

Artificial intelligence and business

Legal insights and practical strategies for the future

Contents

- 3** Foreword
 - 4** What is AI?
 - 8** Navigating the AI and intellectual property landscape
 - 12** Employment law and AI – opportunities and risks
 - 16** Data protection and privacy in the age of AI
 - 18** Legal risks and litigation in the age of AI
 - 20** Internal AI governance – policies, risks, and best practice
 - 26** AI integration in the energy sector
 - 28** AI in Private Equity – strategies and challenges
 - 32** The future of AI and Generative AI
-

Forewo

Never before has a single topic taken the oxygen out of the room and dominated the news in the way artificial intelligence ('AI') has. It is a rapidly evolving area, and we are still very much in a period of exploration, development, and uncertainty, while we await the effect of much anticipated regulation from the UK Government.

Every week, AI providers are announcing new partnerships, investment and integrations with business core technology that effect our own strategy and ultimately the day-to-day workings of our staff, and it is interesting to see the impact of this rapid growth of AI on operations and obligations of businesses across different sectors.

Technology is an enabler and it's a very exciting time to be working within innovation! The last year has seen a new chapter for the firm. We launched TrowersEvolve, our portfolio of advanced client solutions, created to enhance our legal services. TrowersEvolve solutions incorporate machine learning, Generative AI, workflows, document automation, client portals, data analysis, apps and more. These practical technology solutions are designed to deliver our services to our clients faster and more efficiently with data driven insights. As the name suggests, TrowersEvolve is going to continue to evolve, at pace with the advancements of AI and technology to meet the needs of our clients.

Our goal is to support our clients in their journey of efficiency and AI. The growing incentives to explore AI's wide-ranging capabilities will naturally come with risks for businesses. As a result, organisations need to consider their approach to integrating this technology into business operations, whilst understanding its rapidly evolving nature.

This publication provides an overview of the legal implications posed by AI and Generative AI, the practical considerations of using this technology, and how we can offer our expertise through innovative applications.



Anna Browne

Head of Innovation and Legal Technology

+44 (0)20 7423 8270

abrowne@trowers.com

what



is AI?

What does '**Artificial Intelligence**' actually mean? To its core, AI is a machine-based system which enables computers and machines to simulate human intelligence through various elements of autonomy. The comparison to human intelligence derives from the fact that AI algorithms replicate the decision-making processes of the human brain, in the sense that it can learn from accessible data, produce outputs such as classifications, predictions, decisions and content which will become increasingly more accurate over time.

The term 'machine learning' is the process of improving the AI systems' performance with experience and by training it with 'input data'. It is considered a subset of AI. The AI system will proceed to learn and improve on its own with neural networks, a series of algorithms mimicking the human brain. Machine learning works well with data that is constantly evolving or where the nature of tasks required from the AI system are susceptible to change.

The rise of Generative AI

Generative AI is a groundbreaking subdivision of AI. Definitions of what this actually is vary, but the EU AI Act has defined Generative AI as a type of foundation model used in

AI Systems “specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video”.

This leads us to the question, what are foundation models? Foundation models provide wider AI functionality through a series of neural networks with the ability to analyse unstructured data and learning to generate specific outputs. These models can be categorised by: Single Modals, which can receive a single source or type of data and generate content using text; and Multi-Modals which can receive multiple sources and types of data, including video, images, audio and text that generate detailed perceptions of the data which have been input.

The major global shift and focus on AI can be attributed to the rise of Large Language Models (LLM) such as OpenAI's ChatGPT. LLMs are a type of foundation model and Generative AI which transformed the potential of AI for two key reasons:

- Language complexity: LLMs can learn language, apply the context and generate creative outputs; and
- Pre-trained on large quantities of data: LLMs can utilise the analysis on vast quantities of varied data and the models can be employed for a wide range of tasks.

Language underpins every aspect of how a business operates on a day-to-day basis, whether that is through emails, contracts, document management systems, videos or audio.

Generative AI is transforming businesses across sectors. In healthcare, Generative AI is revolutionising the patient-clinician experience with tools that can transcribe patient consultations and generate preliminary clinician notes. AI innovation in the finance sector has included applications such as algorithmic trading, gathering market intelligence, monitoring financial performance and detecting data anomalies to prevent fraud. The adoption of Generative AI across all sectors will become inevitable and will ultimately transform the way business is conducted.

The application of AI in the workplace has the potential to speed up routine aspects of daily tasks across a wide range of businesses. The integrated use of AI allows for specialist tasks to be completed cost-effectively, for example summarising documents with specialist language at faster speeds. Accenture has predicted that 40% of all working hours can be impacted by LLMs. The collaboration between AI and human input will allow for employees to delegate certain tasks to focus their time on more important aspects of their work, enabling businesses to deliver time and cost-effective services.

The barriers to adoption of Generative AI

Accuracy: Perfect accuracy and reliability of any AI system's final output cannot be guaranteed and businesses must be cautious of this risk. The quality of the output will depend on specific factors such as specific factors such as: the type of data being used; how the

data is being used; and the type of task required from the AI System. For instance, the Generative AI's algorithm can present false content known as 'hallucinations' which can be highly damaging to a company relying on the output for decision making and without human input. Ultimately, AI should be treated as a collaborative tool with caution, employees should always check the final output and monitor the type of data the algorithms have been trained on.

Ethical Use: Ethical concerns have been raised globally as there is potential for AI Systems to be embedded with bias and discrimination, consequently threatening fair process and in some cases human rights. Bias can infiltrate the AI System during the input of data, training or output stages of its lifecycle. For instance, representation bias could be evident at the 'input stage' if an algorithm is only fed data which is either under representative or over representative of certain social groups, resulting in social inequality. Furthermore, the data itself could contain bias which the algorithm learns and copies. From a recruitment perspective, if the AI is only trained with racially biased data, the bias will be evident in the decision it makes on a potential employee. This threat could exacerbate existing inequalities and prejudices across marginalised groups and lead to detrimental impacts on individuals.

These concerns led to UNESCO producing the first global standard on AI Ethics which was adopted by 193 Member States, including the UK, at UNESCO's General Conference in November 2021. The recommendation highlights core values such as protecting human rights, dignity, diversity and inclusion of people to be found in the foundations for all AI. The UNESCO "Women4EthicalAI" expert collaborative platform is one of the results of this recommendation which aims to advance gender

equality in the design and deployment of AI Systems. Fairness must be ensured by identifying and mitigating biases from the data used by AI Systems in order to produce reliable final outputs.

AI Security: AI is vulnerable to attacks in its security similar to traditional computer systems and cybersecurity. There are multiple ways AI can be attacked: the outputs can be manipulated to lead to harmful or inaccurate outputs and information can be stolen.

Adversarial attacks are designed to lead the AI model to make a mistake and cause harm. For instance, 'data poisoning' is where new data is maliciously injected into the dataset when it is being trained which enables attackers to manipulate the model's future actions. An example would be introducing harmful images and classifying them as safe, so that the AI model will learn this and apply it to similar images. A further method of attacking is 'model extraction' which enables attackers to reverse engineer the model by feeding it inputs and tracking outputs to expose sensitive information. This can be dangerous for businesses if the AI model holds proprietary or classified information that cannot be shared publicly.

AI and the law

There has been a mixed approach worldwide in relation to regulating the AI phenomenon, from legislative frameworks, voluntary guidelines, national policies and the creation of regulatory bodies. The rapidly evolving nature of AI has posed a regulatory challenge in many jurisdictions but there have been differences in national approaches.

The UK has taken a 'pro-innovation' approach to AI regulation driven by the Department of Science Innovation and Technology (DSIT). The AI Regulation White Paper

published in 2023 and subsequent government response introduced a framework which applies a cross-sectorial, principle-based and non-statutory approach to AI. The cross-sectorial principles for existing regulators to integrate within their remits include: safety; security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

Regulators, such as the Financial Conduct Authority, Information Commissioners Office and the Office of Communications responded by updating their strategic approaches to AI to align with this framework which were published by DSIT. On the other hand, Lord Holmes aims to re-submit the private member's bill

'Artificial Intelligence (Regulation) Bill under the new Labour Government with the belief that legislation is imperative.

The EU has taken a comprehensive legislative approach in contrast to the UK's position. The EU AI Act is the world's first legal framework for the regulation of AI through a 'risk-based' system. Whereas the US has taken a lighter approach by introducing mandatory reporting requirements for foundation models which pose a security risk to the country.

However, the UK's position will soon change. The prospect of AI legislation in the UK was made clear by the new Labour Government in its election manifesto, as it proposed to "ensure the safe development and use of AI models

by introducing binding regulation on the handful of companies developing the most powerful AI models". The potential 'AI Bill' was not announced as anticipated during the King's Speech on 17 July 2024. However, it was stated that the Government would "seek to establish the appropriate legislation" and in the interim, the Government has announced the introduction of a Cyber Security and Resilience Bill, to address the increasing risks of cyberattacks, and a Digital Information and Smart Data Bill.



Navigating the AI and intellectual property landscape

Legal considerations and emerging challenges

As AI continues to revolutionise our ways of working and innovating, the intricate relationship between **AI and intellectual property (IP)** has been at the forefront of debate. Interestingly however, despite the ongoing debates, there is little, if any legislative guidance around the interaction of IP and AI. The UK has yet to implement any AI legislation, and the incoming EU AI Act says very little about IP. So where do we stand with AI and IP? Two key issues at the forefront of the debate are: i) the use of IP protected material in the training of AI, and ii) who owns the IP in the output of AI creations.





ChatGPT

Use of IP protected material in AI – the conundrum

AI tools, such as ChatGPT, are large language models (LLMs) which are built by “training” on trillions of words through written works. AI companies have been hit with a series of legal actions from IP owners. Open AI is currently being sued by the New York Times, the root of whose complaint is that the dataset used to train ChatGPT contains a “mass of Times copyrighted content” and is therefore a copyright infringement. Open AI simultaneously faces a similar action from numerous authors in California for the same reason. Meanwhile in the UK, many eyes are on the proceedings between Getty Images and Stability AI. Getty accuses Stability AI of scraping more than 12 million images from Getty’s library of stock images and using them to train its AI tool. When the tool then creates images from users’ prompts, the images created, as argued by Getty, are reproductions of Getty’s images and thus, a copyright infringement. The High Court recently rejected Stability AI’s application to strike out Getty’s claim, and the trial is expected to take place in 2025.

Therefore, the crux of the matter is whether the use of copyright protected material in AI tools an infringement of the owner’s IP in such materials? A definitive answer to this question is yet to be given but it will be interesting to watch the case law emerge on this point. In reality, it may be that the answer is very fact specific, but we will continue to follow the decisions for guidance on this topic.

In terms of available defences to such copyright infringement and the UK legislative framework, current UK copyright legislation has an exception for ‘research for non-commercial purpose’ which permits ‘text and data mining’ (TDM), but non-commercial purposes clearly would not extend to training the likes of ChatGPT. The

UK Government recently U-turned on a decision which would have opened up this exception to also allow commercial scientific research outcomes and allow TDM of databases, in line with the EU. This would have allowed TDM “for any purpose” and the Government (rather optimistically) claimed the wider exception would “ensure the UK’s copyright laws are among the most innovation-friendly in the world”. Therefore, the current UK legislative position is that: AI companies cannot copy third-party owned copyright material to train their AI models save for non-commercial purposes (which is likely to be virtually never). Similarly, creators and owners of copyright works have limited ability to police or monitor the use of their works by such AI companies - thus, no party is truly satisfied.

An interesting solution to this issue is for the two parties to enter into a licensing agreement to permit the AI company to use the copyright materials on the terms agreed by the owner of the materials. This played out recently in a licencing agreement between Google and Reddit earlier this year. In essence, this agreement, worth a reported \$60m per year, gives Google full access to Reddit’s content for the purpose of training Google’s AI models. Such agreements highlight how AI companies and content creators can navigate the IP challenges and avoid expensive litigation by fronting up the issue early on. This may well be something we see more of in the future.

Outside of this, the UK Intellectual Property Office (IPO) has also consulted with industry executives from the AI space and creatives, in the hope of establishing a code of conduct for AI and copyright material. AI companies want easy access to vast troves of content to train their models, while creative industry companies (in print and music) are concerned that they will not be fairly compensated for its use. Unfortunately, the outcome of the consultation was

that an agreement could not be reached, and those talks broke down, shelving the code. The response to the consultation concludes that there will now be a period of engagement between stakeholders which allows creators and AI developers to effectively work together in partnership, with further “proposals” soon to be set out. This perhaps suggests that amendments to legislation may be back on the agenda, but in the interim, we will need to wait for outcomes in decisions such as Getty’s litigation against Stability AI, to help shape the rules and policies on AI and copyright.

Who owns the IP in the work generated by AI?

Another consideration is whether any IP protection can be given to work that is created by Generative AI produced by the AI tools. For example, what happens if a Generative AI model conjures up an invention? Who owns it? The AI company? Or, the client of that company, if such invention was created during their usage? What if the invention has come about because the AI was trained using works belonging to third parties? These are all questions that need answering.

When it comes to “inventions” we are in the realms of patent law. Under the Patents Act 1977, an ‘inventor’ is defined as ‘the actual deviser of the invention’ and, under the patent application process, the application must name the inventor(s). In a recent landmark decision, the UK Supreme Court had to consider whether the named inventor could be a non-human. Dr Thaler, a computer scientist, created an AI model called DABUS, which is capable of autonomously generating new inventions across various fields, without direct human intervention. DABUS created two inventions which Thaler attempted to patent, citing DABUS as the ‘inventor’. The

applications were refused on the basis that the inventor named on the patent application must be a human being. Thaler appealed all the way to the Supreme Court, who upheld the decision, holding that “an inventor within the meaning of the 1977 Act must be a natural person”. The decision does not answer the key question, however, as to whether an invention created by AI is in principle patentable and, if so, who has the right to the patent. On this fundamental issue, the Supreme Court commented inconclusively that, had Thaler presented himself as the inventor, with DABUS being a highly specialised tool, “the outcome of these proceedings might well have been different.” Therefore, the scope of IP protection afforded to works created by such AI tools is just as unclear as the position on the use of IP protected materials in such AI tools (above). However, on the former, the Supreme Court does seem to leave open the door that inventions produced by such AI tools in the future may be afforded patent protection (subject to human inventors being recorded on the patent application and not the AI tool itself).

Are there any (IP focused) benefits to AI?

AI has brought some benefits to the IP sector, and this is through the use of AI algorithms to tackle IP infringements. AI algorithms can scour the internet, analysing data,

texts, images, and patterns across various online platforms, flagging unauthorised use of trade marked or copyright works and counterfeit goods. This is likely to identify and provide helpful evidence of IP infringements in a quick and efficient manner. Similarly, other AI programmes such as ‘Relativity Patents’ harness the power of AI to perform prior art searches, delivering search results quicker and easier than ever before. We will likely see more utilisation of these tools to assist with IP infringement and clearance searching of IP rights.

Practical considerations

So where does that leave us? Whilst we appear to be in a state of flux on the position on AI and IP longer term, there are some key takeaways:

- Businesses with IP rights should develop a comprehensive IP strategy which addresses the challenges and opportunities provided by AI, strategies for enforcing IP rights in the AI world and dealing with litigation and setting internal policies regarding how they wish AI and IP to interact within the business and giving clear guidance to their employees.
- Any organisations in the business of building AI models should be wary as to the content they are using to train those models, acquiring

the correct permissions and licences where appropriate, to avoid litigation down the line.

- Organisations should ensure that any agreements between themselves and AI vendors include indemnities from any IP litigation that may potentially arise in relation to the use of those AI models and are clear who will own the IP in any outputs created using the models.
- If your business has IP rights to protect or requires evidence in respect of an alleged IP infringement, consider the use of AI in assisting with this.

Summary

As AI continues to play an increasingly central role in technological innovation, as well as artistic creation, a burning question remains unanswered – how will the balance be struck between the protection of creators’ works and fostering the development of AI works? The position in the UK is largely up in the air, with no specific legislation (or policies) and an abandoned code of conduct. The UK Government has refrained from promising any AI regulation any time soon, so for now, the UK’s legal landscape in relation to AI and IP will be shaped by the courts in legal battles such as that of Getty.



Employment law and AI – opportunities and risks

AI is being used increasingly by employers for recruitment, monitoring and workforce management. Whilst AI can improve decision making and boost workforce productivity, it can also bring potential issues and risks, which need to be considered carefully.

The traditional recruitment process has been evolving over recent years with AI now playing a key role in talent acquisition. Whilst AI can remove certain biases by focusing on the qualifications and skills relevant to the job description, it can potentially introduce other biases. AI algorithms learn through observing and repeating behaviours and so, if not audited regularly, can present a real risk of adopting or exacerbating unchecked biases. Specific types of AI, for example, facial recognition technology used at interview stage, can also present challenges. The technology has been found to provide less accurate results for female and ethnic minority candidates in some instances, resulting in them receiving lower scores. Examples such as this carry clear risks of discrimination complaints under the Equality Act 2010, which employers need to be alert to.

Monitoring employees through AI is another key concern. With hybrid and remote working being the norm for many employers, some are now relying on AI tools to monitor employees' activities, productivity and performance. Employees, however, have the right to privacy under Article 8 of the Human Rights Act 1998. Although it is possible for employers to justify any interference with employees' privacy rights, the legal scope of this justification is

not always clear cut. In addition, employers must comply with the requirements of the Data Protection Act 2018, by ensuring any personal data obtained and processed concerning employees is done in a fair, lawful and transparent way.

Finally, there are further issues concerning the use of AI in workforce management processes and procedures which should be considered before and during use. For example, when using AI for the purposes of decision making concerning the dismissal of an employee, there is potential for unfair dismissal claims under the Employment Rights Act 1996, as well as risks under the other legislation mentioned above.

Practical considerations

A key way to overcome the challenges presented by use of AI in employment is to ensure there is robust human oversight. Ensuring any AI-led decisions are overseen by a human reviewer will allow any issues with AI technology or algorithms to be identified and rectified quickly. The implementation of specific AI policies governing what this oversight should look like in each workplace or decision-making process can be helpful.

If monitoring employees, employers must establish monitoring policies which are reasonable and proportionate and do not unlawfully interfere with an employee's right to privacy. By adopting monitoring policies which establish clear practices and expectations, employers can ensure transparency in their communications with employees and minimise risk of breaching the relevant legislation.

AI systems used for recruitment purposes should be tested, challenged and updated regularly to ensure there are no issues which may cause biases. In addition, ensuring that systems and decision making is reviewed by humans within relevant teams will minimise the risk of developing unchecked issues.

Summary

Although AI may save employers time and money in some areas by accelerating recruitment, streamlining decision-making processes and efficiently monitoring employees, organisations must ensure they are retaining an appropriate level of human oversight to reduce risk. Complying with relevant legislation should remain a priority for employers, not only to avoid legal risk but to also ensure trust within the workforce and to maintain positive employer brand and reputation.





Data protection and privacy in the age of AI

The advances in AI in recent years highlight the importance of carefully reviewing the processing and **sharing of personal data**, as use cases for AI often involve the usage of personal data. The current data protection legislation in the UK is the Data Protection Act 2018 (DPA 2018) and the UK GDPR, which is an amended version of the EU GDPR.

Sir Keir Starmer stated in his introduction to the King's speech that "we will harness the power of artificial intelligence as we look to strengthen safety frameworks". The only further detail given though in the speech itself was that the Government will "seek to establish the most appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models".

Whilst we do not yet have any further details on what this legislation may involve, in the meantime there are elements of UK GDPR and the DPA 2018 which regulate AI in relation to personal data. We have set out below the key principles of current data privacy legislation in relation to AI, and some practical tips.

UK GDPR – key principles

Article 5 of the UK GDPR sets out key principles which lie at the heart of the general data protection regime. Applying these principles to AI:

- **Lawful, fair and transparent processing:** Ensure you have a lawful basis of processing in relation to your usage of AI, and are open about your use of AI-enabled decisions.
- **Purpose limitation:** Tell individuals what their data is being used for and do not process it in ways which they would not expect. Ensure that your usage of AI is in line with what you have told individuals that your usage of their data will entail.
- **Adequate, relevant and not excessive:** When using AI to analyse data, review which data is actually necessary for the processing and do not analyse other data.
- **Accuracy:** make sure that the data being used is accurate and review it to ensure it is up-to-date.
- **Storage limitation:** personal data must be kept no longer than is necessary for the purpose for which it is processed. For example if you collect data about job applicants and use AI to sift candidates, do not indefinitely keep data of rejected applicants.
- **Security:** personal data must be processed taking appropriate security measures for the risks that arise from the processing. When you appoint a processor using AI, ensure that you carry out due diligence and are comfortable that they are dealing with data in a secure manner.

This is normally by way of a privacy notice.

The UK's data protection regulator, the ICO, has published guidance to assist organisations in complying with Data Protection requirements in relation to AI. AI systems may involve processing personal data in different phases or for different purposes. This means you can be a controller or joint controller for some phases and a processor for others. The ICO's AI guidance includes more information on this point, which can be read in conjunction with its wider controller and processor guidance and checklists.

Privacy notices and data protection impact assessments (DPIAs)

Articles 13 and 14 UK GDPR set out the information that must be provided to individuals whose data is being processed. You must set out the purposes of the processing, the legal basis of processing and the individuals' rights in relation to the processing. Where AI is being used, it is important to assess whether this will result in any new form of processing or individuals' personal data being used to train AI models, as this could result in a requirement to update your privacy notice and inform individuals about any changes.

Article 35 UK GDPR sets out that a DPIA must be undertaken where a type of processing (in particular using new technologies) is likely to result in a high risk to the rights of individuals. This will include an assessment of the risks involved in the processing, and the mitigating steps which could be taken to reduce that risk.

Automated decision making and profiling

AI is frequently used with personal data to undertake automated decision making and/or profiling. This is the process where decisions are made using an algorithm based on uploaded data, without any human involvement in the decision (beyond setting parameters such as, in the recruitment context, specifying that the applicant must have a degree). Data controllers must be mindful of their obligations and carefully consider their responsibilities when using automated processing. The UK GDPR provisions on automated processing state that an individual has the right not to be subject to a decision based solely on automated processing, where that decision has a legal or similarly significant effect on them.

There are limited exceptions available where automated decision making and profiling can be undertaken where the decision will have an effect on an individual. These are where the decision is necessary for a contract (such as credit scoring for a loan application), authorised by law (such as banks identifying potential fraudulent activity), or where explicit consent is provided.

This means that, for example, if AI is used to make recommendations to individuals upon holiday destinations they may like, this is not restricted, but if AI is used to assess whether an individual should be offered a heart transplant, this will require human intervention unless an exception is available.

Where AI is used to undertake direct marketing purposes, individuals have the right to object and their data can no longer be processed for that purpose.

Where AI is used to undertake profiling, individuals have the right to object and unless the controller can demonstrate that they have compelling legitimate grounds for the processing then that individual's data must no longer be used for profiling.

Contracts with AI providers

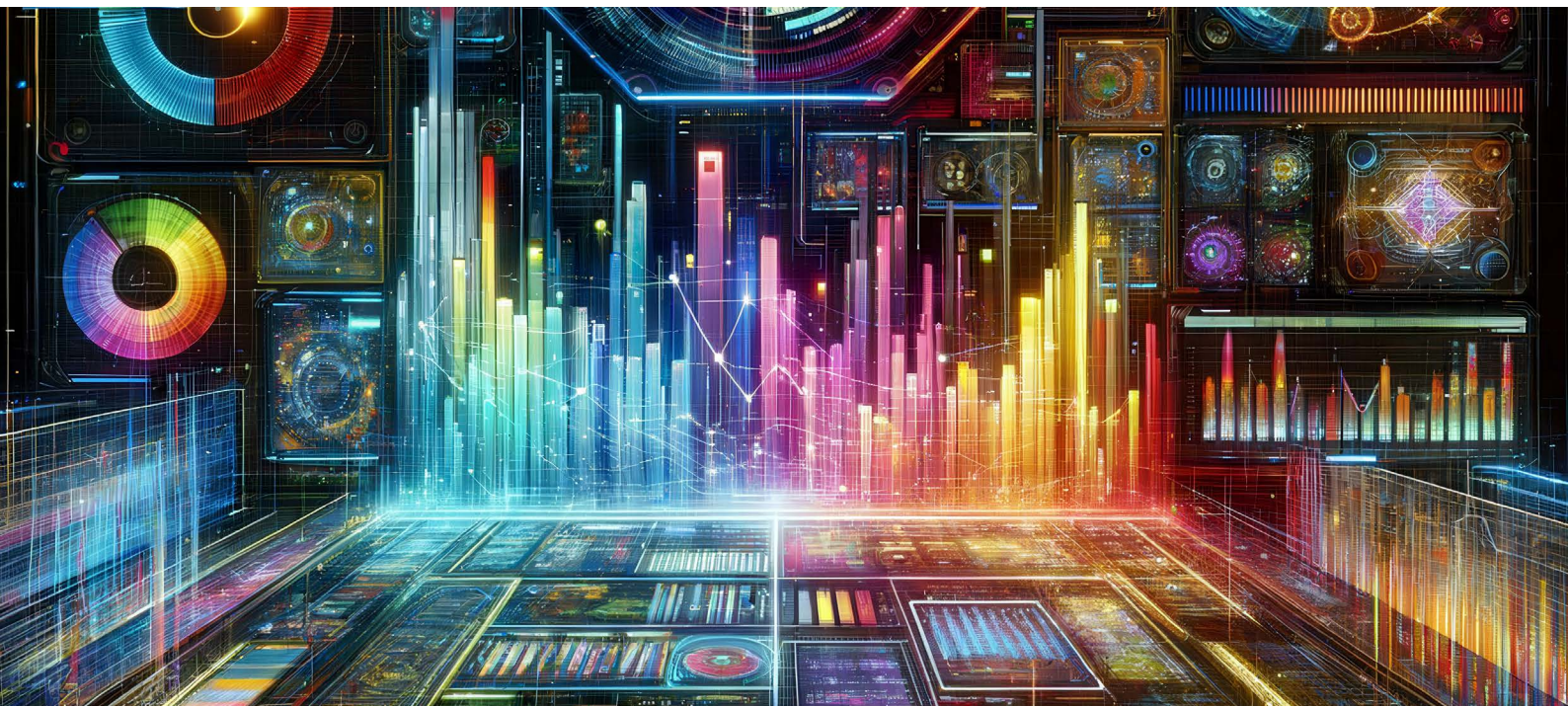
AI providers usually act as a processor on behalf of the controller of the data. Where this is the case, article 28(3) UK GDPR sets out the minimum requirements for a contract between the two parties. This includes requirements to only process data on documented instructions, requiring staff to maintain confidentiality and to only engage sub-processors with general or specific consent. Most data controllers view the article 28(3) provisions as a starting point.

If data is to be transferred abroad for processing you will also need to consider whether a restricted international transfer is taking place. If so, you will need to have appropriate transfer documentation in place and undertake a transfer risk assessment.

Practical considerations:

Compliance with data protection law

Data privacy should be by design not by default, and transparency is key.



Privacy notices

If you use AI, you should review your privacy notices to ensure that you set out any changes to how individuals' personal data is processed in using AI. This review should include an assessment of whether disclosure should be made of any automated processing and profiling.

You should also, when using third-party AI, identify whether the third party is acting as a controller or a processor and be transparent about this. If a third party is acting as a controller then their privacy notice should also be made available to individuals.

DPIAs

The UK and EU guidance state that in most cases when AI technology is implemented, this will trigger the need for a DPIA.

A DPIA will need to make clear how and why you are going to use AI to process the data. This includes describing the nature, scope, context and purpose of the processing. A DPIA should detail:

- how you will collect, store and use data;
- the volume, variety and sensitivity of the data;
- the nature of your relationship with individuals;
- the nature, scope, context and purpose of the processing;
- risks to individuals and any mitigating measures; and
- the intended outcomes for individuals or wider society, as well as for you.

Contracts with AI providers

Where an AI provider is acting as a processor on behalf of a business, then that business, as a controller, has responsibility for the data processed. This means that a contract with an AI provider should set out very clearly what the obligations of the provider are and

what it is permitted to do with the personal data in question.

The processes of the AI provider should also be reviewed as part of due diligence, including an assessment of whether the provider is acting as a controller in relation to their usage of training data.

The risk of bias

Maintaining data accuracy is key for training AI and is achieved by ensuring that the data used is accurate, up-to-date and relevant. If the training data or input data is inaccurate or biased, an AI system is at risk of producing an output that reflects this.

AI systems and algorithms must be regularly monitored and tested to detect and mitigate biases that could result in unfair treatment or discrimination. This could be done through regular bias audits or by using statistical methods and fairness metrics to evaluate and mitigate bias.

You should assess, on an ongoing basis, whether the data you are gathering is accurate, representative, reliable, relevant, and up to date.

Data security and storage of data

You must take appropriate security measures to protect the data collected, stored, and used in AI systems as well as the data produced by AI systems. This may involve the use of encryption technologies or authentication, and putting the data into a separate software system. You should ensure that AI providers detail their security measures and that you review these to ensure that they are sufficient.

Robust security measures must be in place to protect personal data and regular security audits must be conducted.

You need to consider the impact of third parties accessing the data and whether personal data can be anonymised or pseudonymised to mitigate any risks.

If personal data is transferred or stored outside the UK, companies must ensure compliance with data protection laws regarding international data transfers.

Key takeaways

- Undertake due diligence on AI providers and check what training data they use, whether they act as a controller or a processor, and their data security measures. Undertake regular audits to check compliance.
- If using AI to undertake automated decision making or profiling, assess whether the decisions will have a legal or otherwise significant impact on individuals. If so, human involvement must be built in.
- Review and risk assess contracts to ensure that protective measures are in place in relation to personal data and that the AI provider's obligations are clearly set out.
- Review and assess your current privacy notices and ensure that you are being transparent about new types of processing personal data.
- Undertake DPIAs where there is any high risk for individuals.
- Consider the location of the processing and if any restricted international transfers are to be undertaken as part of the processing.
- Train your staff upon data privacy compliance and confidentiality. Update data protection policies to take into account any usage of AI.



Legal risks and litigation in the age of AI

The term '[machine learning](#)' is the process of improving the AI systems' performance with experience and by training it with 'input data'. It is considered a subset of AI. The AI system will proceed to learn and improve on its own with neural networks, a series of algorithms mimicking the human brain. The use of AI across businesses can result in a range of legal issues, and ultimately litigation, if the risks associated with AI are not properly considered and addressed from the outset. This is a key issue that organisations across all sectors need to consider before embarking on their AI journey.

AI related claims could arise in the context of a range of matters such as copyright, data protection, equality and employment related issues. For example, a US radio host and an Australian mayor have both threatened the AI research organisation, OpenAI, with claims for defamation after the OpenAI chatbot wrongly stated that they had defrauded a charity and been found guilty of bribery. There are also potential cases that might arise relating to breach of consumer protection laws; for instance, AI may provide misleading information about products or services during interactions with customers.

AI has a potential use case in almost every area of business. Organisations should think about the kind of liabilities that may arise from the use and deployment of AI. However, given the extensive number of use cases and potential areas for dispute, this is not a straightforward task. Risks and subsequent litigation may arise from both the information that is input into the system and the output that is produced. Therefore, it will be important to keep an eye on the development of the legal landscape, as well as the technology.

The issue is compounded by a lack of clarity on who should be responsible for any damage or harm caused and specifically, whether liability should sit individually or jointly, with the creator, supplier, or user. As there is no AI specific legislation in the UK, the existing law, most notably from tort and contract, applies to govern this debate. Whilst it has been proposed that AI entities should have a separate legal personality, it remains to be seen whether this will be adopted in English law. In the meantime, an emerging body of case law will be required to fill in the gaps.

Furthermore, given the global nature and use of emerging technologies, the difficulty of

establishing responsibility creates jurisdictional challenges. For example, where AI is developed and rolled out in different countries, the question arises as to which laws govern the dispute. If governed by the law of the jurisdiction in which the AI is developed, then this gives rise to fears of 'forum shopping' where AI is deliberately created in permissive jurisdictions before being deployed elsewhere, notwithstanding that any harmful effects of the AI may be felt elsewhere.

The risk of 'forum shopping' may, however, be quelled by the implementation of international agreements enhancing uniformity of obligations and standards. For example, the UK, US and EU all recently became signatories of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which creates a legal framework covering the entire lifecycle of AI systems.

Practical considerations

Despite these difficulties, businesses can take proactive steps to manage litigation risks. For instance, attention should be paid to the content of agreements for the supply or purchase of AI where clarity of roles and responsibilities will be key. For example, it would be desirable to include provisions, such as warranties and indemnities, to apportion liability. Depending on the circumstances, it may be appropriate to seek a warranty for non-infringement of third-party IP rights or an indemnity in respect of the same.

Equally, it is prudent to add clauses specifying the level of testing that the AI has and will be subject to throughout its use. There are also insurance policies available, such as Technology Errors and Omissions Insurance, which might offer coverage in the event of certain AI related claims. Naturally, robust internal

governance can work to mitigate litigation risks, however litigation and risk management strategies must be tailored to a business and the particular issues that arise.

A silver lining is that where litigation does arise, AI can be utilised to streamline the process. Already, eDiscovery platforms have become widely used to carry out document reviews. Moreover, Generative AI technologies have the potential to bolster eDiscovery's utility by providing summaries and translations. AI can even be used as a predictive tool with algorithms examining past cases to help establish the chances of a claim's success. Understanding how these algorithms work, and how they can be deployed with confidence will be key.

In criminal matters, algorithms have already been used to establish a person's risk of reoffending and help judges with sentencing decisions. However, the risk of bias and potential discriminatory effects has been and remains a strong argument against the use of AI in making such assessments. Despite this, as the technology develops it may also be that we see AI being adopted in civil matters to assist with determination of certain categories of cases. Litigators and judges alike should always ensure that AI is approached and used with caution. The perils of not doing so are well illustrated in a recent American case where a lawyer filed a court document citing cases that were entirely fictional courtesy of AI.

Key takeaways

The use of AI gives rise to a wide array of potential risks and claims that should be thought about in advance. The types of claims that may be faced will be dependent on the particular use of AI and a business-specific assessment should be carried out to identify and mitigate the risks of litigation.



Internal AI governance

Policies, risks, and best practice

Whilst many organisations are required to have certain policies in place by law, there is currently **no legal requirement in the UK** to have policies in place governing the development or usage of AI.

However, it is important to consider putting these policies in place in order to ensure that:

- AI is being used consistently and transparently across your organisation;
- suppliers are properly assessed;
- data privacy legislation is being complied with; and
- staff are fully aware of the risks of AI and how to use it safely.

Practical considerations

Internal governance regimes should account for the risks and opportunities the usage of AI presents for an organisation. The key risks include accuracy, lack of transparency, bias, accountability, data privacy and reliability issues. AI systems may produce erroneous output and if the correct processes are not in place to review information generated by AI, this could lead to misuse of sensitive information, ethical issues and

over-reliance, creating the potential for errors and a lack of clarity over liability.

It is useful to start with AI usage reviews within your business (i.e., looking at both the intended and current use of AI) with a focus on each system's scope (i.e., what it is trained to do and not do) to identify risks. Doing so determines the type and level of internal governance required and informs the creation of policies and procedures.

Even if an organisation has not formally adopted any AI, it is likely that employees have spotted opportunities for AI and are already using AI for a variety of purposes including, for example, the use of Generative AI when drafting marketing material or other communications. On this basis, it is important to foster an open environment so that organisations know what their employees are using, in order to set sensible parameters based on the opportunities and risks presented by the use of AI.

Policies and procedures

Some organisations may prefer stand-alone AI policies and others may prefer to update their IT usage or governance policies. Whichever approach is taken, it is important to ensure that clear guidance is in place, setting out the organisation's principles and aims in relation to its usage of AI, and its internal rules to follow when procuring or using AI.

For many organisations, the best route will be a combination of implementing new policies with a clearly defined set of rules, as well as updating other internal and external documents, such as privacy notices and security policies. This is particularly the case when an organisation operates across multiple jurisdictions, having differing legal and regulatory requirements.

In addition to having clear policies in place, we also recommend creating procedures to back up those policies, in order to set out the steps to be taken when

considering adopting AI, and giving employees clear directions on how they can use any approved AI.

Training and staff communications

It is vital to communicate policies and procedures to staff, especially when new expectations and rules are being set. We suggest this should be through regular updates, meetings, and training sessions, covering both how to safely use any approved AI, and the risks involved in both approved AI and open-source AI. Technical information should be provided in a clear and easy to understand way, with demonstrations and examples of risks to ensure that staff understand the organisation's attitude toward AI and compliance requirements.

Clear parameters over the usage of widely available and particularly open-source AI, such as Chat GPT, should also be communicated. A sensible approach to the risks should be taken as there is, for example, a difference between employees using publicly available AI to help them with short LinkedIn updates about non-confidential matters, and employees using the same AI to summarise business critical information.

Assessment of suppliers

Given the wide variety of AI available on the market and the relatively low cost of licensed usage as opposed to the cost of building and developing in-house AI systems, organisations frequently use AI systems provided by external suppliers. To minimise risks, organisations should ensure that they undertake supplier due

diligence before using third-party AI systems. A sensible approach is to request that suppliers complete a questionnaire detailing how both personal data and non-personal data will be stored and other important security and ethical considerations.

However, despite thorough due diligence, it still may be that adverse effects will arise. Therefore, it is important that internal governance regimes provide for preventive measures, such as testing and human oversight and also risk mitigation, such as detailing how security breaches and incorrect or misleading outcomes are to be handled.

Information security and testing

It is crucial that AI systems are as secure as possible to reduce the risk of security breaches and to



protect data, confidentiality and IP rights. Suppliers should be asked to detail their strategies for ensuring information security and mitigating against cyberattacks. For example, it is important to ask what network controls are in place and what physical security measures are in place at suppliers' premises.

Suppliers should also be asked about their testing of the AI system. It is particularly important to ask if penetration testing (a simulation cyberattack used to check for vulnerabilities) has been undertaken. Also, the supplier should be asked to supply details of any other testing and how often it has been and will be carried out. This is important to determine both that the AI system will work as desired (through functional testing) and that there will not be any unexpected issues (through exploratory testing).

In addition, supplier accreditation can provide reassurance, so it is worth asking if potential suppliers can produce relevant certificates from accredited organisations, for example, the ISO 42001 certification which indicates that a supplier has robust processes in place to manage risks, and the ISO 27001 certification which is the international standard for information security.

Data protection

Supplier due diligence should also determine whether the supplier's provision of and the proposed usage of an AI system is compliant with applicable data protection laws.

An assessment should be undertaken to establish what personal data is used or will be used, how it is processed, how it is stored, what protective measures are in

place, and if there is any third party processing or restricted international transfers of personal data.

Generally, suppliers of AI act as a processor of personal data, with the organisation which is the customer of the AI supplier being the controller of the data (and determining the purpose of the processing). However, this should be reviewed on a case-by-case basis by assessing the actual usage of the relevant personal data by the supplier. If a supplier retains data without express instructions from the controller, or uses it for training their system, they will likely be deemed to be acting as a controller. This can bring in additional complications and considerations, particularly where a supplier is being provided with sensitive personal data. The data processing activities being undertaken by a supplier should be carefully assessed in each proposed usage of AI.



Licence terms

The supplier is usually the owner of the AI system, and a licence is usually granted to the customer within a supply agreement. The terms of these agreements should be checked to ensure that the licence permits the organisation to use the AI system for its intended commercial purpose. There may also be certain restrictions, such as prohibitions on modifications, which end-users will need to be made aware of.

Insurance

When using AI, it is essential to review your insurance policies. Organisations should ensure the potential risks associated with AI use and misuse are covered. AI associated risks may already be covered under standard policies, such as professional indemnity and D&O insurance. However, more specialised policies may also be required depending upon the AI product used.

In addition to reviewing your own insurance coverage, it is important to check the relevant supplier's insurance coverage and to request copies of insurance policies and certificates.

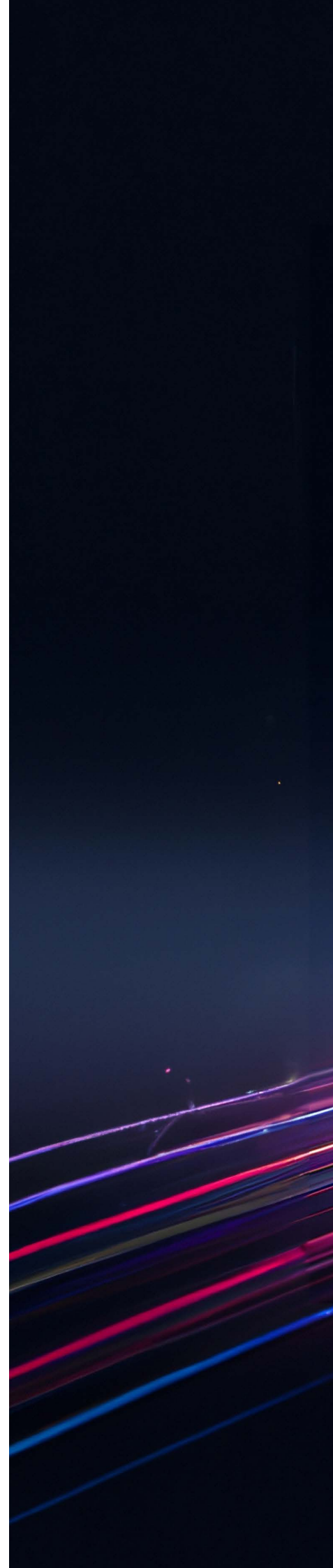
AI governance groups

Having a specialised governance group within your organisation to oversee AI operations and strategy is beneficial. Given the extensive and inter-disciplinary effects of AI, this group should be made up of individuals with a range of expertise across your organisation as the group is likely to have broad responsibilities involving monitoring the legal landscape and identifying commercially useful AI systems for the business.


Key takeaways

Effectively governing the use of AI will require a framework that is bespoke to the obligations, risks and issues AI presents to each organisation. Once in place, the rapid development of both AI and the legal and regulatory landscape means it should be kept under continuous review. When devising or updating internal governance regimes to account for AI there are several key considerations:

- Clearly identifying the legal and regulatory obligations and/or restrictions that are imposed on your organisation in connection with your use of AI systems.
- Whether new or revised policies and procedures are required to provide clarity on and adherence to the rules relating to intended or existing use of AI.
- The organisational rules on AI usage and the risks it carries need to be effectively communicated to staff alongside training on correct and appropriate use of the AI.
- When procuring AI systems, organisations need to ensure that thorough due diligence is carried out on suppliers and systems.
- Insurance policies should be reviewed to ensure that there is sufficient coverage for the risks associated with the use of AI.
- The potential benefits of having an internal governance group in place with responsibility of overseeing AI operations and strategies.







AI integration in the energy sector

The energy sector has historically been behind the curve compared to other sectors, such as telecoms and finance, when it comes to the integration of digital technologies. The use of AI in the energy sector is no exception, however, this is now rapidly developing. A key challenge for the industry is the need to navigate the complex and rapidly evolving energy sector and its intricate regulatory landscape, which is undergoing a generational shift, as the UK looks to develop an energy market increasingly based on low carbon generation.

Part of the challenge stems from the fact that the UK is transitioning from a historic system based on centralised and predictable generation, with largely unidirectional flows of energy from the generator to end users. The new energy landscape has increasing reliance on disaggregated and intermittent generation and increasing complexity of both generation and demand profiles. This results in a step change in the amount of data and data points measuring generation and supply

of electricity, and a need to balance increasingly complex supply and demand profiles across all scales. Digitalisation and the use of AI has emerged as a potential solution in the energy sector to address this challenge, allowing vast amounts of data to be processed and processes to be automated and respond to market signals in real time.

The energy sector is investing heavily in AI for a wide range of uses, including:

- Forecasting and optimisation: AI enhances energy supply and demand forecasting and optimises thermal and renewable power generation as well as Energy Storage.
- Smart technology: utilises machine learning for energy efficiency monitoring (smart meters) and grid management (smart grids);
- Oil and gas: improves drilling accuracy and operations using data analytics;
- Diagnostic and predictive

- maintenance: uses AI for data analysis, fault prediction, and maintenance scheduling;
- Weather prediction: assists with renewable energy production;
- Market efficiency: enhances efficiency in energy markets and grid management.

Key challenges of AI in the energy sector

When it comes to AI in the energy sector, energy businesses must consider certain challenges for successful integration. A few common challenges to be aware of include:

- Ensuring data accuracy and reliability when AI is trained on vast data sets. Issues with data access and standardisation has meant that there are limits to what can be achieved, but the industry is moving toward more open-source data sharing standards to combat this and unlock the potential of energy data to provide both individual services and whole-system efficiencies.
- Data security and protection – large volumes of energy system data will relate directly to household consumption and ensuring robust processes are in place to put appropriate controls on access and use of data will continue to be a key consideration for the foreseeable future.
- IP considerations – data protection under various IP laws, copyright as well as database rights.
- Staying up to date with the ever-changing technology uses and trends in an industry that is based on assets with long lifecycles and multi-year/decade investment cycles.
- Contract documents in the renewable energy sector may be bespoke and unique to individual projects or stakeholders. This means there are significant parts of the industry without long-term market standard positions, or where contract terms are kept highly confidential. This makes AI driven document production more challenging due to insufficient training data being freely available.
- Regulatory frameworks vs technology: Given the speed with which new technology is introduced, it is unsurprising that rules and regulations lag behind. This is a real concern in highly regulated energy markets and carefully balanced energy systems (electricity and gas grids in particular). There is a risk that regulatory frameworks are insufficiently flexible or otherwise unfit for purpose to allow the full benefits of new technologies to be realised. Of at least equal concern is the risk that they are unable to prevent abuse or mitigate market shocks (such as price spikes) when technology allows decisions to be taken quicker than rules and regulators can respond.
- Liability where things go wrong – determining liability in the event of AI system failures or incorrect decisions can be complex. Clear legal frameworks are required in order to address who is accountable when AI systems cause harm or loss.
- Questions about accountability for public spending, energy prices or outages where AI is used.
- AI itself uses up a lot of energy and this will increase as AI grows. Corporations will need to make informed decisions when choosing AI providers, partnering with those who are energy-efficient and sustainable.

Key takeaways

The integration of AI into the energy sector clearly presents significant opportunities and enhancements, however, these advancements come with practical and legal challenges that must be carefully managed. Ensuring robust cybersecurity measures, addressing data privacy concerns, and maintaining compliance with regulatory frameworks within the sector is critical for mitigating the risks that have been discussed above.

As the energy sector continues to evolve, propelled further by AI, stakeholders must balance innovation with diligent oversight. By adopting best practices and ensuring collaboration between the technologists, regulators and industry leaders, the energy sector can harness the full potential of AI, whilst safeguarding against its inherent risks. This approach will not only enhance the reliability and efficiency of energy systems, but also contribute to a more sustainable and resilient future for energy.

Legal considerations

- Cybersecurity and data protection issues – the World Energy Council has warned that increasing interconnection and digitisation of the industry makes it a prime target for cyber criminals, state-sanctioned cyberattacks, terrorists and hackers. Such attacks can disrupt energy supply, lead to data breaches, and compromise sensitive information.
- Miscorrelations due to insufficient training, data or coding mistakes, for example, faulty AI predictions in demand forecasting could lead to either a surplus or shortage of energy, affecting grid stability.

AI in Private Equity

– strategies and challenges



Integrating AI and Generative AI into business strategies is no longer a choice for private equity (PE) firms, it is imperative to **maintain a competitive edge**. There are a range of use cases across an investment lifecycle, from sourcing and conducting due diligence, to analysing data and financial performance, portfolio management and ultimately exit. However, harnessing this new technology comes with inherent risks which should be considered and managed carefully. This article explores some of the benefits and challenges which PE firms might face when integrating AI at different stages of an investment.

Investment

Investment sourcing and analysis for PE firms is traditionally the result of utilising well-established relationships, networks and extensive market research. AI and Generative AI tools can enable a quicker, wider and more proactive approach to identifying and evaluating potential investment opportunities. By integrating large language models into a PE fund's knowledge base, AI tools can analyse huge quantities of data from multiple sources. This can include financial data, company data and market data (such as analysis on market conditions, sector trends and industry reports). Once the data is collected, machine learning algorithms use predictive analysis to identify attractive investments, for example through consistent revenue growth or low debt levels. AI tools could also be used for scenario analysis, at Investment Committee stage, where AI algorithms predict impact on an investment's potential performance, from looking at interest rates to economic growth.

The PE landscape remains competitive with funds competing for the highest quality assets. The ultimate prize is always an off-market transaction, where a fund

can avoid becoming involved in an auction process; consequently, funds which can identify investment opportunities early by integrating the benefits of AI tools, whilst mitigating the potential risks, are likely to find themselves with an edge. However, it remains true that successful transactions always have, and always will be, forged out of strong personal relationships between investors, sellers and management teams. Whilst AI tools might assist with target identification and scenario planning, there is no replacement for that human connection.

Risk management

Once an investment has been made, the focus shifts to managing portfolios to ensure growth and maximise potential returns. AI has the potential to play an integral role in this process by offering advanced analytical tools and insights that support strategic management and improve decision-making. For instance, it can utilise historical data and machine learning models to predict the performance of portfolio companies. Some firms have already leveraged AI capabilities across their portfolios to identify, for

example, those that might require further funding to support them through challenging upcoming periods. AI can predict declining sales performances based on market conditions and anticipate shifts in customer behaviour. By predicting performance, PE firms and management companies can take proactive measures to mitigate potential risks or re-evaluate the lifespan of investments.

Most PE firms are in the early stages of integrating AI into their portfolio management process, and it's important to understand the challenges associated with greater adoption. One of the primary concerns is the accuracy of AI prediction, which is heavily dependent on the data used. If the input data fed into the AI to develop its algorithms is biased or outdated, it can lead to incorrect predictions, poor decision-making, and reputational damage. Furthermore, using historical data could also fail to account for new and unforeseen market trends and conditions, resulting in unreliable predictions that do not accurately reflect the market dynamics at the time of usage. There is also a risk of sharing sensitive information and breaching confidentially if AI models use input data collected from portfolio companies or historic

investments to further train their algorithms. This is especially the case where the AI tool is not proprietary to the PE firm and may be used by other third parties. If proprietary information, confidential investor, or client data becomes available to other users of the AI tools, including competitors, this could lead to both financial and reputational damage.

Ultimately, using AI and Generative AI during the holding period of an investment can enhance risk analysis and drive a forward-thinking approach to portfolio management; but it will be important for the investment team to challenge and interrogate the outputs from any AI tools being used and to remain aware of the importance of taking steps to ensure confidentiality of proprietary information.

Exit phase

The exit phase is an essential phase for realising returns on investments. AI can assist with crafting a successful exit strategy by helping PE firms assess the optimal time to exit an investment. A data driven approach can provide valuable insights during negotiations and help firms to secure the best possible deal. By analysing potential buyers, current market conditions and investor sentiment, AI can streamline the exit process and ensure that firms are maximising the returns on their investments with greater efficiency. The time saved can be re-distributed into human creativity, in discovering new investment opportunities.

Using AI during the exit phase introduces its own set of challenges, such as ensuring the complete and seamless integration of this new technology with the traditional investment process and decision-making frameworks. It is essential that AI compliments rather than disrupts existing practices. Poor integration could lead to inefficiencies and slow down the exit process. We expect that most firms will embrace a phased implementation of AI; allowing teams to gradually adapt, trust and learn to use the technology effectively alongside current frameworks.

Practical considerations

To successfully utilise AI as a PE firm, there are a few practical considerations which should be implemented to assist in mitigating the risks.

Data: Firms should ensure input data is current, comprehensive, and free of any bias. Ensuring models are being updated regularly is essential to account for sudden changes in the market and to prevent a one size fits all approach. In addition, teams should be aware of the limitations of AI and its potential lack of accuracy. Firms should therefore use AI as one of many inputs in the lifecycle of a portfolio rather than relying solely on the technology and use the technology to supplement human input, not to replace it.

Policies and procedures: Establishing AI risk management systems will ensure that PE firms can adopt AI tools safely. For instance, introducing strict internal governance policies and conducting regular security audits are essential to protect sensitive data and ensure confidentiality, and ensuring that those policies and procedures are adopted across the business.

Summary

AI has the potential to transform the PE industry by streamlining deal sourcing, enhancing portfolio management and supporting exit strategies. The integration of AI can provide an advantage amongst competitors, and firms must embrace the disruption that AI brings and naturally evolve alongside AI, as its capabilities continue to grow.



The future of AI and Generative AI



Victoria Robertson
Partner

+44 (0)161 838 2027
vrobertson@trowers.com

“The era of AI is here, ushering in a transformative wave with potential to touch every facet of our lives and enhance our experiences in unprecedented ways. It is not just a technological advancement; it is a societal shift that is propelling us into a future where innovation takes centre stage.”

Chris Barry, Microsoft Canada

As AI continues to evolve at a rapid pace, businesses must remain agile and adapt their strategies to navigate the complex landscape of legal and ethical challenges. The key risks, including accuracy, transparency, bias, accountability, data privacy, IP infringement, and reliability, necessitate a proactive approach to mitigate potential harm and maximise the benefits of AI.

While the EU AI Act provides a comprehensive legal framework, the UK's approach remains in flux. The potential adoption of similar regulations could significantly impact the AI landscape, particularly in terms of trust, adoption, and the development of AI products. However, the absence of detailed UK legislation may lead to companies adopting defensive measures to protect their content and intellectual property.

Following the change in Government in July 2024, the UK's approach to AI regulation has undergone another significant transformation, reflecting the dynamic nature of AI development and its far-reaching implications. Under the previous Conservative Government, a non-binding approach to AI governance prevailed, emphasising voluntary measures and industry self-regulation. However, the current Labour Government has signalled a plan for a marked shift towards a more prescriptive regulatory framework.

The proposed binding regulations outlined by the Labour Government represent a significant departure from the previous approach. While the specific details of these regulations remain to be clarified, they suggest a greater emphasis on ensuring that AI is developed and used responsibly, aligning with ethical principles and legal frameworks. This shift aligns with growing international concerns about the potential risks and benefits of AI technologies.

As the UK navigates the uncharted territory of AI governance, it is essential to consider the potential impact of these regulatory changes on AI development and innovation. While a more stringent regulatory environment may be necessary to address



certain risks, it is crucial to avoid stifling innovation and hindering the UK's competitiveness in the global AI landscape.

The UK's approach to AI regulation must also be considered in the context of emerging international norms and standards. As countries around the world grapple with the challenges and opportunities presented by AI, there is a growing need for international cooperation and the development of common frameworks. The UK's regulatory framework will hopefully be aligned with international best practices, while also reflecting our unique circumstances and priorities.

The UK recently signed a new international agreement on 5 September 2024, alongside the US and the EU, amongst others. This agreement signifies the UK's commitment to international cooperation in AI regulation and highlights the growing recognition of the need for global frameworks to address the challenges and opportunities presented by AI technologies. As the UK continues to play a leading role in shaping the international landscape of AI governance, the signing of this agreement underscores a commitment to responsible AI development and willingness to collaborate with other nations to address the shared challenges and opportunities of the AI age.

To prepare for the future, regardless of the legislative approach, businesses must prioritise AI literacy among their staff, ensuring they understand the risks and opportunities associated with AI technologies. This includes training employees on how to identify and address misinformation, prevent AI impersonation, and mitigate the potential for bias and discrimination. Additionally, businesses should consider implementing robust governance frameworks to oversee AI development and deployment, ensuring that ethical principles and legal requirements are adhered to.

Moreover, investing in high-quality data is crucial for maximising the potential of AI. By ensuring data accuracy, reliability, and diversity, businesses can improve AI performance, reduce bias, and minimise

the risk of errors. Collaborating with AI experts and researchers can help businesses stay informed about the latest advancements and best practices in AI development.

In addition to these measures, businesses should also consider the broader societal implications of AI. The potential for job displacement, economic inequality, and social disruption must be carefully addressed to ensure that the benefits of AI are distributed equitably. By working with governments, educational institutions, and other stakeholders, businesses can contribute to the development of policies and initiatives that mitigate negative impacts and promote positive outcomes.

As AI becomes increasingly integrated into various aspects of our lives, it is essential to foster a culture of ethical AI development and use. This involves promoting transparency, accountability, and fairness in AI systems, as well as ensuring that AI is used for the benefit of society as a whole. By adhering to ethical principles and engaging in open dialogue about the implications of AI, businesses can help shape a future where AI is a force for good.

The future of AI is marked by both promise and uncertainty. By proactively addressing the risks and seizing the opportunities, businesses can harness the power of AI to drive innovation, improve efficiency, and create sustainable value. As AI continues to evolve, it is essential for businesses to remain vigilant, adapt their strategies, and embrace the transformative potential of this technology.

AI is a rapidly evolving area. Our team is here to support you in navigating the complexities of the evolving AI regulations, ensuring best practice for your businesses to safeguard from potential risks but embracing its potential. Our multidisciplinary practice is here to support you. Please reach out to Victoria Robertson, Partner, if you require help or advice.



© Trowers & Hamlins LLP. This document is for general information only and is correct as at the publication date. Trowers & Hamlins LLP has taken all reasonable precautions to ensure that information contained in this document is accurate. However, it is not intended to be legally comprehensive and it is always recommended that full legal advice is obtained. Trowers & Hamlins assumes no duty of care or liability to any party in respect of its content. Trowers & Hamlins LLP is an international legal practice carried on by Trowers & Hamlins LLP and its branches and affiliated offices – please refer to the Legal Notices section of our website <https://www.trowers.com/legal-notices>

For further information, including about how we process your personal data, please consult our website <https://www.trowers.com>

