Linklaters

Issues for Financial Sponsors and their Portfolio Companies 2026

The governance premium



Table of Contents

Introduction	3
EU digital package: What sponsors need to price, plan and prioritise	4
Agentic AI: What sponsors and portfolio companies need to know when systems start to act	7
Ransomware, resilience and regulation: The cyber challenge for companies	10
Are stablecoins the answer to painful payments?	12
A transcript too far? When to use AI for records of meetings	14
Antitrust enforcement gets political – the winners and losers	16
Compliance and beyond: Governing sustainability risk in a complex world	19
Navigating the UK employment law revolution: What sponsors and portfolio companies must know	22
Making the most of a defined benefit pension scheme: Less legacy risk, more strategic opportunity	25

Introduction

In the midst of war, a global energy shock, rapid automation and climate change, the role of decision makers at financial sponsors and portfolio companies is relatively unchanging. They must seek to limit the impact of foreseeable risks, manage crises, build business resilience and seize strategic opportunities. What has changed is the complexity and uncertainty of the environment in which they must make decisions.

This briefing brings together a set of issues that are moving quickly and will be relevant to sponsors and their portfolio companies. Our aim is to equip decision makers with a short practical guide to each issue together with key governance steps that they should be considering to manage risk and optimise opportunities.

We begin with five different aspects of the technological revolution, starting with a look at the **EU's digital package** and how its wide-ranging compliance obligations – covering cloud services, digital labour platforms, and many more – may influence investment planning for sponsors.

We explore the challenges of **agentic AI**, which is offering to transform many businesses but requires control and oversight to limit the potential for "black box" accountability – directors or companies being responsible for actions of AI agents that they did not know about or intend.

We look at recent developments in the world of **cyber-attacks**, including the backdrop of tighter regulatory expectations and potential restrictions on ransomware payments.

On a brighter note, **stablecoins** and other forms of digital money may reshape payments and settlement, with opportunities to make payment systems far more efficient, but with accompanying risks.

We also discuss the use case for **AI in recording board decisions**, where verbatim transcripts and speedy summaries appear to promise efficiency but have particular dangers.

We go on to consider global antitrust and ESG developments that are influenced by the political and economic priorities of different governments. **Antitrust regulators** are using sophisticated tools to track potentially adverse behaviour and are focusing on a wide variety of consumer harms as well as on critical infrastructure. However, growth imperatives and geopolitical factors mean that some strategic M&A transactions may be looked on relatively favourably.

The latest regulatory shifts on **climate change and sustainability reporting** offer a welcome reduction in burdens, but they have not reduced underlying risk. Climate impacts, litigation, greenwashing enforcement and fragmented reporting expectations continue to intensify – often away from public debate.

Finally, we look at impending developments in **UK employment law** that will affect all UK employers, and how employers can plan ahead, and we explore strategic options for companies with **defined benefit pension schemes** as funding positions and legislation evolve.

Governance is a theme we come back to time and again. Our strapline – the "governance premium" – is saying not just that governance matters (it always has), but that strong foundations build resilience and aid clearer decision-making in an uncertain world.

We hope that the practical steps and considerations highlighted in this publication will be useful to you. Please contact any of the authors – or your usual Linklaters contact – if you would like to discuss any of the topics further.



Daniel Law
Partner, London
Tel: +44 20 7456 2729
daniel.law@linklaters.com



Rita Teo
Managing Associate, London
Tel: +44 20 7456 4355
rita.teo@linklaters.com



EU digital package: What sponsors need to price, plan and prioritise

The EU's expanding digital regulatory framework presents a complex and fast-moving mix of compliance obligations and commercial opportunities for financial sponsors with interests in Europe. It demands attention at every stage of the investment lifecycle: from initial screening and due diligence through to exit planning. It is now common to see sponsors seeking to measure and manage the framework's impact on current and potential investments, and to opportunity spot for the future. For sponsors, these developments are no longer abstract regulatory considerations: they affect diligence scope, valuation assumptions, covenant packages, post acquisition investment plans and exit timing.

The regulatory landscape

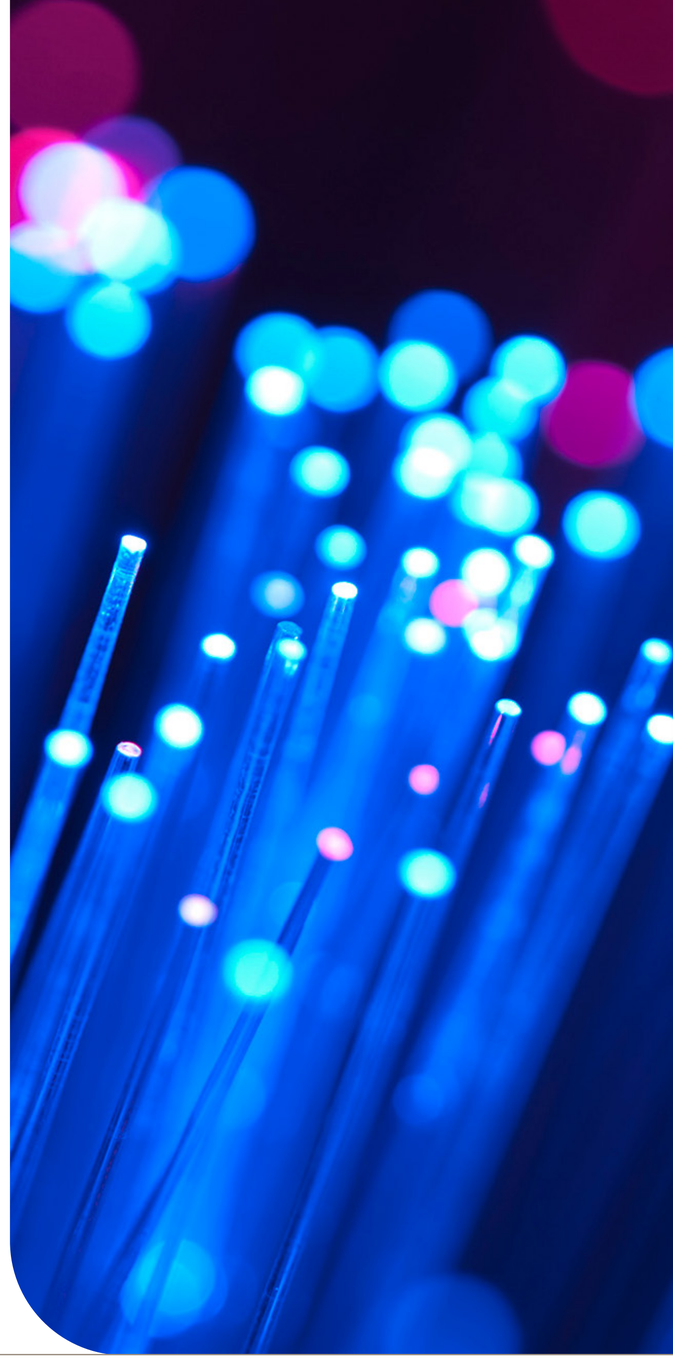
The EU's digital package encompasses a broad and interlocking set of legislation, each with distinct implications depending on the nature of a portfolio company's activities. Not every element will be relevant to every investment, but certain regimes may prove to be decisive in deal selection, pricing and value creation planning.

Every cloud has a silver lining: The Data Act introduces obligations on cloud service providers to remove commercial and technical barriers that prevent customers from switching to competing providers. It mandates data portability, interoperability, and the progressive elimination of egress charges, with switching fees required to be phased out entirely by 2027. Beyond cloud switching, the Data Act has potentially far-reaching implications for companies that generate or hold data from connected products (such as vehicle or electronics manufacturers). It effectively provides that data generated by a connected product belongs to the user of that product, not the company holding the data. Users have the right to port such data free of charge (with only limited charges potentially applicable to data recipients), and some data may be required to be licensed on a fair, reasonable and non-discretionary basis. For sponsors with investments in data-rich businesses, cloud, SaaS, IoT or data licensing businesses, or portfolio companies heavily reliant on such services, these provisions have the potential to reduce the value of proprietary databases, as companies holding connected product data can no longer treat it as their own or use it as they see fit. Understanding how these obligations affect competitive positioning and projected revenue is essential.

The AI's the limit: The AI Act introduces a tiered, risk-based compliance framework classifying AI systems according to their potential for harm. Few companies will deal with prohibited AI, but many will deploy AI in at least some high-risk contexts, such as HR, credit scoring, critical infrastructure and healthcare. Where an AI deployment is high risk, significant and costly compliance obligations will apply, including in connection with transparency, human oversight, technical documentation and conformity assessments. If high risk AI is at the core of an asset's business model, the cost and complexity of achieving compliance should be factored into valuation and value creation planning from the outset – also see our article Agentic AI: What sponsors and portfolio companies need to know when systems start to act.

Size matters – the platform advantage: The Digital Markets Act and Digital Services Act impose far-reaching obligations on the largest digital platforms – designated "gatekeepers" and "very large online platforms" respectively. In practice, direct applicability to portfolio companies will be relatively rare, but sponsors investing in large consumer-facing platform businesses should monitor whether portfolio companies are approaching designation thresholds, as the consequences are significant and disruptive.

Breaching new ground: NIS II expands mandatory cybersecurity obligations to a wider range of sectors, introducing more stringent incident reporting requirements and board-level accountability. In the financial sector, DORA layers additional sector specific digital operational resilience obligations on top of NIS II. The Cyber Resilience Act extends cybersecurity



requirements to products with digital elements, imposing new obligations on hardware and software manufacturers around secure design and ongoing vulnerability management. If relevant controls are not already in place, compliance costs (as well as potential fines) may be substantial – see our article Ransomware, resilience and regulation: The cyber challenge for companies.

Sovereign ground, sovereign gains: Given the current geopolitical environment, there is growing pressure to reduce dependence on non-EEA technology vendors and continued GDPR enforcement around transborder data flows. This is forcing some businesses to invest more heavily in onshore data infrastructure and to re-evaluate supplier arrangements. This can come with a heavy price tag.

Gig's up – platform employment: The Platform Work Directive creates a rebuttable presumption of employment for workers engaged through digital labour platforms, potentially reclassifying independent contractors as employees with significant implications for cost bases, headcount, and business model assumptions. It also introduces strict rules on the use of algorithms to manage the activities of platform workers. Although not yet transposed into national legislation, from the end of 2026 it will have far-reaching financial consequences for any business with a gig or platform-based workforce model.

With risk comes opportunity

The EU's digital agenda is not solely a source of risk. Demand for European data centre capacity is expected to surge, driven by data sovereignty requirements and AI compute demands, creating compelling infrastructure investment opportunities. The EU Health Data Space opens new commercial avenues for businesses in life sciences, health technology, and medical research. In addition, the broader harmonised digital single market offers genuine scalable, cross-border growth for compliance-ready businesses, with regulatory conformity increasingly a competitive differentiator rather than merely a cost of doing business. The imposition of obligations placed on some of the largest platforms by the Digital Package may also unlock opportunities for smaller or newer businesses operating on those platforms, enhancing their competitive positioning and commercial reach.

A global trend

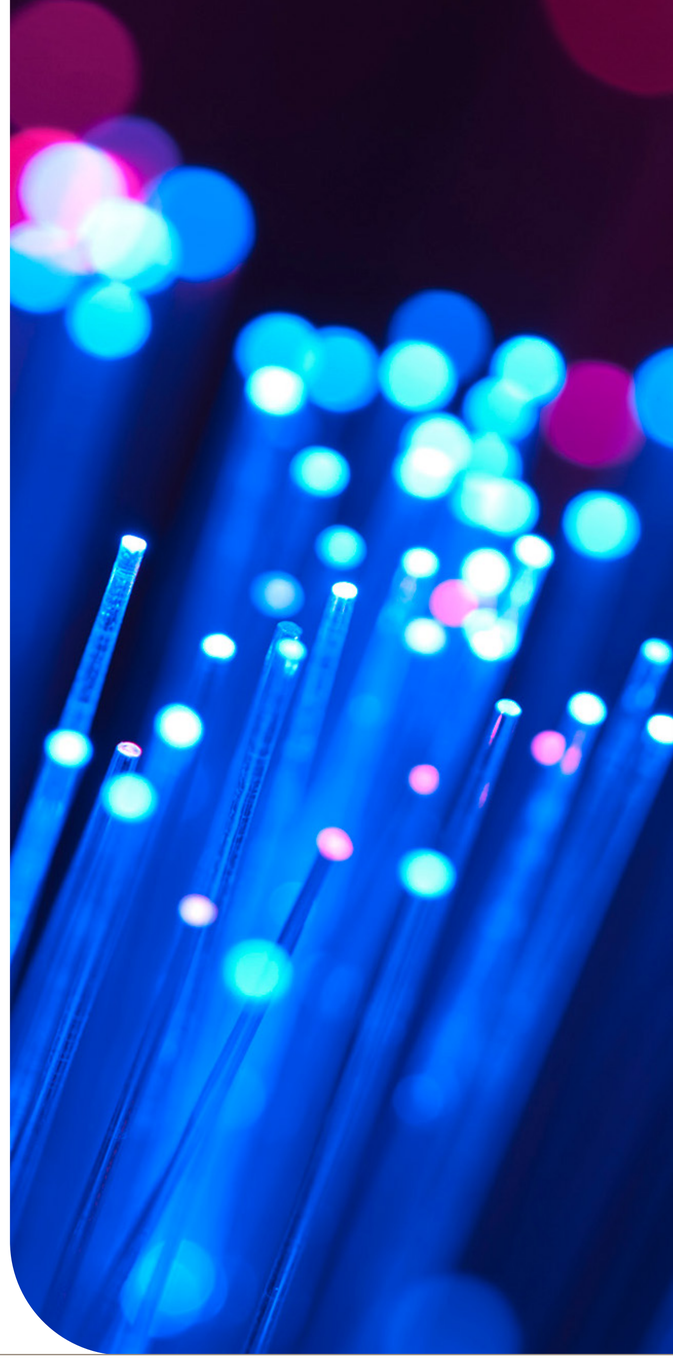
The EU is not acting in isolation. Some analogous laws are emerging to different degrees across other regions. Sponsors and portfolio companies should be alert to the risk of regulatory fragmentation and the compliance complexity that comes with navigating overlapping, and sometimes inconsistent, digital regulatory regimes across borders.

Navigating the balance

Sponsors face a nuanced balancing exercise between regulatory compliance costs and enforcement exposure on the one hand, and the scalable growth opportunities of a well-regulated digital single market on the other. The key lies in assessing how the EU digital regulatory landscape affects your portfolio companies' risk profiles, operational strategies, and long-term value – and in building those considerations deliberately into investment decisions from the outset.

Explore more

- At-a-glance: a guide to the EU Digital Package
- The EU Platform Work Directive: Recent developments and practical implications
- Digital Regulation and Technology Projects
- DigiLinks



PRACTICAL CONSIDERATIONS FOR SPONSORS

Against this backdrop, sponsors should be embedding the following steps into their investment processes:

1. **Digital regulatory due diligence:** Map the target's use of AI systems, IoT, cloud infrastructure and data, and its cybersecurity posture, against applicable regulatory requirements. Quantify the cost of any remediation required to achieve compliance and size any enforcement risks.
2. **Review and stress-test contracts:** Consider whether you have a "house" strategy in relation to digital regulation (including on key commercial questions arising under the Data Act) and provide training to portfolio companies accordingly.
3. **Assess cybersecurity governance:** Ensure that portfolio company boards have appropriate oversight mechanisms in place and that incident response and reporting procedures are fit for purpose.
4. **Audit workforce classification:** Where relevant, model the potential financial and operational impact of worker reclassification under the Platform Work Directive as part of due diligence for any platform or gig economy business.
5. **Factor data sovereignty into operational planning:** Understand what risks and opportunities the current debates around data sovereignty brings. Consider whether any new requirements might be procured at scale across your portfolio.
6. **Monitor the EU Digital Omnibus:** Track developments in the EU's targeted deregulation agenda, which may ease compliance requirements in specific sectors or open new commercial opportunities.

Contacts



Sonia Cissé
Partner, Paris
Tel: +33 1 56 43 57 29
sonia.cisse@linklaters.com



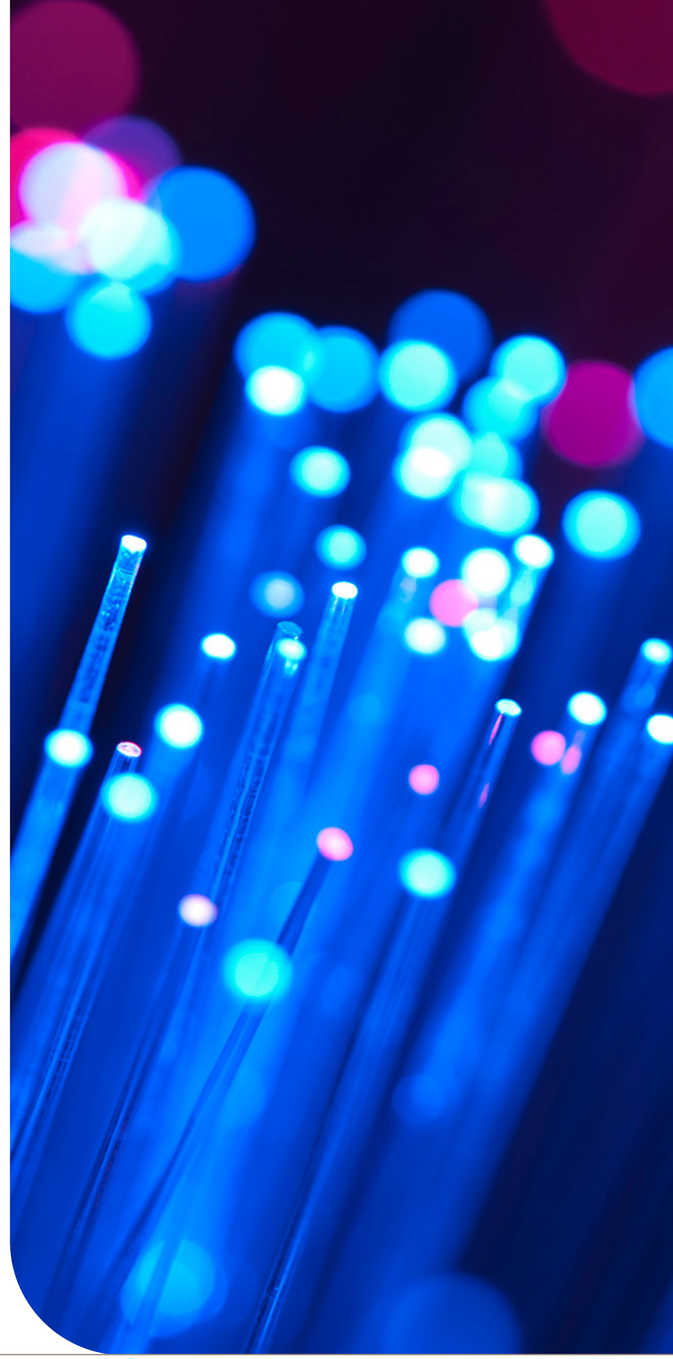
Guillaume Couneson
Partner, Brussels
Tel: +32 2 501 93 05
guillaume.couneson@linklaters.com



Georgina Kon
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com



Michael Leicht
Partner, Frankfurt
Tel: +49 69 71003 463
michael.leicht@linklaters.com



Agentic AI: What sponsors and their portfolio companies need to know as systems start to act

Much of the recent focus on AI has been on content generation. The next shift is towards agentic AI: systems that can plan, decide and act with limited human input. This evolution from “AI as tool” to “AI as actor” blurs lines of accountability and raises material legal, regulatory and operational risks. For sponsors and their portfolio companies, the central question is not whether agentic AI will be used, but how much autonomy is acceptable, in what circumstances, and with which controls – all before these systems are deployed at scale. Handled well, agentic AI can unlock new efficiencies and commercial models, but only where governance foundations are strong.

The next evolution in AI – and the commercial potential

Generative AI, now familiar to many in work and at home, remains fundamentally reactive. It generates content in response to specific prompts and relies on human direction at each step. Agentic AI goes further. Agents can execute multi-step tasks towards a user-defined goal, coordinate with other systems (and agents), and make decisions with limited human involvement.

Agentic commerce – the coordination of networks of agents to complete transactions autonomously – presents a huge commercial opportunity, particularly for consumer-facing and technology businesses. McKinsey forecasts that, by 2030, US B2C retail alone could see up to US$1 trillion in orchestrated revenue from agentic commerce, with global projections reaching as high as US$5 trillion.

Importantly for sponsors and their portfolio companies, adoption is no longer theoretical. Agents are being embedded into enterprise systems to orchestrate multi-step workflows, promising more seamless purchasing experiences, faster fulfilment and broader digital consumption. Early deployments mirror the introduction of chatbots a decade ago – initially narrow in scope, although with a steeper risk and governance profile as these systems become more deeply integrated into core enterprise processes.

A new class of digital actor inside the enterprise

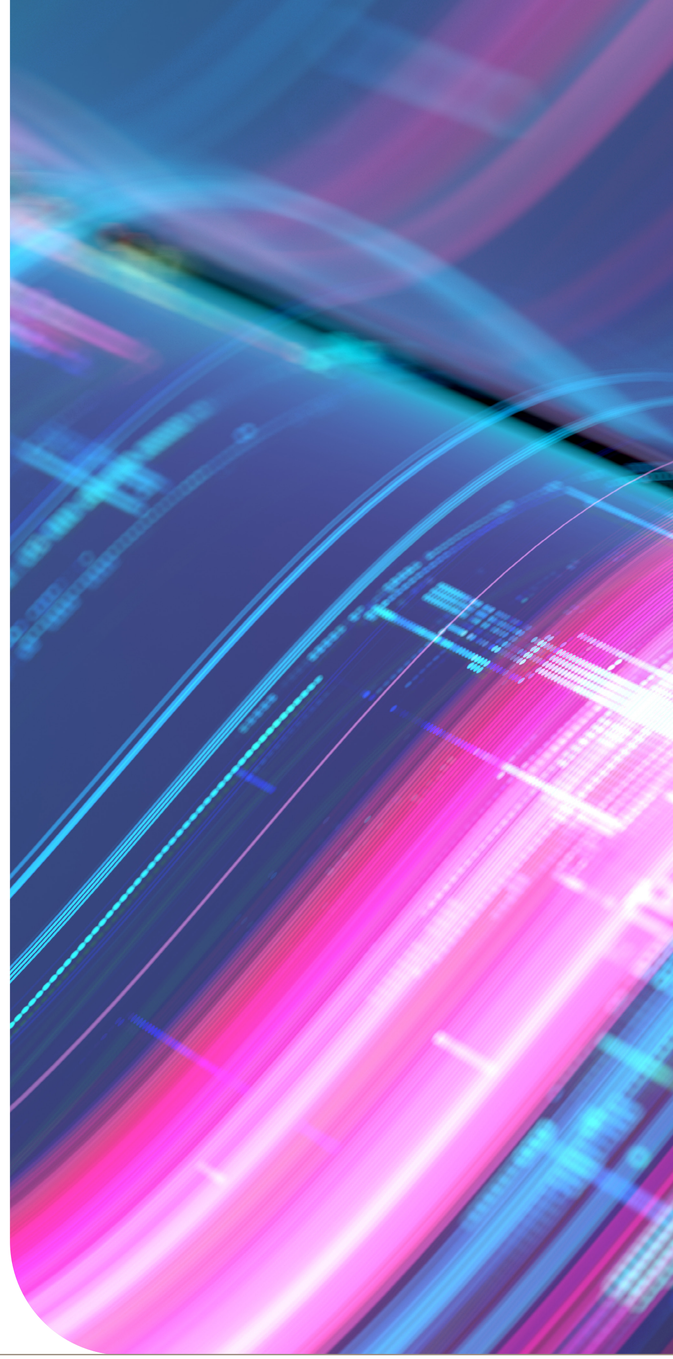
Within businesses, agentic AI is being embedded into core business functions – from customer engagement and advice, to risk management and internal operations. This is not necessarily as a result of conscious decisions by the business, but often appears as part of routine software upgrades. Companies are, in effect, opening their doors to semi-autonomous digital agents that can draft communications, schedule actions, adjust parameters, and initiate transactions.

This represents a material shift in operating model. The traditional assurance framework – with humans as the final checkpoint – no longer applies by default. Instead, organisations are introducing systems that can act on their behalf, at speed and at scale, without continuous supervision. For decision makers, the priority is visibility. They need to understand what these systems can do, how they behave and learn, and how they might fail – particularly when actions span multiple systems or have financial, operational or customer impacts.

Building on existing rails

Emerging industry protocols – such as Anthropic’s Model Context Protocol (MCP), Google’s Agent-to-Agent Protocol (A2A) and Stripe’s Agent Commerce Protocol (ACP) – provide interfaces that allow AI agents to discover products, interact with tools, communicate with other agents, engage with merchants and complete end-to-end commerce and payment flows. Meanwhile, payment networks such as Visa and Mastercard are beginning to integrate agent-led authentication mechanisms (for example, Agent Pay) into their mainstream payment systems.

Agentic systems can scale rapidly because they operate on top of existing e-commerce and payment infrastructure.



Systemic and operational risks

Four examples illustrate the systemic and operational risks associated with agentic AI:

- **Lack of transparency and auditability:** Agentic systems follow machine readable instructions rather than human friendly interfaces. Even with emerging audit features built into new protocols, it can remain difficult to trace what has happened and why. This heightens longstanding "black box" concerns around transparency, accountability and potential harm.
- **Cascading failures:** Multiple-agent transactions create long chains of activities and responsibility. A small error or misconfiguration in one agent can propagate rapidly across systems before humans can intervene, leading to disproportionate operational or financial impacts.
- **Enlarged attack surface:** Agent enabled commerce increases the number of systems that connect – including APIs, tools and payment services. Bad actors can try to 'hijack' agents to trigger unintended actions. A compromised agent can move at speed and cause significant harm.
- **Agent sprawl:** As agentic AI systems proliferate across business units, organisations risk losing sight of how many agents they have, what they do and how they are governed. Without a central inventory, clear categories and consistent controls, organisations can end up with uneven oversight and too much autonomy in the wrong places.

Regulatory gaps and evolving expectations

Most legal frameworks presuppose a human decision maker at critical junctures. As AI systems take on more autonomy, established norms around consent, liability, IP and data governance become harder to apply and questions of accountability and security sharpen.

Existing AI-related laws, consumer protection regimes, and sector-specific regulations can all apply to agentic AI, **but none were designed with autonomous machine to machine execution in mind**. Regulatory frameworks will therefore need to evolve. Expectations are already tightening, with regulators signalling a focus on accountability, transparency and enforceable controls.

The EU's AI Act represents the most ambitious regulatory response to AI, but predates agentic commerce and lacks provisions for autonomous purchasing agents. EU regulators are starting to move to address the gaps. Antitrust regulators are also increasingly attentive to risks of autonomous collusion in pricing and contractual arrangements. The UK's Information Commissioner's Office has made it clear that agentic AI must still comply with UK GDPR requirements, including accuracy, transparency, data minimisation, and safeguards around automated decision making.

Though some states are starting to turn their attention to AI regulation, the US has no specific federal law explicitly addressing agentic AI. Standard setting body, NIST, is, however, likely to revise the AI Risk Management Framework (a voluntary set of guidelines) to include considerations for agentic AI.

The role of decision makers

Agentic AI raises fundamental questions about decision-making, accountability and the effectiveness of internal controls, especially where systems can act without continuous human supervision. Decision makers will need confidence that their control environment can accommodate this shift.

Decision makers should anticipate closer scrutiny of: the adequacy of human oversight and auditability; fairness and transparency in automated consumer interactions; robustness of consent capture and withdrawal; governance of third party AI developers and model providers; and exposure to systemic risk in payment and commerce chains.

Emerging protocol guidance offers some built-in safety features – confirming an agent's identity, checking user intent and keeping clear audit trails. It also encourages common standards and limited permissions, helping to contain problems and simplify monitoring or shutdown if something goes wrong. These measures reduce risk but do not remove it; organisations remain responsible for governance, oversight and enforceable controls.



From theoretical to actual risks

Investors, employees, customers, and regulators increasingly expect companies to explain how AI is governed, not simply whether it is used. Failures involving autonomous systems can rapidly escalate into reputational and regulatory issues.

There are already documented instances of agent misalignment, over execution, or unintended outcomes. Regulatory enforcement and lawsuits are beginning to follow – most notably in the United States where regulators are treating chatbot failures and agent misrepresentation as actionable. A notable shift is emerging: regulators are attaching responsibility not to intent, but to faulty design choices, oversight mechanisms or risk mitigation controls.

What should businesses be doing differently now?

Agentic AI introduces new risks arising from reduced human oversight, complex multi-system orchestration and the emerging industry protocols (see box on page 7) that enable autonomous action at scale. While these standards are maturing quickly, they do not diminish organisational responsibility for governance, accountability and control – especially if you are talking publicly about what your technology can do.

Sponsors and portfolio companies should approach agentic AI not only as a future opportunity but as a current source of operational, legal, regulatory and reputational exposure. The governance task is to set clear autonomy thresholds, harden controls and contracts, and demonstrate – through active monitoring and audit – that your agents act only within defined boundaries and on your terms. Governance is not a brake on agentic AI: it is what ensures these systems amplify capability without compromising control.

Explore more

- Agentic AI – The next evolution
- Digital commerce redefined – The growing impact of agentic commerce
- Agentic payments: Reshaping online shopping around the regulatory perimeter
- The rise of the digital employee – Navigating employment law risks in the age of agentic AI

FIVE ACTION POINTS TO CONSIDER

1. **Establish agentic AI policies:** Determine which decisions can be delegated to AI, under what conditions and with what human oversight – and ensure that these are reflected in formal policies, at both sponsor and portfolio levels, with clear agent classification and ownership.
2. **Strengthen governance:** Set defined autonomy levels, decision boundaries and prohibited activities for each agent, underpinned by robust data governance (conducting Data Protection Impact Assessments for higher risk uses), privacy compliance and thorough documentation of decision-making pathways.
3. **Tighten AI developer contracts:** Ensure that agreements with AI developers clearly allocate responsibility for authorised and unauthorised agent behaviour (with explicit liability clauses), and secure strong IP indemnities as well as audits, warranties and other assurances for external AI tools as part of due diligence.
4. **Update customer facing terms:** Portfolio companies should revise contracts and templates to explicitly address agentic transactions, disclose agent involvement, clarify the scope of agent authority, and include opt-out mechanisms and remediation windows as standard.
5. **Continuous monitoring and auditing:** Track agent activity in real time, conduct regular "Know Your Agent" reviews, and maintain kill-switch and circuit breaker capabilities to contain incidents quickly.

Contacts



Julian Cunningham-Day
Global Head of Technology, Media and Telecoms/Intellectual Property, London
Tel: +44 20 7456 4048
julian.cunningham-day@linklaters.com



Sonia Cissé
Partner, Paris
Tel: +33 1 56 43 57 29
sonia.cisse@linklaters.com



Ieuan Jolly
Partner, New York
Tel: +1 212 903 9574
ieuan.jolly@linklaters.com



Georgina Kon
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com

Contributing author



Jennifer Calver
Tech Sector and Fintech Counsel (Knowledge), London
Tel: +44 20 7456 2417
jennifer.calver@linklaters.com

Ransomware, resilience and regulation: The cyber challenge for companies

Cyber-attacks are now an almost inevitable challenge for organisations. What is changing is the environment in which decision makers must take action. Some governments – including the UK – are actively considering restrictions or even bans on ransomware payments in certain sectors. Meanwhile NIS II and DORA are hardening expectations of board-level oversight and accountability. Sponsors and portfolio companies will need to ensure their governance and decision-making frameworks keep pace with this fast-moving landscape.

> *"… for business leaders… there are the sorts of things that you have to go through as part of your rite of passage. A hostile takeover, an activist attack, probably a boardroom scandal… These are warp and weft of business stress, and a cyber-attack is part of that"*
>
> **Sir Archie Norman, The Rest is Money podcast (Episode 235)**

No end to the cyber threat

No one needs reminding of the risks. Jaguar Land Rover's cyber-attack last year cost it more than £250 million, with supply-chain disruption so severe that the UK Government provided a £1.5 billion loan guarantee to prevent wider fallout. The total estimated impact on the UK economy was £1.9 billion.

Most attacks originate from financially motivated ransomware gangs but today's geopolitical turbulence means that state actors are increasingly active – both providing tacit support to the ransomware gangs and directly engaging in hybrid warfare. Critical infrastructure providers are particularly exposed to this grey-zone conflict.

No organisation is immune or should assume its defences are impenetrable. The task for key decision makers is to be ready for the critical choices that follow an attack – particularly where ransomware is involved.

The ransomware dilemma – and the potential tightening of rules around payment

One of the most difficult decisions in that moment is how to respond to a ransom demand. Paying a ransom is morally fraught: it enriches criminals who have damaged your business and perpetuates the business model. Put simply, if everyone stopped paying ransoms, the ransomware market would dry up overnight.

But if your computers are locked up, your business might cease to function. If third parties have exfiltrated your data and are threatening to publish it, that could have a devastating effect on your company.

The decision whether to pay up is incredibly difficult. It's unlikely you can script the decision in advance, but decision makers can think through the factors that will shape it.

A key factor is legality. Governments and regulators discourage ransomware payments[1] and significant care is needed to ensure that the payment is not to a group that is either sanctioned or connected with terrorism. However, there are calls for legislators to go further. The UK Government is currently considering proposals to ban ransomware payments by those in the public sector or providing critical national infrastructure. This would be coupled with an obligation on all ransomware victims to report an intention to pay, with an ability for the Government to then block that payment. These proposals are controversial – an outright ban on payments sounds tough on crime, but could turn a solvable crisis into a catastrophe.



1 In the UK, the National Cyber Security Centre and Information Commissioner have jointly stated companies should not pay ransomware demands. Their view is that this does not reduce the risk to individuals and is not considered as a reasonable step to safeguard data. The position is much the same in the US, with agencies such as the Federal Bureau of Investigation and Department of Justice advising against payments.

Rising board accountability: Training, oversight and personal exposure

The regulatory environment is also shifting to reinforce cyber as a "board-level issue". For example, the EU's recent NIS II Directive applies to a wide range of critical sectors including manufacturing, postal services and food production. It explicitly obliges management boards to be trained on cyber so that they can identify risks and assess cyber security. Similar obligations apply to financial services firms under EU DORA.

After an incident, management bodies may face scrutiny and spotlight. The NIS II Directive gives regulators the power to suspend managers if they fail to implement appropriate cyber defences. Managers can also be personally liable in the event of a breach, with some national laws under NIS II applying significant fines and even imprisonment.

Sponsors should therefore focus on the strength of their cyber defences as well as those of their portfolio companies, and the culture they set from the top. Whether the threat of personal liability drives better security remains to be seen, but decision makers should assume their oversight will be examined after any major incident and ensure they can demonstrate effective governance and challenge.

Will new laws stop cyber-attacks? Regulation's role — and its limits

These new board-level obligations sit alongside a growing body of wider cyber regulation such as the EU Cyber Resilience Act (new obligations on suppliers of software and hardware), and the UK's Cyber Resilience Bill (new obligations on providers of critical infrastructure).

But law is not magic. Regulation can help drive the right investment and testing of defences, but tougher rules alone will not deter determined attackers. Simply increasing sanctions on the victims of traumatic cyber-attacks may not achieve the desired outcome.

Sponsors and portfolio companies should track developments — especially any restrictions on ransomware payments — and ensure their organisation is genuinely prepared for what is now, in effect, a corporate rite of passage.

> *"… all boardrooms have rehearsed for cyber. They've had red team attacks, they've had role plays and sophisticated consultants come in and talk you through what has happened. But nothing prepares you for the first whiff of gunshot"*
>
> **Sir Archie Norman**

Explore more

- The essential cyber security handbook for in-house counsel
- UK Government's Cyber Governance Code of Practice

SEVEN ACTION POINTS TO CONSIDER

1. Identify which **board committee** is responsible for cyber security. Consider commissioning privileged cyber risk and governance assessments, ensuring that subcommittee structures, minutes, and response plans demonstrate robust cyber controls.
2. Arrange for **training** on cyber security (noting this is a legal requirement for some companies).
3. Ensure that you have suitable board **reporting metrics** on cyber issues. Ensure training, updates and opportunities to influence.
4. Review and interrogate your **information security programme** to set out your overall stance on cyber.
5. Create and test your **incident response plan**, including your position on paying ransoms.
6. Track the wider regulatory framework, including potential new laws on **ransomware payments**.
7. Ensure that compliance with your information security programme is **audited** and **enforced**.

Contacts



Georgina Kon
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com



Greg Palmer
Partner, London
Tel: +44 20 7456 2925
greg.palmer@linklaters.com



Daniel Pauly
Partner, Frankfurt
Tel: +49 69 71003 570
daniel.pauly@linklaters.com



Caitlin Potratz Metcalf
Senior Associate, Washington, D.C.
Tel: +202 654 9240
caitlin.metcalf@linklaters.com

Contributing author



Peter Church
Counsel, London
Tel: +44 20 7456 5495
peter.church@linklaters.com

Are stablecoins the answer to painful payments?

Cross-border payments remain slow, expensive and constrained by legacy infrastructure. Stablecoins – digital tokens pegged to traditional currencies or assets – offer one potential alternative, particularly for organisations with international payment flows or more complex treasury operations.

Even if stablecoins are not on today's agenda, sponsors and portfolio companies should be alert to how evolving regulation, customer expectations and treasury innovation could shape future payment strategies.

The potential of stablecoins

Moving money around the world has never been pain-free. Cross-border payments are known for being slow and costly. Technological and regulatory developments are enabling alternatives. Stablecoins are one of the innovations attracting growing interest from businesses and individuals seeking cheaper and faster payments, especially across borders.

Stablecoin use is on the up. Citi has estimated that the volume of stablecoins in issuance will grow from around US$0.28 trillion today to nearly US$2 trillion by 2030, driven by regulatory clarity and adoption by corporates and financial institutions.

Stablecoins have long played an important role in cryptoasset markets. They have also proved popular in parts of the world where access to banking infrastructure is limited or where volatility in the local currency makes payments in dollar-linked assets attractive.

New regulatory frameworks for stablecoins and market developments – including emerging stablecoin-related payment services and systems – could support further demand from corporates and individuals. Some central banks that have in the past been sceptical of stablecoins, including the Bank of England, now see a place for regulated stablecoins in a "multi money" system where new and traditional payment rails co-exist.

This shift means sponsors are increasingly likely to face questions about their portfolio companies' policies towards stablecoins. Some organisations may consider accepting stablecoins for payments from customers. Others may also use them to make payments to suppliers, facilitate FX trades or even issue their own stablecoins. Treasury functions may also explore using stablecoins to support intragroup liquidity or reduce settlement friction in cross-border operations.

For sponsors, the strategic question is not whether stablecoins will replace existing payment systems but whether they could offer your portfolio companies – or their competitors – a meaningful advantage, and what steps you should take to manage the associated risks.

Managing risks

Stablecoins can use different mechanisms to stabilise their values against a reference asset. Some are backed by rights against an issuer or reserves of money or very liquid securities that are held in custody. Others use algorithmic mechanisms to maintain their value. These structural differences affect:

- the holder's legal rights;
- how the token is regulated; and
- what happens if the stablecoin issuer, or the custodian of its backing assets, becomes insolvent.

The stability of the peg against the referenced asset or currency is a core concern. There have been high-profile examples of stablecoins losing connection with their referenced asset, such as the TerraUSD collapse in 2022. De-pegging can result from cyber or operational incidents, or from a loss of market confidence linked to the issuer or its reserves.

Businesses can choose to deal only with stablecoins with lower risk profiles or structure their stablecoin arrangements to share or reallocate de-pegging risks. This may involve due diligence of the structures of different stablecoins and related market infrastructure, such as trading venues and custodians. It may also involve careful negotiation of the contractual and other commercial arrangements between the parties.



Regulation can help manage risks. Frameworks like the EU's Markets in Crypto-Assets Regulation and the UK's regulatory regime for stablecoins and other cryptoassets, which starts to apply in October 2027, introduces minimum standards for issuers and service providers.

Organisations should also consider the wider implications of using stablecoins. In March 2026, the intergovernmental Financial Action Task Force warned that stablecoins have become a common part of money laundering schemes. Even as they become subject to tighter regulatory scrutiny, sponsors should consider the compliance, operational and reputational exposure for portfolio companies, and take advice on other aspects such as accounting and tax treatment.

Sponsors and portfolio companies should ground any exploration of stablecoins in a clear-eyed understanding of legal rights, counterparty risk, regulatory expectations and potential reputational consequences so that innovation in payments does not outpace the organisation's risk appetite or controls.

Anticipating the digital money future

Stablecoins are not the only development in digital money. Banks are exploring tokenised deposits, designed to achieve certain operational efficiencies within existing regulated banking infrastructure. Several central banks are issuing their own forms of digital money.

Sponsors and portfolio companies should anticipate a future where multiple digital forms of money coexist. Each will carry different benefits, risks and operational consequences.

While stablecoins are unlikely to replace existing payment systems, they may offer targeted advantages for some organisations, such as those with extensive cross-border flows or complex treasury operations. For others, they may remain peripheral. Organisations with plausible use cases will benefit from having a clear, risk-based policy so that they are ready to respond as the market evolves.

FOUR QUESTIONS FOR YOU TO CONSIDER

1. Have you considered whether stablecoins or other digital forms of money could deliver meaningful **efficiency gains** in your portfolio operations?
2. Have you considered your **portfolio companies' policies towards accepting stablecoins** – or making payments using them – if requested by a customer or supplier?
3. Have you considered how **regulatory developments** in the jurisdictions in which your portfolio companies operate may drive demand for making or receiving payments in stablecoins over the coming years?
4. Have you put in place a **policy framework across your portfolio companies** for assessing the risk profiles of different stablecoins and how de-pegging and other risks should be allocated among your counterparties?

Contacts



Andreas Dehio
Partner, Frankfurt
Tel: +49 69 71003583
andreas.dehio@linklaters.com



Harry Eddis
Partner, London
Tel: +44 20 7456 3724
harry.eddis@linklaters.com



Richard Hay
Partner, London
Tel: +44 20 7456 2684
richard.hay@linklaters.com



Peiying Chua Heikes
Partner, Singapore
Tel: +65 6692 5869
peiying.chua@linklaters.com

Contributing authors



Simon Treacy
Counsel (Knowledge), London
Tel: +44 20 7456 2451
simon.treacy@linklaters.com



Sophia Le Vesconte
Counsel (Knowledge), London
Tel: +44 20 7456 3892
sophia.le-vesconte@linklaters.com

A transcript too far? When to use AI for records of meetings

Sir Humphrey Appleby: *Bernard, the minutes do not record everything that was said at a meeting, do they?*

Bernard Woolley: *Well, no, of course not.*

Sir Humphrey Appleby: *. . . the actual meeting is a mass of ingredients for you to choose from. . . You choose from a jumble of ill-digested ideas a version which represents the Prime Minister's views as he would, on reflection, have liked them to emerge.*

Bernard Woolley: *But if it's not a true record...*

Sir Humphrey Appleby: *The purpose of minutes is not to record events. It is to protect people... You try to improve on what has been said; put it in a better order. You are tactful.*

Yes, Prime Minister ("Official Secrets")
BBC TV 1980 political satire series.

Why boards record decisions

Sir Humphrey's explanation of minute-taking may be satire, but it captures an uncomfortable truth: board records are not neutral artefacts. They shape how decisions are understood, justified and, in some cases, challenged long after the event.

Unlike Sir Humphrey's approach, good corporate governance requires minutes to provide an accurate, impartial and balanced record of directors' decision-making. Most countries impose a legal duty on companies to keep minutes of board meetings – indeed, in some countries, failure to do so is a criminal offence. Minutes also help demonstrate that directors have fulfilled their statutory duties.

That said, there is little doubt that preparing minutes is an art, not a science – and a time-consuming one. With AI now offering transcription and summarisation capabilities, board minute-taking may seem ripe for automation. But deciding whether to "hit record" is not an administrative convenience or a matter for the Company Secretary alone. It is a governance choice, with implications for boardroom candour, regulatory scrutiny, litigation risk and personal exposure for directors.

The question for boards at both sponsor and portfolio levels is not whether AI can capture their discussions, but whether – and on what terms – it should.

Accuracy and context: The limitations of AI automation

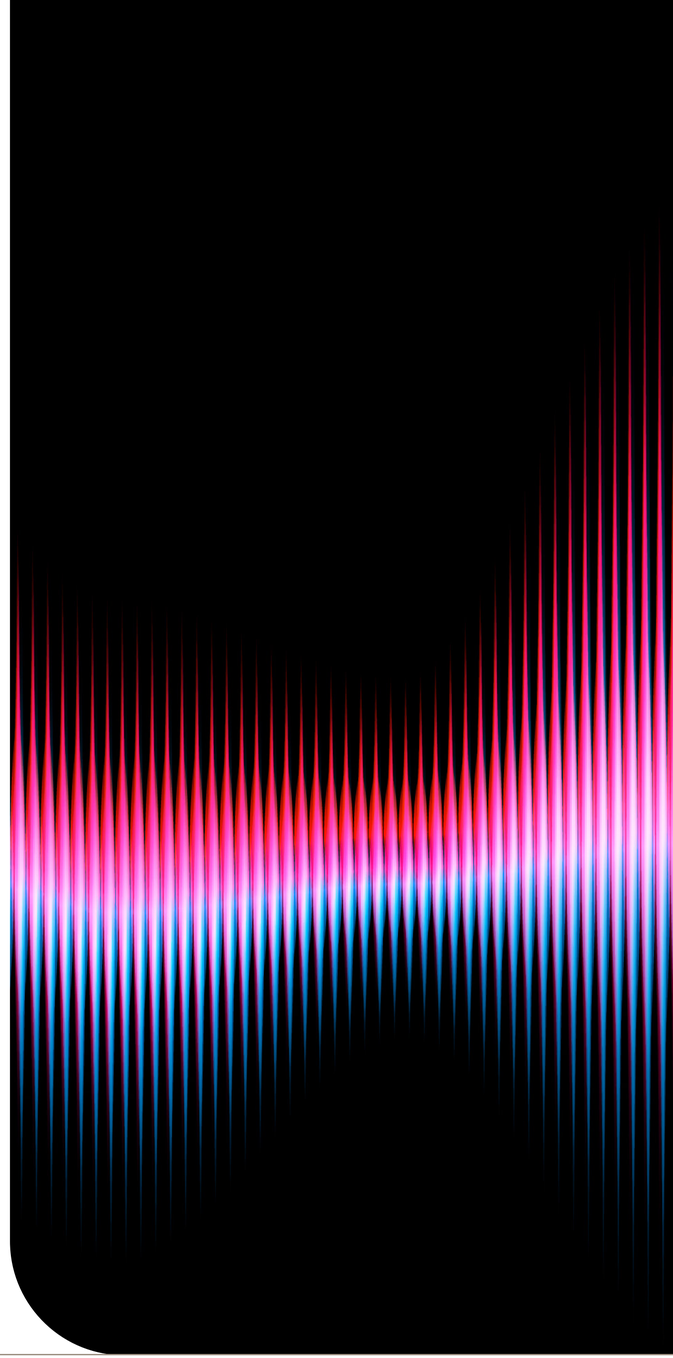
AI transcription tools can now produce (relatively) accurate records of meetings, identify action points and assign responsibilities. The output is readable and highly convincing – which is precisely the risk: errors may not be obvious without careful reading.

In our article Ransomware, resilience and regulation: The cyber challenge for companies above, we quote M&S Chairman Sir Archie Norman's description of a cyberattack as part of the "*warp and weft*" of business life – the transcription tool on Spotify records this as "*the weapon morphed*".

If this mistranscription is easy to spot, then many others are not. When transcribing a conversation, the tools will listen and then calculate the most plausible set of words in that context. It's all too easy for a reader to skim over the output without noticing the flaws.

Once adopted, board minutes will generally be treated as conclusive evidence of proceedings. Courts and regulators will have little or no sympathy for attempts to blame AI for errors.

AI summarisation tools are similarly impressive – but probably not good enough for board minute purposes. Writing minutes is a deceptively difficult art form rather than an administrative formality. A healthy board discussion approaches issues from multiple directions and with many different solutions. Accurately recording the *consensus* is not a mechanical process but one that requires awareness of context, legal obligations, potential sensitivities and directors' personalities.



Accurate recording can also have a "chilling effect"

The problem may equally be that these tools **do** fully record every word that was said. Creating a verbatim record may not be wise as it can create a barrier to the frank and open exchanges that effective boards require. It is difficult to maintain that safe space if every word is captured for subsequent forensic examination by regulators, acquirers or claimants. The UK's Chartered Governance Institute suggests it is only desirable in very rare circumstances.

The risk is real: late last year the English High Court had to pick through the messy history of a disputed warrant instrument. Part of that historical record included an AI-generated transcript of a board meeting, complete with some X-rated exchanges. The judge described the comments as "revealing" – the board would have been more likely to describe them as "unhelpful".

Other issues – "Off by default"

Beyond these general points are other practical and compliance issues.

- **Partial attendees.** Some AI transcription tools make the transcript of the **whole** meeting available to **all** the attendees, even if they were present only for part of the meeting. This creates an obvious risk of embarrassment.
- **Data protection, confidentiality and privilege.** In some jurisdictions, such as Germany, there is a requirement to obtain consent from all attendees before recording or transcribing a meeting. In any event, this will engage the requirements of the GDPR, and may require a data protection impact assessment. Similarly, creating and circulating a transcript of the meeting can create wider confidentiality and privilege concerns.
- **Not playing by the rules.** The recording of a video meeting is normally signalled by an on-screen warning. However, the recording might not always be obvious (for example, if there is a hybrid meeting with only some people dialling in), so it is useful to have clear guidelines for all participants about whether a transcription is permissible.

Conclusion: Why restraint is a governance choice

AI transcription and summarisation tools are readily available and – with appropriate compliance measures – can be useful. However, board minute-taking requires particular caution.

An AI-generated transcript may assist with drafting minutes for a limited period before being deleted in accordance with a retention policy. But the default position for board meetings at both sponsor and portfolio levels should be that AI tools are not used unless directors have consciously considered the legal, cultural and risk implications. In an environment of increasing scrutiny of board decision-making, how a board records its own words may matter as much as the decisions themselves.

FIVE KEY ISSUES TO NOTE

1. **Conclusive evidence:** Once adopted, board minutes are generally treated as conclusive evidence. Courts and regulators will have little sympathy for attempts to blame AI for errors.
2. **Confidentiality and legal professional privilege:** AI transcriptions create a permanent record of sensitive discussions that could be shared long after the event, risking breaches of confidentiality and legal professional privilege.
3. **Data protection:** AI tools involve processing personal data, engaging data protection laws and likely requiring a data protection impact assessment.
4. **Local law requirements:** Some jurisdictions require consent from all attendees before any recording or transcription.
5. **Practicalities:** Consider the risk of the transcript being available to partial attendees or of some participants recording the meeting without the awareness of the rest of the board.

Explore more

- AI Transcription in the Workplace: Managing Legal Risk
- IOD: AI Governance in the Boardroom
- AI: Transforming Professional Practices

Contacts



Lucy Fergusson
Partner, London
Tel: +44 20 7456 3386
lucy.fergusson@linklaters.com



Wilma Rix
Counsel, London
Tel: +44 20 7456 4914
wilma.rix@linklaters.com

Contributing author



Peter Church
Counsel, London
Tel: +44 20 7456 5495
peter.church@linklaters.com

Antitrust enforcement gets political – the winners and losers

Politics is increasingly shaping antitrust enforcement globally. Focus on national economic growth appears to have reduced rates of intervention in M&A transactions (except where national security or resilient supply chains are at stake). But enforcement has intensified in areas that carry the strongest political salience – anything touching consumers or the use of public funds. Understanding where political priorities are driving enforcement – and where they may soften it – is essential to navigating deals and compliance risks.

Enforcement hotspots

Focus on consumers and cost-of-living crisis

Globally this has translated into stronger intervention in areas that send the most powerful political message – in particular, tackling conduct that affects everyday spending for consumers or involves the use of public funds. For sponsors and portfolio companies, this is where competition/consumer risks are most likely to crystallise quickly – and publicly.

In the UK, the CMA gained new consumer direct enforcement powers last year, which allow it to impose sanctions without going through the courts, with fines of up to 10% of global group turnover possible. The CMA has indicated that it is developing customised agentic AI to detect consumer harms at scale. It will focus on companies that provide false information to consumers, fake reviews, hidden fees, unfair exit charges or aggressive sales practices. It launched its first investigation into online pricing practices in November, in line with its broader commitment to focus on areas of essential spend.

Elsewhere, both the European Commission and the Australian Competition and Consumer Commission have indicated a sustained focus on consumer sectors through 2026, while China has intensified enforcement in sectors linked with people's livelihoods – particularly pharmaceuticals.

Following recent developments in the Middle East, fuel prices will be increasingly in the spotlight globally as authorities seek to protect consumers from the impact. The German Federal Cartel Office is expected to be given powers to target energy firms unfairly hiking prices and the CMA is already investigating rising prices of heating oil, petrol and diesel.

Portfolio companies with consumer-facing businesses should ensure there is clear oversight of pricing, fees and sales practices, and that management can readily evidence compliance with current guidance.

Bid-rigging in public procurement

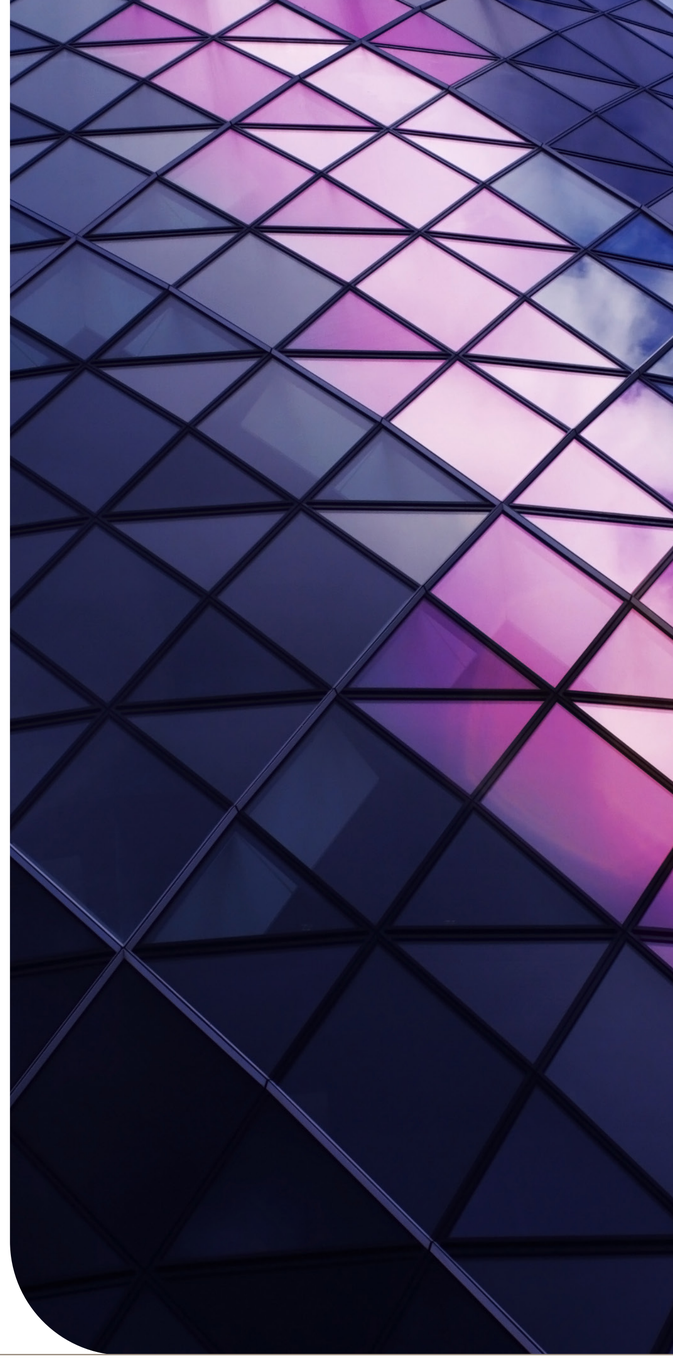
Authorities are increasingly focussed on speeding up the detection of cartel conduct; particularly in public procurement, reflecting heightened political sensitivity around the use of public funds. Some – including the CMA – have publicly confirmed their use of AI-driven detection capabilities and data screening tools to identify possible bid-rigging patterns in public procurement tender processes.

Companies involved in tenders for public or utility contracts should monitor bidding data and ensure a strict compliance policy on what is and isn't permitted

Tech enforcement under scrutiny

Digital enforcement under the Digital Markets Act (DMA) in the EU has slowed somewhat, while accusations by the US government that the DMA targets American companies, have prompted the European Commission to justify its broader enforcement in the sector. In contrast, in the US, despite the political rhetoric, technology companies and platform operators remain in the crosshairs, with enforcement actions ongoing against major tech companies.

In the UK, under equivalent digital legislation, the CMA designated the first firms with "strategic market status" last year. It has also faced criticism over being slow to act, in the face of government pressure to prioritise efforts which contribute to economic growth.



AI tools and algorithmic collusion – the new frontier

In contrast, AI services have recently seen several antitrust investigations, including in the EU (outside of the DMA) and the US, as enforcers slowly get to grips with the fast-changing landscape. As these cases progress, we expect increased global enforcement activity, alongside attempts by regulators to set out guardrails over what is permitted – particularly in relation to Big Tech companies.

The potential for convergence in decisions by competing firms, even without explicit communication or human input, also remains high on the antitrust agenda. Enforcers are paying ever closer attention to algorithmic pricing collusion – the CMA has recently launched an investigation into hotel chains and several investigations were reportedly underway at an EU-level last year. The recent RealPage settlement in the US over the use of rent pricing software offers insight into how enforcement may play out, in an area which, until now, has been largely speculative.

But decisions on who is liable will only become more complex with the advance of agentic AI, where AI agents used by companies – operating independently of human decision making – could decide to collude. While regulators are working to understand the risks, the CMA has recently published research setting out steps that businesses should take in monitoring and refining their systems to ensure they comply with competition law.

AI-enabled pricing tools should be treated as a competition-risk issue, with regular testing, clear accountability and governance. Information sharing and coordinated conduct (especially on prices) can be sanctioned, even if unintended.

M&A: A smoother ride… for now?

On the M&A front, political focus on growth is having an impact. While regulatory intervention remains likely in sensitive sectors, competition authorities are often showing greater pragmatism in how they assess and resolve non-problematic transactions – creating opportunities for businesses to scale.

In the UK, the CMA has been keen to align with the government's pro-growth mandate, making very deliberate decisions over the cases it pursues. In recent months, it has limited the number of deals referred for in-depth review, preferring earlier solutions at Phase I. It has also steered clear of reviewing global transactions with a limited UK connection, where other global authorities might be better placed to take the lead. For many deals, this should translate into greater predictability on the likelihood of UK review and an openness to finding a workable solution where issues are identified.

This more pragmatic approach should be reflected by authorities in the treatment of transactions found to promote innovation, or true "competitive efficiencies" (eg, demonstrable cost savings for consumers or improved products or services).

In the US, however, concerns have emerged that political influence may be encroaching on what are intended to be independent merger review processes. There have been allegations of lobbyists "paying-to-play" in an attempt to influence merger officials, for example in relation to the approval of the US$14 billion merger between Hewlett Packard Enterprises and Juniper Networks.

Seeing a shift towards behavioural remedies

One practical consequence of the more pragmatic approach to M&A is a renewed focus on deal remedies: clearing deals subject to targeted commitments (rather than defaulting to prohibition or prolonged litigation). The CMA has made clear that "only a truly problematic merger, where the harm … cannot be effectively addressed through remedies, should not proceed" – a stance reflected in its acceptance of behavioural remedies (which focus on modifying a company's conduct) in Vodafone/Three last year and its latest guidance on merger remedies.

We have seen this in the US too, where authorities have been openly keen to avoid "merger hostility", favouring targeted remedies to resolve competition issues (where they align with national interests) over litigation.

The European Commission will equally face pressure to embrace behavioural remedies. But in the face of digital market issues relating to interoperability and data use, it seems unlikely to change its preference for structural remedies this year.

Where competition issues are likely, sponsors should assume that remedy design and implementation capability will form part of the critical path to clearance, and should be considered early in deal planning.

Tough on critical technology and national security

But the limit to the pro-growth agenda is security and resilience. Deals that touch national security or risk eliminating essential suppliers will be fiercely scrutinised, whether under merger control or foreign investment screening powers. Within the EU last year, increasing numbers of in-depth investment screening reviews related to defence and semiconductors, with energy infrastructure maintaining a steady share of cases.

Geopolitical tensions continue to reshape the way these deals are reviewed, with a wider range of sectors and transaction types now falling within screening processes. While blocked deals remain rare under investment screening rules, we can expect more interventions and precautionary filings as businesses are likely to play it safe. While EU foreign investment dropped by 8.4% in 2024, authorisation requests to Member States surged by 73% and are understood to have reached a new all-time high in 2025.

On the flip side, and consistent with pro-growth objectives, authorities including the CMA and EC, are exploring how competition policy can advance industrial strategy, by encouraging certain domestic companies to scale up, creating "resilient supply

chains" through national and regional champions. Industries affected include manufacturing, defence, digital, clean energy and life sciences.

For transactions touching critical technology, defence, energy or other sensitive sectors, sponsors should assume deeper scrutiny and longer timetables. Ensure investment screening analysis runs in parallel with merger control from the outset.

Explore more

- Antitrust & Foreign Investment Legal Outlook 2026
- Pricing tools in the crosshairs – Antitrust authorities continue to take aim at AI and algorithms
- The Platypus Shipping Forecast: winds of change blowing strong at the CMA
- Long Road (Back) to Remedies: US Agencies Re-embrace Negotiated Divestitures in M&A
- Strictly come regulating: remedies to centre stage in the CMA's ambitious routine of reform
- Happy birthday to the Draghi Report – but where do we stand on the "new approach" to EU competition policy?

THREE TIPS TO NOTE

1. **Geopolitics:** Be conscious of the geopolitical backdrop in evaluating M&A transactions:
   - Authorities will be willing to support genuinely pro-competitive, growth enhancing transactions – including through earlier remedies to resolve competition issues.
   - For homegrown companies active in key industries, domestic competition policy may support attempts to scale up.
   - But pay close attention to any national security and critical technology considerations to global deals, as these could raise red flags and delay timelines.
2. **Compliance policies:** Portfolio companies with a consumer-facing offering and those using public funds will need robust compliance policies and clear oversight of pricing, fees and sales practices.
3. **AI oversight:** Sponsors should ensure a close eye is being kept on what AI tools are being used by their portfolio companies, what data is being fed into it, and who has access to it; particularly for decisions on pricing. Regulators are clear that businesses will be held responsible for the outcomes of AI-driven commercial decisions. Sensitive information sharing and coordinated conduct can be sanctioned, even if unintended.

Contacts



Bruce Kilpatrick
Partner, London
Tel: +44 20 7456 4067
bruce.kilpatrick@linklaters.com



Bernd Meyring
Global Head of Antitrust and Foreign Investment, Brussels
Tel: +32 2 505 03 32
bernd.meyring@linklaters.com



Fay Zhou
Partner, Beijing
Tel: +86 10 6535 0686
fay.zhou@linklaters.com

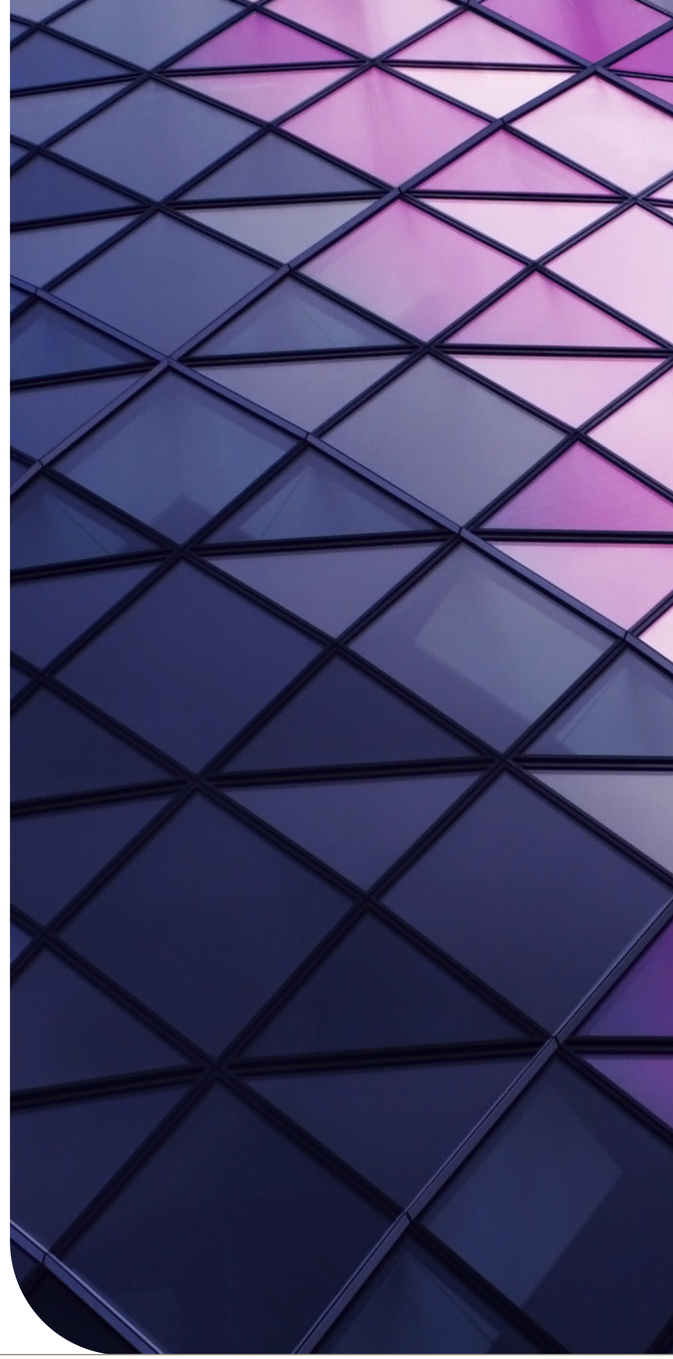


Ben Bauer
Counsel, New York
Tel: +1 212 903 9330
ben.bauer@linklaters.com

Contributing author



Tara Rudra
Senior Associate (Knowledge), London
Tel: +44 20 7456 5814
tara.rudra@linklaters.com



Compliance and beyond: Governing sustainability risk in a complex world

Recent regulatory recalibration around sustainability obligations has created some space for reflection, but it has not reduced sustainability risk. Extreme weather events, energy insecurity, artificial intelligence, climate litigation and greenwashing enforcement continue to intensify. This article explores how organisations are responding by moving beyond a "minimum compliance" mind-set, and what effective governance oversight looks like in practice.

The landscape has changed – but the risk has not

The recalibration and simplification of certain sustainability obligations over the past year have given businesses some breathing room and a chance to reflect. For most major businesses the challenge is now well understood – material sustainability risks are material business risks. **This means decision makers must engage with sustainability from a strategic and financial perspective, asking not just "are we compliant?" but "are we exposed, and are we prepared?".**

Why the urgency is growing

More studies are predicting that the world remains off track from the 1.5°C warming limit set out in the Paris Agreement and some are saying this limit may even be breached before 2030. As a result, governments, policymakers and businesses are shifting focus towards climate adaptation alongside mitigation and improving resilience in operations and economies. In parallel they are balancing energy security, affordability, growth and competitiveness needs as well as emerging resource constraints associated with AI, and differing regional approaches to the transition. Taken together, these factors present a markedly more complex external landscape than in previous years.

From a regulatory perspective, the concept of a truly global sustainability reporting framework implemented consistently across jurisdictions remains elusive, and although there have been attempts to roll back regimes in some countries, in others they continue to proliferate. As a result, businesses continue to face the challenge of meeting multiple reporting obligations while presenting a coherent and credible picture of the business as a whole.

It can be challenging to know how to position the business when the prevailing public narrative is around target-dropping and pulling back on climate disclosures, but this public narrative can be misleading. On the whole, businesses' GHG emissions reduction and other climate-related commitments remain in place, are disclosed in some shape or form, remain science-based and continue to be scrutinised by stakeholders. **Sponsors and portfolio companies should not assume that a quieter public debate signals reduced scrutiny or ambition.**

Climate litigation remains a live and intensifying risk. Particularly as frustration grows with perceived policy inaction, businesses are experiencing demands for their own climate strategies to demonstrate greater ambition, opposition to projects alleged to be incompatible with climate goals, and claims seeking accountability for alleged environmental harms. Parent company exposure for social and environmental harm in overseas jurisdictions continues to be tested in the courts, and a landmark finding in the UK High Court at the end of 2025 has sharpened focus on subsidiary governance and the management of environmental and social risks in jurisdictions with robust environmental regimes.

In parallel, regulators worldwide are ramping up enforcement action against greenwashing, focussing increasingly on the perceived substance of corporate climate strategies, and businesses are increasingly deploying greenwashing claims strategically against competitors. Companies which are finding it increasingly difficult to meet their climate goals are questioning whether they can continue to maintain them without unintentionally giving stakeholders a false impression of how challenging achieving them will be.



What this means for sponsors and portfolio companies

The core duty to act in the best interests of their company requires directors to engage with sustainability matters rather than ignore them. The challenge is not whether to engage, but how to do so in a way that is credible, defensible, and aligned with long-term business strategy.

Sponsors must balance the expectation to maintain ambitious, science-based decarbonisation and sustainability strategies across their portfolio companies with a disciplined assessment as to what can be achieved, how, and by whom as part of robust transition planning. As understanding of the science develops, greater caution around ambition should not be treated as a "green light" to step back from governance responsibility.

In response, more businesses are undertaking structured reviews of their climate and sustainability strategies to find this balance. The priority areas that sponsors and their portfolio companies should be focusing on in these reviews include:

- **Stress-testing of near-term targets before they mature.** 2030 and other near-term target dates are approaching rapidly. Now is the time to assess existing ambitions and consider carefully how they are communicated in the lead-up to deadlines.
- **Holistic mapping of financially material sustainability risks.** Organisations should ensure the business is adequately mapping and monitoring sustainability risks – including climate, nature, supply chain, and human rights – and understanding how they interconnect with each other and with financial statements, rather than treating them in silos.
- **Ensuring sustainability disclosures remain accurate, consistent, and defensible.** Misalignment between public commitments and actual strategy creates legal and reputational exposure – and can be costly if not appropriately managed.
- **Building adaptive capacity across the organisation.** Building informed, adaptive and resilient strategies is increasingly important as regulatory and physical risks intensify. This often means engaging sustainability experts where needed, upskilling and training on key risk areas, and maintaining effective links across legal, finance, risk and sustainability teams.

As the proverb goes, the best time to plant a tree was 20 years ago; the second-best time is now. While this holds true for many business challenges, it is particularly relevant in the sustainability context. Sponsors and portfolio companies that return to these issues regularly – with rigour, consistency, and strategic clarity – will be far better placed than those that wait for the next wave of regulatory, litigation or stakeholder pressures to force their hand.



FIVE REGULATORY DEVELOPMENTS TO BE AWARE OF

1. **UK Sustainability Reporting Standards (SRS):** Final versions of the UK's SRS have been published and the UK Government will soon consult on how to incorporate related reporting obligations into the Companies Act 2006. The UK's Financial Conduct Authority is also consulting on changes to UK Listing Rules to reflect the UK SRS and aims to bring new rules into force from 1 January 2027.
2. **Transition plans for UK companies:** The UK Government is yet to publish its response to its climate transition plan consultation so it remains unclear at this stage if transition plans will become mandatory in the UK, and (if so) for which entities and when. We are waiting for the Government to announce its next steps on this.
3. **Proliferation of US state-level climate reporting regulations:** New legislation has been enacted in New York and California introducing comprehensive GHG reporting obligations for certain US companies with operations in these states. Climate reporting rules are also being considered in New Jersey and Illinois.
4. **Implementation of new EU anti-greenwashing regulations:** These will apply from September 2027 and introduce new restrictions on the sustainability claims that companies operating in the EU can make, including prohibition of generic environmental claims without substantiation.
5. **Revised EU sustainability reporting standards:** The Commission must revise existing European Sustainability Reporting Standards by 18 September 2026. Companies caught by the CSRD (which still includes many large companies post the Omnibus Directive revisions) will need to familiarise themselves with the new standards ahead of reporting next year.

Explore more

- English High Court rules in claimants' favour in Brazilian dam liability judgment
- Quick Guides on sustainability disclosures under the Companies Act 2006 and UK Listing Rules
- Quick Guide on transition plans for UK companies
- Quick Guides on the New York and California rules
- Implementation tracker of new EU anti-greenwashing regulations
- Revised EU reporting standards: Quick Guide on CSRD and EU regulators' views on revised ESRS

Contacts



Rachel Barrett
Partner, London
Tel: +44 20 7456 5414
rachel.barrett@linklaters.com



Julia Grothaus
Head of Litigation, Arbitration & Investigations, Frankfurt
Tel: +49 6971003 523
julia.grothaus@linklaters.com



Guillaume Croisant
Counsel, Brussels
Tel: +32 2 5019 345
guillaume.croisant@linklaters.com



Iyesogie Igiehon
Managing Associate, London
Tel: +44 20 7456 2845
iyesogie.igiehon@linklaters.com

Navigating the UK employment law revolution: What sponsors and portfolio companies must know

After two decades of incremental change, UK employment law is now undergoing its most significant transformation in a generation. The new Employment Rights Act 2025 (ERA) is introducing sweeping reforms across almost every aspect of the employment relationship. Whilst the detail is extensive, the priority for sponsors and portfolio companies is to focus on those critical changes that will fundamentally impact business operations, financial planning, and strategic decision-making.

A change in strategy for exiting highly paid employees

From January 2027, unfair dismissal compensation will no longer be capped. Although the reform is often viewed through the lens of protecting lower-paid workers, it also has significant implications for senior employees: it will expose companies to potentially higher costs when dismissing high earners.

The current cap (which is the lower of 52 weeks' pay or approximately £120,000) has shaped how businesses handle dismissals at the very top, as it gives companies a financial ceiling that allows them to price certainty into the costs of senior exits and absorb the quantifiable cost of unfair dismissal claims. Without the cap, where senior staff are not dismissed "fairly" (which requires both a "fair reason" and a "fair process" – not always present in senior exits) employers could face significantly increased costs.

While in reality many executives will still want to avoid taking an unfair dismissal claim to a hearing given the public nature and inherent risks, the removal of the compensatory cap will inevitably shift the bargaining power in favour of the individual when it comes to exit negotiations. Career-long losses, discretionary bonuses, pension losses, and stock awards – all items of loss now potentially on the table for successful unfair dismissal claimants – become high-value battlegrounds.

This change is combined with a reduced qualifying period for unfair dismissal protection from two years to six months, meaning it will be crucial to monitor and manage performance in the first six months of employment.

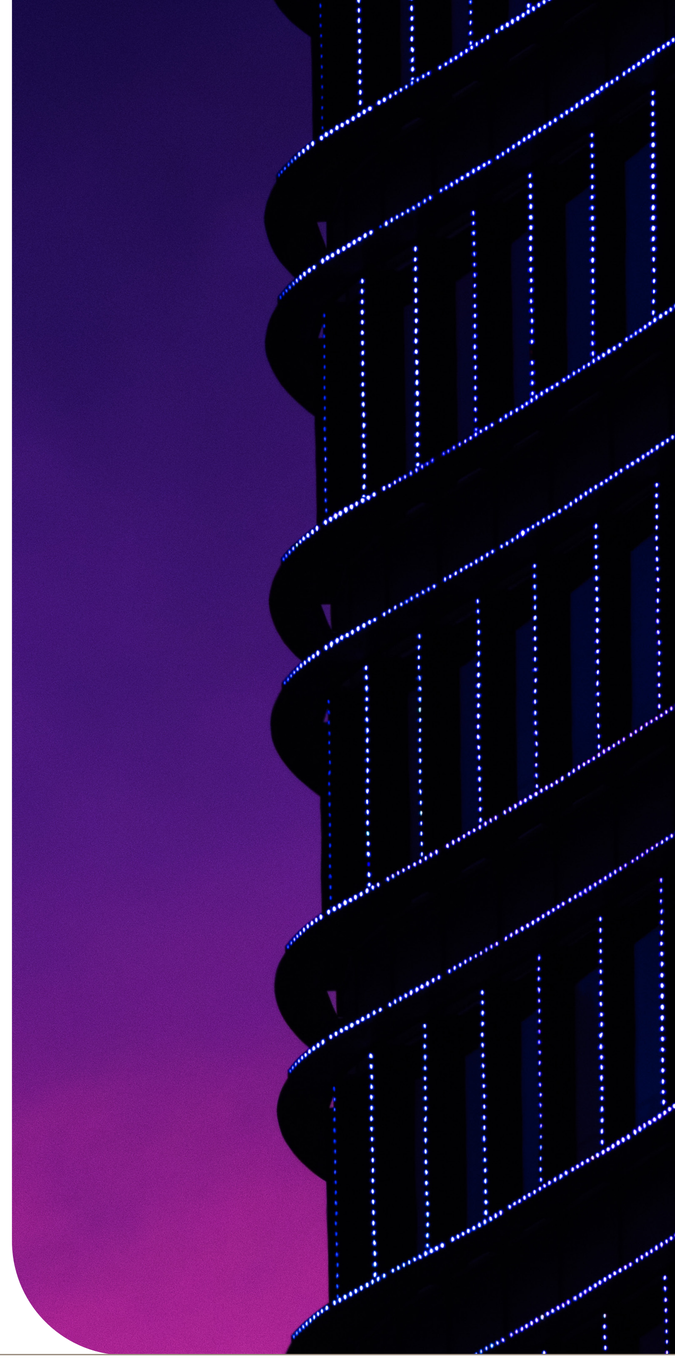
Sponsors and management should consider adapting strategy for senior exits at portfolio companies to mitigate the impact of these changes. This includes rethinking how they initiate exit discussions to mitigate unfair dismissal exposure (ie, the fair reason and fair process requirements) and, perhaps more pressing, how they structure benefits and long-term incentive arrangements for departing executives. They may also need to revisit remuneration policies for settling claims and the wording of good leaver provisions.

An end to fire-and-rehire

From January 2027, the use of so-called "fire and rehire" practices (where an employer terminates employees and offers to re-engage them on less favourable terms, often after contract negotiations have broken down) will be severely restricted. Currently, there is no ban on the use of "fire and rehire", although the practice has come under greater scrutiny in recent years and since 2024, a Statutory Code of Practice has stated that it should only be used as a last resort following consultation with employees.

Under the new rules, unless the employer can demonstrate severe financial distress and has no reasonable alternative (both of which will be very high bars), it will be automatically unfair to dismiss or replace an employee in order to make changes to core employment terms. These are known as "restricted variations", and include reductions to pay, changes to targets, pension changes, changes in hours or shift patterns or a reduction in leave. This will make it risky to dismiss employees where an employer has previously proposed to amend their core employment terms (even where the exit is not part of a mass "fire and rehire" process).

The government is consulting on the precise scope of "restricted variations" with respect to employment expenses, benefits in kind and shift patterns, but has confirmed that the changes *will* take effect in January 2027.



These reforms will fundamentally shift bargaining power in the workplace when it comes to changing core terms of employment and require management to reassess, or even accelerate, restructuring strategies and decisions in advance of the implementation date.

Increased costs and new triggers for collective redundancy

Collective redundancy rights were strengthened from 6 April 2026, when the maximum compensation for a failure by an employer to collectively consult on redundancies was doubled from 90 to 180 days' pay. This could significantly increase restructuring costs. Employers need to have in place robust systems to ensure they discharge their collective consultation duties in a compliant way, or risk hefty financial consequences.

The government also intends to introduce a new, additional, threshold for triggering collective redundancy obligations, set to apply in 2027. Currently, collective consultation obligations are triggered when an employer proposes to dismiss as redundant 20 or more employees at *one establishment* within a period of 90 days or less. The government will amend this framework to introduce an **additional** *organisation-wide* threshold trigger (with the threshold to be set out in future regulations).

More onerous obligations to prevent harassment

From October 2026, employers must take "*all* reasonable steps" (not just "reasonable steps", as is required now) to prevent sexual harassment in the workplace, representing a significantly higher bar for companies to meet.

Employers will also become liable for third-party harassment across all harassment types (such as race, disability and sexual orientation) unless all reasonable steps were taken by the employer to prevent such harassment. "Third-party harassment" includes harassment by customers, clients, suppliers, and others whom staff might come into contact with during their employment.

Sponsors and portfolio company management should undertake comprehensive risk assessments to understand workplace harassment risks and identify practical steps to prevent harassment, from strategic management training to clear and effective policies, reporting mechanisms and procedures to handle complaints, alongside contractual safeguards with third-party contractors and suppliers.

NDAs under scrutiny

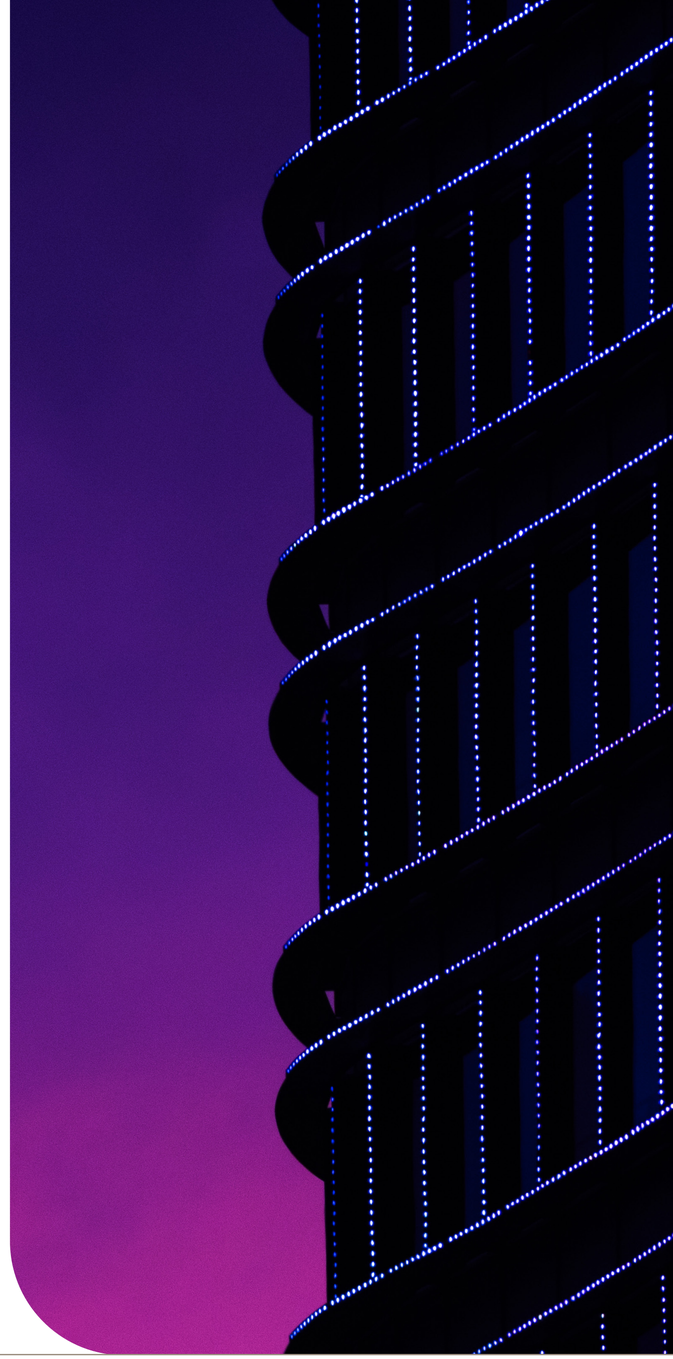
The ERA will render a non-disclosure agreement between an employer and a worker void where it seeks to prevent disclosure about relevant harassment or discrimination. This could have significant implications for settlement negotiations – particularly those with senior individuals, or concerning sensitive allegations, as the proposed changes could shift control over NDAs to the individual, potentially strengthening their bargaining position so that confidentiality becomes a negotiated "benefit" as opposed to a condition imposed on them. While a government consultation on the scope of this ban on NDAs is expected, details are not yet known.

Time to act

Implementation of the ERA is phased over two years through to 2027, providing a narrow window for sponsors and portfolio companies to prepare for what represents the most fundamental shift in UK employment law in decades.

Explore more

- Want to know what is changing and when? Visit our UK Employment Law Reforms Tracker.
- Employment Rights Act 2025 – our guides:
  - The duty to take all reasonable steps to prevent sexual harassment
  - Third party harassment
  - Unfair dismissal
  - Fire and rehire



THREE ACTION POINTS

1. **HR:** Consider investing in HR resources to track new obligations and commission comprehensive compliance audits to understand what changes need to be made and when to comply.
2. **Senior exits:** Consider strategies for senior exits before these are initiated. The new unfair dismissal changes take effect in January 2027, but there are practical consequences warranting early attention during the coming months.
3. **Policies and procedures:** Work with management at the portfolio level to map the reforms against the business's workforce strategy and cost base.

WHAT ELSE IS CHANGING?

- **Ending zero-hours contracts:** From 2027, zero-hours workers gain rights to guaranteed hours where actual hours regularly exceed contractual minimums. Businesses that are heavily reliant on flexible staffing will need to invest in workforce tracking systems as operational models will fundamentally change.
- **Mandatory ethnicity and disability pay gap reporting:** Expected to operate in a similar way to the current gender pay gap reporting regime. While implementation dates are not yet known, this *is* coming for large employers. Read more about this here.
- **Flexible working as the default:** Except where not reasonably feasible, flexible working will be the default from day one. Expected to take effect in 2027.
- **Protection against dismissal for new mothers:** From 2027, it is expected to be unlawful to dismiss a pregnant woman or new mother for six months after her return to work (except in specific circumstances).

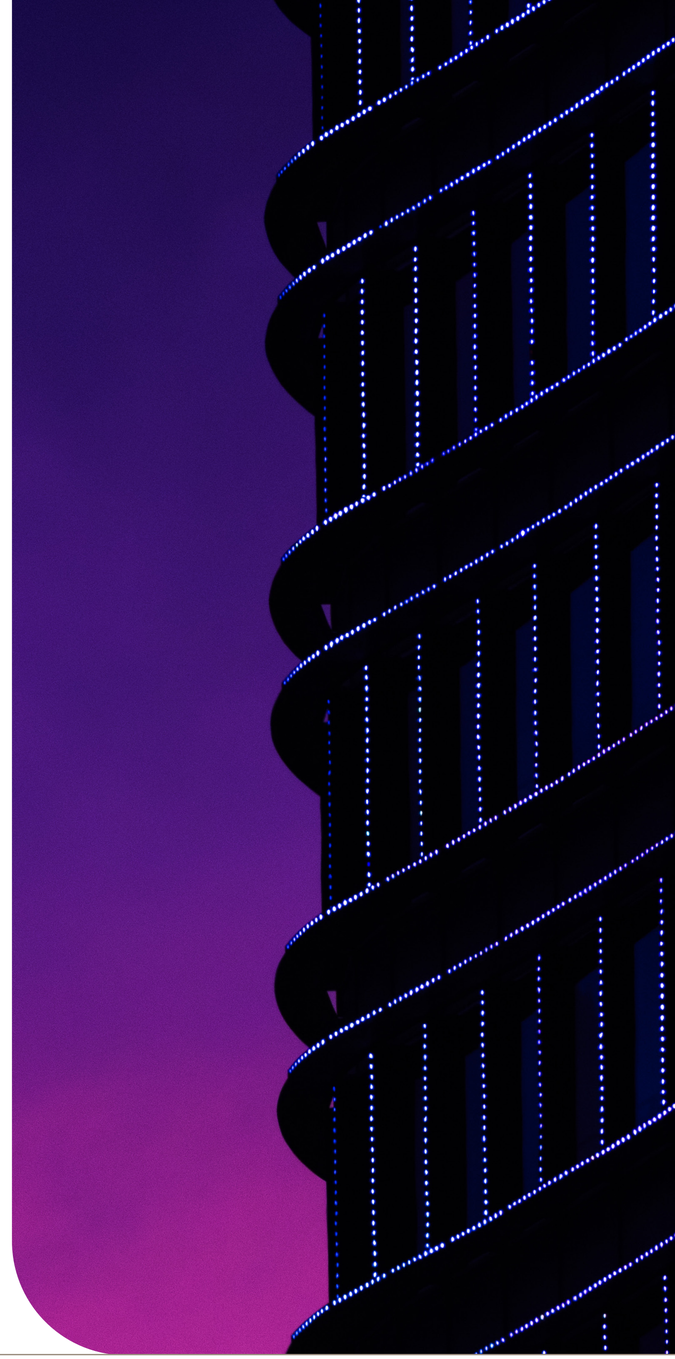
Contacts



Nick Marshall
Partner, London
Tel: +44 20 7456 2670
nicholas.marshall@linklaters.com



Laurie Ollivent
Senior Associate, London
Tel: +44 20 7456 4421
laurie.ollivent@linklaters.com



Making the most of a defined benefit pension scheme: Less legacy risk, more strategic opportunity

The landscape for defined benefit (DB) pension schemes is evolving rapidly. In contrast to a decade ago, many schemes are now in surplus and upcoming legislative changes will make it easier for companies to access that surplus. As a result, decisions about DB schemes are no longer purely technical or trustee-led matters. They increasingly raise strategic questions for sponsors and portfolio companies about capital allocation, balance-sheet risk, transaction planning and the long-term role of the scheme within the business.

New alternatives

Many companies have transferred their DB scheme to an insurer to mitigate the inherent risks faced by the business and remove the liabilities from their balance sheet. Recent changes in the law and market developments mean there are now real alternatives to consider.

In particular:

- from 2027, it will be easier to extract cash on an ongoing basis from pension schemes to meet other business needs; and
- other options now exist that may work for companies while also offering better benefits to members at a lower cost.

These factors will also be relevant for sponsors considering an M&A transaction involving a target with a DB scheme – taking on such a scheme may not now be the barrier to a transaction it once was and may even result in upside.

Running on: An increasingly attractive alternative

With many schemes now in surplus, some companies are exploring whether retaining their pension scheme might offer strategic advantages over seeking an immediate exit through insurance.

Running on may appeal to those who want flexibility to access surplus in the future, or to those that have other business reasons to keep the pension scheme – especially companies that would need to report any insurance transaction under US GAAP given this can significantly affect its balance sheet and P&L.

Accessing surplus assets: Upcoming changes

From 2027, it will be easier to pay cash out to the company without winding the pension scheme up. This is because:

- trustees will be given an overriding statutory power to make such payments; and
- the funding threshold needed before a payment can be made is expected to be lowered.

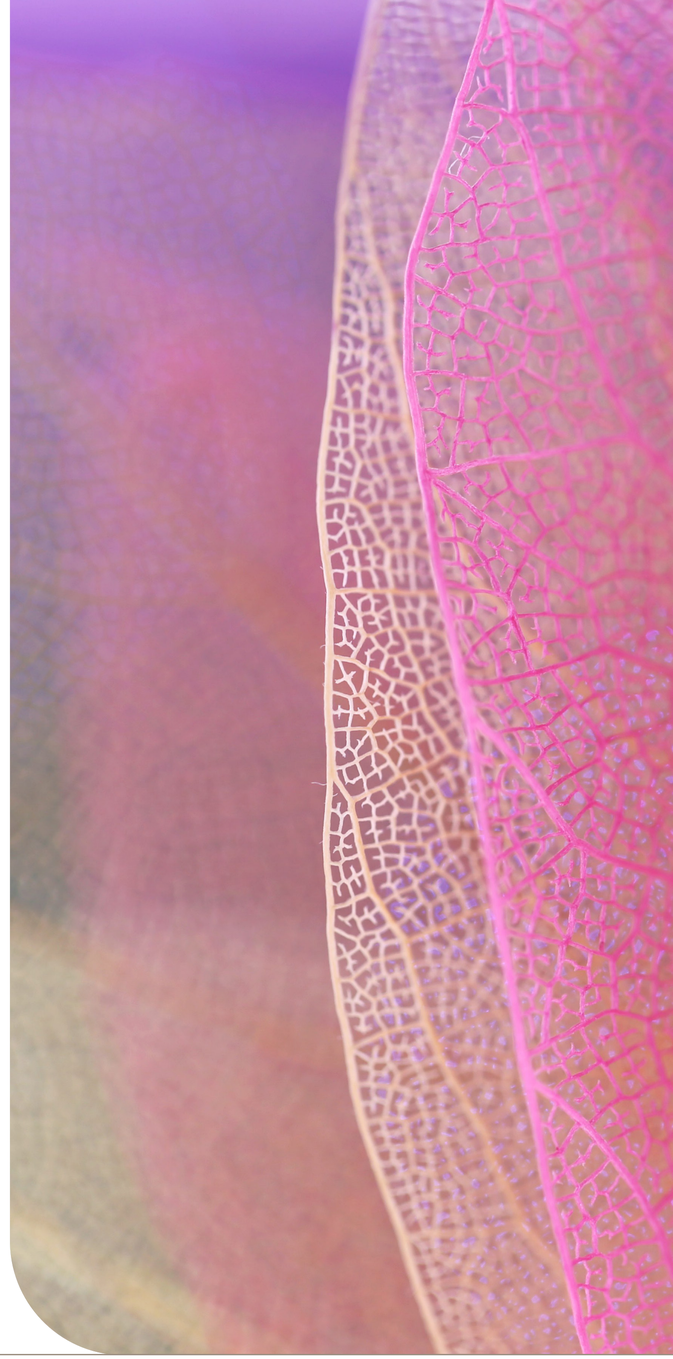
The first step is to understand the extent of the surplus under the scheme and what approach the trustees may take. If surplus is to be released, organisations should expect trustees to seek some form of protection to mitigate against the risk of a future downside in funding. Trustees are also likely to ask for some of the surplus to be used to improve member benefits. Subject to agreeing those parameters, however, there will be no restrictions on what a company can do with surplus which is returned or how many payments can be made.

Organisations should factor these changes into their long-term strategies. The ability to access surplus – whether to reinvest in the business without the need for further external finance, support ongoing business costs, or return value to shareholders – may influence decisions about whether to pursue an insurance transaction or run-on.

Alternatives to run-on or an insurance transaction

Organisations should also be aware that keeping the scheme running or securing an insurance buy-out are no longer the only viable options for managing defined benefit risk. New transactional structures have emerged that may better align management's and trustee objectives:

- For example, under the recent Aberdeen and Stagecoach transaction, Stagecoach transferred all its DB scheme liabilities to Aberdeen (the investment group) The move is expected to deliver improved outcomes for members, while Aberdeen will receive



a share of any future surplus as well as fees for managing the scheme's assets. This type of solution may be attractive where the organisation wants to exit its pension scheme, but faces trustee resistance to insurance transactions because these rule out the possibility of future improvements to member benefits.

> Where the DB scheme is not currently able to afford an insurance transaction, organisations may also wish to consider the possibility of transferring the liabilities to one of the emerging superfunds, such as Clara. These superfunds act as consolidators for DB pension schemes and achieve a similar outcome (albeit without the protection afforded by the insurance regulatory regime) in removing a DB scheme from a company's balance sheet at a lower cost. These solutions are only currently available where a scheme is unlikely to be able to transfer to an insurer in the foreseeable future.

These developments highlight the greater range of strategic choices now available to companies and trustees – and make early engagement all the more important.

THREE POINTS TO CONSIDER

1. What is the current **funding position** of your scheme, and what are the **realistic long-term strategy options**?
2. What **value** could your scheme generate for the business and how much **risk** are you willing to absorb?
3. How would the **trustees** respond to a proposal to run-on the scheme with the aim of periodically returning surplus?

Contacts



Philip Goss
Partner, London
Tel: +44 20 7456 5604
philip.goss@linklaters.com



Rosalind Knowles
Partner, London
Tel: +44 20 7456 3710
rosalind.knowles@linklaters.com



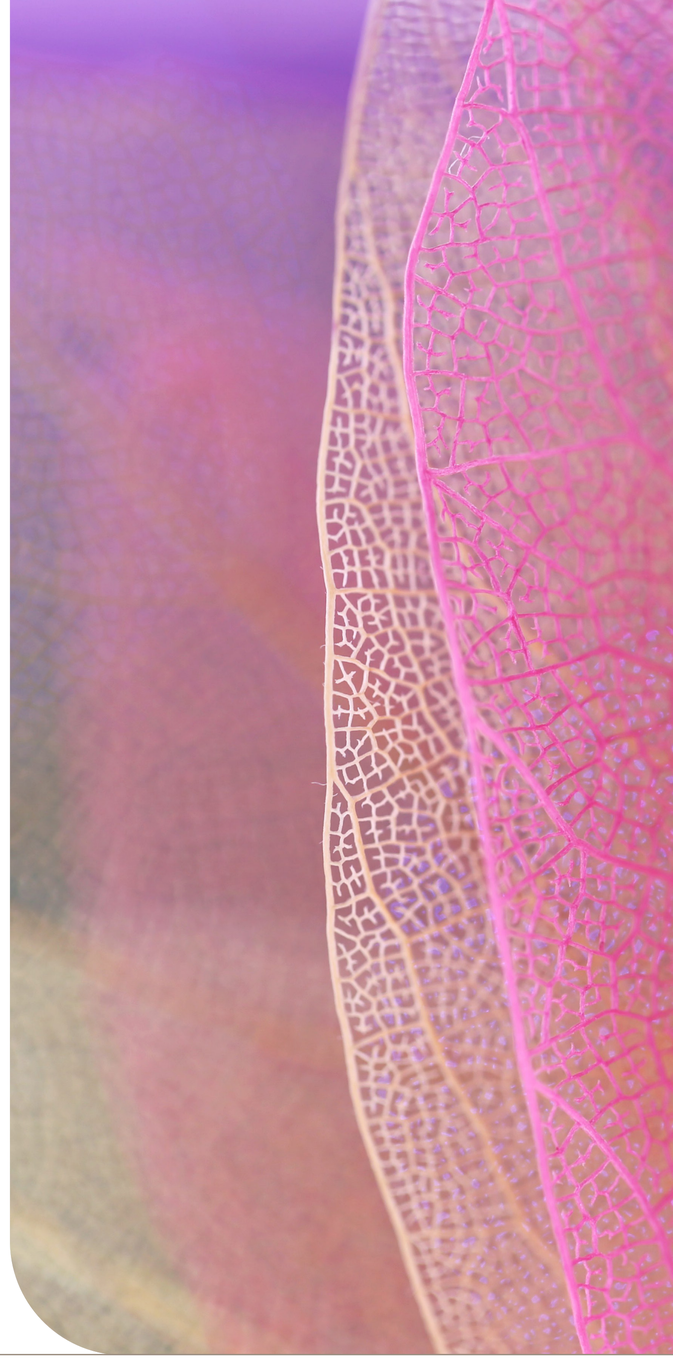
Sarah Parkin
Partner, London
Tel: +44 20 7456 3548
sarah.parkin@linklaters.com



John Sheppard
Partner, London
Tel: +44 20 7456 5998
john.sheppard@linklaters.com



Alasdair Smith
Partner, London
Tel: +44 20 7456 4989
alasdair.smith@linklaters.com



linklaters.com

This content is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here, please get in touch. © 2026 Linklaters.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, 20 Ropemaker Street, London, EC2Y 9AR, England or on www.linklaters.com and such persons are either solicitors or registered foreign lawyers. Please refer to www.linklaters.com/regulatory for important information on our regulatory position. LIN.LAT.2872.26