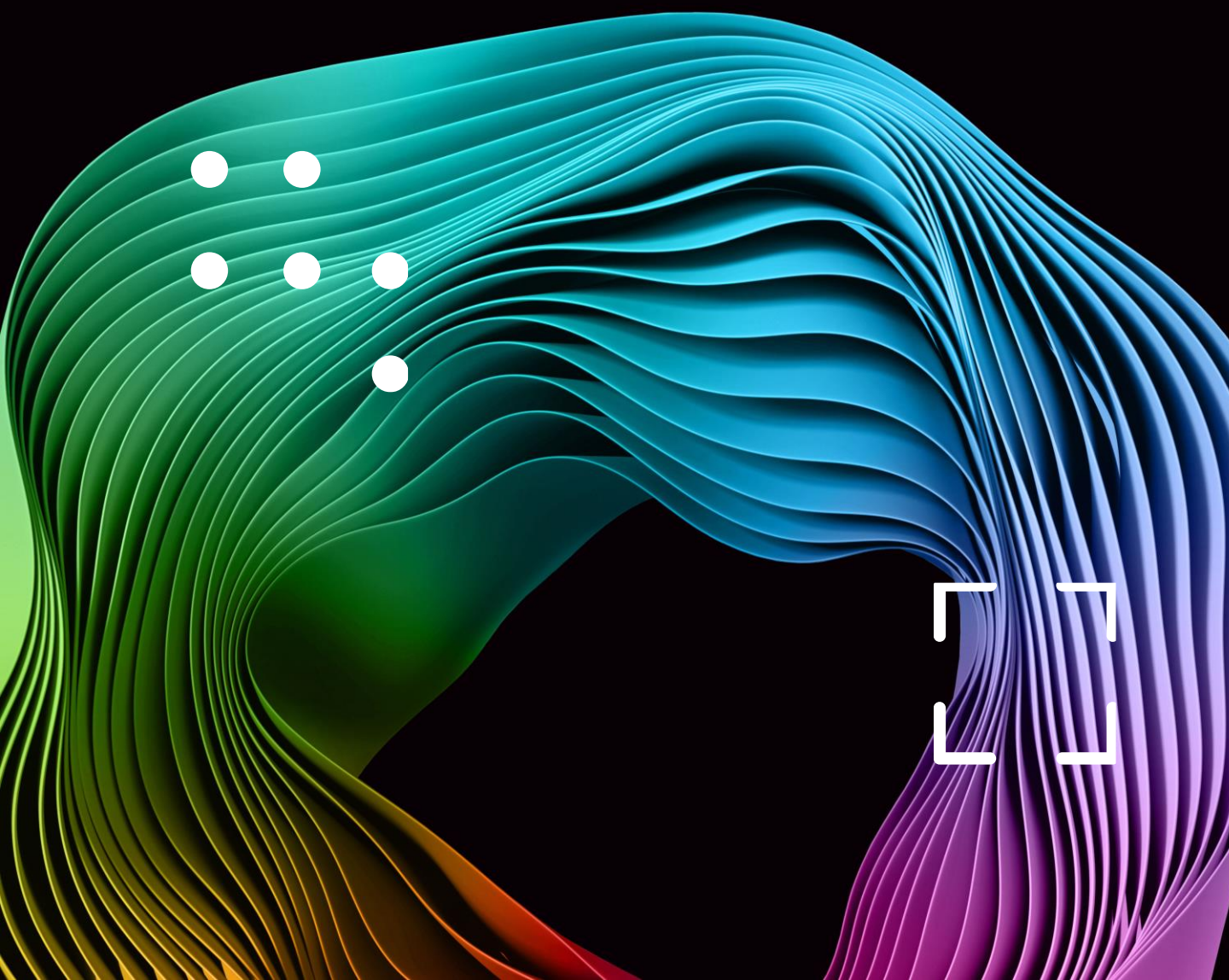
Deloitte.
Legal

Contracting for Generative AI and Mitigating Generative AI Supply Chain Risks

February 2025

Contents

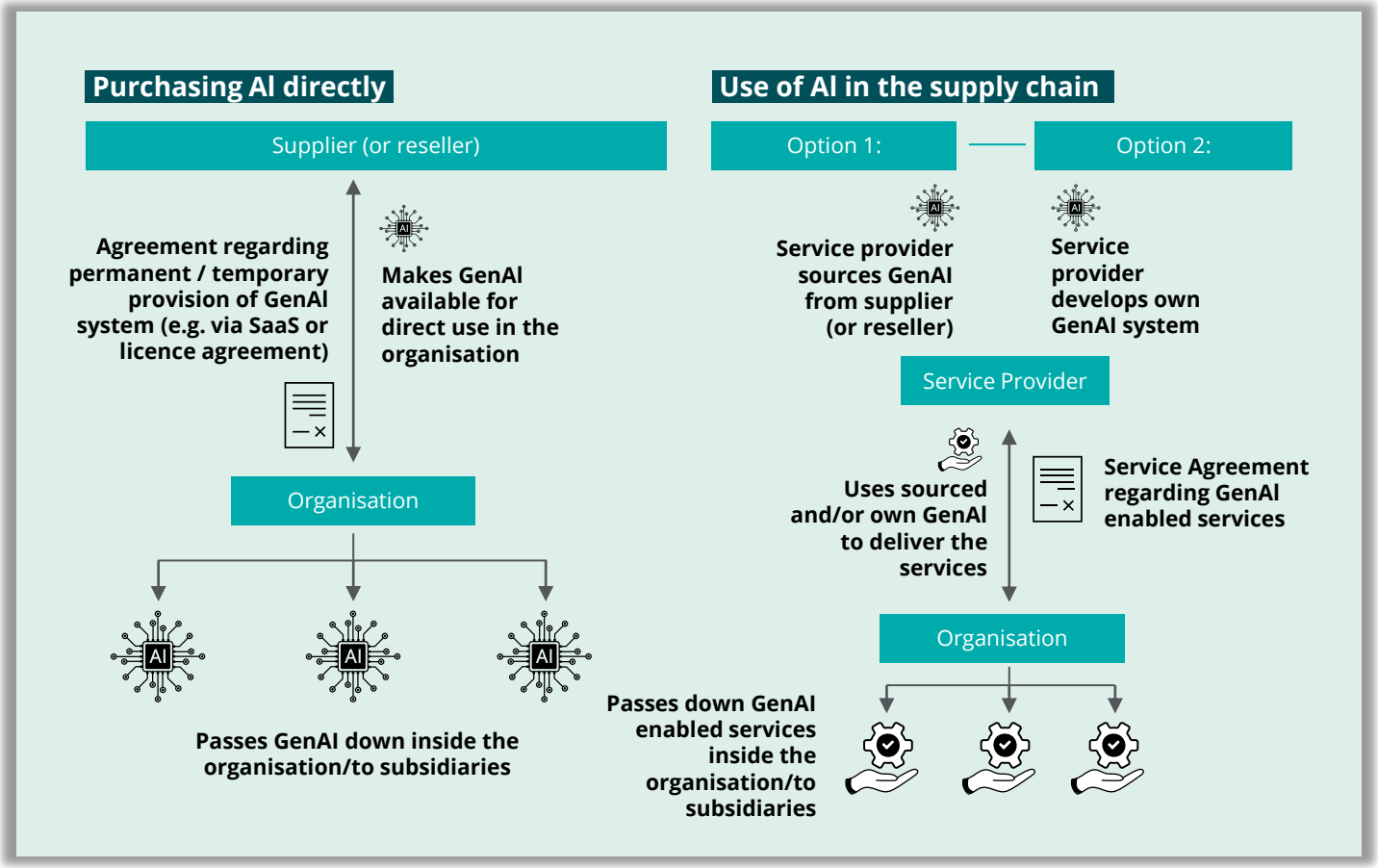


Introduction

Generative AI (GenAI) is a subset of artificial intelligence (AI) that uses training data to produce new content, including text, images, audio, video, and software code. Its use is becoming increasingly prevalent as organisations seek to increase productivity and drive growth through the efficiencies in time, resources and cost which GenAI offers. According to a Deloitte survey in 2024, over 79% of CEOs expect GenAI to transform their organisations in the next three years.

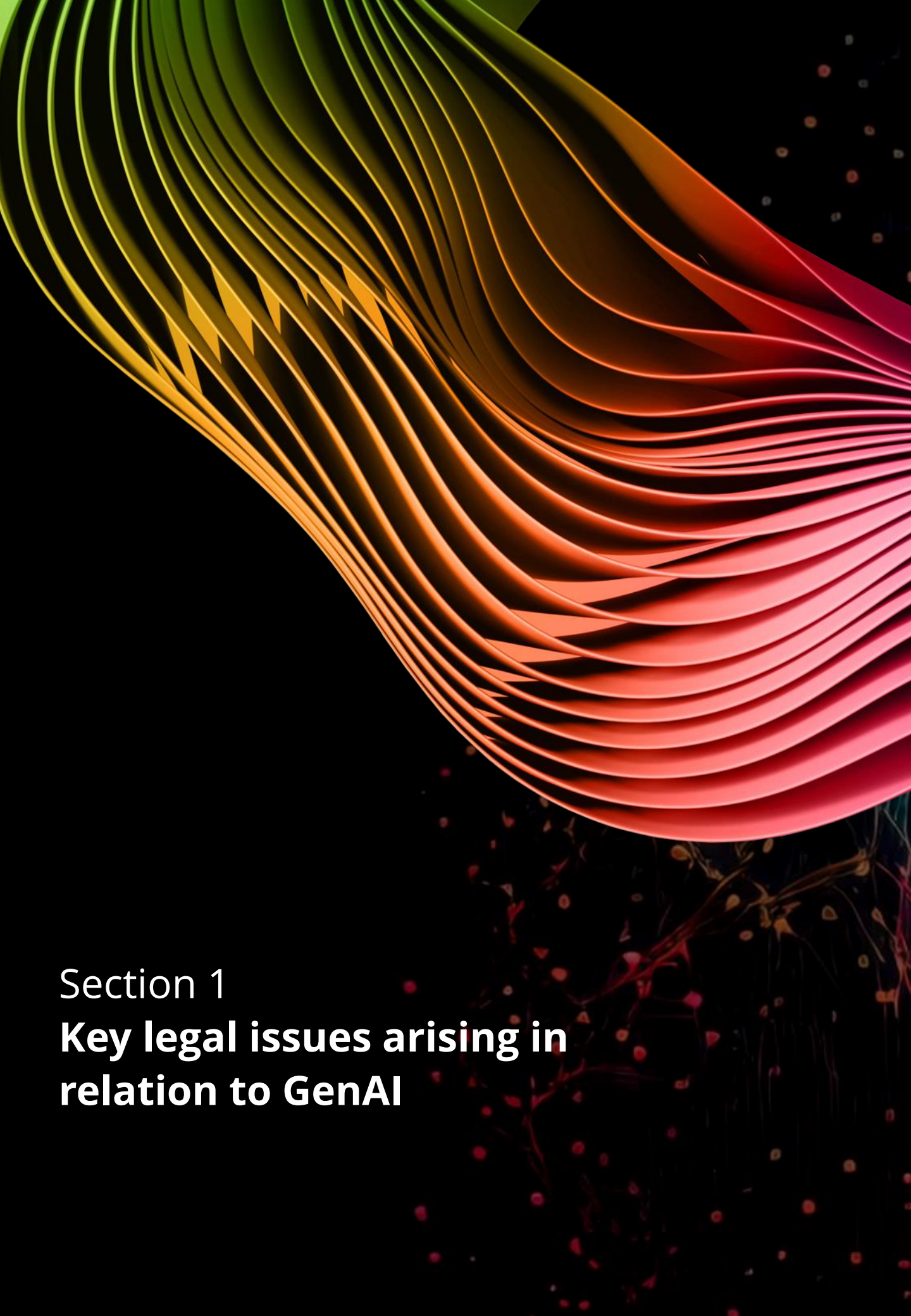
Alongside the opportunities that it creates, however, GenAI presents numerous legal, ethical, and operational challenges. These include the creation of content that may infringe third party intellectual property rights, data privacy and security concerns, the risk of bias in the materials GenAI produces, and the increasingly complex web of law and regulation which impacts GenAI.

When buying a GenAI system from a third party, there are key legal and operational risks which need to be addressed in relation to both the procurement and the use of the GenAI system. But even if an organisation is not procuring a GenAI system for its own use, GenAI is increasingly becoming embedded in workflows throughout the supply chain and being used by suppliers and service providers in the development or delivery of products and services. Such use of GenAI in the supply chain, or "indirect" use of GenAI, can still pose significant risks to customer and intermediary organisations if appropriate mitigations are not put in place. For example, if an outsourced provider of recruitment services has used a biased tool to make hiring recommendations, or an external design firm has created materials using GenAI which gives rise to challenges around intellectual property right ownership, that could have a reputational impact for, give rise to legal claims against, and negatively impact the value of an organisation.



As the prevalence of GenAI continues to grow, it is becoming increasingly important to manage the risks associated with it, both when procuring it for direct use and when GenAI is used in the supply chain. The purpose of this white paper is to explain, on a largely jurisdiction-neutral basis, critical contractual issues and risks to consider in relation to GenAI procurement and to give an overview of some of the key steps an organisation should consider to address and mitigate these issues and risks effectively. The majority of GenAI systems being used within businesses currently are cloud-based, whether private or public cloud, and therefore this paper focuses on issues arising when GenAI is provided on an as-a-service basis.

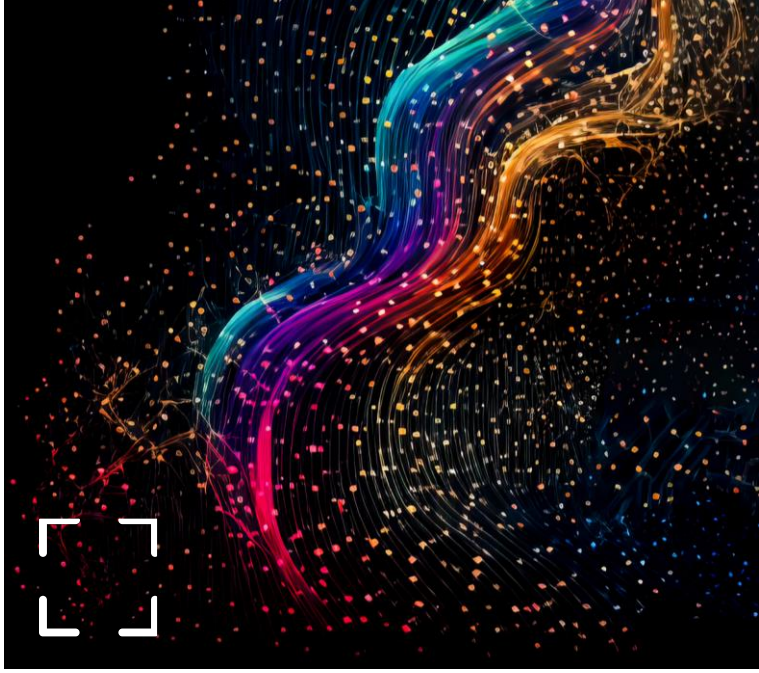
We start with a summary of the key legal issues arising in relation to GenAI in section 1 before examining contracting for GenAI in section 2. In section 3, we explore the implications of GenAI being used in the supply chain by examining a number of scenarios and provide a list of key points to consider addressing contractually. As the EU AI Act has now been finalised, we have included in section 4 a brief introduction to its contractual implications, both when procuring GenAI and when GenAI is or may be used in the supply chain. In section 5, we look at some changes organisations may wish to put in place to ensure they are addressing the risks of GenAI, both when procuring a GenAI system for use in their organisation and when addressing the risk of GenAI use in the supply chain.



Section 1

Key legal issues arising in relation to GenAI

Key legal issues arising in relation to GenAI



GenAI gives rise to a wide range of legal issues which must be evaluated and addressed when contracting for GenAI and when looking to address the risk of GenAI in the supply chain.

These include:

Data privacy: GenAI systems often process vast amounts of data during their training and operation, and additional legal obligations can apply to the use of personal data in and by GenAI systems. For example, EU and UK law set specific requirements in relation to automated decision-making about individuals which produce legal or similar significant effects, on top of standard data protection obligations.

Intellectual property rights: Due to varying levels of protection across jurisdictions, questions of whether intellectual property rights may be infringed because of the way GenAI models are trained or because GenAI outputs potentially include protected works, and the separate question of whether the output generated by GenAI is subject to protection by intellectual property laws, must be assessed on a country-by-country basis. Issues can also arise in relation to who owns the prompts which are inputted into GenAI systems.

Confidential information: Often the benefit to an organisation of using GenAI comes from being able to extract and analyse themes and trends from their own data, but when using confidential information obtained from a third party there is a risk of breaching non-disclosure agreements or other contractual confidentiality obligations.

AI regulation: Different regulatory approaches are being taken globally which means that there is already overlapping sector-specific ("vertical") regulation in some jurisdictions and sector-agnostic ("horizontal") regulation in others. Failing to meet the regulatory requirements can result in material penalties.

Inaccuracy: GenAI tools can provide inaccurate results or "hallucinations", where a system provides responses which are objectively false but presented as correct. Where such outputs are presented as accurate on behalf of an organisation, that organisation can be legally liable for the misleading statements.

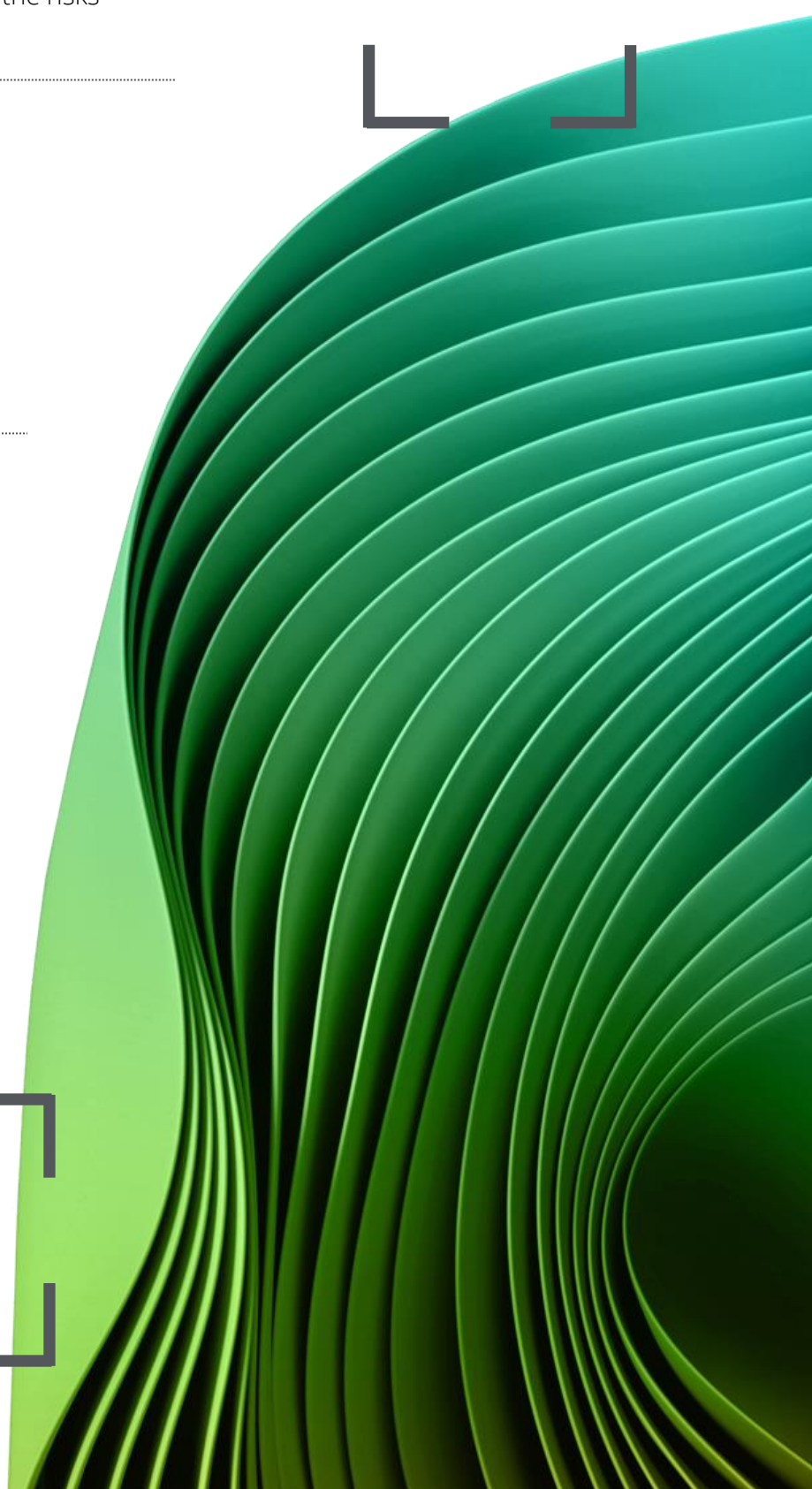
Opacity: The "black box" nature of GenAI systems means it is often unclear as to why/how a GenAI system has reached a conclusion. This can make compliance with legal transparency and fairness obligations challenging.

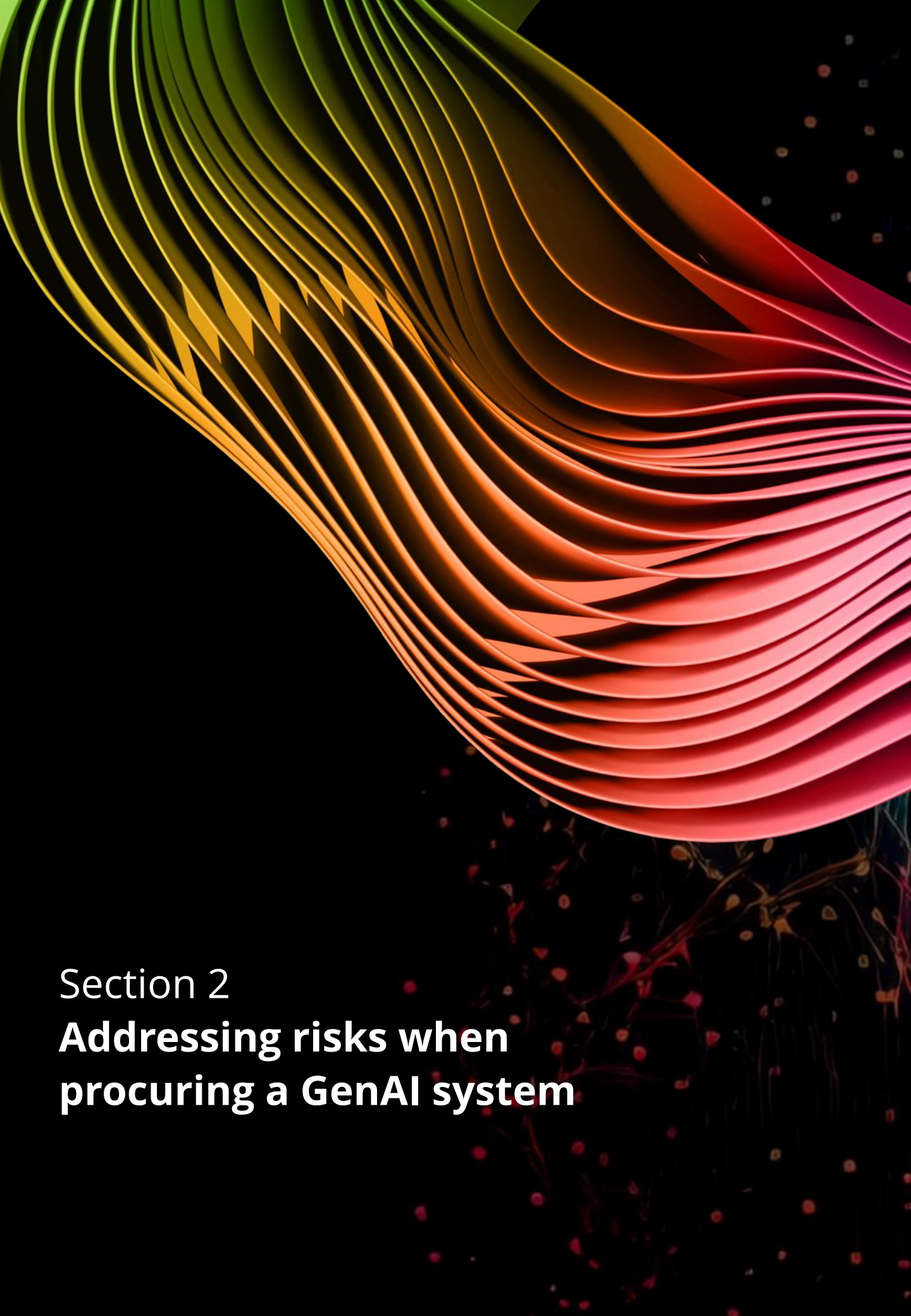
Liability and redress: In addition to liability issues arising out of inaccuracies, AI gives rise to many other novel legal questions relating to how liability is apportioned, and redress is provided. Organisations need to understand what they can be liable for and the extent to which such liability can be limited, in order to protect themselves and manage the risks appropriately.

Bias: There are already numerous public instances of GenAI systems exhibiting bias, which could result in discrimination on grounds protected in many jurisdictions, such as race or gender.

Environment, social and governance (ESG): GenAI systems use large amounts of energy, and the bias issues flagged above can also have social consequences. This can impact organisations' ESG commitments, policies and ESG laws and regulation.

The impact of GenAI on existing organisational governance frameworks, as well as the governance of the use GenAI within organisations, should also be assessed.





Section 2

Addressing risks when procuring a GenAI system

Addressing risks when procuring a GenAI system

When procuring a GenAI system from a vendor, the purchasing organisation should consider addressing in the relevant contract the specific risks discussed below.

Experience shows that, in many cases, the general terms and conditions vendors propose for GenAI do not address the interests and legal requirements of the procuring organisation fully, or at all, since contractual market practices have not yet been established.

When contracting on the vendor's terms or on a version of these, we recommend evaluating them against your own minimum contractual requirements as part of the vendor selection process. Inability to meet these requirements may render certain vendors ineligible, or become a key differentiator.

Be cautious of data privacy:

Since the processing of data is key for a properly functioning GenAI system, making sure that all privacy requirements are met is essential for compliant use.

- Compliance with data privacy laws can prove difficult due to the 'black box' nature of GenAI systems and the resulting difficulty in complying with data protection law requirements for transparency.
- Under EU and UK law, organisations using personal data within GenAI will usually act as a 'controller' of the data they collect, e.g. data relating to their own employees, and the provider of a GenAI system on a software-as-a-service basis would typically act as a 'data processor' of the data that customer organisations enter into their GenAI systems. However, the standard terms of use and data protection related documentation used by GenAI vendors commonly allow those vendors to use the data for their own purposes, often including further training of their GenAI systems. This casts doubt on the usual roles described above: the GenAI system provider could now be seen as a separate controller or even a joint controller with the purchasing organisation.
- The characteristics of GenAI systems may also hinder or complicate compliance with data privacy laws, as the technical conditions may affect an organisation's ability to comply with the requests from data subjects when using GenAI.

Suggestion:

For successful integration of GenAI systems, data protection compliance must be a priority from the outset. Contracts should clearly define the scope of data processing and limit it to what is necessary for the intended purpose.

They should also appropriately allocate responsibility and liability for security and compliance between the GenAI provider and the deploying organisation, taking into account the extent to which the deploying organisation understands and can influence the GenAI's data processing. Organisations should involve their privacy officers and, if applicable, employee representatives before and throughout the procurement process.

Avoiding the negative consequence of unlawful training materials:

Since GenAI is regularly trained on large publicly-available datasets subject to the laws of numerous jurisdictions, it is not always clear whether the training complies with relevant laws or infringed intellectual property rights.

Non-compliance may occur for many reasons, including because there is no legal basis for processing the personal data contained in the dataset, or because the training set contains intellectual property rights owned by third parties which have not been appropriately licensed. This may impact the customer organisation in two ways: firstly, the vendor providing the GenAI model may face legal consequences such as injunctions, administrative fines, claims for damage and even criminal penalties, any of which may temporarily or permanently impact its capability to provide the GenAI system to the customer organisation; secondly, individuals who can claim against the vendor may also consider bringing similar claims against the customer organisation. This may lead to legal consequences, operational restrictions, and reputational damage for the customer organisation.

Suggestion:

Organisations should obtain a clear understanding of the datasets used to train the GenAI and the measures taken to ensure compliance. Where not publicly available, organisations should consider requesting that the relevant information is provided by the vendor and contractual assurances given about its provenance. Organisations should also consider requiring an indemnity at an appropriate financial level against any losses arising from a breach of these commitments or third party claims.

Make sure your data is not misappropriated:

An organisation using GenAI feeds into the GenAI system data and questions relevant to its business. This data can be very valuable to the vendor, as it can help to fine-tune this GenAI model and be used for future training of other GenAI models. In many cases the customer organisation has an interest in keeping the information confidential, since it contains trade secrets of the organisation or is protected by non-disclosure agreements which allow it to be used only for specific, agreed purposes. Use by the vendor could threaten the business model of the customer and the secrecy of the information, potentially leading to a loss of confidential information and claims for breach of the confidentiality agreements.

Suggestion:

The boundaries of what the vendor of a GenAI system may do with the inputs and outputs should be clearly stated, and should be aligned with both the intended use cases and the permitted use of the data which may be entered into the GenAI system. It may also be appropriate for the vendor to be obliged to implement specific technical and organisational measures to ensure that the inputs, and outputs cannot be accessed without authorisation.

Obtain the rights you actually need:

Just as crucial as agreeing which party – the customer or the vendor – will own the GenAI system's outputs (i.e., the content the GenAI system generates), is addressing in the agreement what rights the non-owning party has to use the outputs. The customer will typically wish to own the outputs and to impose restrictions on the vendor's use of those outputs, restrictions that the vendor may resist. Any such contractual agreement will however only apply between the parties, so a third party will not be bound by it. Only the acquisition of certain statutory intellectual property rights (which may not be possible in all jurisdictions) provides protection against use by any third party.

Suggestion:

The organisation must ensure that appropriate contractual usage rights are granted to reflect its actual needs. If statutory intellectual property right protection is required, appropriate measures must be taken to ensure that intellectual property rights do in fact arise. Do not assume that intellectual property rights will arise, as this will depend on the intellectual property laws of the relevant jurisdiction(s).

Do not let costs get out of hand:

Operating GenAI systems is generally considered costly compared to other technologies. This is mainly due to very high energy consumption, expensive hardware, and sunk costs for training and development. It is therefore important that transparent pricing mechanisms are agreed which meet the customer's needs. Common pricing mechanisms include consumption-based (per token/output), user-based (per concurrent/named user) and value-added-based (per customer interaction).

Suggestion:

To maintain cost efficiency in GenAI procurement, it is important to evaluate pricing mechanisms critically. It is also essential to weigh up long-term price stability and minimum volume commitments within a rapidly evolving market.

Keep an eye on interdependencies with sector regulation:

More and more business sectors are subject to additional regulations which must be taken into account when procuring GenAI systems. For example, in the health care industry GenAI models may be treated as medical devices, in the financial industry regulators may have their own sets of rules that must be considered when using GenAI, and in the aviation industry regulations could require the certification of GenAI models, such as autopilot functionalities or air traffic management, by aviation authorities. New sector-specific regulations are also emerging, which may impose additional contractual requirements which must be addressed.

Suggestion:

Organisations should consider including clauses in their contracts for GenAI systems that mandate the vendor to provide ongoing support for compliance with relevant legal and regulatory obligations in their particular sectors. Contractual obligations to support regular audits, compliance updates, and transparent communication channels can also help to ensure adherence to these obligations.

Liability:

As outlined above, while there are many benefits to using GenAI, it can also expose an organisation to new procedural, operational and legal risks. Existing liability clauses do not always allow for these risks to be balanced and shared between the parties appropriately. For example, when procuring a GenAI system an organisation may wish to pay particular attention to any cap on the vendor's liability for infringing third party intellectual property.

Suggestion:

Carefully assess the risks to which use of GenAI will expose your organisation, for both your internal and customer-facing purposes. Based on that assessment, ensure that all risks and responsibilities are reasonably allocated between the parties through appropriate indemnities, warranties, representations and liability caps. This includes assessing and addressing any gaps regarding third parties such as end customers who are indirectly affected by the procured GenAI system, e.g. where the organisation uses the GenAI model to provide its own services.

Check your Environment, Social and Governance (ESG) policies:

GenAI systems often require significant computing power, leading to high energy and water consumption compared with other technologies. This can strain local resources and contribute to the organisation's carbon footprint. As well as the environmental aspects, there are also ethical issues to consider when contracting for GenAI. It is crucial to ensure that GenAI is used ethically and that the results are transparent and accountable.

Suggestion:

Check your applicable ESG policies and consider whether these should be incorporated into the contract for a GenAI system or incorporated by reference. Consider also how to reflect the evolution of your ESG policies during the life of the contract.

Don't get locked in:

The more deeply GenAI systems are integrated into the organisation's core processes, the greater the dependency for the organisation. Especially since GenAI is a relatively new technology where new and improved products are constantly being launched, organisations should consider for how long they wish to be committed, both contractually and commercially.

Suggestion:

The organisation should carefully consider whether the contractual terms are in effect "locking-in" the customer to the GenAI system vendor. Such an effect could result from lengthy contract terms, minimum volume commitments, unfavourable termination rights, or lack of exit support.

Keep cybersecurity in mind:

As with all IT systems, aspects of cybersecurity and cyber resilience must be taken into account when negotiating with the vendor. In the European Union ("EU") this has gained even more importance due to various legislative acts such as the EU's second Network and Information Security Directive (NIS2) and the EU's Digital Operational Resilience Act (DORA). The applicable regulatory requirements depend on numerous factors such as the sector and size of the organisation, the location of the data processing, and the types of data being processed.

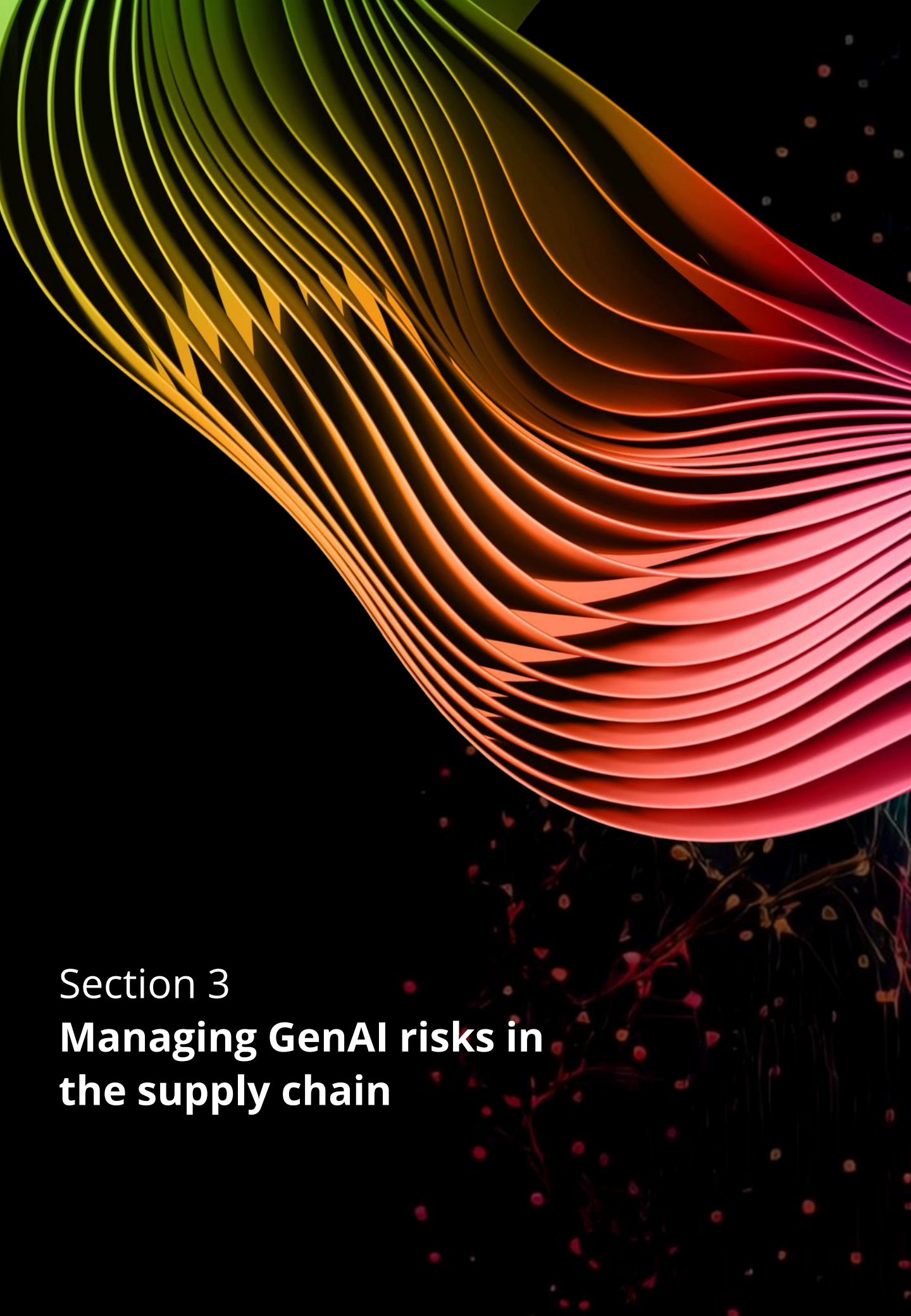
Suggestion:

Any organisation procuring a GenAI system should ensure that, as well as the particular and enhanced risks which relate to GenAI specifically, the broader risks applicable to any IT system are also addressed. Assess which regulatory requirements apply to the organisation and the intended data processing. The organisation might be obliged to pass on some obligations to its vendor, or might need to rely on the vendor's support in order to fulfil its own regulatory obligations. This will need to be reflected in the agreement with the vendor.

Key questions to ask

In addition to following their own usual contractual guardrails relating to the procurement of cloud-based IT systems, when contracting for a GenAI system customers should also ask themselves the following key questions so as to identify and mitigate potential GenAI risks, and to ensure alignment with legal, technical, and operational norms:

- ✓ What datasets is the vendor using to train the GenAI system, and what customer data will be used to further train it or fine-tune it (if any)?
- ✓ Does using the GenAI system require the processing of personal data provided by the organisation? If yes, who is responsible for the processing of such personal data and who is the controller?
- ✓ Are measures in place to ensure that the GenAI system will not infringe the confidentiality of the customer's inputs?
- ✓ Who owns the input data (customer training data and prompts) and who will own the output data? What restrictions on the use of the customer's input data and/or output data by the vendor need to be put in place? Are contractual rights sufficient, or is the protection of statutory intellectual property rights required for output data?
- ✓ Is the pricing mechanism transparent, and is there a risk that the costs are disproportionate to the benefit?
- ✓ Does the customer need the supplier to support the customer's compliance with new obligations under AI law or sector-specific regulations arising from the procurement of the GenAI system?
- ✓ Are there any provisions in place in case of the GenAI system's failure or service disruptions?
- ✓ What warranties and indemnities does the vendor give about non-infringement of intellectual property rights, use of personal data, use of open source material, accuracy, bias and discrimination, relevance and timeliness of training data, and transparency?
- ✓ Is the customer locking itself into a specific product or vendor? Is termination assistance available when needed?
- ✓ Are the vendor's ESG policies in line with the customer's needs?
- ✓ Does the vendor have, or will it otherwise agree to, appropriate cybersecurity measures?



Section 3

Managing GenAI risks in the supply chain

Managing GenAI risks in the supply chain

The use of GenAI by suppliers and service providers in connection with the development and delivery of the services and products that they supply to customers needs to be carefully evaluated within the context of the existing supply chain, and managed on an ongoing basis. The introduction of GenAI systems can give rise to additional legal and operational risks that have not previously been considered. This also underscores the need for organisations to understand clearly how the goods and services they procure are sourced and delivered.

Below are some increasingly common scenarios where GenAI use in the supply chain is exacerbating risks, along with an explanation of why the risks arise and potential contractual mitigations.

Scenario 1

Supplier is generating materials the customer wants to own

Uncertainty persists in many jurisdictions about whether GenAI systems can be used to generate intellectual property rights, as many countries require some aspect of human involvement in order to create new intellectual property rights.

In the context of creative services, such as the creation of branding or design materials, or where research and development is being carried out, this can pose a particular risk for service recipients who expect to own the intellectual property rights in the output of the services. Such contracts commonly assign to the customer the ownership of the intellectual property rights which arise, but if the use of a GenAI system means no intellectual property rights have arisen, there are no intellectual property rights to transfer.

This could mean that an organisation uses the output of such services believing that it owns them and can prevent others from using them, only to discover later that, as no intellectual property rights have arisen, any third party can use the relevant materials.

This can be addressed contractually by obliging the supplier to take jurisdiction-appropriate steps to ensure that intellectual property rights do arise in the output of the services. The required steps will vary from jurisdiction to jurisdiction and are evolving, but could include ensuring that any GenAI is only used to prepare an initial draft of the output, which a human refines and finalises, or avoiding the use of GenAI entirely in particularly challenging jurisdictions.

Scenario 2

Service provider is making decisions which impact individuals

GenAI can make it very easy for organisations to use off-the-shelf tools to automate decisions which previously would have required a system developed for the specific task. These decisions in a supply chain context could, for example, include a third party recruiter determining whether an individual should be put forward for an interview or a third party consultant short-listing employees for promotion, a pay rise or redundancy.

Such decisions would need to comply not only with existing requirements around automated decision-making and equality legislation, which requires that such decisions do not discriminate on the grounds of protected characteristics, but also with new AI-specific regulation which imposes additional obligations on "high-risk" uses of GenAI. Use of general purpose GenAI systems to make such assessments can carry significant risk for the end customer of the service. If a hiring, promotion, pay review or redundancy decision was later found to have been based on the use of a tool which was biased or did not comply with either general or AI-specific legal requirements, this could cause material reputational damage for the customer organisation and expose it to the risk of claims.

The contract with such a service provider should expressly require the provider to comply with all relevant laws and regulations on automated decision making when using a GenAI system and to provide evidence to the customer that such requirements have been met. Ideally, the provider will also provide insights into the automated decision-making logic to the organisation; however, in practice providers are hesitant to do this as it risks exposing their trade secrets.

The customer needs to be confident that its supply chain is using GenAI lawfully in situations where misuse could have serious consequences for individuals and for both the customer and service provider organisations. It is also important that if an issue does arise, the customer can demonstrate that it took appropriate measures to mitigate the risks.

Scenario 3

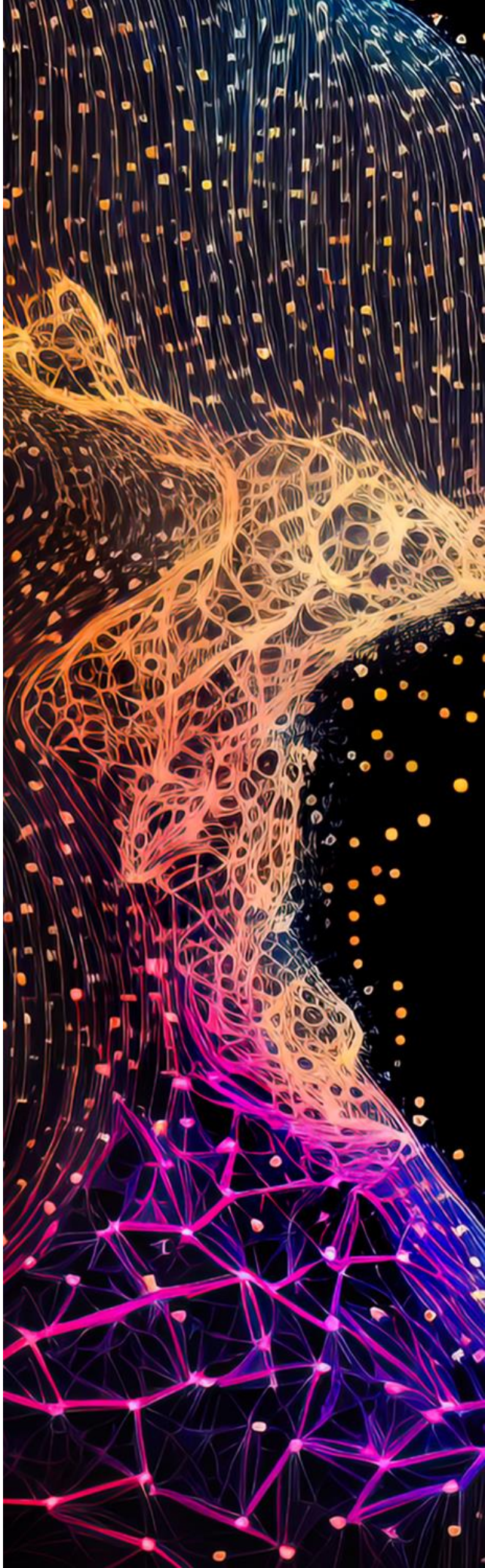
Confidential information is shared with the supplier or service provider

Where suppliers and service providers who have access to confidential information use GenAI, the risk of that information being inadvertently made public or used in unauthorised ways is increased.

For example, if historic sales data is provided to a marketing agency to support the development of a new data-based marketing strategy, and that agency puts the data into a public GenAI system, the owner of that system may be allowed under its terms and conditions to train and improve its own systems using the submitted data.

Often, confidential information shared by a third party can contractually only be used for a specified purpose. If an organisation wishes to provide such protected information to a third party to benefit from GenAI analysis and from the manipulation of such data, the organisation will also need to ensure that such data-sharing is permitted.

Use of such confidential data by a third party in a GenAI system would create a risk of the confidential information being disclosed. This risk can largely be addressed contractually by obliging the supplier or service provider only to use GenAI systems which meet certain criteria, and where appropriate, contractual restrictions on the use of such data by the owners of those GenAI systems. Alternatively, the customer could mandate that the supplier/service provider uses the customer's own GenAI system, if that provides a sufficient level of protection. Such obligations could be accompanied by liability and indemnification provisions that put the organisation into a position to claim damages in case of any breach of confidentiality. However, a right to damages would not protect the customer if the owner of the confidential information obtained an injunction restricting the customer's further use of the confidential information.



Scenario 4

Supplier is developing code for use by a customer on the customer's systems

One of the most powerful uses of GenAI is to support the writing of code and software development more generally.

Where the code writing is done by a third party, it gives rise to a number of legal risks. These include an increased risk of the code infringing the intellectual property rights of a third party by replicating an existing, known solution, and the inadvertent use of "copyleft" open-source software, the licence terms of which can mean the end software must also be made publicly available.

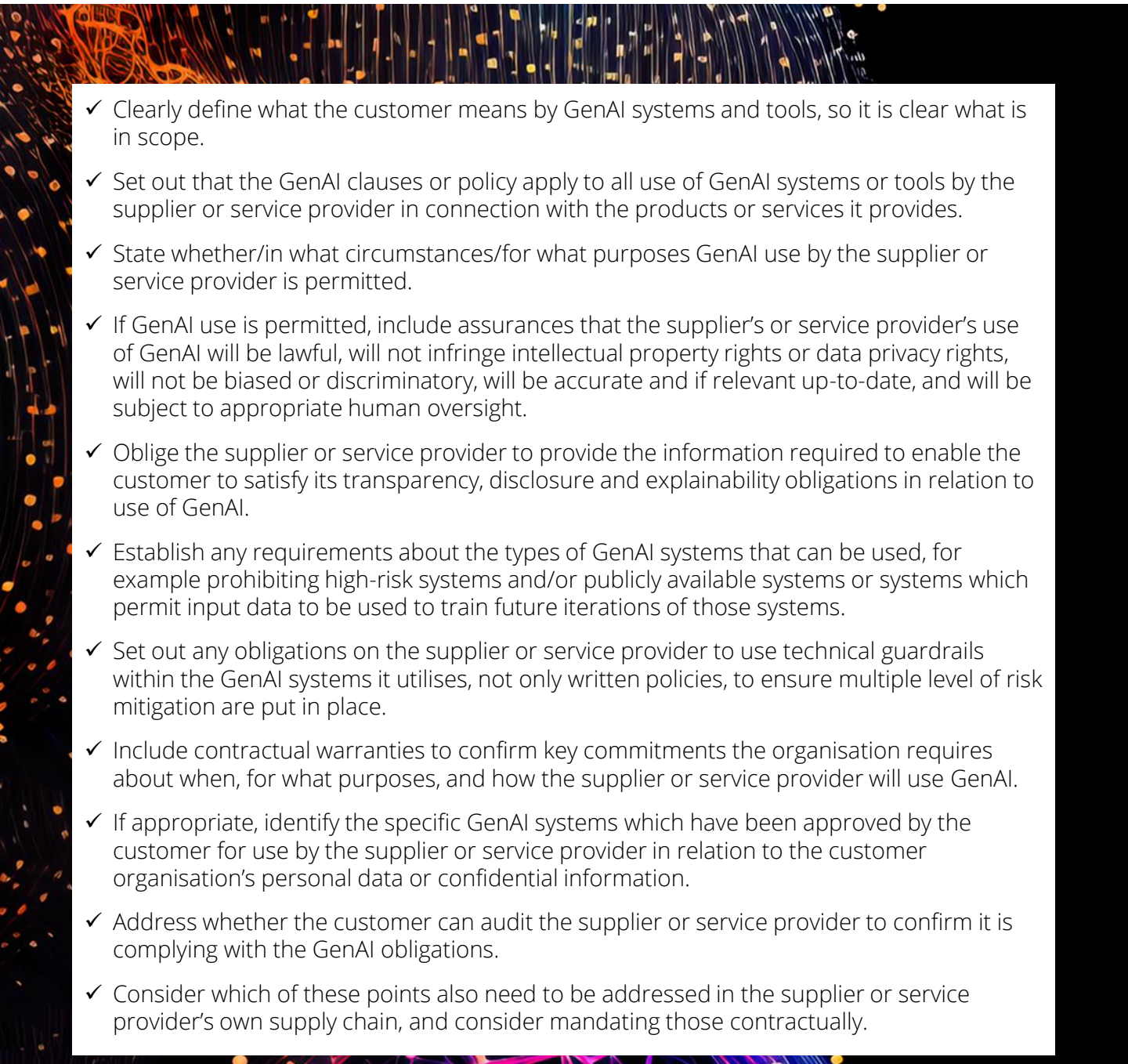
The financial advantages of using GenAI supported software development are such that, despite these risks, GenAI-supported software development is quickly becoming the industry norm. The risk of this type of intellectual property right infringement needs to be addressed technically, by marking replicated code or taking technical measures to ensure such replication or use does not occur.

When looking to manage this risk in the supply chain, the contract should clearly specify to what extent GenAI tools can be used to support the work, the mitigating technical measures which will be put in place to address the risks, and any specific areas where such use is prohibited. In the case of software development, it could be feasible to specify the areas where use of GenAI tools is permissible (clearly separable code of low importance where a replacement could be drawn up quickly) and where use of GenAI tools is forbidden (the "core intellectual property" of the software to be developed).

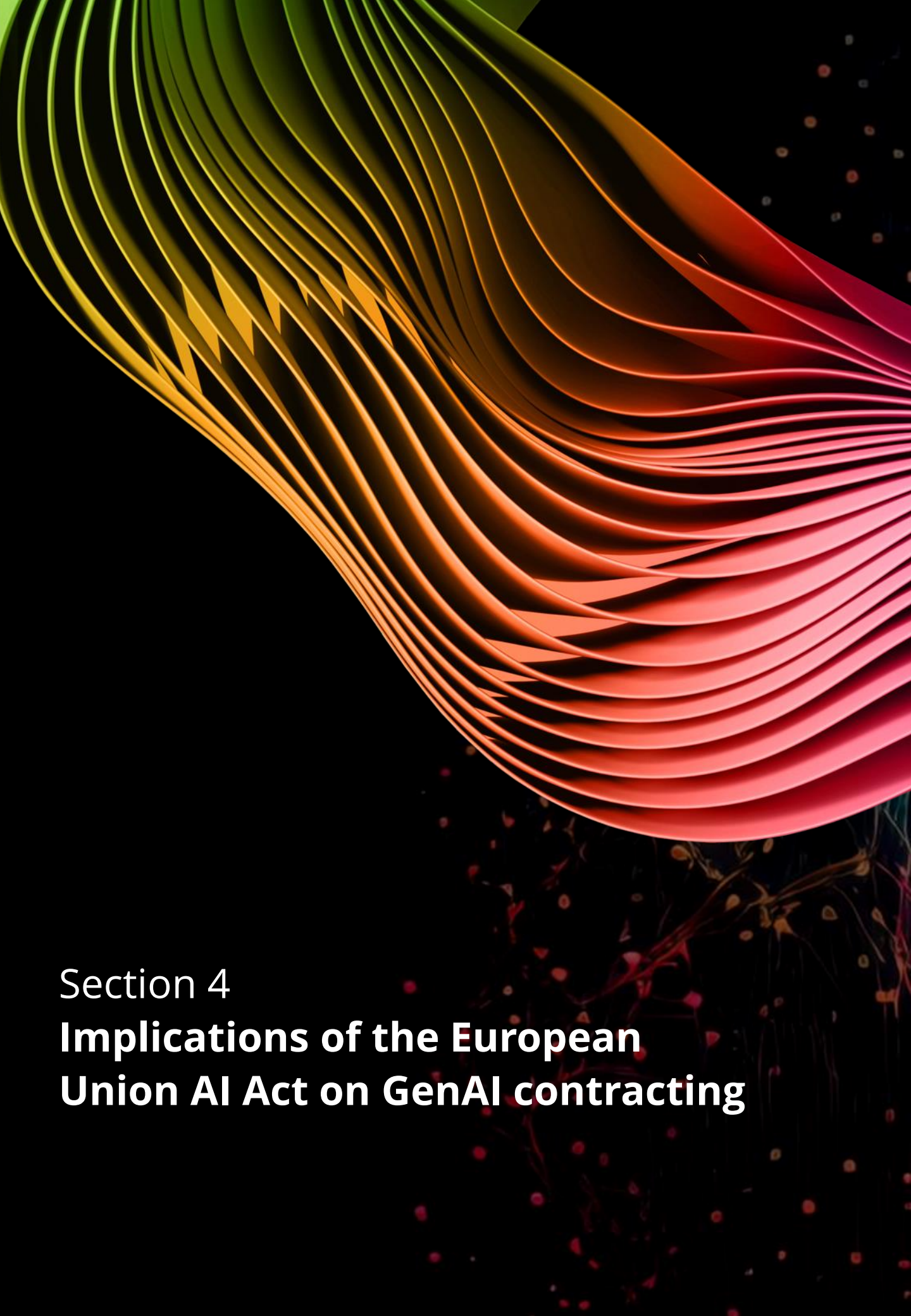
Consideration should also be given to the strength of the intellectual property right infringement indemnities and liability provisions being given, as well as to the audit rights the customer requires, though suppliers and service providers are also increasingly sensitive about risks that they may not feel well placed to manage.

Using GenAI-specific clauses to manage risk in the supply chain

Whilst the above scenarios identify key risks that arise in certain scenarios, many other circumstances exist where the use of GenAI by suppliers and service providers will create new risks or exacerbate existing ones. As well as taking measures targeted at the particular context, organisations should also consider including in their template contracts and playbooks clauses which specifically address the risk of GenAI in the supply chain. Such clauses should:



- ✓ Clearly define what the customer means by GenAI systems and tools, so it is clear what is in scope.
- ✓ Set out that the GenAI clauses or policy apply to all use of GenAI systems or tools by the supplier or service provider in connection with the products or services it provides.
- ✓ State whether/in what circumstances/for what purposes GenAI use by the supplier or service provider is permitted.
- ✓ If GenAI use is permitted, include assurances that the supplier's or service provider's use of GenAI will be lawful, will not infringe intellectual property rights or data privacy rights, will not be biased or discriminatory, will be accurate and if relevant up-to-date, and will be subject to appropriate human oversight.
- ✓ Oblige the supplier or service provider to provide the information required to enable the customer to satisfy its transparency, disclosure and explainability obligations in relation to use of GenAI.
- ✓ Establish any requirements about the types of GenAI systems that can be used, for example prohibiting high-risk systems and/or publicly available systems or systems which permit input data to be used to train future iterations of those systems.
- ✓ Set out any obligations on the supplier or service provider to use technical guardrails within the GenAI systems it utilises, not only written policies, to ensure multiple level of risk mitigation are put in place.
- ✓ Include contractual warranties to confirm key commitments the organisation requires about when, for what purposes, and how the supplier or service provider will use GenAI.
- ✓ If appropriate, identify the specific GenAI systems which have been approved by the customer for use by the supplier or service provider in relation to the customer organisation's personal data or confidential information.
- ✓ Address whether the customer can audit the supplier or service provider to confirm it is complying with the GenAI obligations.
- ✓ Consider which of these points also need to be addressed in the supplier or service provider's own supply chain, and consider mandating those contractually.



Section 4

Implications of the European Union AI Act on GenAI contracting

Implications of the European Union AI Act[2] on GenAI contracting

As one of the most far-reaching pieces of AI-specific legislation in force, the EU AI Act has contractual implications both for procuring GenAI systems and for the use of GenAI systems in the supply chain.

The Act introduces a risk-based approach, with the stringency of requirements increasing with the level of risk. It imposes obligations not only on the 'providers' of an AI system (i.e. the entity developing an AI system or a general purpose AI model, and the entity placing it on the market) but also on deployers of AI systems (which would include both an organisation which has procured a GenAI system for its own use, and a third party which uses GenAI within its business). There are also other operator roles, such as an importer or distributor.

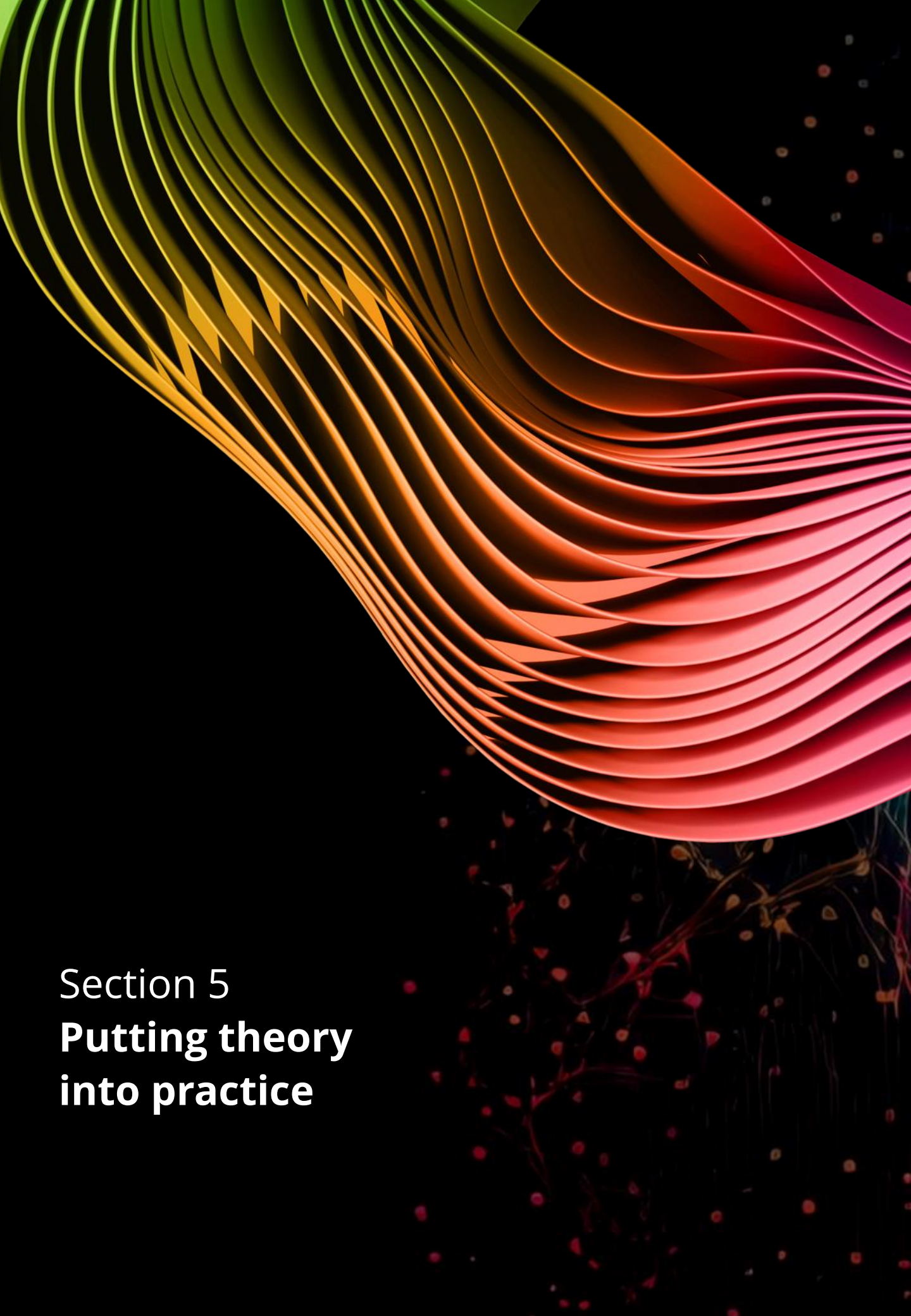
The obligations under the EU AI Act include implementing risk and quality management systems, taking technical and organisational measures, verification of input data, and meeting transparency, system monitoring and record-keeping, human oversight, and cybersecurity requirements. A deployer will also often be dependent on the provider of a GenAI system to enable the deployer to meet its regulatory obligations.

When contracting for a GenAI solution or assessing the implications of GenAI in the supply chain, consideration should be given as to which "role" or "roles" the customer organisation is taking on.

This will not always be straightforward. For example, does the organisation explicitly authorise or even commission the use of GenAI by the supplier or service provider in the performance of its contractual obligations? Could the use of a GenAI system be attributed to the organisation as use under its own responsibility and authority? Or is the supplier's or service provider's use of a GenAI system entirely under its own responsibility? These are questions that should be carefully assessed and taken into account contractually, to ensure EU AI Act obligations can be met.

Depending on the role(s) that the procuring organisation and the vendor (in case of a procurement of GenAI) or the supplier or service provider (in case of indirect use of GenAI) take on under the EU AI Act, the procuring organisation should ensure that the contractual agreement enables it to receive both the information and support it needs to comply with its own obligations under the EU AI Act and provides assurance that the vendor or supplier/service provider is complying with its obligations.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence

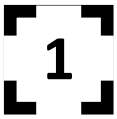


Section 5

Putting theory into practice

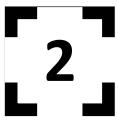
Putting theory into practice

In order to address the risks discussed in this white paper, both when procuring a GenAI system for internal use and when evaluating the use of GenAI in the supply chain, we recommend putting this guidance into practice by focusing on four key pillars:



Contract templates and playbooks

Organisations should consider updating their contract templates and playbooks to address the risks set out above. For risks in the supply chain, this could include developing a one-size-fits-all approach with any changes to be agreed by the legal and compliance teams by exception, or a detailed playbook which addresses approved positions in high-risk scenarios. The procurement of GenAI systems will often take place on supplier/service provider standard terms, so consider developing a checklist of key points which should be evaluated and addressed.



Procurement processes

Whilst ensuring the right terms are included in contracts is a critical step to address the risk of GenAI, it is not sufficient by itself. Procurement processes should be updated to reflect the approach the organisation wishes to take, starting with updating third party risk assessment questionnaires and onboarding processes to require information relating to the GenAI and, in the case of supplier/service provider supply chain risk, how GenAI is being used in the supplier's or service provider's business. Customer organisations should also look to identify and analyse key information about how they will use the product or service to ensure risks are addressed appropriately.

Due diligence

The extent of due diligence on GenAI vendors, and on suppliers and service providers using GenAI, may also need to be expanded, to enable key information to be verified. This should include looking at the technical guardrails an organisation may require of GenAI vendors, suppliers and service providers which could have access to particularly sensitive confidential information or personal data, or suppliers and service providers which are undertaking coding or providing other goods or services which give rise to material additional risks.

Governance

Monitoring, audit and other governance rights only benefit the customer if they are used. Organisations should ensure that the relevant teams include people with appropriate knowledge of GenAI, know what rights the customer organisation has and how to exercise these, and exercise these rights when relevant.

When developing your organisation's approach to managing GenAI risk, it should always be remembered that different jurisdictions have varied legal and regulatory requirements. Your organisation's approach should reflect its geographical distribution, the markets in which it operates, and its risk appetite.

As always with the procurement of technology solutions, it is close to impossible to remedy all risks. This is even more true in relation to cutting edge and quickly evolving technologies such as GenAI. Having effective contracts, governance and related practices in place can help to materially reduce exposure to these risks, and enable organisations to identify those risks which require a technical or organisational remedy.

Get in touch

By providing comprehensive contractual templates and playbooks, advising on specific contractual negotiations, refining procurement processes, enhancing due diligence and advising on the exercise of governance rights, we can help your organisation to effectively navigate potential risks while also seizing the significant opportunities offered by GenAI.

If you would like to discuss any of the points raised in this paper or to hear more about how we can support you, do not hesitate to get in touch with us.

Louis Wihl
Director, Commercial Technology Advisory, Deloitte Legal UK
lwihl@deloitte.co.uk

Paul O'Hare
Partner, Commercial Technology Advisory, Deloitte Legal UK
pohare@deloitte.co.uk

Dr Till Contzen
Partner, Service Area Head Digital Law, Deloitte Legal Germany
tcontzen@deloitte.de

Elizabeth Lumb
Associate Director, Commercial Technology Advisory, Deloitte Legal UK
elumb@deloitte.co.uk

Deloitte.
Legal