AI and the law

Spotlighting the potential legal and ethical pitfalls

Corporate executives, government leaders and the public at large have expressed cautious enthusiasm about the significant promise of artificial intelligence (AI). And with good reason: this transformative technology has the potential to drive economies, boost cost efficiencies and improve the quality of life throughout our society.

At the same time, many have pointed to the pitfalls at play with AI. Both the public and private sectors must consider the inherent ethical and legal risks of AI to ensure its safe and lawful use. Legal teams should also do their part to balance the opportunities against the risks.

Applying a trustworthy approach to AI adoption will be crucial not just for compliance. Customers and users increasingly require that companies they deal with guarantee their basic rights and explain clearly how AI will augment services or products. By taking a proactive approach, leaders of legal departments can position their organization and inspire confidence in the market.

The coming years are expected to be pivotal for AI, with significant developments on the horizon in both AI innovation and regulation. In this article, we explore some of the key legal and ethical issues that must inevitably be addressed by in-house legal departments.

Regulatory and governance landscape

The regulatory landscape for AI continues to evolve rapidly as jurisdictions grapple with today's rapid and unprecedented advances in technology. The landscape is diverse across regions and countries, with new policy initiatives being developed and introduced on an ongoing basis.

The EU has adopted an approach based on its fundamental values and principles. In doing so, it is anticipating the impact of AI's explosive growth to ensure the protection of important interests and people's fundamental rights.

AI legislation in the form of the EU AI Act came into force in August 2024, making some AI practices unlawful.

The EU Act defines and sets out specific requirements for high-risk AI systems — including AI literacy, risk management, technical documentation, human oversight, impact assessments, data governance and cybersecurity measures. Anyone using or deploying AI in the EU — and AI users not based in the EU whose outputs are used there — will need to ensure that AI use meets the obligations set out in the AI Act. Many of the obligations become applicable in full in August 2026, leaving limited time to properly embed the relevant obligations.

UK framework mirrors EU's AI Act

The UK government, rather than introducing legislation at this stage, has adopted a different strategy. Emphasizing a "pro-innovation approach to AI regulation," it is leveraging the expertise of sector regulators to create industry-specific rules based on a consistent set of principles. The principles within the UK framework mirror those in the EU AI Act, focusing on safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress.

There are proposals in the UK to introduce laws around improving access to training data and supporting growth in the AI sector to further drive uptake. The AI Safety Institute will play a critical role in ensuring the safety and reliability of AI models, with consultations on AI safety regulation expected later this year (2025).

What is clear is that all who seek to make the most of AI will need to be aware of a changing regulatory and legal landscape. The rapid pace at which AI is emerging will always far outstrip the speed at which the law can respond, but regulators and lawmakers will be keen to ensure that AI use remains appropriate. Businesses will need to ensure ongoing monitoring of legal regimes and expectations to remain compliant. Regulators will take enforcement action where they see inappropriate or unlawful practices, and all business will need to ensure that they can take prompt steps to remediate where necessary.

Ethical considerations

Alongside legal issues, ethical considerations remain at the forefront of AI development. Issues around the extent to which it is appropriate to use AI remain, particularly where deployers have insufficient knowledge or understanding of what the technology does and how it uses available data. Ethical concerns around AI transparency, explainability, data quality and equity, bias, discrimination and automated decision-making need to be addressed amid mistrust in the power and implications of AI use.

Recognized international documents and standards — such as the *UNESCO Recommendation on the Ethics of Artificial Intelligence*, the *OECD AI Principles*, and the G7 leaders' agreement on *Guiding Principles and a Code of Conduct on Artificial Intelligence* — are important when defining corporate ethical models. The five principles outlined in the UK's AI white paper serve as a foundation for ethical AI practices and aim to prevent harm, ensure reliability and address biases in data and algorithms.

Transparency and explainability are particularly challenging in the AI context, as explaining complex AI processes and outcomes can be difficult. In the UK, regulators have already made it clear that they expect deployers to be able to explain decision-making processes and outcomes to users. Businesses are already establishing ethics boards to ensure that these issues are considered and that appropriate skillsets are in place to adopt AI safely.

Third-party risk

Given AI's proliferation, it is very likely that all suppliers of services will augment their offerings with AI. This means businesses will need to assess and mitigate the risks of adopting AI themselves, but it will also require an assessment of how key suppliers are using AI.

Those in the legal sector often rely on a wide range of third parties to provide IT systems, and suitable due diligence and contractual protection will need to be in place. The recent legislation requires those using AI to demonstrate proactive diligence toward compliance by requesting appropriate safeguards from suppliers and other third parties.

Businesses should not simply adopt AI without fully considering its impact. This requires them to understand AI and the key issues and risks associated with using any AI products — a skillset that may well need to be developed.

Data protection and privacy

Data protection and privacy are critical issues in the AI landscape. Even in the absence of AI-specific regulation, personal data use must meet relevant data-protection laws when used in conjunction with AI services or products.

In Europe, the data-protection principles enshrined in the GDPR and UK GDPR provide a useful framework to ensure that data processing is lawful. A number of these principles mirror those within the UK's AI regulation, particularly around transparency, fairness and minimization.

This requires a detailed understanding of AI's personal data use and outputs. Businesses must be satisfied that personal data use is compatible with the original purpose for which it was obtained, and they must be able to establish a suitable lawful basis.

Protecting personal data is critical

GDPR transparency requirements dictate that privacy notices clearly provide suitable information to data subjects — allowing them to understand how their data will be used by AI and where decisions are being taken about them using AI. Rushing to adopt AI without understanding what the technology does will undoubtedly undermine the ability of any business to be transparent with customers, users or employees.

Businesses must also consider the extent to which AI products provide suitable security to protect shared personal data, as well as considering how they respond should any data subject object to their data being used by, or to train, AI.

For those in Europe and the UK, conducting a data protection impact assessment (DPIA) will be an important step. This assessment will help ensure compliance with data protection laws associated with any AI product before personal data is processed in conjunction with or by the AI product. The DPIA will also pursue ways to mitigate the impact on data subjects and reduce risk.

AI impact on copyright

The tension between AI innovation and the creative industry is evident in the ongoing debate around copyright and AI. The UK government's consultation on copyright and AI seeks to balance the interests of the AI industry and the creative sector, whose output in the public domain is a vital source for training AI systems, particularly Gen AI.

The current proposed text contains a data mining exception which would allow the use of copyrighted material for AI training if lawful access is available. This consultation represents a significant step toward greater transparency and collaboration between AI developers and rights holders. This is still subject to much debate, however, and striking a suitable balance between parties with such competing interests will take time.

Legal departments must consider the extent to which they are entitled to use advice, contracts, documentation and personal data gathered in the course of supporting clients or managing the business to train AI. The benefits of using Gen AI to accelerate the drafting process must still take into account who owns the information and whether law firms have the right to use it for these purposes.

In any case, legal teams must adopt a heightened protection approach, taking into account the law and the ethical criteria associated with the legal profession. In fact, most relevant bar associations have issued clear guidelines regarding the use of Gen AI in the legal field.

The recent development of GPAI models

Technological advancements in AI continue to drive innovation and reshape industries. The development of general purpose AI (GPAI) models has raised new challenges and opportunities. These models, capable of performing a wide range of tasks, require robust risk management and technical documentation to ensure safe and effective deployment. The EU AI Act's provisions for GPAI models highlight the need for detailed summaries of training data and ongoing monitoring to maintain accuracy and reliability.

The Law Society in the UK has already published guidance that endorses the use of GPAI by in-house legal departments. The guidance recommends that in-house legal teams use GPAI models to 'optimize' efficiency — a very clear indication that the Law Society sees AI playing a central role for in-house legal going forward.

A challenge among departments seeking to make the most of GPAI models is the need to ensure that data inputted into AI is suitably digitized, cleansed and curated to maximize output quality — which can take time, money and skill. Those using third-party models need to consider whether models pulling data from the internet are suitably reliable and don't produce biased or misleading results.

AI and the legal sector

Using AI in general, and Gen AI in particular, will improve how law firms and in-house legal teams work — making them more efficient, more agile and potentially more profitable. It will also unlock more time for them to contribute greater value to their organizations, while mitigating the legal risks.

The range of AI already on the market is being adopted at pace, with further developments poised to increase the number of departments seeking to utilize and integrate AI into every aspect of their work. But beware — the desire to be an early adopter must be tempered by the risks associated with AI, from both a legal and ethical perspective.

In-house teams are justifiably risk averse and indeed must ensure there are checks and balances in place to identify how and where they may be interacting with AI, and how to mitigate those risks. Conducting risk assessments and, in particular, taking steps to mitigate privacy risks will be a vital first step.

New skills for legal teams

Many use cases are already being widely implemented using Gen AI, such as legal drafting, contract management and monitoring, legal risk and compliance control, regulatory oversight and more.

Embedding accountability will likely require in-house teams to develop new skillsets not only to understand and make the most of AI capabilities, but also to identify and assess the associated risks. The future will see the roles of in-house legal professionals augmented by AI, and parts of every job are likely to be supplanted or supplemented by the technology.

It is undoubtedly a good moment to redefine the role of corporate legal teams and the legal profession at large, and to establish how they will make the most of AI. Legal teams should actively participate in defining the digital transformation and innovation strategies of their organizations. They should also reimagine their operating and management models to optimize processes and efficiencies, as well as to provide greater strategic corporate value.

KPMG specialists are making a difference

Working across over **85 jurisdictions**, KPMG Law firms have a truly global offering for clients seeking to tap into AI's remarkable power in a responsible and legally compliant manner. KPMG Law specialists advise organizations on how to embed AI into their business and provide support on **commercial, data protection and data ethics questions**, as well as conduct risk assessments, develop policies and procedures and create accountability frameworks.

Contributors

James Cassidy

Director, Data Protection
KPMG in the UK
james.cassidy@kpmg.co.uk

James is a data protection and privacy lawyer, with a particular specialism in advising those in the health sector. James has over 17 years of advising clients from the NHS and the private health and social care sector on all aspects of data protection compliance including data breaches, commercial and contractual issues and data rights requests. James also advises clients in medical technology, life sciences, pharmaceuticals and the wider public sector. Alongside advising on Data Protection, James also has expertise in advising on wider rights of access including Freedom of Information and the common law duty of confidence.

Emma Ritchie

Director, Head of Data, Digital and Technology
KPMG in Ireland
emma.ritchie@kpmglaw.ie

Emma is a Director and Head of Data Protection and Privacy in KPMG Law LLP. Emma previously worked with one of the world's largest consumer electronics companies where she was the lead privacy counsel on data protection compliance projects, cookies, the use of personal data in consumer and business products, management of data security incidents, complex personal data transfer arrangements, AdTech and marketing. As an in-house lead counsel for a multinational organization, Emma has experience providing strategic and practical advice on all aspects of data protection and privacy law to business leaders and lawyers on a global scale.

Noemí Brito

Partner, Commercial Law; and Head of the Intellectual Property and New Technologies
KPMG Abogados
noemibrito@kpmg.es

Noemí is a lawyer specializing in Digital Law. She has over 20 years of experience in the field of personal data protection, having advised on multiple projects in various jurisdictions around the world.
She is a certified DPO according to the ENAC-AEPD Scheme, and one of the first professionals to obtain this certification in Spain. Noemí is a lecturer at various prestigious universities and business schools and has been recommended by the international directory Best Lawyers in 2020, 2021, and 2022 as a recognized lawyer in the categories of Technology Information Law, Privacy & Data Protection Law, and Technology Law. In 2021, she was awarded in Spain as "Lawyer of the Year in Privacy" by the international directory Iberian Lawyer.

Christopher Overton

Director
KPMG in the UK
christopher.overton@kpmg.co.uk

Chris is an international payments, financial services and technology lawyer providing commercial, transactional, strategic and regulatory advice. He supports businesses in regulatory readiness, regulated outsourcing and incorporating or providing technology, including supporting financial services, technology and government clients.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com