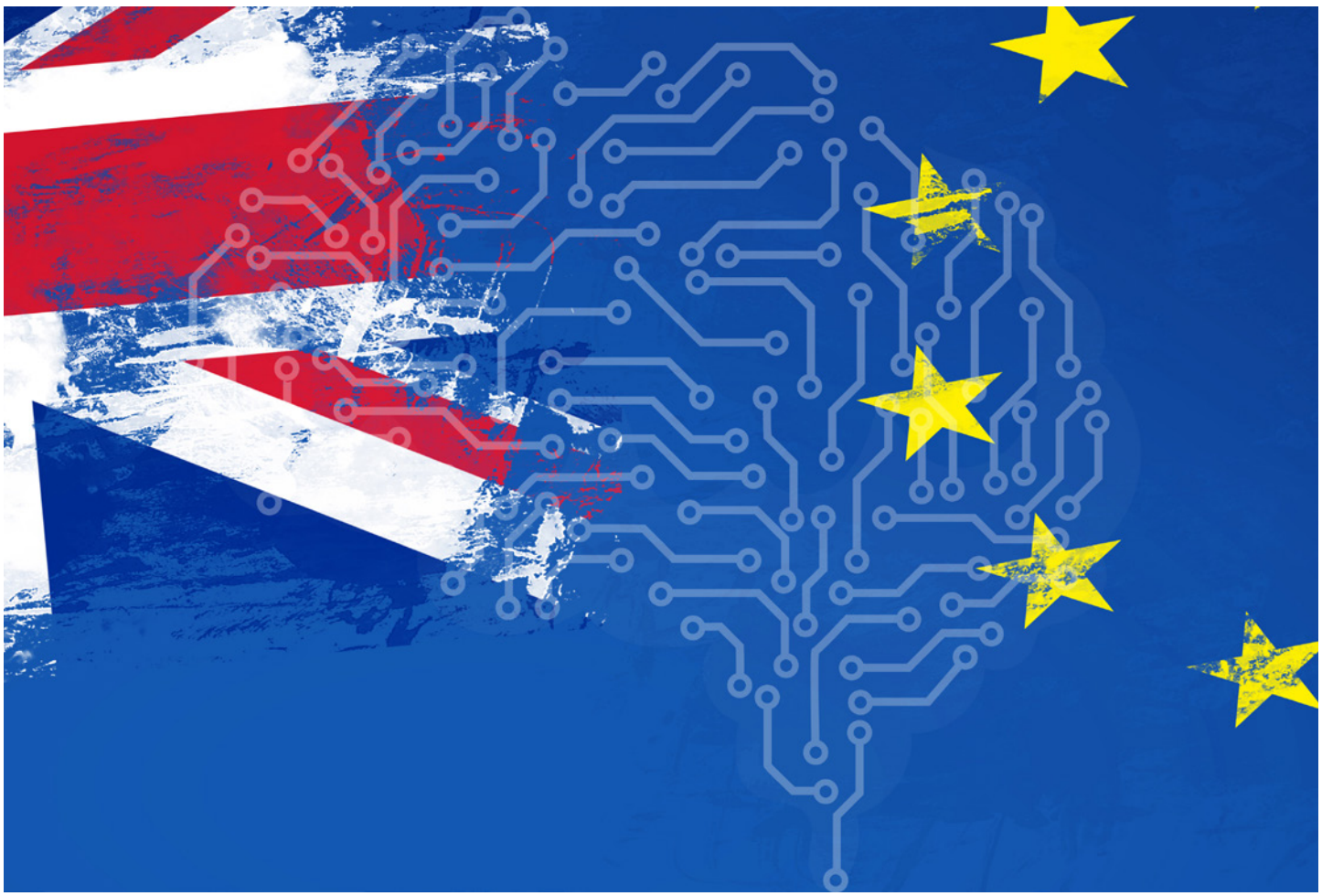
Kennedys

TALKINGPOINT REPRINT December 2024

AI regulation in the UK and EU

FW discusses AI regulation in the UK and EU with Deborah Newberry, Richard West, Nathalie Moreno, Karim Derrick and Joe Cunningham at Kennedys.



FINANCIER WORLDWIDE corporatefinanceintelligence

THE PANELLISTS

Deborah Newberry
Corporate Affairs Director
Kennedys
T: +44 (0)20 7667 9508
E: deborah.newberry@kennedyslaw.com

Deborah Newberry is a corporate affairs director in Kennedys' London office. She leads on the firm's global public affairs and thought leadership initiatives, which involves examining emerging insurance risks, as well as the impact of legal and political shifts on the international insurance business environment. She also takes a strategic lead in the firm's innovation group – a progressive client focused consultative group designed to identify the disruptions to the legal insurance market.

Richard West
Partner
Kennedys
T: +44 (0)20 7667 9166
E: richard.west@kennedyslaw.com

Richard West is the global head of liability defence at Kennedys, acting for businesses and insurers defending motor and casualty claims, including complex catastrophic injury claims. He also leads Kennedys' innovations group and is a director of Kennedys IQ, Kennedys' technology driven company that provides innovative solutions for insurance companies and large corporates to help them manage claims efficiently.

Nathalie Moreno
Partner
Kennedys
T: +44 (0)20 7667 9452
E: nathalie.moreno@kennedyslaw.com

Dr Nathalie Moreno is a data protection, cyber security and AI partner at Kennedys and a member of the firm's global cyber and data team, in London. Her focus is on data rich industry sectors, including technology, financial services, healthcare and life sciences, retail and consumer, hospitality and leisure, advertising and marketing, automotive, and media and publishing. Her practice encompasses the full range of data protection, e-privacy and cyber security issues.

Karim Derrick
Chief Products Officer
Kennedys IQ
T: +44 (0)20 7667 9776
E: karim.derrick@kennedyslaw.com

Karim Derrick is product and innovation director at Kennedys IQ. He and his team of data scientists, analysts and claims experts focus on the development of innovative tools that combine human and machine intelligence to help Kennedys' clients manage claims efficiently. In 2022, he led the consortium – comprising Kennedys, a major global corporate client, a data science business and a university – that won a government grant to develop AI claims.

Joe Cunningham
Product Manager
Kennedys IQ
T: +44 (0)20 7667 9184
E: joe.cunningham@kennedyslaw.com

Joe Cunningham is a product manager at Kennedys IQ. He joined Kennedys IQ in 2022 after a decade of handling marine and casualty claims in the maritime industry and within the Lloyd's market. He is ACII qualified, holds an MSc in legal technology and is a doctoral student, where his research sits at the intersection of insurance, law and artificial intelligence.

FW: Could you provide an overview of the developing artificial intelligence (AI) landscape? What emerging risks have you observed?

Derrick: The concept of artificial intelligence (AI) has a shifting definition. It has been used at different times to label different technologies which have led to multiple hype cycles, including, for example, excitement around expert systems in the 1990s that, when their limitations were understood, was then followed by an AI winter where expectation and investment largely evaporated. With attention now turned to transformer models, the AI winter is definitely over and we are arguably now in a new hype cycle. In our view, transformers are statistical models – labelling them as AI creates a mysticism around them that is misleading. In 2024, AI has thus become a catch-all term for what, in recent public discourse, is largely referring specifically to transformer models used to generate data, text, image, audio and video based on contextual prompts, which is where the step change

in capabilities resides. Robotic automation in public discourse is also unhelpfully lumped together as AI and is not new – it is largely rules based and adopts techniques that predate transformer models. A key shift with transformer models has been an ability for models to be generalised. Where before models needed to be trained on specific tasks with significant data, large language models have demonstrated high levels of competence across a wide range of tasks out of the box. That though, in turn, creates new risks. The probabilistic output of transformer models means that for a given input, their output is a distribution of possible responses based on the distribution of judgement within their training data. Output may be excellent, average and, at times, a hallucination. Performance of the large public models like GPT and LAMA is, however, being improved all the time, with multiple models employed for a given input, to enable output to be increasingly optimised and the tendency for hallucination to be reduced. Importantly, the training data on which the biggest transformer models have been trained remains opaque. Privacy and copyright rules were not written with transformer models in mind and a re-evaluation of existing frameworks like the General Data Protection Regulation (GDPR) is now underway. Moreover, as efficacy of models is shown to exceed human performance for an increasingly wide range of tasks, not using transformer models for some tasks may itself start to be seen as negligent and a new type of liability may evolve for professionals who fail to use them when their superior performance is widely acknowledged.

Cunningham: The nature of the language model is giving rise to an array of emerging risks and related issues. Such issues include algorithmic transparency and privacy issues. In particular, the 'black box' problem refers to a lack of opacity and explainability of complex language models – meaning it can be impossible to understand how they arrive at their decisions. In turn, a risk of bias and discrimination will arise if models are trained on biased data, leading to unfair outcomes. Such outcomes can impact a variety of areas and products, including healthcare, employment and law enforcement. Where language models are incorporated into systems that result in harm or injury, who should be held accountable remains unclear, particularly where such systems are automated or lack appropriate levels of human oversight. Privacy and data protection risks arise when AI systems rely on vast amounts of personal data in training, development and in deployment.

> "A RISK OF BIAS AND DISCRIMINATION WILL ARISE IF MODELS ARE TRAINED ON BIASED DATA, LEADING TO UNFAIR OUTCOMES."
>
> JOE CUNNINGHAM
> Kennedys IQ

FW: How would you summarise the goals and provisions of the EU's AI Act? What particular compliance challenges does the Act present to entities within its scope?

Moreno: The European Union (EU) AI Act came into force in August 2024, marking the world's first comprehensive AI law. The Act's primary goals are to promote safe and trustworthy AI, safeguard fundamental rights and foster innovation while mitigating potential risks associated with AI technologies. It also aims to close regulatory gaps not covered by existing sector-specific regulation. The Act adopts a risk-based approach to AI regulation, assigning obligations to a broad range of entities connected to the EU market – including providers, deployers, importers, distributors and product manufacturers of AI systems. Crucially, the Act prohibits certain AI systems deemed to pose unacceptable risks, such as systems that are harmful, deceptive, or that exploit vulnerabilities, or which support social scoring systems. It categorises other AI systems into high-risk, limited-risk and minimal or no-risk categories – based on the scope of the risks presented. So-called 'high-risk' AI systems in particular, present significant compliance challenges due to the enhanced regulatory obligations imposed on providers and deployers. These systems include AI used as a safety component of products, or as standalone products governed by EU legislation. Before deployment, high-risk AI systems must undergo a third-party conformity assessment. Providers must demonstrate compliance with stringent requirements, including transparency, human oversight, accuracy, cyber security, data governance and the data quality of the datasets used. High-risk AI systems must also be registered in a European Commission (EC) database. For organisations, the first challenge lies in determining the risk category of their AI systems, especially for novel technologies where risks may not be fully understood at the development stage, in order to assess their obligations under the Act. Incorrect risk classification could expose organisations to significant regulatory penalties. In practice, the wide-ranging governance requirements for high-risk AI systems – such as auditing, monitoring, record keeping and risk management – will likely lead to increased operational costs for businesses to manage. Finally, businesses should consider the interplay between the Act and other existing regimes, such as the GDPR, the EU Medical Devices Regulation and sector-specific standards. Overlaps may create legal complexity, particularly where multiple regulatory frameworks apply concurrently. A key compliance challenge will be ensuring that AI systems meet the requirements of all applicable regulations without duplication or conflict. To navigate this evolving regulatory landscape, businesses should adopt a proactive, cross-functional compliance

strategy, ensuring they can mitigate risks of non-compliance. This involves closely monitoring developments in EU regulatory guidance and establishing cross-disciplinary teams, including legal, technical and compliance experts, to ensure alignment with the Act and its interaction with other legal frameworks.

FW: How does the approach to AI regulation in the UK compare with that in the EU, as well as jurisdictions elsewhere? To what extent do approaches converge or diverge?

Newberry: In contrast to the EU's more stringent regulatory framework, the previous UK government had adopted a light touch, principles based 'pro-innovation' approach to AI regulation, as set out in its White Paper published in March 2023. The framework is based on the following five cross-sectoral principles for existing regulators to interpret and apply within their domains in order to promote safe and responsible AI innovation. First, safety, security and robustness. Second, transparency over how AI works and decision-making processes. Third, fairness so as to avoid discrimination and bias. Fourth, accountability, to ensure that organisations developing AI systems are responsible for making them safe as well as for the outcomes of their use. Lastly, proportionality, so as to ensure a flexible and adaptive approach to AI regulation to encourage and promote innovation. Earlier this year, key industry regulators, including the Financial Conduct Authority, the Information Commissioner's Office and the Medicines and Healthcare products Regulatory Agency, published their respective AI strategies which were mapped against the five cross-sectoral principles. The new government looks set to continue with this 'pro-innovation' approach for the time being, although there are indications that some form of AI legislation could be on the cards.

West: The US approach to AI regulation, as compared to the EU, is more free flowing, focusing on entrepreneurship with the aim of driving commerce and economic growth. While this approach should foster an environment that will facilitate greater adoption of generative AI (GenAI), it arguably risks consumer protection becoming secondary, but it does contrast with the European approach of a more stringent regulatory framework. Although there is currently no specific federal law or regulation akin to the EU's AI Act governing the development or use of AI, there are some existing federal laws that address AI-related systems within certain industry sectors, including aviation and defence, as well as a series of federal proposed laws relating to AI. Examples include the draft No Fakes Act, which aims to protect voice and visual likenesses of individuals from unauthorised recreations from GenAI, and the AI Research Innovation and Accountability Act, which calls for greater transparency, accountability and security in AI while establishing a framework for AI innovation. There are also a number of state-led initiatives to guide the regulation of AI in a manner that fosters innovation while maintaining global competitiveness in AI development. This includes President Biden's White House Executive Order on AI – 'The Safe, Secure and Trustworthy Development and Use of Artificial Intelligence' – issued in October 2023. The Order requires developers of the most powerful AI systems to share safety test results and other critical information with the US government, with a view to ensuring that AI systems are safe, secure and trustworthy before being made available to the public. Similar to the UK's principles-based approach, the Order also lists eight principles and priorities to promote the safe, responsible development of AI technologies, with some of these focusing on the safeguarding of civil rights, including privacy and protecting the interests of Americans who use, interact with or purchase AI-enabled technologies.

Newberry: Overall, the EU has taken a more structured, rights-based approach to AI regulation, while the UK and US have adopted more flexible, pro-innovation approaches. While some commentators see the EU AI Act as a prescriptive piece of legislation, others consider the streamlined, horizontal approach to be helpful for businesses as it is broad enough to cover all markets. While the UK is currently focusing on oversight by sectoral regulators, the US is turning to existing federal laws and voluntary standards. Notwithstanding the differences in approach to AI regulation, the US, EU and UK all recognise that AI governance decisions will become increasingly challenging as the AI systems become more powerful. Safeguarding fundamental rights, having accountability and transparency in AI systems, and adhering to ethical principles remains, for the time being, a consistent goal of all. Each jurisdiction also provides for industry regulators having a role in the overall framework, although the extent of regulatory involvement does differ. As AI continues to evolve, the global conversation around regulation is likely to influence the eventual convergence or divergence of these approaches further. For businesses operating in multiple jurisdictions, the divergent approaches to AI regulation present significant compliance challenges. Companies will need to navigate differing regulatory requirements, particularly when it comes to transparency, data governance and risk management. Developing a coherent, cross-jurisdictional compliance strategy will be essential to avoid regulatory

> "WITH ATTENTION NOW TURNED TO TRANSFORMER MODELS, THE AI WINTER IS DEFINITELY OVER AND WE ARE ARGUABLY NOW IN A NEW HYPE CYCLE."
>
> KARIM DERRICK
> Kennedys IQ

penalties and ensure that AI systems meet the varying legal obligations in each market.

FW: How important is it for regulators to protect citizens and society from the risks of AI without curtailing AI innovation and application for businesses? To what extent is this being accounted for by policymakers in the UK and EU?

Newberry: Given the immense societal and economic benefits that AI innovation offers, it is absolutely critical for legislators to strike the right balance between protecting citizens and society from the risks of AI without curtailing innovation. The importance of achieving this balance was highlighted by the previous UK government in its 2021 National AI Strategy, of which a stated aim was to ensure that the UK gets the national and international governance of AI technologies right to encourage innovation and investment while protecting the public and our fundamental values. The UK is striving to achieve that balance through its current 'pro-innovation' approach to AI regulation, which so far has appealed to AI developers. Indeed, when British AI company Wayve secured a $1.05bn investment in March to develop the next generation of AI-powered self-driving vehicles, Wayve's co-founder cited the UK's approach as integral to the organisation's ability to build AI for assisted and automated driving so quickly. Nevertheless, some stakeholders consider that the UK's approach swings too heavily on the side of the innovators, and that there needs to be a more centralised approach to AI regulation. This approach was advocated for by Lord Holmes of Richmond earlier this year, who introduced a private members' bill aiming to "put regulatory principles for artificial intelligence into law". While this bill was dropped in anticipation of the recent general election, the government confirmed in its pre-election manifesto its commitment to introduce binding regulation on "the most powerful artificial intelligence models". The introduction of a new private members' bill by Lord Clement Jones on 10 September that proposes regulating the use of AI in the public sector, may be a first step in that process.

> "A KEY COMPLIANCE CHALLENGE WILL BE ENSURING THAT AI SYSTEMS MEET THE REQUIREMENTS OF ALL APPLICABLE REGULATIONS WITHOUT DUPLICATION OR CONFLICT."
>
> NATHALIE MORENO
> Kennedys

Moreno: The EU's AI Act takes a more prescriptive and stringent regulatory approach, prioritising transparency, protection of citizens and safeguarding fundamental rights. While its risk-based framework offers some flexibility – particularly for low-risk AI systems – the Act places heavy obligations on high-risk AI systems, especially in sectors such as healthcare, law enforcement and finance, where the potential for harm is significant. However, many commentators, including Mario Draghi, an Italian economist and former president of the European Central Bank, argue that the EU's regulatory approach could stifle innovation. The report acknowledges that EU businesses, especially start-ups and small and medium-sized enterprises, face significant challenges due to the significant technology gap between Europe and other jurisdictions like the US and China. Regulatory barriers, including those introduced by the AI Act, are seen as a hurdle for scaling AI technologies and staying competitive globally. That said, the EC is aware of these concerns and is taking steps to mitigate some of the burdens associated with compliance. Initiatives like the 'AI Factories' and the 'Apply AI Strategy', recently introduced by Ursula von der Leyen, president of the EC, aim to support AI start-ups and promote the use of AI in industrial sectors by granting access to advanced computing resources. These measures reflect the EC's understanding that regulation must be balanced with incentives for innovation to ensure the success of the AI Act. But, as with the GDPR and the recently adopted EU Digital and Data Regulations, their full impact will only become evident over time.

FW: What steps should companies take to establish appropriate processes and policies to manage AI-related risks and keep systems operating as intended?

Derrick: Transformer models are just the latest range of statistical models to be deployed with new generalised capabilities. Their output is probabilistic and black boxed. That makes testing efficacy more important than ever, not less important. Testing and retesting at scale and at volume is essential for reliable deployment of models. In our observation, we have seen organisations deploy transformer models directly into their business without the rigour of quality assurance and testing that previous generation technologies enjoyed. Equally, we believe that transformer models are not a silver bullet. Where judgement is required rather than analysis of text, the probabilistic nature of the models means the judgement is rarely optimised. Organisations would do well to consider whether transformers are the best solution in all cases. We have found that hybrid solutions that combine techniques that model expert humans, with the incredible text analytical capabilities of transformer models, to be a better approach than transformers on their own. More broadly, companies should take a proactive and structured approach to establishing processes and policies to manage AI-related risks. A robust and comprehensive AI governance framework will help them manage AI systems responsibly and address the technical, operational, legal and ethical aspects of AI development and use within their organisations. This will enable companies to leverage the benefits of AI while mitigating its risks, ensuring systems

operate safely and as intended, while promoting business aims responsibly. At the heart of an AI governance framework should be a designated cross-business AI risk management team, made up of a wide range of stakeholders responsible for priority business areas, including data scientists, risk and compliance, internal auditing and data management. Their role is to ensure that appropriate processes and policies address all relevant legal, regulatory and technical requirements. In-house legal teams should keep an eye on the rapidly evolving AI regulatory landscape and ensure that they are properly resourced to ensure that they can implement and comply with new AI laws and guidance as they emerge. Given the potential risks around transparency and bias, organisations may also wish to form a specific AI ethics committee to oversee the ethical implications of deploying AI systems, particularly those that could have societal-related implications. Companies may wish to adopt the international ISO 42001 AI Management System standard, which provides a structured framework to help companies develop an appropriate AI policy for the responsible development and use of AI. In particular, the ISO highlights the need for businesses to have an AI policy that aligns with the goals, legal requirements and ethical considerations of the company.

FW: In a global context, to what extent do agreements such as the 2023 AI Safety Summit's Bletchley Declaration help create a shared understanding of the opportunities and risks posed by AI? Do AI-related laws need to be widely harmonised to achieve their goals?

Newberry: Agreements such as the Bletchley Declaration play an integral role in creating a shared understanding of AI opportunities and risks, as they create a framework for international collaboration on addressing the most critical AI risks, particularly in relation to safety and governance. Taking the Bletchley Declaration as a case in point, it is seen as a landmark moment in global AI collaboration – having been endorsed by 28 countries – and has been described as a 'world first' agreement. It represents a collective acknowledgment by its signatories to proactively manage the opportunities, challenges and risks presented by AI. In a nod to the 'inherently international' nature of AI, and the cross-border risks that it poses, the Declaration underlines the importance of addressing the risks and challenges of AI through international cooperation. This encourages shared responsibility by all key stakeholders, including businesses, governments and regulators, and highlights the value of working together to achieve common goals, notwithstanding differing approaches to AI regulation. As to whether AI-related laws need to be harmonised to achieve their goals, the degree to which harmonisation is required is likely dependent on the goals of the proposed laws and the areas of regulation. For example, AI risks associated with advanced, high-risk AI, such as autonomous weapons, cyber security and the misuse of information, are inherently global in nature and require a coordinated, international response. Harmonisation of AI laws can also prevent regulatory disparity and provide certainty for businesses that may move their operations to different countries. However, achieving harmonisation is not straightforward. As demonstrated by the comparable approaches to AI regulation, countries have differing priorities when it comes to AI regulation. The different approaches taken by the US, EU and UK reflect the broader political, economic and cultural divergences that could make harmonisation incredibly difficult, if not impossible, to achieve.

FW: Going forward, what additional demands are UK and EU laws likely to place on companies that develop or deploy AI as part of their business processes? Can we expect an escalation of regulatory compliance challenges?

West: As AI technologies and systems continue to develop and are integrated into business processes, UK and EU laws are likely to place additional demands on organisations in relation to a number of areas, including data protection, consumer protection and product safety. Recent legislative proposals, as well as ongoing sector analysis by industry regulators, indicate that further requirements of business is the likely direction of travel. In the UK, the government is proposing to introduce a Digital Information and Smart Data Bill that includes proposals to reform data protection legislation. Based on the information so far, these appear to be limited to where the government perceives such laws to be impeding the safe development and deployment of 'new technologies', which could very well be a reference to AI. The government is also proposing to update the UK's existing cyber security legislative framework through the introduction of a new Cyber Security and Resilience Bill. This proposes placing requirements on organisations working to develop the most powerful AI models. In the competition space, the Competition and Markets Authority (CMA) also continues to consider the competition-related risks that AI poses to consumers within UK markets, having identified that firms' misuse of AI and other algorithmic systems, whether done intentionally or not, can create risks to competition by exacerbating or taking advantage of existing problems and weaknesses in the market. The CMA's ongoing work in this area could

> "THE US APPROACH TO AI REGULATION, AS COMPARED TO THE EU, IS MORE FREE FLOWING, FOCUSING ON ENTREPRENEURSHIP WITH THE AIM OF DRIVING COMMERCE AND ECONOMIC GROWTH."
>
> RICHARD WEST
> Kennedys

lead to further obligations being placed on businesses using AI systems to prevent them from engaging in anti-competitive practices.

Moreno: The EU already appears to be placing additional demands on businesses that deploy AI. Another significant area of compliance escalation relates to data protection. The intersection of AI regulation with existing data privacy frameworks, such as the GDPR in the EU and the UK's Data Protection Act, will create further challenges. For instance, companies that deploy AI systems reliant on large datasets may need to demonstrate that their AI tools comply with data minimisation, anonymisation and purpose limitation principles. This may require rethinking how data is collected, processed and stored, to avoid the risk of non-compliance. The use of AI for automated decision making, particularly when involving personal data, will continue to attract scrutiny, potentially leading to even more stringent requirements in this area. Additionally, we can anticipate a rise in sector-specific AI rules. For example, the financial services sector, already subject to significant regulatory oversight in the UK and EU, is likely to see further AI-specific regulations aimed at mitigating the risks associated with algorithmic trading, fraud detection and credit scoring. Similar sector-specific requirements may emerge in other high-risk industries like pharmaceuticals, automotive and education. The EU's Digital Markets Act (DMA), which aims to make the digital marker fairer and more contestable, imposes rules and obligations on the largest digital platforms acting as 'gatekeepers' in the technology sector. The EU is now actively enforcing those rules, having recently warned Apple to launch the AI features of its devices in the EU in accordance with its obligations under the DMA, failing which it will face substantial fines. Apple had previously announced that it would not be launching its AI features, citing that interoperability obligations could impact user privacy and security. As regulation becomes more stringent over time, particularly in high-risk industries such as life sciences, healthcare and finance, an escalation of compliance challenges can be expected. This is likely to arise in circumstances where digital regulations overlap and are potentially contradictory. For example, businesses may find it challenging to comply simultaneously with AI-specific regulations, the DMA, and existing data protection frameworks like the GDPR. Such overlaps create legal complexity and will require businesses to adopt a more integrated approach to compliance. Ultimately, businesses will face an escalation of regulatory compliance challenges as AI adoption increases and regulatory frameworks evolve. Developing a proactive, cross-jurisdictional compliance strategy will be essential, allowing businesses to navigate the complex, overlapping and sometimes contradictory requirements of AI regulations, digital market rules and data protection laws. ■

> "FOR BUSINESSES OPERATING IN MULTIPLE JURISDICTIONS, THE DIVERGENT APPROACHES TO AI REGULATION PRESENT SIGNIFICANT COMPLIANCE CHALLENGES."
>
> DEBORAH NEWBERRY
> Kennedys