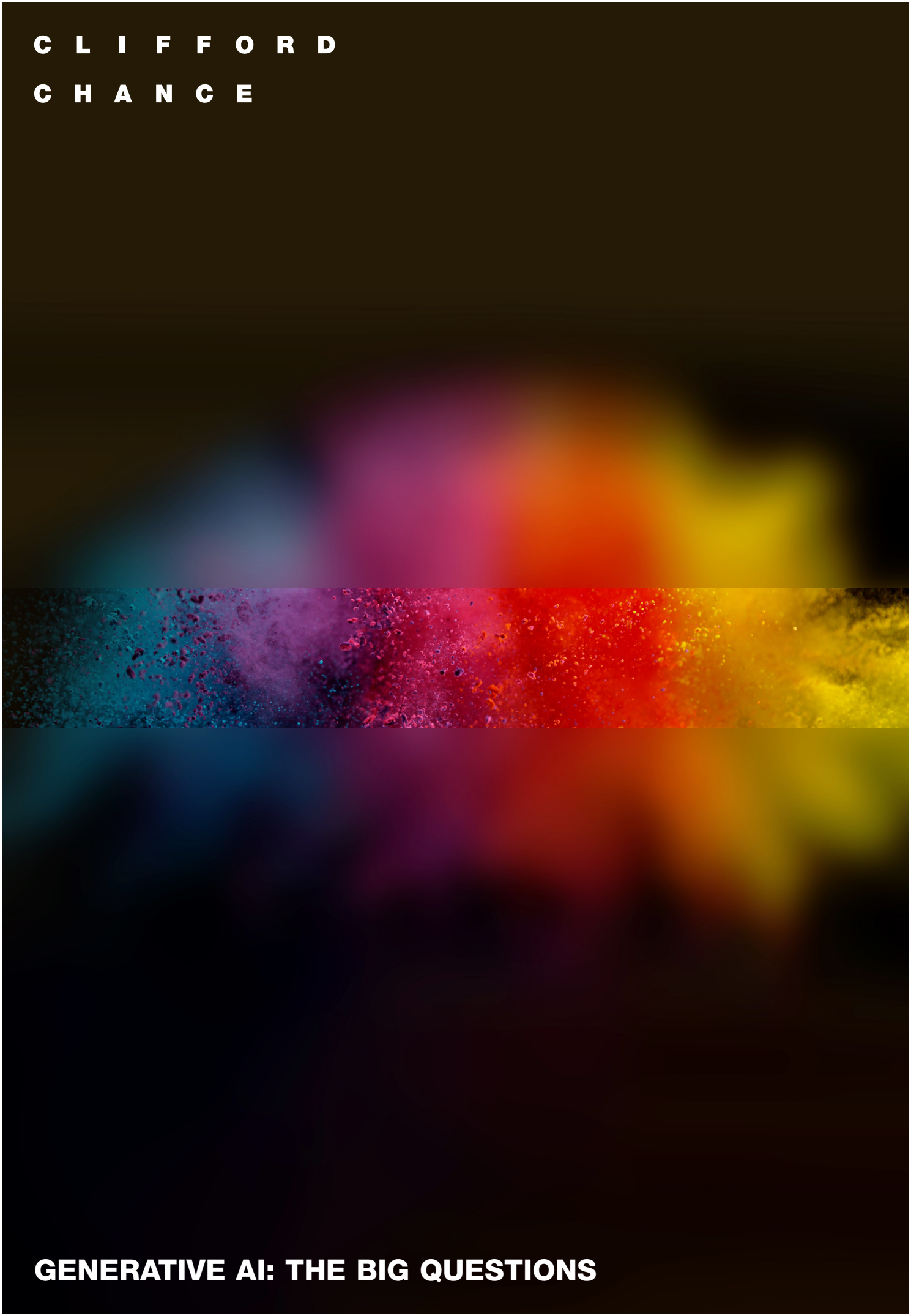
CLIFFORD

CHANCE



GENERATIVE AI: THE BIG QUESTIONS

GENERATIVE AI: THE BIG QUESTIONS

With last year's public release of OpenAI's ChatGPT, generative AI went from niche to nova. Generative AI has reached an astonishing level of capability, from producing near-human text responses and photorealistic images of non-existent events, to suggesting software code and creating websites. In turn, political and regulatory focus has sharpened regarding how to ensure responsible AI use and development. Balancing risk and reward in the deployment of AI has entered uncharted territory as the legal landscape for AI evolves and this versatile technology disrupts the way we work and create across sectors.

As legal, technology and risk-management teams collaborate to support business-critical decisions, establish forward-looking frameworks and embed responsible AI in company strategy, being able to assess and advise on AI with a holistic understanding of the changing legal and policy landscape has never been more important.

Our experts examine some of the big questions to address when exploring generative AI opportunities.

Using Generative AI in your business – the questions you should be asking

Across a broad range of sectors, organisations are exploring uses of generative AI. While the approach to AI will differ according to the nature of the organisation and the maturity of the associated risk management framework, there are questions that all organisations should consider in relation to the use of generative AI.

1. AI mapping: How is your organisation using generative AI today, and how could you use it tomorrow?

Does your senior leadership know where generative AI is already used in your business, and what use cases are in the pipeline?

- **What are the use cases for generative AI across your business?**

  Generative AI could augment or streamline many internal processes such as desktop research, generating meeting notes and calendar scheduling, assisting software development, creating first drafts of presentations, papers, emails and marketing materials, and much more. Generative AI can also be used in connection with customer-facing products, services and support – potentially revolutionising certain interactions, client offerings and business models.

  Whether these use cases appear on the board agenda iteratively and organically or as part of a project to proactively investigate generative AI opportunities, organisations will need to ensure that proposals to use generative AI are raised to appropriate levels for key stakeholder interrogation, support and oversight.

- **Is your company already using generative AI?**

  Some generative AI tools are freely available online – either as stand-alone tools or as products that can integrate into a chain of tools that are provided by multiple

What is Generative AI?

Generative AI refers to a broad class of artificial intelligence systems that can generate new and seemingly original content such as images, music or text in response to user requests or prompts. It encompasses a wide range of models and algorithms, which can be used to create a variety of outputs depending on the application. Although research and development in this space goes back a number of years, the recent public release of generative AI systems, tools and models has catalysed its adoption and scale.

One of the most well-known examples of generative AI is the GPT (Generative Pre-trained Transformer) series which relies on a large language model (LLM) to interpret text prompts and, in a tool like ChatGPT, generate natural language text in response in the way a human would. Combined with other models such as diffusion models, GPTs also allow images to be created based on text prompts. These LLMs use an architecture that mimics the way the human brain works (a "neural network"), analysing relationships within complex input data through an "attention mechanism" that allows the AI model to focus on the most important elements. They are typically trained on massive amounts of data, which allows for greater complexity and more coherent, and context-sensitive, responses. In many cases these AI systems have general (not task-specific) potential.

developers. Although early adoption and experimentation with generative AI is key to realising its potential, if your business does not adequately govern the use of these tools, they could potentially be used by your personnel in unanticipated and undesirable ways.

Your suppliers may also be incorporating generative AI in the products and services they provide to your organisation, which could result in your business unknowingly using or relying on such AI, or your business and customer data being shared with third-party generative AI developers. Do you have a process for identifying AI in your tech stack and data supply chain, as well as associated decision-making, contracting and ongoing monitoring processes for receiving AI-assisted services and products?

2. AI ethics and legal strategy: How *should* your organisation use generative AI, and is it prepared for the changing legal landscape?

Of the numerous ways your company *could* use generative AI, how will it determine the ways in which it *should* use this technology? Will you allow employees to use publicly available generative AI software for work – if so, for which purposes? What guard-rails will be in place? Will your company invest in supporting use of generative AI for certain use cases – for example, procuring a private instance of a generative AI system, or developing in-house capabilities?

Ethical, reputational, legal and commercial considerations will need to be addressed holistically when answering these questions. AI oversight principles and robust governance programs increasingly help organisations to centre, and appropriately frame, these transformational discussions.

- **Which laws and frameworks apply to AI use today, and what's on the horizon?**

  The regulatory framework that applies to generative AI is complex and multilayered. Existing laws include privacy, employment, cyber and operational resilience, intellectual property, antitrust, product safety, content moderation, environmental, human rights and consumer protection, as well as sector-specific or technology-targeting legislation. These will sit alongside new AI-specific laws and guidance as the capabilities of generative AI continue to develop and regulators across the world explore what AI-specific legislation looks like. For example, the EU, China, Canada, India and various US states are proposing and enacting AI-specific laws, while the **US Blueprint for an AI Bill of Rights**, the **UK's AI policy paper** and Singapore's Model Artificial Intelligence Governance Framework all set out principles for responsible AI use and governance.

  In the EU, the AI Act is being negotiated and will sit alongside the proposed AI Liability Directive (as well as other laws such as the Revised Product Liability Directive and the Digital Services Act) in regulating how certain AI can be placed on the market, put into service and used and who is liable for harm caused by the use of AI. The current text of the EU AI Act specifically covers generative AI, by bringing 'general purpose AI systems', those which have a wide range of possible use cases (intended and unintended by their developers) in scope.

  In the US, the Department of Commerce's National Telecommunications and Information Administration **published a request for comment** on how to achieve "trustworthy AI", which sits within an existing administration policy framework (including the White House Office of Science and Technology Policy **Blueprint for an AI Bill of Rights** and the National Institute of Standards and Technology's **AI Risk**

Management Framework) and alongside a host of State-level AI-specific legislation and bills. In addition, Senate Majority Leader Chuck Schumer has announced an early-stage legislative proposal aimed at advancing and regulating American AI technology.

At the same time, China is working hard to show leadership both on AI investment, home-grown technology and regulation – addressing specific issues such as deep-fakes whilst seeking to minimise social disruption. For example, the Regulations on the Administration of Deep Synthesis of Internet Information Services focus on 'deep fake'-type use cases as well as generative AI-based chat services. China has also issued for public consultation its draft measures on the administration of generative AI services. These targeted measures sit alongside important regional approaches, notably in Shanghai and Shenzhen.

At the international level, G7 leaders recently announced the development of tools for trustworthy AI through multi-stakeholder international organisations through the 'Hiroshima AI process' by the end of the year.

As the laws governing AI evolve, definitions such as 'AI system', 'AI user', 'AI provider' and 'AI-generated content' are being created and negotiated. Some of these definitions may be broadly drafted and could capture companies that have not previously considered themselves to be AI providers or users. Organisations will need to understand the countries and manner in which they intend to roll out the use of generative AI, as well as the scope of potentially relevant laws, in order to identify the laws applicable to their procurement and use of generative AI.

- **What data was, or will be, used to train the system? What types of data will be entered into the system when it is being used?**

Data must be processed in compliance with any ownership rights, legal requirements, contractual terms and company policies. Some of the key areas for legal risk management – privacy, intellectual property (IP) infringement, and other legal and commercial restrictions on data use – are discussed below.

Privacy: Where AI uses personal data protected by privacy laws, its developers and users will have to comply with relevant requirements. For example, the range of obligations under the EU's General Data Protection Law (GDPR) for developers and users of generative AI include having an appropriate legal basis for data processing, providing notices and adhering to privacy principles (such as transparency, fairness, purpose limitation, accuracy and data minimisation). Data subjects would also need to be able to exercise their rights, such as rights to deletion and rectification of their personal data. More broadly, AI system developers and users would also need to consider how requirements for 'privacy by design and default' and appropriate security measures should be (or have been) approached.

The application of privacy laws to generative AI is new and untested. Data accuracy, rectification and deletion could be technically challenging in relation to generative AI which has 'learnt' incorrect information (even if that information is later deleted from, or corrected in, the data used in training the AI) and which is capable of 'hallucinations' (incorrectly generated answers). Other open points include whether 'legitimate interests' can be relied upon for processing of data scraped from the internet in this context, how compatibility of processing will be seen in this context, and whether exemptions to privacy notice requirements will apply. Early application of privacy law to generative AI developers is being seen in the activity of European data

protection authorities (DPAs), such as the interim order on OpenAI's ChatGPT issued by Italy's *Garante*, which temporarily restricted ChatGPT in Italy until such time that OpenAI was able to provide it sufficient assurances relating to the services' compliance with GDPR.

While users have not been in the enforcement spotlight, they should ensure they apply their privacy compliance frameworks to generative AI use and procurement – including understanding whether use of the AI system involves any restricted transfers of personal data and communicating to personnel any restrictions regarding submissions of personal data when using generative AI.

IP infringement: IP risks and challenges can arise from the data and materials used to train generative AI, as well as the outputs produced by the models. For creators of generative AI models (and, in some cases, their users) there are risks of IP infringements in relation to the training data used. For example, where datasets are derived from scraping publicly accessible materials online without a licence from copyright owners, or where datasets licensed for one specific use are re-purposed for training an AI model, the training process will typically make copies of works that are unauthorised by the rightsholder. Whether those copies constitute infringements of copyright will often depend on the scope of any applicable data mining or fair use exceptions (which vary significantly between countries), and the way in which the training process stores or deletes the source materials. Generative AI users should also be aware of the risk that the output generated in response to a user prompt could infringe copyright (and ancillary laws) if a given output is too similar to specific input materials. This risk is heightened where small training data sets are used, although some AI tools implement filtering systems aimed at this very risk, which prevent the models from returning outputs which are too similar to any specific inputs. As users of generative AI may often be reliant on the AI developer's controls in how it trained the system, exploration of these aspects should form part of a company's review of any generative AI system.

Contractual restrictions and confidential information: There could be other restrictions on a company's ability to share data with a generative AI system – for example, contractual restrictions on how a client's or supplier's information may be used or shared with third parties, such as usage restrictions in contracts with content providers. There may also be legal restrictions regarding certain data such as material non-public information and price-sensitive information. A company may also wish to keep confidential certain of its own data (including proprietary information such as software code, product designs or trade secrets). As information provided while using generative AI is likely to be accessible to its developers, inputting such data to that system without appropriate consents and licenses could breach legal or contractual restrictions or a company's own protective policies. Unless otherwise specifically agreed with the AI provider, there is also a risk that the information submitted may form part of the system's iterative development and a risk that this could inform (or form part of) answers given by that system to other users in the future. A company may have concerns regarding such AI systems learning from the company's data, even if that data is not sensitive, where competitors may also use a version of the system that has "learnt" from the company's use.

- **How will the output be used? What quality control checks will be applied?**

  Organisations that will roll out generative AI systems, or otherwise allow their personnel to use such AI, must consider the uses for which they will permit AI-generated output to be used, how they will educate staff regarding the limitations

of the relevant AI system, and the policies or guidance to be implemented to ensure the output is quality checked and used appropriately.

Accuracy, completeness and bias: The textual responses of generative AI systems are based on patterns in the "corpora" (bodies) of data they have been trained on, and fundamentally operate by predicting the next word in a particular context. As with other AI, generative AI is dependent on the quality of its training data, and therefore susceptible to the introduction of errors and bias through the training and development process; particular vulnerabilities typically exist in the early stages of model building. The outputs of a generative AI system that has been trained using vast amounts of data of unknown provenance that is available on the internet could reflect the societal biases that are evidenced (and in some cases magnified) online, as well as make use of inaccurate or out-of-date information published on the internet. Some of the complex neural-network based techniques used in generative AI can make it difficult to understand how an answer has been created, which can lead to challenges in identifying inaccurate or biased responses. Generative AI can also produce 'hallucinations': responses which appear authoritative but are factually untrue and might not be traceable back to real-world, factual data. Even citations generated by the AI can be inaccurate – increasing the importance of robust human-in-the loop governance and auditing processes, particularly for high-risk use cases.

Organisations using AI will have a range of legal obligations regarding equality, diversity and fair treatment, as well as ethical and reputational imperatives. The accuracy and completeness of an AI system's output may also be important, with the degree of importance varying depending on the use for which the output will be used and the level of human review, expertise and judgement that will be applied. In some cases, accuracy will be operationally, commercially or reputationally critical, or legally required.

Before using generative AI in business processes, organisations should consider whether generative Ai is the appropriate tool for the relevant task. Where use of generative AI is appropriate, organisations should identify the guard-rails they will put in place to ensure their staff understand the limitations and potential risks regarding inaccuracy and bias in AI output, the organisation's restrictions regarding the purposes for which such AI output may be used (and what the consequences of breaching these would be), and its requirements regarding an effective layer of human quality control. Factors such as cost will also have a role to play here, with the cost of generative AI system based searches currently far outweighing the cost of using, for instance, internet search engines.

IP protection: As AI becomes more sophisticated and 'creative', key legal issues include the concepts of "inventorship", "authorship" and "patentability" of products created by or using AI. There can be uncertainty regarding ownership of AI-generated or AI-assisted output, and whether IP rights can subsist in an output at all. If there is no IP protection, there may be nothing to stop widespread copying of the outputs of generative AI. The availability of IP protection is significantly affected by the nature of the output, the degree of human involvement and the jurisdictions involved. Can an AI system be an author or an inventor under IP laws? What about AI-assisted works? Jurisprudence is evolving – and, in some cases, with diverging approaches between jurisdictions. In general, AI-assisted creations will more readily attract IP protection than works that are wholly or substantially created by generative AI without human input. Organisations will need to consider whether generative AI might be used to create something (such as software code, a written paper or a product design) which

the organisation wishes to protect under an IP regime, and how it will go about maximising the availability of those protections through the manner in which it guides internal AI use.

Employee concerns: Where generative AI output will streamline or alter processes and impact and/or remove the roles of certain personnel within an organisation, careful thought will need to be given regarding how the roll out and associated communications are managed. In some cases, individual employees and/or employee representatives (including works councils) will need to be informed and consulted.

- **How will you ensure business continuity, cyber-security and resilience?**

  Generative AI systems may be processing legally or commercially sensitive data and may be deployed in the context of regulated or operationally critical processes, with varying degrees of human involvement. As with other software, cyber-security and operational resilience requirements and considerations will apply to the use and procurement of generative AI systems. There are a number of emerging security threats specific to generative AI, such as indirect prompt-injection attacks which can result in AI systems behaving in ways beyond their established operating limits.

  More broadly, where the use of generative AI involves sharing data to a publicly available AI system or to a private instance on a third-party cloud-based platform (rather than being available on-premises) your company will want to understand and assess the risks of message interception and other cyber-attacks and any security measures applied by the supplier. As part of any AI procurement your company would also need to understand its responsibilities regarding system use and configuration, the supplier's business continuity plan and how the unavailability of that platform would affect your business.

  In addition to requirements for appropriate security measures under privacy laws where personal data is processed, organisations will need to consider cyber, business continuity and operational resilience or broader governance requirements in relation to certain sectors and products. Such requirements are particularly important where AI systems are relied on for operationally critical, regulated or customer-facing processes, especially as it may not be immediately obvious when the operation of an AI system has been hijacked.

  Some sectors, such as the financial services sector, may also have overarching governance and oversight frameworks under which cyber-security and operational resilience considerations may apply to certain uses of generative AI.

  Will data entered on the AI system be protected, and will the operation of the system be robust? To what degree will your personnel rely on the use of that AI, and are contingencies needed in the event it becomes unavailable (for a temporary period, or permanently)? Before putting any generative AI into operation, organisations need to consider how they will identify system issues or failures, whether they need to have backup options and remediation plans in place, and whether stakeholders need to be informed in advance of any likelihood of failure, the responsible team, and the best course of action to take in case of any issue.

3. AI governance: How will your organisation oversee AI use and procurement?

Appropriate governance is central to responsible AI use and procurement, and is an area of focus for lawmakers and regulators globally. Organisations deploying generative

AI will need to consider what systems and controls they will have in place to underpin and oversee the application of the legal and ethical framework discussed in section 2 above, including governance structures that include senior management responsibility and clear lines of accountability.

- **Which laws and frameworks apply to AI governance today, and what's on the horizon?**

  Many of the laws and regulatory principles referenced above (see section 2 above) include requirements regarding governance, oversight and documentation. For example, the EU GDPR includes a principle of accountability alongside a number of specific requirements for assessments and record-keeping, and the draft texts of the EU's AI Act include a number of requirements relating to risk-management systems, oversight, audit and record-keeping. In addition, sector-specific frameworks for governance and oversight can affect what 'responsible' AI use and governance means in certain contexts. For example, financial services regulators in many jurisdictions have rules and guidelines on oversight and governance in areas such as retail banking products, outsourcing arrangements, model risk management, operational risk management and the responsibilities of senior management. Additionally, laws that apply to specific types of technology, such as facial recognition software, online recommender technology or autonomous driving systems, will impact how AI should be deployed and governed in respect of those technologies.

- **How do your existing governance frameworks apply? Will you have a generative AI policy?**

  Organisations will need to consider where AI sits within their governance and risk-management frameworks and how those frameworks may need to be tailored or expanded to address generative AI.

  For many organisations, existing governance frameworks, including policies on advanced analytics innovation, data governance and IT risk management, could be a helpful starting point for governance of generative AI systems. Organisations could also produce a set of AI principles and map them to the existing risk frameworks. Alternatively, or in addition, some organisations may wish to create an overarching AI governance framework that applies (in a risk-adjusted manner) across use cases, and/or specific policies targeting particular uses – such as a policy for use of a specified generative AI system. In some cases, internal guidelines may be more appropriate. Consideration will need to be given to (i) the interplay between existing policies, (ii) regulatory expectations, (iii) how the approach chosen affects the ease with which the intended policy audience will understand the requirements and restrictions, (iv) company culture, and (v) the organisation's ability to implement supporting processes as well as monitor and enforce compliance.

  Processes that exist in other contexts regarding procurement, development, implementation, testing and ongoing monitoring of IT systems should be reviewed, adapted and applied as necessary across the roll-out and use lifecycle of a generative AI system. This adaptive governance would need to be sensitive to differences between types of AI systems in order to apply effectively to the changing technology landscape. Organisations should also review how their related processes, including for training, record keeping and audit, would be applied in this context to support any policies, principles and guidelines.

- **Who will be responsible for AI decisions? Who supports those decision-makers?**

Organisations will need to determine who will be responsible for AI oversight and decision making at senior levels, whether the organisation would benefit from establishing any AI-specific governance structures (such as an internal AI council, board or committee) and what the lines of accountability will be.

Some regulators may require designated senior management responsibility for oversight of AI technology in the context of wider senior management responsibility regimes. Even where not expressly required by a law or regulator, many organisations will find it beneficial to designate an appropriate senior individual or group of individuals with the relevant skill set and knowledge to consider, challenge, steer and approve AI-related decisions.

Consideration should also be given to establishing clear and appropriate accountability lines throughout the company up to senior management, and having in place people with the right skills, expertise, experience and information to support and advise. Recruitment, talent pipeline management and staff training will be aspects to consider in planning for effective AI risk management.

- **What protections can you achieve through your supplier contracts?**

Contracts for AI procurement, development or investment form part of the wider governance framework mitigating AI risk. Contracts for the procurement or use of a generative AI system require careful review to understand and, as far as possible, negotiate appropriate terms to address AI-specific risks in the allocation of rights, responsibilities and liability. Such contracts can look very different from a standard contract for a traditional piece of software. Each implementation of AI needs to be evaluated on a case-by-case basis, considering the proposed uses for the system and how it will interact with other systems.

With non-deterministic systems, performance will vary over time. Questions therefore arise as to how to: define performance criteria; monitor performance; allocate liability; and define remedies for poor outcomes or any damage caused by the system. For private instances of an AI system that can be fine-tuned based on an organisation's own data, other questions to consider include the rights relating to a privately 'trained' instance of the AI system, where responsibility lies for various aspects of legal and regulatory compliance in the system's operation, and how the system will be supported, monitored and audited.

In some cases, these AI systems may be made available only under supplier-friendly terms, which will require companies to understand the risks they are accepting regarding things such as system availability and updates, supplier data access, cyber-security protection and possible IP infringement – with little by way of precedent in terms of market practice or positions. Further, where generative AI products are integrated into a chain of tools provided by a number of suppliers, there will be multiple applicable contractual terms.

Although the degree to which an organisation can negotiate a contract for a generative AI system with the supplier will vary depending on the parties involved and type of procurement or use, the contractual framework will need to be understood by relevant stakeholders as part of an organisation's risk management and governance process for generative AI.

4. AI transparency: How will you communicate your use of AI within your organisation and externally?

With requirements around transparency and explicability continually appearing in AI-specific legislative proposals and policy discussions, as well as being required in certain circumstances under existing laws, it is crucial that these aspects are addressed in any deployment of generative AI.

Organisations will need to consider the level of disclosure they are required to make regarding their use of generative AI, both internally to personnel and more publicly, depending on the AI use cases. A number of existing laws and regulatory requirements, as well as laws that are on the horizon, will require disclosure of certain types of AI use. Increasingly, there are also customer and staff expectations regarding levels of transparency regarding AI use that may affect them.

The level of explicability – or "explainability" – required or expected depends on the type of activity, the relevant legal jurisdictions of deployment, the recipient of the explanation and the nature of the AI used. For example, the EU GDPR contains transparency requirements regarding use of personal data, and specific requirements regarding fully automated decisions with legal or similarly significant effects on a data subject. There are, in particular, legal and reputational risks in relation to any customer receipt of AI output that has not been identified as such, or misleading statements relating to AI. The EU AI Act is likely to include different transparency requirements, including certain requirements to inform people that they are interacting or communicating with an AI system instead of a human or that content is generated by an AI system rather than a human. China's emerging laws relating to AI also include labelling requirements for certain AI-generated content. In the US, the Federal Trade Commission is focusing on whether companies are accurately representing their use of AI.

Regulating explicable – or "explainable" – AI models is completely different when it comes to AI models that cannot be explained or interpreted; the regulatory framework will only apply to their inputs and outputs.

Explaining how a generative AI system operates to generate output becomes increasingly challenging as the level of sophistication of these systems increases. The challenge of explicability can be further complicated when the AI technology is supplied by another provider or a chain of providers who themselves lack the visibility of how such system operates or functions. Organisations will need to consider how they themselves receive the necessary information, as well as how to achieve the appropriate level of transparency for their use of AI.

Key takeaways

When identifying and exploring opportunities for the use of generative AI, having multidisciplinary teams involved to ask the right questions to support responsible, informed decision making is crucial. Organisations will also need to identify appropriate decision-makers, look at their governance structures and processes, and consider their AI-related communications. Although the legal landscape for AI is evolving, now is the time to develop AI legal and ethical strategies and risk-management frameworks.

CONTACTS

Devika Kornbacher
Partner
New York
T: +1 212 878 3424
E: devika.kornbacher@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Paul Landless
Partner
Singapore
T: +65 6410 2235
E: paul.landless@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Phillip Souta
Global Director of Tech Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Don McCombie
Partner
London
T: +44 207006 2010
E: don.mccombie@cliffordchance.com

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Megan Gordon
Partner
Washington, D.C.
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Caroline Dawson
Partner
London
T: +44 207006 4355
E: caroline.dawson@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Terry Yang
Partner
Hong Kong
T: +852 2825 8863
E: terry.yang@cliffordchance.com

Claudia Milbradt
Partner
Düsseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

André Duminy
Partner
London
T: +44 207006 8121
E: andre.duminy@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Michihiro Nishi
Partner
Tokyo
T: +81 3 6632 6622
E: michihiro.nishi@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com

Jennifer Chimanga
Partner
London
T: +44 207006 2932
E: jennifer.chimanga@cliffordchance.com

Chad Bochan
Partner
Sydney
T: +61 2 8922 8501
E: chad.bochan@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group Amsterdam
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Andrea Tuninetti Ferrari
Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Andrei Mikes
Counsel
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Herbert Swaniker
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2305-006373