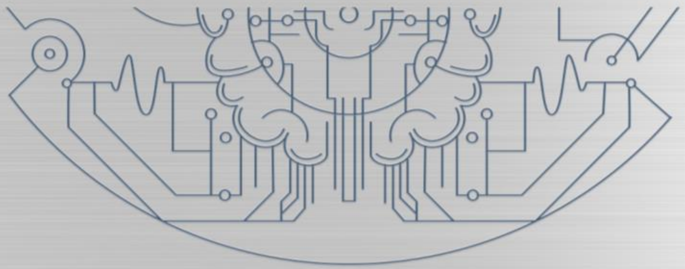
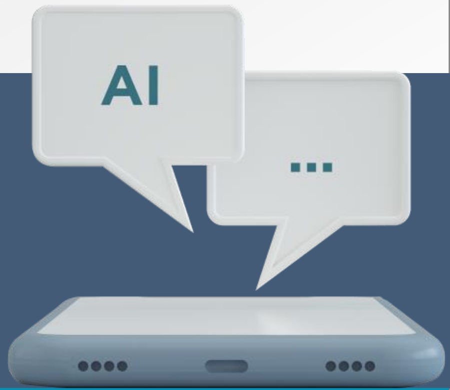
HARNESSING GENERATIVE AI



ADDLESHAW
GODDARD

MORE IMAGINATION MORE IMPACT

HARNESSING GENERATIVE AI:
PRACTICAL AND LEGAL ADVICE



While the power and possibility of Generative AI (**GenAI**) in business is clear to see, working out how to deploy it in practice is a lot more challenging. Our approach is honed by a number of years working in this space and our pragmatic approach to tech implementation - our clients don't always need to understand how GenAI technology works, but they do need to know how it affects their business in practice. **Please get in touch if you'd like to know more about how we can help you be GenAI ready.**

KEY AREAS OF RISK:

Data Ethics and Security

Intellectual Property

Contractual terms

Regulatory Regimes

Competition / Consumer Protection

HOW ARE WE HELPING CLIENTS:

Designing GenAI governance frameworks

Advising how to protect IP/confidential information

Advising on Gen AI vendor terms

Helping clients to keep ahead of global regulatory landscape

Advising on legal safeguards for proposed use cases

DATA, ETHICS & SECURITY

1. **Fairness: risk of bias and discrimination**

- Fairness is a key principle under the UK GDPR and global AI ethics guidelines.
- Organisations using GenAI must be alert to the risk of biased algorithms, which can result in biased/discriminatory decisions.

2. **Transparency/Explainability and rules on automated decision-making**

- Organisations must be transparent with the individuals whose personal data they are processing about how their details will be used.
- Explainability is an ethical principle which requires GenAI users to enable people affected by the outcome of an GenAI offering to understand how it was arrived at.
- If an organisation is using GenAI to make automated decisions based on personal data, it must provide the individual with meaningful information about the logic involved. Individuals have the rights not to be subject to a decision based solely on automated processing which produces legal effects, obtain human intervention, express their point of view and contest the decision.

3. **Data minimisation v Large Language Models**

- Data protection principles require organisations to ensure that the personal data they process is limited to what is necessary and not kept for longer than needed for those purposes.
- These principles can be difficult to reconcile with the use of GenAI, which relies on processing large amounts of data.

4. **Purpose limitation and managing data subject rights**

- If personal data is collected for one specific purpose, it cannot be reused for incompatible purposes, which may include training an GenAI model or processing the data using GenAI.
- Data subjects have the right to object to processing and to erasure of their personal data. If their data has been used to train an GenAI model or processed using GenAI, this may be difficult to manage.

5. **Accountability, security and impact assessments**

- Controllers must be able to demonstrate compliance with data protection law and be accountable for the proper functioning and respect of the ethical principles.
- Security is a key principle under the UK GDPR and AI ethics guidelines, where it is linked to the 'robustness' of a system.
- Most uses of GenAI which involve processing personal data will require impact assessments to identify the risks and how to mitigate them.

INTELLECTUAL PROPERTY

1. **Ownership of output is unclear**
   - GenAI offerings are jurisdiction agnostic, but intellectual property laws across the world differ in the position they take on who, if anyone, owns any machine-generated works. There is also the possibility that no IP may be created. Companies will need to update their policies to take account of content generated through GenAI offerings and check the terms of the GenAI provider carefully.
2. **Unauthorised data usage**
   - Most GenAI offerings have been built on a vast amount of data that has not always been used with the copyright owner's permission. GenAI owners have instead sought to rely on statutory permitted uses, which is now heavily questioned. Coupled with the fact that a well crafted prompt could generate an output that is identical or very similar to the input data, the use of the output could actually lead to third party infringement claims.
3. **Protection of your IP/confidential information**
   - GenAI often retains and reuses code, images, or text entered by users and this information could be provided to another user in response to a prompt. Companies will need to carefully consider and educate their employees and contractors as to what information may be used in a system. Switching to a closed environment, which is typically a paid version of the GenAI model, should give companies more control over how their data is shared.
4. **Risks that output may infringe the copyright in a third party work**
   - Where there is close similarity between two works and one owner had access to the other owner's work, there is a presumption at law that the first owner has copied the other owner's work.
   - Bear in mind that most AI offerings offer limited contractual protection on use of the output and therefore the risk remains with the user in terms of how they use that output. This makes it difficult to defend your use of that output because it is very difficult to know how the training data was obtained.
5. **Deepfakes and the risk of defamation claims**
   - If a GenAI generated a 'statement', which could include a deep fake picture or video, makes or implies an allegation defamatory of a third party, which causes, or is likely to cause, serious harm to her or his reputation, the victim will be able to sue in defamation. The company behind the GenAI application may be sued, but so can anyone who makes the defamatory statement available to a wider audience, e.g. by posting it online, distributing it by email, etc. Companies will need to ensure that they have policies in place for their employees on how they can use any content generated via a GenAI offering.

STOP PRESS OCTOBER 2023:

Providers of GenAI offerings are regularly updating their terms to address customer concerns. Most recently, those changes have focussed on IP infringement cover, with Microsoft and Google broadening their third party infringement indemnities to offer customers some protection against potential copyright infringement claims for paid for services. We expect changes to keep coming as providers try to achieve an appropriate allocation of risk that keeps pace with the rapid growth in the development and use of GenAI offerings.

CONTRACTUAL RISKS

1. Use of GenAI at company's risk

○ Many GenAI offerings are in active development and developers are providing them for use "as is", they are excluding liability for output or are requiring the deployer to have human oversight of output. Content generated by the GenAI offering is also likely to be provided without warranties as to quality or accuracy. Companies should assess the risks of use and whether the developer will provide adequate protection for possible failures.

2. Opaque use rights

○ The scope of use rights tends to be further detailed in product or technical documentation which can be extensive. Specific use rights are not obvious or apparent and are subject to change without notice. Also be alive to restrictions on use – including using output from one GenAI model with another GenAI model.

3. Data use

○ GenAI systems may reserve the right to use a business's input data beyond providing the output for the customer. Paid options typically limit that use to debugging and carrying out checks but some solutions go further. Solutions tend to differentiate between personal and other data but that may include commercially sensitive data. Companies should control data input and GenAI access to documents/data.

4. Ease of use

○ Online and app based solutions can be easily accessed by staff and others. They can also be readily incorporated into solutions by developers through APIs. This can expose companies to contractual and other risks of GenAI use. Companies should have clear use policies, staff training and contractual controls on third parties the business contracts with.

5. On premise or cloud-based solutions

○ Many GenAI offerings are provided to customers through a cloud-based platform. This inherently brings with it risks over security and confidentiality. Many organisations have reservations over sharing their commercially sensitive or propriety information with technology which may reuse such information with their competitors or the public more widely.

○ A solution may be to seek "on-premise" or closed-environment alternatives allowing you to train your version of the GenAI offering on your own data-sets. However, the benefits you gain from a security and confidentiality perspective needs to be measured against the potentially weakened output by training the programme on a narrower data set.

REGULATORY REGIMES

1. UK regulatory regime

- The UK has adopted a principles based approach for UK regulators to develop their own set of rules that would apply within their own regulatory regime. There is likely to be a patchwork of regulations and guidance from these regulators that the companies will need to understand and apply.

2. EU Artificial Intelligence Act

- The EU regulatory landscape for GenAI is getting ever more sophisticated, and providers must stay on top of the various pieces of relevant legislation which come with different obligations.
- Most notably, the evolving EU AI Act sets out various requirements for providers of a foundation model, including the establishment of a risk management system, the use of appropriate data sets, ensuring adequate quality (performance, predictability, safety, etc.) through appropriate measures, compliance with energy efficiency standards, the preparation of adequate technical documentation and instructions for use, the establishment of a quality management system, and the registration of the foundation model. For providers of GenAI, additional obligations apply, such as transparency obligations, the obligation to design it to prevent it from generating illegal content, and the obligation to publish summaries of copyrighted data used for training.
- Further pieces of legislation will have an impact on GenAI as well, such as the EU Digital Services Act, the Draft AI Liability Directive, the Draft Data Act, and others.

3. Other jurisdictions

- Other jurisdictions take different approaches to regulating GenAI which makes drafting a global strategy for the use of GenAI within a global business challenging.

COMPETITION/CONSUMER PROTECTION

1. **Risk of collusion between competitors**

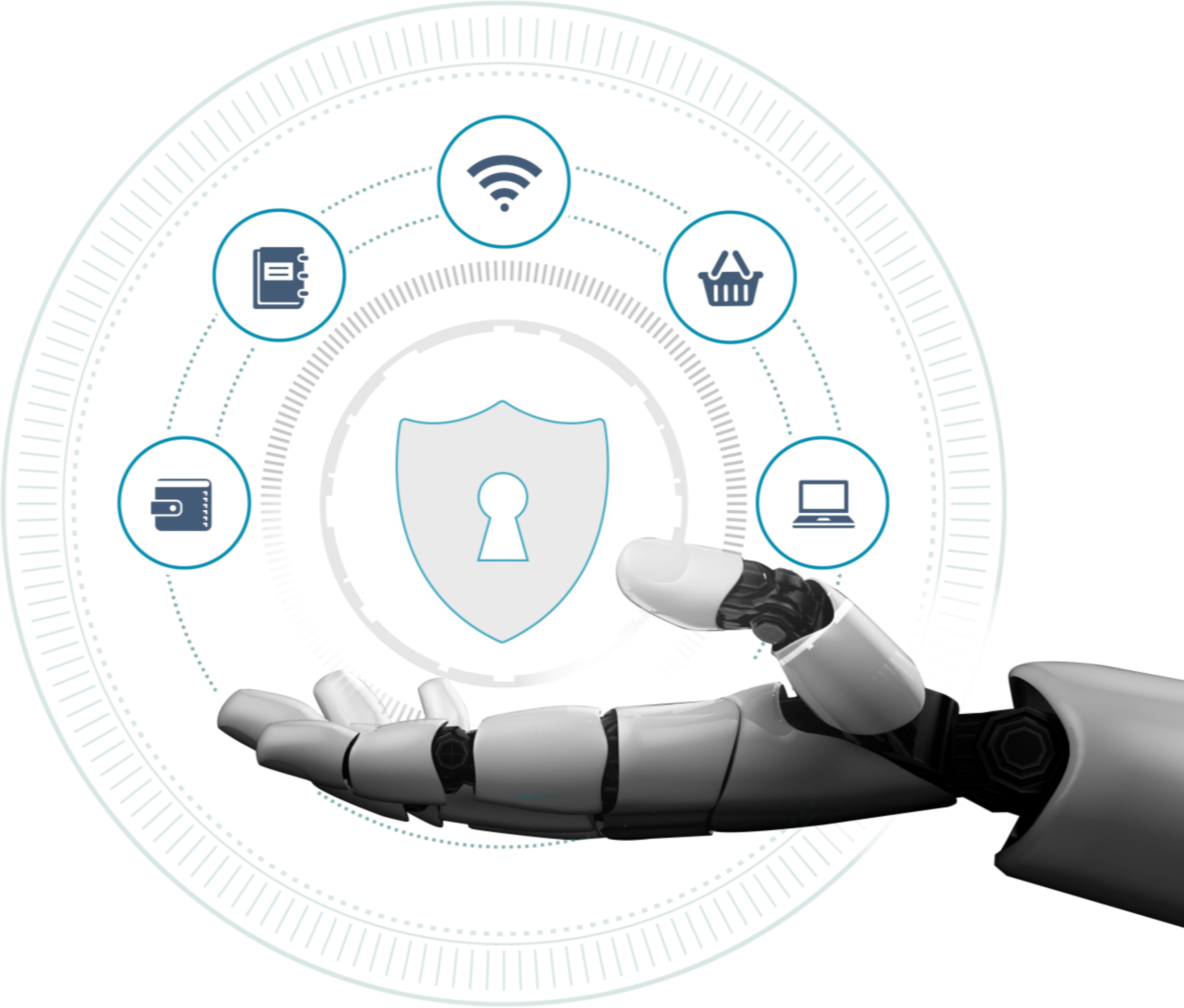
   ○ GenAI algorithms can enable access to competitor pricing and data in real time and assist in monitoring compliance with anti-competitive commercial clauses (e.g., certain price parity clauses). Exercise caution where multiple companies use the same GenAI system / complex algorithm to determine competitively sensitive strategic decisions and where the output is transparent and visible to users.

2. **Risks of harm to consumers**

   ○ GenAI personalised pricing could result in unfair or anti-competitive price discrimination and opaque pricing techniques that are not clear or visible to consumers. Companies should exercise caution in their use of GenAI offering to avoid manipulating consumer choices “by design” , e.g., exploiting human biases via scarcity messages integrated into the user interface

3. **Exclusionary practice risks (if a company is dominant/has market power)**

   ○ GenAI offerings can be used to self-preference own products and services in terms of ranking and appearance to consumers (particularly relevant for online platforms). They can also created targeted predatory pricing risks. This is especially the case where the GenAI offering is used to identify and selective target customers at most risk of switching, and to implement personalised discounts and prices at a level that marginalises or forecloses competitors.



HR CONSIDERATIONS

Key Benefits:

1. **Automation of documents** can save time and cost
2. **Improve quality control** by swiftly finding mistakes and maintaining high standards
3. **Review of documents**, AI can save time and cost, provide valuable insights for market research, customer behaviour analysis, and financial forecasting;
4. **Improve customer service**, by handling common questions, reducing wait times, and providing personalised recommendations and targeted marketing.
5. **Contribution to cybersecurity**, by identifying threats and bolstering fraud detection.

Key Risks:

1. **Biases and discrimination**
   - AI can perpetuate biases present in the data they are trained on which can lead to discriminatory outcomes such as hiring decisions.
2. **Lack of transparency**
   - It can be difficult to understand how AI comes to the decisions it makes, this can be problematic when it comes to accountability
3. **Job displacement**
   - Use of AI can lead to job losses or for the need for employees to acquire new skills to remain employable
4. **Overreliance and dependency**
   - Overreliance on AI systems without critical evaluations can have negative consequences. AI systems are not infallible and they can make mistakes therefore it is important to maintain human oversight
5. **Employee work product**
   - Employees may be using programmes such as ChatGPT to produce their work without the employer being aware

Next steps for Employers

1. **Develop clear AI policies** covering fairness, transparency, accountability, bias mitigation, data privacy, and security.
2. **Retain human oversight** to ensure fairness and ethical decision-making, leveraging critical judgement and intervention when necessary.
3. **Regularly monitor and audit AI systems** to identify and address biases, errors, and unintended consequences in AI systems.
4. **Ensure transparency** in AI systems by using interpretable algorithms, clear documentation, and providing explanations to affected individuals.
5. **Continuously train and educate employees** about AI systems and their limitations, and foster collaboration to identify and address potential issues or biases.
6. **Regularly update and improve AI systems** to enhance performance, address biases, and improve accuracy.
7. **Collaborate and share best practices** with the industry to establish standards and guidelines for responsible AI implementation.

GET IN TOUCH

Over the past year, major companies covering various industries, including energy and utilities as well as financial services, have actively sought guidance from Addleshaw Goddard regarding critical inquiries stemming from GenAI. These inquiries revolve around topics such as intellectual property complexities, the potential liabilities associated with GenAI, and the implications for data privacy.

We field a combined team of Technology, IP, Data Privacy, Commercial, Reputation Management and Dispute Resolution lawyers, plus a specialist team of over 50 innovation experts, that together help organisations harness GenAI in two fundamental ways: advising companies on how to safely integrate generative AI into their businesses; and specifically helping in-house legal functions approach and adopt AI / GenAI.

In the wider technology sphere, our specialist lawyers have advised over 300 major organisations on over 1000 technology-related projects, ranging from helping to launch a new digital bank to resolving seemingly intractable cybersecurity disputes, and everything in between.

Whatever is driving your business' use of technology - whatever you are trying to achieve with it – whatever your role in deploying, supplying or investing in it – and whatever legal questions stand in the way of progress – our Technology group can help you find and protect a commercial path forward.

GEORGINA POWLING
PARTNER
georgina.powling@addleshawgoddard.com

MANUELA FINGER
PARTNER
manuela.finger@aglaw.com

HARRIET TERRITT
PARTNER
harriet.territt@addleshawgoddard.com

CHARLOTTE MARSHALL
MANAGING ASSOCIATE
charlotte.marshall@addleshawgoddard.com

DAMON ROSAMOND-LANZETTA
PARTNER
damon.rosamond-lanzetta@addleshawgoddard.com

CLAIRE EDWARDS
PARTNER
claire.edwards@addleshawgoddard.com

MORE IMAGINATION MORE IMPACT

addleshawgoddard.com