belényi

Tel: +361 501 9900 / Email: belenyia@vjt-partners.com

Andrea Belényi leads VJT & Partners' Regulatory & Compliance practice and has been with the firm for nearly a decade. With over 25 years of professional experience, she is a trusted adviser on complex regulatory, compliance and technology-related matters, and plays a leading role in many of the firm's key client mandates and major projects.

Her background includes senior experience at the Hungarian Competition Authority, providing her with valuable insight into regulatory decision-making and enforcement practice. In addition to her work in areas such as competition law and data protection, Andrea is increasingly focused on AI and other emerging regulatory challenges, advising clients on how to navigate evolving legal frameworks.

VJT & Partners

Kernstok Károly tér 8, 1126 Budapest, Hungary

Tel: +361 501 9900 / URL: www.vjt-partners.com

Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

globallegalinsights.com