Osborne Clarke

WAVE

Emerging legal trends in digitalisation

Start reading →

Contents

EXECUTIVE SUMMARY

NEXT IN AI

TRANSACTIONS & TEAMS

REGULATORY IMPACTS

Introduction

Digitalisation is transforming how businesses operate and how they are held to account. As technology becomes increasingly embedded in products and processes, it is changing how businesses operate – often challenging long-held assumptions about responsibility, control and coordination.

This shift introduces new forms of risk, ranging from AI tools that act autonomously to user experiences that raise questions about fairness and control. However, not all this risk stems from fast-moving technologies. Some of the most persistent risks arise from structures which businesses rely on every day. In tech supply chains, operational risk can result from contract terms or technical dependencies that need to adapt to this transformation. In regulatory planning, the challenge lies in managing current fragmentation while anticipating how future legal shifts might disrupt business models. Class actions, meanwhile, are increasingly testing how digital businesses operate – targeting both the outcomes they produce and the design of the interfaces and processes behind them.

The first edition of WAVE brings together insights from senior legal and business leaders to explore the practical implications of this transformation. It examines the governance demands posed by emerging technologies such as agentic AI and hyper-personalised systems, where decisions are made at speed and scale. It also unpacks how structural exposure accumulates through supply chains, contract frameworks and regulatory divergence – and how business and legal strategies must adapt.

From evolving platform liability and cross-border class actions to the future shape of legal teams and shifting M&A priorities in the technology, media and communications (TMC) sectors, WAVE guides you through the new terrain which businesses must navigate.

Our digital expertise

Our team at Osborne Clarke has extensive expertise in navigating the complexities of digital transformation. We understand the legal challenges and intricacies of emerging technologies. With deep knowledge of AI, digital regulation, and platform businesses, we provide strategic guidance in all areas of law to help businesses anticipate and manage risks, optimise operations, and achieve their goals amidst digital disruption.

Contact us today to learn how our expertise can help your business.

Mark Taylor
Global Head of Digitalisation
Osborne Clarke UK
mark.taylor@osborneclarke.com

Nick Johnson
Global Head of Tech, Media and Communications
Osborne Clarke UK
nick.johnson@osborneclarke.com

NEXT IN AI

Agentic AI: Why Governance Can't Wait

As AI evolves, so too does the challenge of managing it

Much of today's enterprise AI use centres on 'zero-shot' models – tools that respond to prompts within defined boundaries. But a new layer of complexity is emerging as organisations experiment with agentic systems: AI tools (autonomous agents) that can initiate tasks, adapt strategies and, in some cases, coordinate with other agents or external systems. While that capability promises faster workflows, it also creates legal and operational risks that are harder to govern – especially when organisations have a poor understanding of how these systems behave.

That combination of autonomy and uncertainty is what makes agentic AI a risk amplifier. As agents begin interacting with third-party platforms, liability and accountability can become difficult to assign – particularly when vendors disclaim responsibility for how their agent tools are used.

In this context, governance becomes more than a compliance obligation, it is a structural safeguard. Without it, organisations risk being blindsided by systems they do not fully understand or lack the ability to track.

> "You can't deploy and use AI on shifting sands. If you don't have a clear vision of what's being used, and defined governance guardrails around it, you face a risk chain reaction. This is especially the case with agentic AI."

Tamara Quinn, Director – AI, Data & IP Knowledge, Osborne Clarke UK

Current Agentic AI Use Cases

Potential may drive headlines, but practical deployments are quietly taking shape.

Agentic AIOps

Agents monitor and manage complex IT environments, predicting failure points and resolving issues without human intervention.

Customer Experience and Call Centre Management

Agents handle customer queries and execute resolution pathways, improving satisfaction and operational efficiency.

Autonomous Drug Discovery

In biomedical research, agentic systems analyse pharmacological data, simulate responses and apply adaptive logic to accelerate discovery.

Procurement and Supply Chain Management

Agents are beginning to take over routine procurement tasks and are being trialled to reroute supply chains and optimise logistics.

What Makes an AI Agent Truly 'Agentic'?

By Satya Nitta
Co-founder and CEO, Emergence AI

The term 'AI agent' is often misused to describe basic LLM wrappers or scripted tools that simply coordinate system calls. However, the classic definition remains unchanged – an AI agent is an autonomous system that sets goals, determines actions and executes tasks while continuously learning and adapting without human intervention. For enterprise, agents go beyond automation, demonstrating contextual reasoning, adapting to unforeseen challenges and dynamically adjusting plans to succeed in complex environments.

Emergence AI recently unveiled the first demonstration of AI agents autonomously creating other agents and multi-agent systems in real time to successfully complete enterprise tasks. Though still early, this capability is expected to advance quickly, enabling the automatic creation of increasingly sophisticated agents and multi-agent systems interacting with one another across a growing landscape of enterprise challenges.

From Legal Burden to Business Essential

AI governance has often been treated as a downstream activity: a policy layer applied after deployment to satisfy regulatory expectations. But that model is becoming increasingly unsustainable, with agentic capabilities already surfacing across enterprise environments.

> **"Given current adoption trajectories, where 50% of enterprises have already deployed AI agents and another 32% plan to do so within a year, mainstream adoption of agentic AI tools is rapidly approaching. We believe the space is set to move even faster."**
>
> **Satya Nitta**, Co-founder and CEO, Emergence AI

This represents a shift in enterprise risk, with even partial agentic functionality introducing accountability gaps and blurring the lines of liability. Many vendors are developing platforms that enable transparency and control, but those capabilities often depend on how businesses configure and oversee them.

As a result, the responsibility for outcomes is increasingly resting with the enterprise, not the provider. And this is happening against a backdrop of intense market forces to adopt and upgrade quickly, often without the luxury of careful planning.

> **"The pressure to adopt and upgrade is relentless. While the need to be agile is obvious, it also means that having your governance in place now is essential."**
>
> **Łukasz Węgrzyn**, Partner, Osborne Clarke Poland

The inevitable conclusion is that AI governance needs to move from compliance safeguard to operational backbone. That means not just documenting policies, but building a structural framework – one that integrates usage rules, ethical guardrails, staff training and escalation protocols. The next step is ensuring those structures are visible and understood across the business.

The Shadow Adoption Problem

How inadvertent risks are created when agentic features are adopted 'under the wire'.

- Agentic AI features are already being bundled into enterprise software, often without clear oversight. This kind of shadow adoption – where tools enter through procurement, partnerships or software updates – creates risk from within.
- Failing to provide staff with an authorised enterprise tool risks unauthorised and clandestine use on personal devices.
- Without visibility into how these systems are used or by whom, governance is undermined before it begins.

No Visibility Equals No Governance

Addressing gaps in visibility requires a structured understanding of the tools in use, who is using them, for what purpose and how they interact with other systems. Balancing carrot and stick incentives vs. prohibition in terms of behaviours is also critical.

Mapping also reveals patterns, such as which teams are adopting AI first and where the pressure to experiment is strongest, serving as a diagnostic tool. This process shows whether governance frameworks are aligned with how AI is actually being used, or whether they are operating on outdated assumptions. Without continuous visibility, even the best-designed policies risk drifting out of sync with reality.

> "Without a clear inventory of AI tools and use cases, businesses risk designing governance frameworks in a vacuum. These frameworks may fail under scrutiny, or worse, create a false sense of compliance."
>
> **Adrian Schneider**, Partner, Osborne Clarke Germany

Raising the Floor, Not Just the Ceiling

AI governance often focuses on high-stakes use cases and advanced model oversight, but the real risk is more widespread. Governance fails when employees do not understand the tools they are using or the risks they introduce.

These risks are not theoretical. Real failures are emerging – not from malice, but from everyday misunderstandings. Sensitive client data pasted into public LLMs, unvetted plugins and unflagged AI outputs in regulated workflows are already appearing across professional settings.

> "An organisation is the sum of its parts – and that collective needs to understand the risk. If awareness is limited to a few, the whole organisation is compromised."
>
> **John Buyers**, Partner and Co-head of Osborne Clarke's International AI Service team

Regulators are starting to respond, with the EU AI Act requiring both providers and deployers to ensure staff possess adequate AI literacy. This is broadly defined as the knowledge and skills needed to make informed decisions about AI use and its potential impact. These responsibilities cannot be delegated, and businesses remain accountable for ensuring their staff can identify and manage the risks AI introduces into daily operations.

Meeting that standard requires a structured training and literacy approach. General users need lightweight onboarding to cover responsible use, common risks and data boundaries. Those designing or embedding AI into business processes need deeper, role-specific training. Regardless of the training adopted, regular testing is essential to confirm that staff can act on what they have learned, not just recall it.

The Governance Steps You Can't Ignore

Without visibility, even the best governance plan will fail.

01

Audit

Begin with a full audit of your AI tools, including usage behaviours (who is using them and for what purpose).

02

Identify

Identify how those tools interact with your internal systems and external data.

03

Evaluate

Evaluate which use cases introduce the greatest data exposure or operational risk.

04

Frame

Use that insight to frame guardrails and escalation pathways.

Don't Mistake Delay for Safety

The EU AI Act is now in force, with some use cases already prohibited, and core obligations for high-risk systems set to apply from August 2025. But questions remain about how, and how aggressively, those obligations will be enforced. The EU's enforcement stance is being shaped in part by transatlantic dynamics, with the US embracing a deregulatory agenda that places pressure on EU and UK policymakers to prioritise innovation over early intervention. However, this should not divert from the essential fact that the EU AI Act is law.

Of course, legal exposure is not limited to new laws, with existing regimes already applying to many AI-related activities. Data protection obligations, such as those under the GDPR in the EU and UK and the CCPA in California, still apply to any AI system that processes personal data or makes automated decisions about individuals.

The use of copyrighted material in model training, and the originality of AI-generated outputs, continues to raise unresolved intellectual property questions. Consumer protection and anti-discrimination rules remain in force, especially for B2C applications. In regulated industries such as finance or healthcare, AI use may also trigger sector-specific compliance obligations.

A phased approach to enforcement does not mean businesses can wait. Governance remains essential to managing risk under law – and to preparing for what is coming next, including agentic AI.

Who's Responsible When AI Fails?

As with intellectual property, AI liability is a constantly evolving area. In the B2C arena, much of the EU's digital regulatory agenda – including the EU AI Act – is focused on protecting consumer rights. In B2B settings, the picture is less clear, and technologies such as agentic AI only reinforce that uncertainty.

The key issue is how responsibility should be divided between those who build the tools and those who use them. Platform providers may develop the technology, but enterprise users must understand the markets they operate in, the regulatory frameworks that apply and the ethical implications of deploying autonomous systems. Some vendors are now framing deployment as mutual, offering compliance tooling while placing ultimate accountability with the user.

> **"Agentic AI deployment is a shared responsibility. We design our platform with regulatory needs in mind, providing audit and policy tools to help customers meet compliance in their specific contexts."**

Satya Nitta, Co-founder and CEO, Emergence AI

Lead with Governance

AI governance is no longer a downstream fix – it is becoming the infrastructure that enables safe, scalable innovation. For forward-looking organisations, and those that are heavily regulated, it is as essential as the tools themselves.

> **"Agentic AI is not just another tech trend, it marks the beginning of a seismic shift. Organisations that harness its potential now will unlock intelligent automation, scalable innovation and new forms of efficiency."**

Satya Nitta, Co-founder and CEO, Emergence AI

That shift is already underway, with agentic features entering businesses faster than many can govern them. Even the perception of autonomy is enough to create legal and reputational exposure. Waiting for legal clarity or technical maturity will not shield businesses from the risks already forming around them.

The organisations best positioned to navigate this moment are not those with the most advanced tools, but those with a clear line of sight into AI use and an enabling governance structure ready to manage it.

> **"We're already witnessing analysis paralysis in the enterprise community. Simply put, indecision and uncertainty will act as blockers to you fully embracing the potential of agentic AI. A failure to implement clear AI governance means you risk being left behind as your competitors race ahead."**

John Buyers, Partner and Co-head of Osborne Clarke's International AI Service team

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

John Buyers

Partner

Osborne Clarke UK

+44 20 7105 7105

Email John

Full bio

Tamara Quinn

Director – AI, Data & IP Knowledge

Osborne Clarke UK

+44 207 105 7066

Email Tamara

Full bio

Łukasz Węgrzyn

Partner

Osborne Clarke Poland

+48 795 576 136

Email Łukasz

Full bio

Adrian Schneider

Partner

Osborne Clarke Germany

+49 221 5108 4370

Email Adrian

Full bio

Satya Nitta

Co-founder and CEO

Emergence AI

NEXT IN AI

AI-Driven Hyper-Personalisation: Future Risks and Opportunities

AI is taking personalisation of online content to a new level

Systems that once personalised in predictable ways using basic pre-existing data are increasingly reacting to user behaviours and context in real time – adapting in the moment to tailor offers, conversations, imagery, tone and service flows based on individual user signals and live online data. This shift to "hyper-personalisation" will reshape both how businesses deliver value and how consumers engage and what they expect.

But as personalisation deepens and becomes more reactive, not only do existing risks become more acute but new kinds of regulatory challenge also arise. The ability for an AI system to generate unique content and experiences for individuals opens the door to different forms of consumer law breach and the potential for liability under AI-specific laws. It also raises complex challenges around ensuring legal and regulatory compliance in real time and at massive scale.

Early Examples of Increased Personalisation

- **Spotify Wrapped** is a personalised annual video generated for individual users highlighting their top songs, artists and genres from the year.
- **Subscription video on demand (SVOD)** streaming services use AI to offer individualised recommendations based on viewing history, time of day and user-entered data.
- **Starbucks** tailors in-app personal offers in real time based on geographic proximity to stores, purchase history and time of day.

Examples of Emerging/Future Hyper-Personalisation

- **Future online advertising** will rely on data-driven algorithms not just to target audiences but also to generate individualised content for recipients based on their real-time behaviour.
- **AI customer service agents** will be able to use historical and real-time data to adapt their accent, tone and vocabulary – creating bespoke user experiences that are optimised to drive the organisation's desired outcomes.
- **Voice-based AI-powered systems** are already being used to comfort and reassure people with Alzheimer's, using best practice techniques tailored to individual needs.

Existing Risks of Personalisation

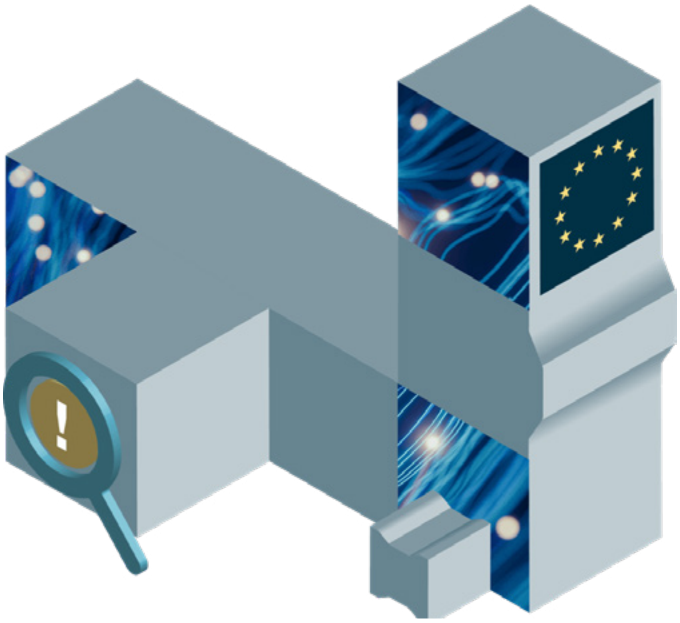
Current forms of personalisation give rise to a number of legal and regulatory risks that are increasingly well recognised and addressed under data protection, consumer protection and anti-discrimination laws. AI-powered hyper-personalisation will amplify those existing risks.

Under data protection laws, if personalisation relies on processing of personal data, then requirements around transparency, legal basis for processing and "special category data" need to be navigated. For instance, if purchase history data is processed and this includes non-prescription pharmacy-only medicine products, then in Europe at least this risks being seen as processing of "data concerning health", which requires explicit consent under the GDPR.

In hyper-personalisation scenarios, risk increases in line with the scale of data use and the wider range of processing purposes, and also because AI processing can be unpredictable and introduce data bias. Additional transparency may be required, and the legal basis for processing will need to be considered.

Special category data issues may also surface in new ways. For example, if an AI voicebot learns to modulate its accent to match customers' accents on a personalised basis, it could be argued this amounts to processing of "data revealing racial or ethnic origin".

Under consumer protection laws, issues can already arise when personalised pricing lacks transparency. For example, the UK's Competition and Markets Authority (CMA) is investigating Ticketmaster's use of dynamic pricing for Oasis tickets. Likewise, if current personalisation techniques result in less favourable treatment of individuals from protected groups, anti-discrimination/equality laws may apply. With at least some forms of AI-driven hyper-personalisation, consumer transparency will be more challenging, and discrimination may arise not just in who receives a message, but also in what that message says and the style in which it is communicated.



New Techniques, New Risks

Hyper-personalisation does not just boost existing risks. Using AI and factoring in real-time data and user reactions can add significant additional legal issues. These predominantly arise from how, when and why systems adapt to individual users. They fall into three categories:

Algorithmic Exploitation of Vulnerability

First, there is the risk of algorithmic exploitation of vulnerability. If an AI-powered system is instructed to optimise for customer spend and can adjust not only when it targets messages, but also what those messages say – and how they say them – the AI system may start to identify and exploit patterns that correlate to individual vulnerabilities. Online gamblers, for example, may be targeted with messaging shaped by behavioural patterns statistically linked to high-risk engagement – such as frequent session restarts or repeated late-night activity – at moments when they are particularly susceptible. This kind of AI-learned targeting is likely to attract attention under consumer protection and/or AI laws in territories where these prohibit unfair commercial practices and/or exploitation of situational vulnerability.

Misleading Output from the AI

Second, if not adequately constrained with technical guardrails, the output from the AI may be misleading. In its attempts to generate content in line with its instructions – whether to optimise sales or otherwise – the AI may "hallucinate" statements that are inaccurate and thus mislead the recipient into making purchases or other transactional behaviour. A recent Canadian court decision involving a major airline found the company liable after its chatbot gave incorrect advice regarding the airline's bereavement policy.

> **"Using AI to personalise content is not inherently unlawful, but hyper-personalised techniques can raise flags under multiple regimes where AI functionality is covert, subliminal and exploitative."**
>
> **Emily Tombs**, Senior Associate (NZ Qualified), Osborne Clarke UK

AI-Specific Legislation

Third, issues may arise under AI-specific legislation such as the EU AI Act. For example, covert personalisation strategies may breach prohibitions on subliminal techniques if they lead individuals to make important decisions they would not otherwise have made if fully aware of the influences at play. Care will also be needed if any element of the system could be seen as an "emotion recognition system" under the EU AI Act, and to ensure AI-generated outputs are appropriately identifiable.

Compliance at Hyper-Scale

Those who use hyper-personalisation will need to address the challenge of how to handle content compliance issues. In scenarios where bespoke content is generated automatically in real time and with a potentially massive number of instances, that challenge may be very significant. Organisations will need to assess the extent to which compliance can be baked into their AI systems and the level of oversight that will be appropriate to monitor the success of any built-in measures.

Platforms that have statutory obligations to maintain repositories of online ads – a requirement for certain large entities under the EU Digital Services Act (DSA) – may face a corresponding technical and organisational challenge in how they comply with those obligations for potentially limitless hyper-personalised variants.

From Risk to Strategic Advantage

Hyper-personalisation also offers potential opportunities. In areas such as consumer law, accessibility and data protection, it might help deliver clearer, more actionable information. For example, AI could help tailor the content and timing of disclosures based on factors such as user understanding and the context of the interaction – thereby aligning with consumer law goals of informed decision-making and timely disclosure. Equally, adaptive font sizing, simplified language modes, audio-assisted navigation and real-time content tailored to user needs could all improve digital access for users with disabilities.

Over time, practices that enhance accessibility may evolve from being seen as optional improvements to becoming standard regulatory expectations. Legal concepts of "reasonable adjustment" may well expand to include digital personalisation, as regulators or courts start to consider this when assessing compliance. By engaging early with accessibility and design colleagues, legal teams can help the business stay ahead of evolving standards – demonstrating a clear commitment to inclusive user experience.

However, certain disclosures – such as withdrawal rights, cancellation terms or product warnings – may need to remain fixed and unaltered to meet legal requirements in some jurisdictions. These should be excluded from certain forms of personalisation to avoid non-compliance.

> **"AI compliance is not only about the EU AI Act. It can include many different legal fields. It is important to hardwire compliance, accessibility and trust directly into the user experience and involve legal teams from the outset."**
>
> **Dr Lina Böcker**, Partner, Osborne Clarke Germany

AI-driven hyper-personalisation will reshape how organisations engage with users, but with its benefits come additional risks and a more complex regulatory landscape. Compliance models will need to adapt quickly. The key challenge will be to embed legal requirements in a way that is both accurate and agile.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

Nick Johnson

Partner
Osborne Clarke UK
+44 20 7105 7080
Email Nick
Full bio

Emily Tombs

Senior Associate (New Zealand qualified)
Osborne Clarke UK
+44 207 105 7909
Email Emily
Full bio

Dr Lina Boecker

Partner
Osborne Clarke Germany
+49 221 5108 4434
Email Lina
Full bio

TRANSACTIONS & TEAMS

The Legal Operating System: In-House Legal in 2040

After three decades of adapting to digital change, in-house legal teams are now facing a shift that will go beyond productivity gains and fundamentally change how they work.

Between 1995 and 2010, the first wave of digital transformation reshaped how legal teams worked – from faxes to email, and from folder-based filing to keyword-based search. The next 15 years changed how legal work was delivered – automation reduced manual steps, and cloud platforms extended access and continuity.

But speed is not the same as transformation. While the infrastructure evolved, the function remained largely the same: legal teams advised, reviewed, approved and responded. The next wave – 2025 to 2040 – will be different. Legal will become less a department and more an operating layer: encoded into workflows, distributed across platforms and delivered through automation.

By 2040, a GC's role may no longer revolve around leading teams – it may extend into the design and governance of the automated legal architecture the company as a whole relies upon. That future may feel distant, but the groundwork is already being laid.

From Today's Tools to Tomorrow's Trajectories

"Each of us has access to an enterprise-grade LLM, and we're encouraged to explore how it can improve our legal output and productivity."

Max Latchmore, Senior Legal Counsel, Octopus Energy

While most in-house legal teams are still experimenting with AI tools, some are already reframing their day-to-day workflows. It is a shift in mindset, where teams are learning both new applications and to share knowledge more fluidly across departments.

Legal as Infrastructure

> "In-house legal teams won't just adapt to AI, they'll redefine how business decisions are made by embedding legal thinking into every workflow."

Dan Wright, Partner, Director of OC Solutions, Osborne Clarke UK

Within the next 15 years, AI tools will become the delivery mechanism for legal, embedding rules and decisions into agentic workflows that touch every part of the business. Much of what legal teams currently manage – contract review, compliance checks, policy enforcement – will shift into automated systems, allowing routine decisions to happen faster and with fewer delays. Escalation protocols and clause logic will be built directly into tools so risks can be flagged and transactions paused before legal steps in. In many organisations, agentic AI will negotiate standardised terms and route only high-ambiguity or high-impact cases to human reviewers, freeing up legal teams to focus on complex decisions where human input in the moment makes a meaningful difference.

When legal becomes embedded into systems the entire company uses every day, its role begins to shift. Business teams will no longer think of legal as a checkpoint. Instead, legal becomes a background function: ever present but largely invisible. When legal logic is encoded directly into the systems that drive business outcomes, the function becomes inherently more proactive – shaping behaviour and data in advance rather than responding after the fact.

> "When legal is embedded into business systems, its role changes. It is no longer there to catch the ball; it helps throw it further."

Antti Seppala, General Counsel, Pigment

However, while legal logic becomes a seamless part of everyday business, the need for oversight and continuous refinement remains. AI's decisions, while faster and potentially more consistent, will still require a human hand to ensure they align with a business' legal standards and ethical expectations.

From Expertise to Probability

Today, AI systems can already perform some of the legal tasks traditionally handled by junior lawyers, including contract reviews. Their outputs are fast and often hard to distinguish from those of a human lawyer. But for most legal teams, the real challenge is not AI's performance; it is understanding how those results are reached and whether they can stand behind them.

Currently, legal expertise is grounded in human context: experience, interpretation, business sense and ethical judgement. Most legal AI systems rely on large language models (LLMs) that generate outputs based on statistical inference – what sounds right according to prior patterns.

Although these systems can mimic judgement and often rival junior lawyers in performance, they do not understand the law. And because their output often appears cogent and well written, while their inner workings remain largely opaque – even to their own designers – their mistakes can be hard to spot and even harder to explain. To date, this appears to have made it challenging for insurers to price for risk.

This will change in time, however, with researchers enjoying early success in mapping how LLMs make planning decisions in narrow use cases. Their success offers hope that even more complex models may become more transparent. Once that transparency is established, AI models become better understood and easier to insure.

At some point in the coming years, parts of the AI stack will have matured to a point where certain legal outputs – under defined scopes and conditions – are insurable. This will be a milestone, one that marks the moment when legal accountability begins to shift from human authorship to system governance.

> "We're replacing judgement with probability. That's not wrong, but it is different – and we must recognise and plan for that change."

Anna Grafton-Green, Senior Director, Head of Legal (UK, Europe and Israel), PayPal

That shift reframes the GC's role from interpreting risk to deciding when machine judgement is good enough and where it should be applied. While edge cases and high-value deals will be the last to be left entirely to machine judgement, by 2040 much of the legal function will focus less on interpreting the law and more on designing the systems that do.

Legal's New Ecosystem

As in-house legal teams redesign how their work is delivered, their external legal support needs will evolve in kind. Internal systems will increasingly absorb tasks once routinely handed off, such as first-line contract review or policy drafting.

There will always be cases that GCs will require formal advice on, particularly where the stakes are high or the context ambiguous. While much of the routine scaffolding around a $200 million transaction will be handled internally, human judgement from outside counsel will still offer assurance when commercial or reputational risks are significant.

In other scenarios, GCs will need outside support in shaping and evolving the logic embedded in company systems. This may involve designing machine-readable policy frameworks, developing AI tools and AI-run playbooks tailored to the legal function, testing agent outputs to ensure compliance and ethical standards, and providing oversight of system updates to ensure regulatory and legal alignment.

Between these ends of the spectrum lies a demand for new forms of legal support. We may not yet have names for them, but they will be critical to facilitating the transformational shifts to the new legal operating system.

The last time we saw a shift of this scale was during the commercialisation of the internet. Entire industries were restructured, with some vanishing only to be replaced by their digital counterparts. Legal will follow a similar trajectory. Routine advisory work may decline, but demand will rise for system-level expertise. This is not just about replacing tasks, it is about building a new operational layer from the ground up.

> **"Legal expertise will no longer be confined to advice, it will also fuse legal and AI skills, to enable data-driven strategic decisions to be made across organisations, constantly supporting the business' strategy."**
>
> **Ashleigh Hegarty**, Chief Legal Officer, Charlotte Tilbury Beauty

The Legal Operating System

The AI revolution over the next decade and a half will reshape every sector, and legal will be no exception. By 2040, the in-house legal function will no longer be a faster version of its current reactive state. Instead, it will operate as a strategic, intelligent layer seamlessly integrated across the organisation.

Delivering on that mandate will require a broader range of skills within the legal function. Legal teams will increasingly depend on product designers, data scientists, governance engineers and behavioural strategists to shape intelligent systems. For those entering the profession today, technical fluency and design thinking might become as important as technical legal knowledge.

While the transition will be slow, in-house legal teams are already exploring the challenges of AI integration and risk management, often using existing enterprise tools to lay the groundwork for the changes ahead. They need to find the answers to these questions sooner rather than later, because the decisions they make today will shape the future of legal work and determine how well they are positioned by 2040.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

Dan Wright

Partner

Osborne Clarke UK

+44 330 313 4100

Email Dan

Full bio

Nick Thody

Director of Knowledge

Osborne Clarke UK

+44 20 7105 7566

Email Nick

Full bio

Ashleigh Hegarty

Chief Legal Officer

Charlotte Tilbury Beauty

Anna Grafton-Green

Senior Director, Head of Legal (UK, Europe and Israel)

PayPal

Max Latchmore

Senior Legal Counsel

Octopus Energy

Antti Seppala

General Counsel

Pigment

TRANSACTIONS & TEAMS

Tech Supply Chains: Rethinking Risk and Resilience

Behind every digital system sits a network of commercial commitments – invisible when things go right, impossible to ignore when they do not. As businesses modernise and scale, many are increasingly relying on a small set of technology providers to deliver critical functions and meet rising compliance expectations.

At the outset, supplier relationships often reflect a shared priority: delivering results that work for both sides. But over time, decisions such as long-term contracts or interconnected systems can reduce a business' ability to pivot.

> "Most buyers and suppliers want the same thing: a project that works on time and on budget, ideally to achieve first mover advantages. The challenge is making sure that the shared goal doesn't unravel over time and under pressure."

Ulrich Bäumer, Partner, Osborne Clarke Germany

What makes these types of concentration risk so difficult to manage is that they often stem from choices made early in system design or supplier selection – long before the consequences are visible. Even minor changes can become difficult to execute if contract terms are rigid or systems are not easily reconfigured. To mitigate those risks, many businesses are redesigning their infrastructure with flexibility in mind. Hybrid and multi-cloud models, portable systems and stronger governance protocols are becoming core safeguards.

But recognising these risks is not always straightforward. Many dependencies stay hidden, buried in overlooked contract terms or untested assumptions that only surface when failure hits.

Identifying Risks Early

What looks simple on paper often masks complex realities beneath, especially when services are layered across teams and technologies.

Some larger suppliers offer steep discounts on multi-year deals, but the trade-off is often reduced flexibility. These contracts may include volume thresholds or narrow exit terms that are difficult to unwind once systems are embedded. At the other end of the spectrum, smaller vendors can carry more risk than they appear to. A low-value contract might support a critical application, but fall beneath legal or commercial review simply because of its price tag. If that supplier fails, the disruption can force costly, improvised workarounds.

> "Some buyers don't realise that the €500,000 supplier is the linchpin for a €20 million service."

Nina Lazic, Partner, Osborne Clarke UK

These structural risks are not always commercial, and technology design can embed rigidity just as easily as contract terms. Systems built around a single cloud provider – or using proprietary tooling that cannot easily be transferred – can seem stable until there is a change in cost or service levels. Moving workloads or reconfiguring complex architecture mid-contract is rarely simple and often expensive.

These risks do not live in isolation, and may not always be fully visible to any one team. Legal may review terms, but miss architectural fragilities. Procurement may focus on cost, but be unaware of operational interdependencies. IT understands systems, but may not see the legal exposure if those systems fail. Without shared visibility – legal, commercial and technical – exposure remains hidden until something breaks.

> **"The CIO knows where the practical points of technical failure are. Licence managers know the intricacies of technical licence models. Purchasing knows the commercial pitfalls. The lawyer usually doesn't know all this that well, focusing instead on the legal intricacies. Until they all talk, the business is exposed."**
>
> **Ulrich Bäumer**, Partner, Osborne Clarke Germany

Concentration risk is not simply a legal or a design issue, it is an organisational blind spot that needs to be addressed early to avoid being discovered when failure occurs and responsibilities are less visible.

Beyond the Fine Print

Contracts remain a core tool for managing supplier relationships, but their strength lies in how they are used. When contracts are drafted early, tailored to operational realities and supported by strong internal coordination, they help organisations act quickly under pressure. When they are approached too late or relied on too heavily, they are much more likely to disappoint.

> **"Clear terms can support resilience, but they cannot create it in isolation."**
>
> **Gianluigi Marino**, Partner, Osborne Clarke Italy

While large providers frequently insist on more standardised templates that limit room for negotiation, that does not mean terms are set in stone. Buyers that engage early – with cross-functional backing and a clear view of their priorities – are more likely to negotiate meaningful changes, such as service levels, termination rights or liability limits. This is particularly true as regulatory scrutiny of supplier lock-in and switching barriers continues to grow. (See: **Regulatory Awareness as Strategy**.) These moves may not be easy, but with the right internal support and clearer expectations emerging across jurisdictions, the possibilities can be worth exploring.

Multi-year deals offer different challenges, as discounts often come with volume commitments or exit restrictions. These can reduce flexibility just when it is needed most, such as when systems need to evolve or supplier performance dips. The value of a long-term agreement must be weighed against its constraints.

On the other hand, smaller or mid-tier suppliers may offer greater flexibility, but that flexibility does not guarantee resilience. If a vendor lacks the resources to fulfil contractual promises, even the best terms may offer limited recourse. In these cases, a strong legal position must be backed by the ability to pivot quickly, whether by rerouting services or activating internal fallback plans.

Contracts matter, but businesses cannot afford to bank on them as their sole contingency. Their effectiveness depends not just on the terms themselves, but on how well the organisation is prepared to act when disruption hits.

Organising for Resilience: A Toolkit

Strong supplier relationships depend not just on terms, but on clear planning and coordinated execution. The steps here outline practical ways to incorporate that capability into day-to-day operations.

Break down silos early

Early coordination between procurement, IT and legal helps teams spot issues that might otherwise slip through review. Create shared checkpoints before key decisions and ensure strategically important suppliers are visible across the business.

> **"Resilience isn't just about what's in the contract, it's about driving multi-disciplinary engagement across your teams."**
>
> **Nina Lazic**, Partner, Osborne Clarke UK

Secure senior sponsorship

When teams are backed by leadership, they are better positioned to engage early, weigh trade-offs and pursue terms that support long-term resilience. A defined mandate ensures risk management is prioritised alongside delivery and cost goals, not sidelined by them.

Understand the trade-offs

Choosing a supplier requires understanding internal priorities and potential compromises. While larger providers offer scale and stability, smaller vendors may be more flexible but harder to assess for resilience. Businesses must consider their current needs and future challenges as well as ensuring providers can adapt to evolving requirements and withstand disruptions.

Own the Business Continuity Plan (BCP)

A supplier's business continuity plan (BCP) outlines their recovery, but it may not align with how their clients need to respond. Develop an internal BCP that sets clear expectations for fallback processes, escalation roles and service levels during disruption. Test the plan under realistic conditions and work with suppliers to ensure alignment, both operationally and contractually where appropriate.

Continually reassess supplier risk

A supplier's risk profile can shift quickly – through regulatory change, technology updates or ownership transitions – weakening contracts that once offered solid protection. Do not wait for renewal cycles. Review whether terms still reflect how services are used and whether they offer practical support when disruption hits.

Engage early with regulators

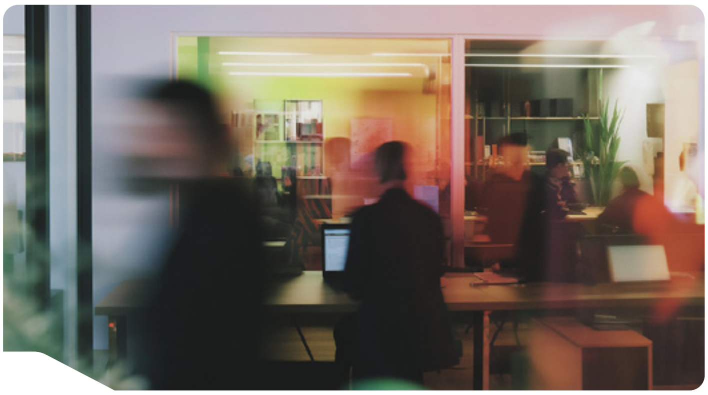
Digital supply chains are being reshaped by emerging regulation, whether that is on cloud portability or AI oversight. Rather than waiting for final laws that could leave businesses looking to retrofit compliance, companies should monitor early policy signals and take part in consultations where possible. This will help them anticipate new obligations and shape regulations in ways that reflect operational realities.

> **"Regulation is evolving faster and earlier input matters. Businesses that engage now will shape the standards everyone else has to live with."**
>
> **Katherine Kirrage**, Partner, Osborne Clarke UK

Planning for Macro Unknowns

Even the best-structured supplier relationship can be tested by global shifts.

Supplier relationships are not insulated from geopolitics. Tariffs, digital taxes, cross-border investment restrictions and regulatory initiatives such as the EU Data Act can all reshape commercial viability mid-contract. Long-term agreements should be structured to accommodate change, allowing businesses to revisit pricing or renegotiate terms when external conditions shift.



Regulatory Awareness as Strategy

Staying ahead means watching where regulators are looking.

Regulators are looking more closely at supplier lock-in, exclusivity and switching barriers. Laws such as the EU Data Act, the UK's Digital Markets, Competition and Consumers Act 2024 (DMCCA) and the proposed Data (Use and Access) Bill are reshaping expectations – pushing for portability, flexibility and fairer terms.

Regulatory signals give buyers a basis to push back against any rigid terms, while giving sellers a preview of where scrutiny may land next. Engaging early is more than just compliance. It is a chance to set expectations before they become obligations.

> "Regulators are pushing for multi-homing, easier exits and more flexible terms. Whether you're buying or selling, this changes how you negotiate."
>
> **Katherine Kirrage**, Partner, Osborne Clarke UK

Where Risk Meets Readiness

As systems become more interconnected and reliant on external platforms, even well-managed supplier relationships can become points of vulnerability if dependencies are not fully understood or planned for.

While strong contracts can help, resilience is not achieved through documentation alone. It depends on how well businesses anticipate change: in their needs, in their suppliers and in the regulatory environment shaping digital infrastructure. That means assessing how contracts align with operational realities, how supplier decisions are made and escalated, and how fast teams can respond when a change or failure occurs. This requires strong cross-functional coordination and a clear method for testing fallback plans before they are needed.

Businesses that treat supplier strategy as an ongoing discipline – rather than a one-off transaction – are more likely to scale effectively and withstand disruption.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

Katherine Kirrage
Partner
Osborne Clarke UK
+44 207 105 7514
Email Katherine
Full bio

Ulrich Bäumer
Partner
Osborne Clarke Germany
+49 221 5108 4164
Email Ulrich
Full bio

Nina Lazic
Partner
Osborne Clarke UK
+44 207 105 7400
Email Nina
Full bio

Gianluigi Marino
Partner
Osborne Clarke Italy
+39 02 5413 1769
Email Gianluigi
Full bio

TRANSACTIONS & TEAMS

TMC M&A Trends: Resilience, Scalability and Discipline Will Define Success

Deal sentiment across tech, media and communications (TMC) entered 2025 on a strong footing, buoyed by momentum built in the post-COVID rebound. After the sharp contraction in the first half of 2020, transactional activity rebounded dramatically through 2021 and 2022, with deal volumes and valuations reaching record highs. By 2023 and into 2024, however, the market had steadied. While deal activity remained healthy, growth rates normalised, and the energy that fuelled earlier years began to temper. Risk sensitivity gradually rose, particularly around deal structuring and operational resilience.

As 2024 drew to a close, there was cautious optimism that this stable environment would continue. Many investors anticipated another year of steady, if selective, transactional flow across TMC sectors.

Instead, the first quarter of 2025 delivered a sharp recalibration. Early shocks – including tariff announcements, stock market volatility and renewed geopolitical tensions – caught many parties off guard, disrupting deal processes and forcing a reassessment of risk appetite.

What is emerging is not a retreat, but a refocus. Buyers remain active, but investment priorities have tightened around businesses that demonstrate operational rigour, digital scalability and sector durability – qualities that are increasingly critical to sustaining capital interest in a more volatile market.

Flight to Quality and Safety

The market's reaction to the volatility of early 2025 is not a sudden shift, but an intensification of investment logic that had already been emerging through 2024. Understanding how deal dynamics evolved last year is critical to anticipating how trends are likely to sharpen through 2025 and beyond.

While TMC deal activity remained healthy throughout 2024, underlying market sentiment was already beginning to shift. Inflationary pressures, rising commodity prices, international conflicts and an evolving, less predictable regulatory environment all contributed to growing caution among buyers. Although transactional momentum remained steady – particularly across pan-European deals and cross-border activity from US-based investors – enthusiasm was clearly tempering compared with the sharp rebound seen in 2021 and 2022.

This caution was reflected in deal structures. Parties increasingly turned to completion account structures to ascertain price, rather than locked box mechanisms. Valuation gaps between buyers and sellers became more visible, prompting wider use of deferred consideration and earn-outs to bridge expectations. Investors increasingly sought mechanisms to align deal pricing with future operational performance.

Distressed M&A activity also began to rise, as businesses under pressure from macroeconomic headwinds sought strategic exits or cost rationalisation opportunities. Even as appetite for quality assets remained strong, buyers were becoming more selective, placing greater emphasis on verifiable fundamentals and structural resilience rather than speculative growth narratives.

By late 2024, this shift was playing out in real time: businesses offering transparent operations, strong market positioning and scalable infrastructure were progressing more smoothly through due diligence and sustaining stronger buyer interest. Businesses with harder-to-price risks, by contrast, faced longer processes, greater scrutiny and valuation pressure.

The disruption that followed in early 2025 accelerated and sharpened this cautious dynamic. Investment committees and boards that had already been tightening their filters in 2024 have moved into risk recalibration mode, further elevating structural resilience and operational clarity as prerequisites for transacting.

In today's selective market, digital maturity, operational control and scalable business models are no longer just competitive advantages. They are increasingly decisive factors in shaping buyer confidence, pricing outcomes and execution certainty.

Why Structure Matters Now

The current caution in the M&A environment means that deal structure has moved to the centre of negotiation strategy. As volatility and valuation uncertainty widen pricing gaps, mechanisms such as earn-outs, deferred consideration, staged acquisitions (majorities or even minorities) and carve-out structures are playing a critical role in bridging expectations between buyers and sellers.

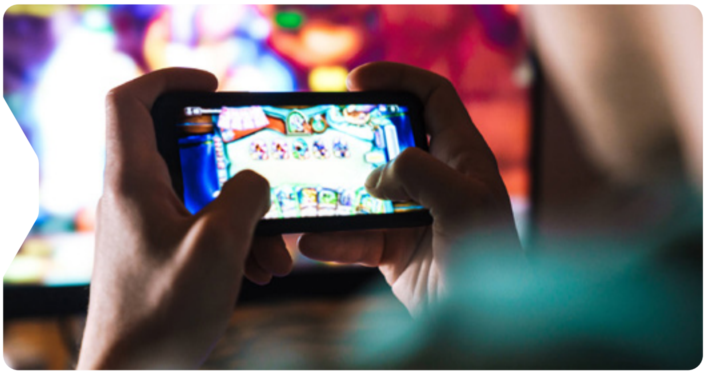
These tools offer flexibility, enabling parties to align deal value more closely with future performance while managing immediate risk exposure. What was once treated as a backend execution detail is now a frontline tactic for getting deals done. In a market defined by selectivity and recalibrated risk appetite, the ability to structure creatively is often the difference between momentum and standstill.

Where Capital is Flowing

While sector focus still plays a role in drawing initial buyer interest, it is no longer solely determinative. Investors are no longer satisfied with sector exposure alone – they are scrutinising how businesses can convert strategic advantage into sustainable growth under pressure. This is especially true in TMC, including areas such as cyber security and technology-enhanced defence solutions, where longstanding advantages such as digital infrastructure, creative ecosystems and strong IP foundations still offer meaningful appeal.

Recent transactions highlight the strategic traits that are drawing capital interest and offer valuable signals of how investment priorities are likely to evolve through 2025 and into 2026.

Scalable Digital Platforms



Content-driven platforms with strong digital distribution models continue to attract sustained buyer interest, particularly where monetisation is tied to user engagement or proprietary ecosystems.

The sale of Fusebox Games to India's Nazara Technologies illustrates this strategic logic: a narrative-led mobile games developer and publisher built around repeatable, scalable revenue and strong digital community engagement. Businesses with embedded monetisation mechanics offer durable value, even when broader market conditions shift.

These businesses appeal for being able to engage users directly, reduce acquisition costs and generate recurring revenue with minimal marginal cost, aligning well with both strategic and financial investor priorities in volatile markets.

Creative Brand Platforms

Brand authenticity and defensible client relationships are gaining renewed importance as AI-driven disruption accelerates. Buyers are rewarding firms that sustain differentiation through creativity, client relationships and proven growth.

Uncommon's acquisition by Havas – partly positioned as a hedge against the commoditising effects of generative AI – and New Commercial Arts' acquisition by WPP highlight the trend: both firms achieved rapid growth after their founding, combining creative leadership with strong commercial execution. These businesses' creative distinctiveness has allowed them to retain pricing power in sectors where automation and generative content risk flattening differentiation.

For investors, creative resilience is not just about brand image – it signals deeper commercial defensibility. Businesses that protect pricing, preserve client loyalty and maintain a clear market identity amid commoditisation are more likely to justify premium multiples, particularly when earnings quality and long-term differentiation are under scrutiny. In a market where AI is levelling functional capabilities, the value now lies in what cannot be easily replicated.

Data-Driven and AI-Enabled Models

Proprietary datasets and technical AI capabilities are playing an increasingly decisive role in due diligence and valuation. Investors are gravitating towards businesses where data ownership, regulatory positioning or analytics engines create defensible moats. Across media, diagnostics and regulatory technology, data and AI are recognised not just as growth drivers, but as valuation protectors – critical assets likely to command premium multiples even in volatile conditions.

Buyers are now looking beyond whether AI is present in a business model, they are assessing how it is deployed and what risks or advantages it creates. Ownership of proprietary datasets, the ability to explain and validate model outputs, and clear alignment with evolving regulatory standards are becoming key differentiators. In a market where regulatory pressure and heightened investor expectations around AI are shaping deal decisions, businesses that demonstrate control and transparency are gaining a clear edge.

Energy Tech and Strategic Innovation

In energy technology, investor focus is shifting to capital-light innovation – such as optimisation software, usage analytics and predictive control systems – that supports efficiency and aligns with policy objectives without the capex exposure of infrastructure assets.

By contrast, investment appetite in autotech, particularly in EV-linked sectors, has softened in the near term. Tariff uncertainty and easing consumer demand have tempered short-term momentum, although next-generation mobility remains a longer-term opportunity.

Across both areas, buyers are favouring innovation that strengthens operational defensibility, not just expansion potential.

Scaled Operators with Strategic Growth Momentum

Mid-sized platforms demonstrating operational control, cross-border scalability and disciplined buy-and-build execution continue to command strong interest from private equity and debt investors.

Focus Group provides a clear example: we advised on its 2020 private equity transaction and again on its 2024 secondary deal, which saw the business' value climb significantly. (See case study: **Focus Group: Building Scale, Securing Value**) Its combination of organic expansion and strategic acquisitions created operational maturity and scale – attributes that are becoming critical differentiators in a more selective market.

In 2025, being able to integrate acquisitions cleanly and scale without repeated capital injections has become a key differentiator, particularly for sponsors looking to de-risk portfolios without slowing growth.

Healthcare and IT services platforms are seeing similar renewed interest, particularly where businesses can demonstrate disciplined integration and resilient fundamentals.

CASE STUDY

Focus Group: Building Scale, Securing Value

Focus Group's trajectory offers a clear example of how operational discipline and strategic growth can position mid-market businesses for large-cap investor interest, even amid volatile conditions.

In 2020, the business completed a private equity transaction with Bowmark Capital just days before the first COVID-19 lockdown reshaped the global economy. Over the following four years, Focus pursued a disciplined growth strategy, combining strong organic expansion with targeted strategic acquisitions. This approach built significant operational scale, strengthened integration capabilities and broadened its geographic reach across the UK and beyond.

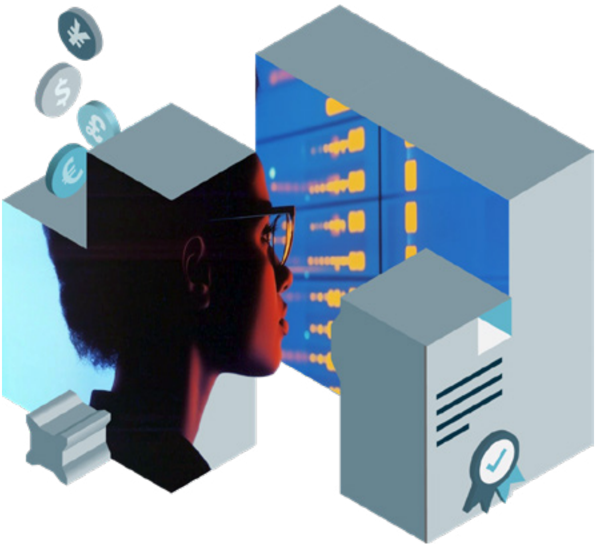
By 2024, Focus' operational maturity and strategic clarity had attracted significant investor interest, culminating in a secondary transaction with Hg Capital that valued the business at circa US$1 billion. The Focus Group transaction offers a window into the market dynamics already taking shape in 2024. The traits that attracted investor interest then are becoming even more critical as buyer selectivity sharpens through 2025 and beyond.

Transacting in a More Selective Market

This is not a lost year for TMC dealmaking, but it is a more discerning one. Volatility will continue shaping the landscape into 2026, and not all businesses will find easy pathways to transact.

Yet meaningful deal activity is happening where fundamentals align. Buyers are committing where they see credible growth, operational clarity and structural resilience. The best-positioned businesses will not only navigate near-term volatility – they will validate their value in ways investors can test and trust.

Looking ahead, the scalability, defensibility and disciplined growth traits will likely become even more decisive filters for investment. In a more selective market, the question is no longer whether deals can be done, it is whether you are the kind of business that investors or strategic buyers will back.



Contributors

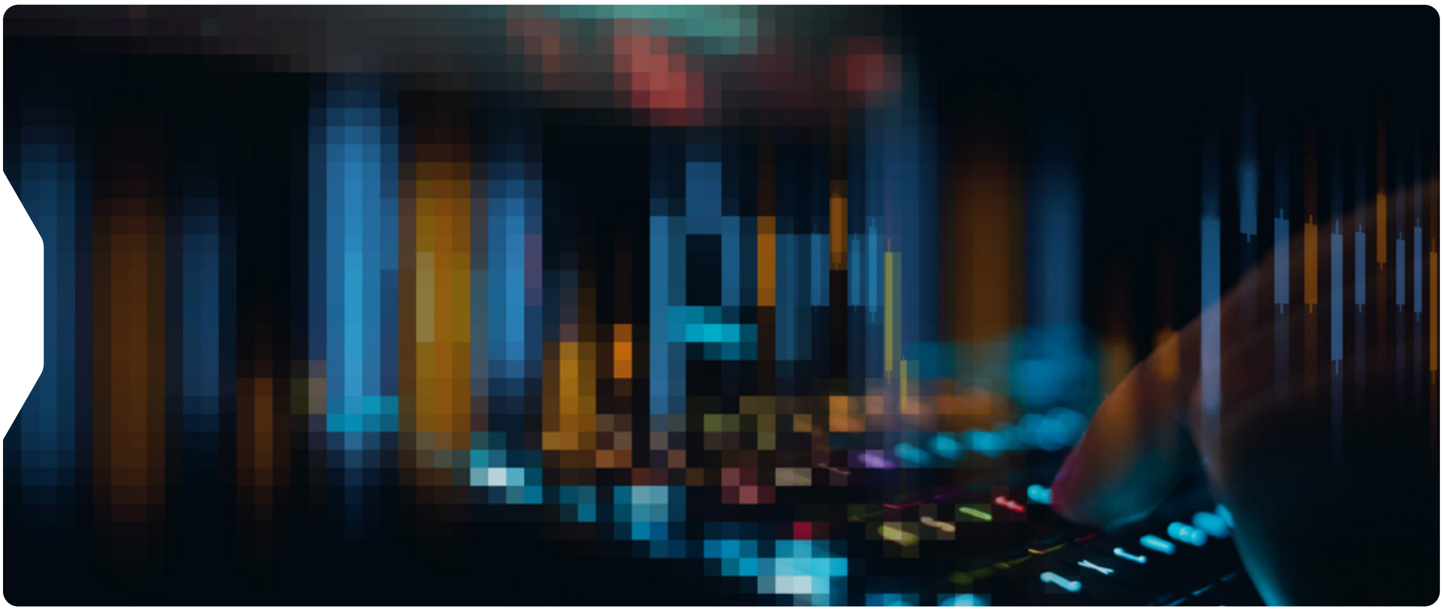
We would like to thank these individuals for having shared their insight and experience on this topic.

Greg Leyshon
Partner
Osborne Clarke UK
+44 20 7105 7587
Email Greg
Full bio

Dr Björn Hürten
Partner
Osborne Clarke Germany
+49 221 5108 4200
Email Björn
Full bio

REGULATORY IMPACTS

How Data Sovereignty Is Reshaping Business Strategies



In a digital world that is increasingly interconnected, data has become the lifeblood of modern business. Its flow, storage and processing are essential for everything from new product development to supply chain logistics and customer relationship management. However, the rise of “data sovereignty” has led to this vital resource being subject to an increasing range of differing laws and regulations. Organisations need to navigate the sometimes conflicting requirements of those laws, and those who do so best will have a distinct competitive advantage.

What Is Data Sovereignty?

Data sovereignty is the concept that data is subject to the laws and regulation structures within a particular nation or bloc – usually that in which it is created or collected. It is not a single rule or standard, but a policy direction that reflects growing concern over external dependencies and control. Related and entwined concepts include:

- **Tech sovereignty,** meaning that a country has control over its own technology infrastructure, including that for storing and processing data.
- **Data localisation,** where data relating to a country or its inhabitants is to be kept in that country.
- **Organisational data sovereignty,** which relates to an organisation having control over its own data and how it is handled.

The Global Rise of Data Sovereignty

Historically, the use of data and its flow across borders was relatively unregulated – governed by contractual agreements and early privacy laws. That changed with the digital revolution which ushered in an unprecedented surge in data creation, collection and processing. Recognising the growing importance of data for their citizens, economic growth and national security, governments began to assert greater control over information originated or held within their borders. This resulted in new laws – some general in application, others sector-specific – that introduced various forms of "data sovereignty". Three key themes tend to feature in the sovereignty aspects of those laws.

The first is restriction of cross-border data transfers, either by way of outright prohibition (leading to data localisation) or with transfer subject to stringent rules and conditions. The specific data and organisations covered by these prohibitions and restrictions, and how those rules are applied in practice, differ significantly across jurisdictions.

Data Transfer Restrictions – Some Examples

- Australian law prohibits transfer outside Australian borders of information from the national digital health record system.
- Canadian provinces British Columbia and Nova Scotia require personal data held by public sector bodies to be kept in Canada, subject to some exceptions.
- The US' Bulk Data Rule, due to be fully implemented in October 2025, prohibits the large-scale sharing of genetic data to certain territories including China, Russia and Iran.

The second key theme is extra-territorial reach. Increasingly, territories' data laws state that they apply to forms of data processing that take place outside the territory's borders, regardless of the location of the entities involved in that processing. Again, the scope and extent of any international reach can vary: it may not apply to all forms of processing or all kinds of data.

Extraterritorial Reach – Some Examples

- **The US CLOUD Act** allows US law enforcement to order US-based technology companies to provide requested data, regardless of where that data is stored globally, provided certain conditions are met.
- **The EU GDPR** applies to organisations outside the EU who process personal data of EU-based individuals where organisations are offering of goods or services to those individuals within the EU or are monitoring those individuals' behaviour within the EU.

> "While many jurisdictions do not ban extra-territorial data transfer outright, they often create enough regulatory friction and legal risk that local storage can become the preferred option."
>
> **Benjamin Docquir**, Partner, OC Belgium

The third key theme is that not all relevant laws are necessarily data specific. Data is central to many digital solutions and services, and so a particular territory's laws governing these activities can also indirectly impact the data which they use or produce. A current example is AI: data is the essential fuel powering the development of many AI models, but laws around AI and its inputs and outputs differ considerably between countries.

The effect of this shift has been profound for multinational corporations. Data and processing activities may no longer be subject solely to domestic laws but also to other data laws worldwide. Those laws are becoming less harmonised and are sometimes driven by different political or economic aspirations.

This means multiple regulatory regimes need to be navigated and direct conflicts of law can arise. As a result, traditional straightforward data strategies – typically involving data centralised in a few key locations for efficiency – are subject to a changed risk profile and are increasingly not fit for purpose.

Instead, businesses need to understand and reconsider where their data resides, which laws govern it and how vulnerable it is to disruption. Further, with data laws continuing to emerge and evolve around the world, businesses need to be prepared to adapt to legislative changes. In short, a much more sophisticated approach is required.

Developing a Resilient Data Strategy

To develop and implement the kind of proactive, robust and future-ready data strategy that can best deal with the shifting sands of global data laws, a number of strategic questions need to be addressed on an ongoing basis:

Where is our data physically located and which countries' laws apply?

Understanding the physical location of data collection and storage, who has access to it, where it is transferred to, what it is used for and the location of the data subjects are all crucial in order to map out the legal jurisdictions that need to be taken into account.

What types of data do we hold?

Granular data classification is also important, so as to understand the sensitivity of particular data and the different sector-specific regimes that may apply. For example, the position differs between health data and financial data.

How necessary is the data?

The more data that is held, the greater the potential exposure to regulatory and cybersecurity risk. Steps can be taken to reduce this risk. For example, where data has no obvious business purpose, could it be discarded? To what extent can historic data be anonymised or pseudonymised, particularly for analytics purposes, in order to reduce privacy risk?

What third party contract terms are we committed to?

Where third-party vendors and service providers are involved, the relevant contract terms with those entities should be examined to assess the position on location and transfer of data. These aspects may open up other risks – for example, where a supplier's location causes additional laws to apply. Contractual lock-in with specific suppliers and locations also needs to be considered.

What data locations are desirable technically and operationally?

Are there organisational or technical reasons why certain locations may be preferable for data collection, storage and processing?

How feasible is it to ring-fence data by territory or region?

Businesses will need to consider factors such as:

- whether data can realistically be kept local
- to what extent this will inhibit growth and the ability to adapt to changing business needs and developing law
- whether data localisation might impact adversely on customer experience, and how operational resilience might be affected if the back-up copies are not kept outside that region.

> **"Operational resilience regulations naturally push companies to focus on service continuity and risk mitigation. They are often interpreted as requiring multi-cloud setups, redundant systems or geographic dispersion."**
>
> **Joanne Zaaijer**, Partner, Osborne Clarke Netherlands

How do I protect against data access being disrupted (criminally, politically, commercially)?

In the face of a growing number of high-profile cyber-attacks – and geopolitical uncertainty – planning for disruption is a key component of resilience and compliance with data laws. Businesses must consider the impact of various forms of disruption and develop contingency plans. Diversifying providers and locations can enhance resilience, but may also cause additional laws linked to those providers and locations to apply.

Are our chosen data havens stable or vulnerable to geopolitical pressure?

Businesses should evaluate whether their data storage locations are susceptible to geopolitical pressures that could impact data security and accessibility, and hence require a rapid change of approach.

Finding the answers to these questions – and having a process to update those answers over time – will help businesses make much more informed decisions around data strategy. Those might include, for example, moving to a multi-cloud strategy with distinct regional footprints and taking a more strategic and intentional approach to data duplication.

Making those decisions will require strong collaboration between legal, IT and business units – and any changes will naturally need to be flowed through into third-party contracts and due diligence processes, employee training, policies, external disclosures and incident response plans.

However, creation and implementation of a resilient data strategy should not be seen as a one-off project, but rather as an ongoing commitment. To successfully maintain that commitment requires a dynamic governance framework – one that drives continuous monitoring of business developments and global regulatory changes, and that enables proactive identification of compliance gaps and an adaptive approach to emerging risks.

Strategic opportunities

Data sovereignty is a geopolitical reality that will continue to add greater regulatory complexity for businesses. Navigating this evolving terrain requires a comprehensive understanding of legal requirements, robust but pragmatic compliance and governance frameworks, and a willingness to make strategic operational changes. The goal is to design systems – both technical and organisational – that can flex as necessary without adding unnecessary complexity and cost.

This can be challenging, and it is as much an art as it is a science. However, a well-articulated and carefully implemented data strategy that meets data sovereignty's challenges head-on can be a powerful differentiator. It will not only mitigate legal and reputational risks but also build deeper trust with customers, partners and regulators. The future belongs to those who can master this art.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

Benjamin Docquir
Partner
Osborne Clarke Belgium
+32 2 515 93 36
Email Benjamin
Full bio

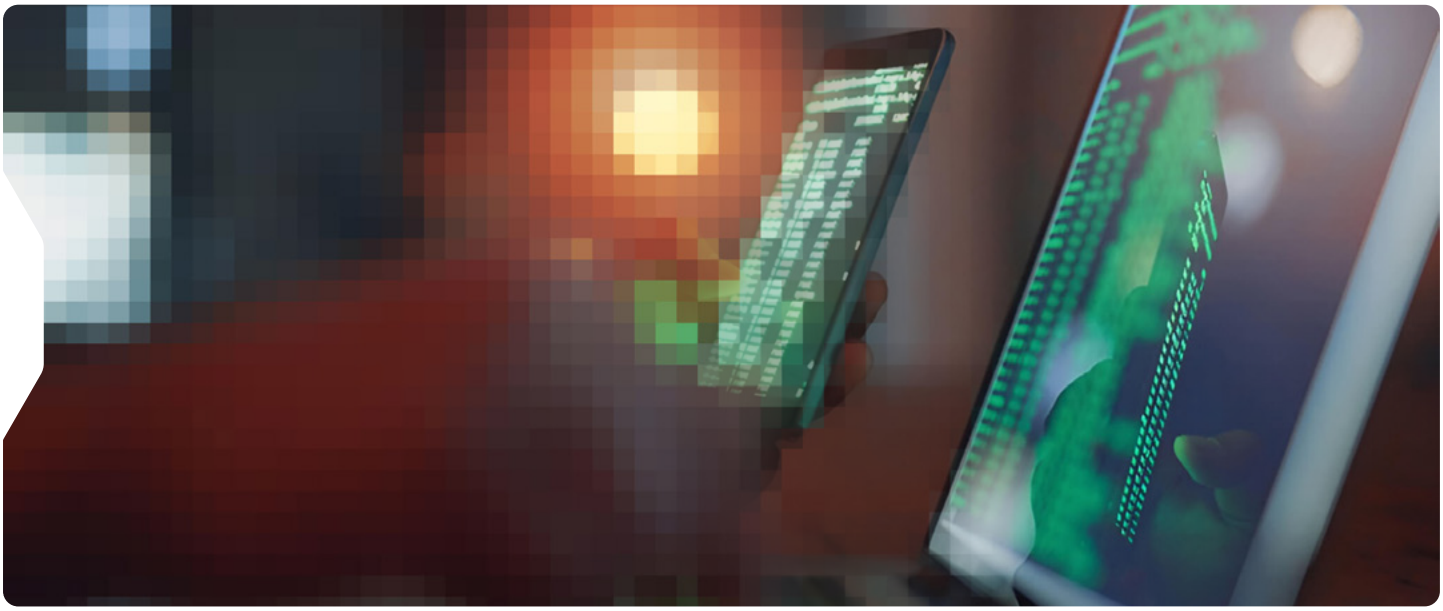
Joanne Zaaijer
Partner
Osborne Clarke Netherlands
+31 207 02 86 22
Email Joanne
Full bio

Mark Taylor
Partner
Osborne Clarke UK
+44 20 7105 7640
Email Mark
Full bio

Paula Margolis
International Key Client Knowledge Lawyer
Osborne Clarke UK
+44 207 105 7177
Email Paula
Full bio

REGULATORY IMPACTS

Class Actions: An Imminent Disruptor in European Digital Markets



Class actions are becoming a defining dynamic in Europe's digital economy, giving private claimants new tools to pursue legal remedies ahead of regulatory enforcement. New procedural tools for seeking redress on behalf of large claimant groups – particularly consumers – have made class actions a viable way to challenge the conduct of large businesses in digital markets through private litigation, rather than waiting for regulators to act on behaviour perceived to harm consumers.

This shift is creating new forms of exposure for digital platforms and other substantial online businesses, particularly those that influence how users engage with online services. At the same time, it is giving online retailers, publishers and start-ups a more collective means of exerting pressure and seeking redress.

Litigation is accelerating, but how quickly – and in what form – still depends on where claims are filed, how they are funded and how businesses operate. For digital businesses, whether defending an entrenched position or pushing for change, class actions are a live and evolving pressure point.

Business Models Under Scrutiny

Class actions in digital markets are increasingly focused on the structure of digital ecosystems. Instead of targeting one-off incidents, this litigation is coalescing around design features that govern pricing, access and user interaction – especially where those features apply systemically and at scale.

Direct-to-consumer (D2C) models remain a common entry point for collective actions. Commission structures, in-app purchase restrictions and third-party payment limitations create repeatable patterns that support competition and consumer law claims.

Exposure grows when one company can influence how others participate in the digital ecosystem – for instance, by controlling distribution, advertising or payment channels. Even where conduct is normalised, these embedded dynamics may trigger legal scrutiny if they appear to distort market outcomes. In this context, risk stems less from isolated policies or pricing decisions than from the structure of the commercial model itself.

> "It's not just what a business does, it's how it structures participation across the market that now invites legal attention."
>
> **Jeroen Bedaux**, Partner, Osborne Clarke Netherlands

While platforms were the initial focus, the logic of these claims is migrating. Legal strategies developed in early platform disputes are now being adapted to challenge a wider range of business models, including those whose operational features – such as data stewardship, interface design or access control – are drawing scrutiny under competition and consumer law frameworks.

As this trend accelerates, exposure is less about whether a company is a platform, and more about how it shapes participation and advantage in digital markets. Increasingly, those design choices are being reinterpreted through today's legal standards, with claims using evolving regulatory expectations to challenge past conduct.

Backward Claims, Forward Regulation

Meeting new regulatory standards is often treated as a milestone, a sign that risk has been mitigated and scrutiny defused. But in the context of class actions, that confidence can be misplaced. New compliance may feel like protection, but in class actions it can serve as ammunition, supporting claimant arguments that earlier conduct had anticompetitive or exclusionary effects.

Just as regulators might impose fines for previous behaviour and require compliance going forward, private litigants might seek damages for the past and seek access – or other types of specific performance – for the future. Their arguments often rest on counterfactuals: how would the market have evolved if a certain design or restriction had never been introduced? A pricing model or access restriction that now meets Digital Markets Act (DMA) requirements can still be used to anchor retrospective claims, particularly if new rules are cited as evidence of what a competitive baseline should have looked like. Without regulatory findings at the time, companies may find themselves defending past conduct against present-day expectations.

> “Even compliant models can become legal battlegrounds when claimants ask: what if you had acted sooner?”
>
> **Aqeel Kadri,** Partner, Osborne Clarke UK

Compliance, in other words, does not equal immunity. Even practices that have been revised or permitted under current regimes may be scrutinised through a backward-looking lens, as general competition rules apply in addition to the rules for the digital industry. In this environment, litigation strategy must account for shifting narratives, evolving benchmarks as regulatory requirements are reinterpreted in court.

This risk calculus becomes even more complex when layered over procedural variation. As litigation narratives start to take form, their viability and impact are sharpened – or softened – by where they land.

Where Claims Land First

In collective litigation, jurisdiction is not a neutral backdrop, it is a tactical lever. Once a claim theory has taken shape – whether based on past conduct or regulatory comparisons – its momentum often hinges on procedural specifics: how quickly a court moves, whether opt-out mechanisms apply and how easily a claim can be certified or funded.

For digital businesses operating across Europe, this creates a shifting procedural map – one where similar claims may surface in multiple venues, each applying different legal and procedural standards to common facts. Navigating this terrain requires more than local awareness. Messaging must remain consistent across borders, as arguments advanced in one jurisdiction may be scrutinised or repurposed in another. These dynamics are most visible in jurisdictions that have become focal points, owing to procedural frameworks that make collective action more viable.

The UK, Netherlands and Germany remain at the forefront of European private enforcement, supported by efficient court systems, structured procedures and familiarity among funders and claimant firms. But other jurisdictions are gaining ground. Portugal has seen steady growth since transposing the EU’s Representative Actions Directive (RAD) into national law in December 2023, introducing a new opt-out regime and clearer procedural rules for collective redress. Likewise, Spain is drawing increasing interest as it finalizes its own RAD implementation – with claimant firms watching closely to see whether opt-out mechanisms will be permitted, a move that could quickly transform it into a key venue for consumer-focused claims. In this regard, the Spanish Parliament reactivated the processing of the class actions bill last March, which is currently in the period for submitting amendments.

> “We’re seeing strong claimant interest in Spain ahead of the RAD’s implementation. If opt-out mechanisms are adopted, it could become an even more active jurisdiction, especially for high-volume consumer claims that are currently looking for a procedural foothold.”
>
> **Rafael Montejo**, Partner, Osborne Clarke Spain

While these jurisdictions offer procedural advantages, claimants are not free to file anywhere. Most systems still require a territorial link – a factual or commercial connection to the forum. But once that threshold is met, procedural and funding dynamics often drive where actions are brought. Sophisticated firms assess where collective mechanisms are favourable, where funders are active and where procedural delays are minimal.

Jurisdiction may shape where class actions land, but the conditions giving rise to those claims are also shifting. As litigation increasingly decouples from regulatory timelines, it is evolving into a flexible tool shaped by a widening range of actors and incentives.

Class Action Triggers

The changes discussed above mean that regulators and consumer groups are no longer solely driving enforcement. A growing ecosystem of funders and claimant-side firms is using litigation to obtain redress for large groups. Many of the latter are working in coordination with experienced US class action teams, whose expansion into European markets has brought expertise in pursuing collective claims. Across this landscape, players are actively identifying opportunities to pursue large-scale litigation, sometimes following the path of regulators in other jurisdictions, or replicating private claims brought elsewhere. As regulatory gaps, media scrutiny and market shifts increasingly serve as catalysts, the sources of litigation risk are increasing – with claims emerging from a wider range of triggers and escalating more quickly than before.

Investor sentiment can amplify the pressure. When legal challenges target core revenue models, perceived exposure may ripple through markets well before any finding of liability. For companies operating across jurisdictions, class actions are no longer a secondary risk. As claims emerge from diverse sources and move on unpredictable timelines, collective litigation is becoming a strategic variable – one that shapes commercial decisions and demands anticipatory legal planning, even in the absence of enforcement signals.

Shaping Digital Markets

Class actions are no longer just a legal aftershock. In digital markets, they have become a meaningful way to test business models – sometimes before regulators act, and often with real operational consequences. As claims shift from isolated incidents to structural design features, they are forcing companies to defend both the outcomes they deliver and the structures that produce them.

For firms that influence access, pricing or user experience at scale, litigation strategy can no longer be reactive. Class action exposure can develop quickly when intersecting factors combine to compound risk. Legal teams must therefore track early signals – from product changes and regulatory drift to competitor pressure and funding activity – while also monitoring how legal arguments evolve and travel across jurisdictions.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

Aqeel Kadri

Partner
Osborne Clarke UK
+44 207 105 7367
Email Aqeel
Full bio

Jeroen Bedaux

Partner
Osborne Clarke Netherlands
+31 207 02 86 14
Email Jeroen
Full bio

Roderick Nieuwmeyer

Partner
Osborne Clarke Netherlands
+32 2 515 9423
Email Roderick
Full bio

Rafael Montejo

Partner
Osborne Clarke Spain
+34 91 576 44 76
Email Rafael
Full bio

REGULATORY IMPACTS

Navigating the Next Phases of Digital Regulation

Over the past decade, digital regulation has moved from the margins to the mainstream, becoming a strategic priority at the heart of global policy agendas. The "lighter touch" approach of the early 2000s – with more emphasis on fostering innovation and protecting expression – has shifted towards intervention, with new rules targeting privacy, consumer protection, online safety and market fairness.

Groundbreaking frameworks such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the UK's Online Safety Act sought to strike a balance between innovation and consumer protection, while transforming how businesses approach compliance and accountability.

This has paved the way for a new era of heightened enforcement. Regulators are now proactive enforcers, issuing multimillion-euro fines and driving global standards. As a result, organisations are working to mitigate enforcement risks, which requires the implementation of internal response structures and cross-function coordination.

Yet the story is far from over. With new technologies expecting to attract regulatory response, legal teams are likely to question how the future digital regulation landscape will present amidst simplification efforts and pro-growth narratives, and whether significant new changes might still be coming down the line.

Put another way, with landmark digital regulations in force, have we now in fact reached the peak of digital regulation, and the dawn of a period of stability and refinement? Or, are we moving into a more complex phase, shaped by strategic divergence, increased and differing approaches to enforcement, and a new and more targeted focus on fairness and consumer welfare?

Geopolitical Pressure Points

Strategic divergence is now a hallmark of the digital regulatory landscape, driven by political and economic priorities.

In the US, a second Trump administration was expected to usher in a deregulatory agenda which would redefine the government's role in overseeing digital platforms and emerging technologies. Focus on AI leadership and development rather than increased oversight reflects a strategic bid to boost US competitiveness and counter China's influence in global tech standards.

In the EU, calls for regulatory simplification are gaining political attention, even as the broader legislative agenda continues to expand. Former European Central Bank President Mario Draghi's 2024 report warned that complex digital laws were constraining growth, prompting the European Commission to explore ways to reduce compliance burdens, particularly for SMEs. While a limited GDPR simplification proposal has been confirmed to ease record-keeping burdens, broader discussions have also emerged around reducing overlap between digital laws including the DSA, the DMA and the AI Act.

The UK, meanwhile, has signalled regulatory reform through its March 2025 policy paper, which outlines plans to reduce friction for businesses, particularly SMEs, and to ensure a more agile and innovation-friendly digital regulatory framework. Nevertheless, this sits uneasily alongside other developments. For example, the Digital Markets, Competition and Consumers Act 2024 introduced a consumer law regime that is, in many respects, more complex than the EU's.

Elsewhere, more protectionist instincts are influencing the agenda. For example, India's proposed Digital India Act introduces tight controls on data and platform governance, with stringent obligations for online content platforms and providers.

These diverging models are reshaping the regulatory risk map and increasing fragmentation.

> "To maintain operational resilience, legal teams must be equipped to adapt to evolving priorities across jurisdictions and to structure flexible compliance strategies that accommodate these new challenges."

Rafael García del Poyo, Partner, Osborne Clarke Spain

A Compliance Paradox?

While simplification and pro-growth initiatives are gaining momentum, this does not always mean fewer rules or reduced burdens. Conversely, they can introduce transitional complexity – what might aptly be described as a compliance paradox.

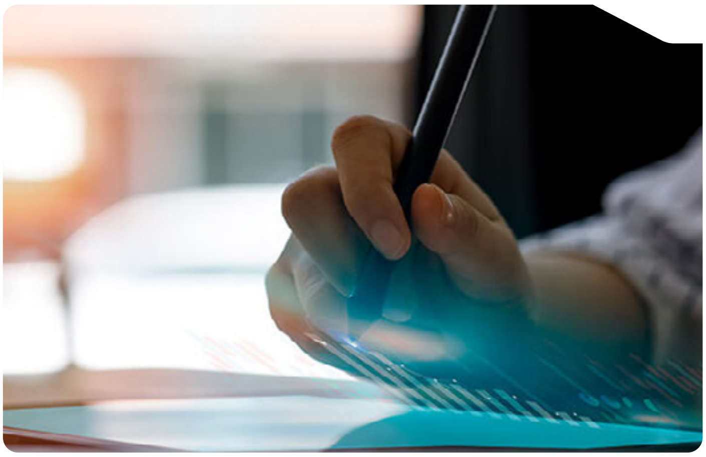
While the UK's Data (Use and Access) Act (DUA Act) aims to modify the UK GDPR to simplify and ease compliance in areas such as clarifying the definition of legitimate interest and easing the requirements around automated decision-making, it also introduces a framework for a new data sharing regime that some organisations will need to comply with. This is likely to involve making adjustments to processes and policies.

Meanwhile, the EU is also exploring ways to streamline digital regulation and make enforcement more effective. This includes efforts to harmonise overlaps and contradictions between the GDPR, the DSA, the DMA and the AI Act. For example, it is working to ensure the proposed Digital Fairness Act (DFA) – which is expected in 2026 and aims to tackle issues including unethical practices relating to dark patterns and addictive design – avoids duplication with digital rules. The slated withdrawal of its proposed ePrivacy Regulation and AI Liability Directive also reflects concerns over unnecessary overlap with new and existing laws.

The EU Competitiveness Compass, introduced in January 2025, includes other simplification proposals. Among its proposed solutions is the "28th legal regime", an optional EU-wide framework that will offer new and growing businesses a single, uniform set of rules, including relevant aspects of corporate law, insolvency, labour and tax laws. Nevertheless, as the proposed regime would sit alongside rather than replace national regimes, it risks creating an optional parallel framework that exacerbates divergence by creating one more way to comply rather than a singular approach.

> "Simplification does not always mean alignment and harmonisation. It can lead to additional divergence and fragmentation between regions."

Henrik Bergström, Partner, Osborne Clarke Sweden



Next-Gen Regulation

Simplification efforts are unfolding alongside the surfacing of a new wave of digital regulation – one that is increasingly values-driven and concerned with societal impact. While the most recent generation of laws established core frameworks for data protection, competition, platform accountability and online safety, this next wave is expanding into social and political domains whilst tackling the complexities of emerging technologies and sector-specific risks. These shifts are likely to generate more work for legal teams, who will be navigating and seeking to comply with this evolving regulatory landscape.

> "Legal departments will need to continue growing their digital regulation teams to keep pace with this next wave"

Claire Bouchenard, Partner, Osborne Clarke France

Key Drivers of New Digital Regulation

New and Emerging Technologies

Technological advancements such as generative AI, synthetic media and quantum computing are drawing regulatory attention, not only for their transformative potential and associated risks, but also for their potential societal consequences. For example, the misuse of generative AI and synthetic media can blur the lines between fact and fabrication, leading to the manipulation of public opinion and erosion of trust. Similarly, with its potential to disrupt critical areas of security and governance, quantum computing challenges current cybersecurity, data protection, and encryption standards.

Policymakers across jurisdictions are responding by establishing frameworks that promote innovation while ensuring transparency, accountability and societal safeguards – although responses vary. Generative AI, particularly in the form of large language models, has prompted renewed scrutiny of existing laws, with legal concerns ranging from misinformation and algorithmic bias to balancing the conflicting agendas of rightsholders and AI developers under copyright law. Some jurisdictions are applying established IP and consumer protection laws while others are developing new instruments. The European AI Office, for example, has been drawing up a voluntary General-Purpose AI Code of Practice to be used by providers to demonstrate compliance with the AI Act. In the UK, concerns around the use of copyright materials to train AI were extensively debated in the lead-up to the passing of the DUA Act. Although the Act does not make changes to copyright law, the government has agreed to publish an economic impact assessment and a report on its copyright and AI proposals within nine months. The UK's recent consultation on AI and copyright outlines potential changes to IP law to address training data concerns, and the government is considering its position in light of the responses received.

Synthetic media also raises complex legal concerns from identity rights and consent to misinformation and content governance. The audiovisual sector has adopted contractual protections, including safeguards secured through the SAG-AFTRA strikes in the US, to protect performers' likenesses. Elsewhere, national responses remain fragmented: the EU AI Act introduces transparency rules for synthetic content whereas the UK and the US are prioritising stronger protections for children and vulnerable users through the Online Safety Act and the US Kids Online Safety and Privacy Act (KOSPA), respectively.

In contrast, India's proposed Digital India Act would give broad discretionary powers to regulate high-risk AI, aligned with its goal of tackling misinformation, although this has drawn concerns over transparency and civil liberties.

Sector-Specific Shifts

Financial services regulators are also tackling broader societal concerns such as financial inclusion and consumer welfare, albeit pulling in different directions. While the UK moves to close gaps in consumer protection – from crypto asset oversight to buy-now-pay-later schemes – the US continues to rely on a fragmented mix of agency guidance and litigation, without a unified crypto regime or consistent lending protections.

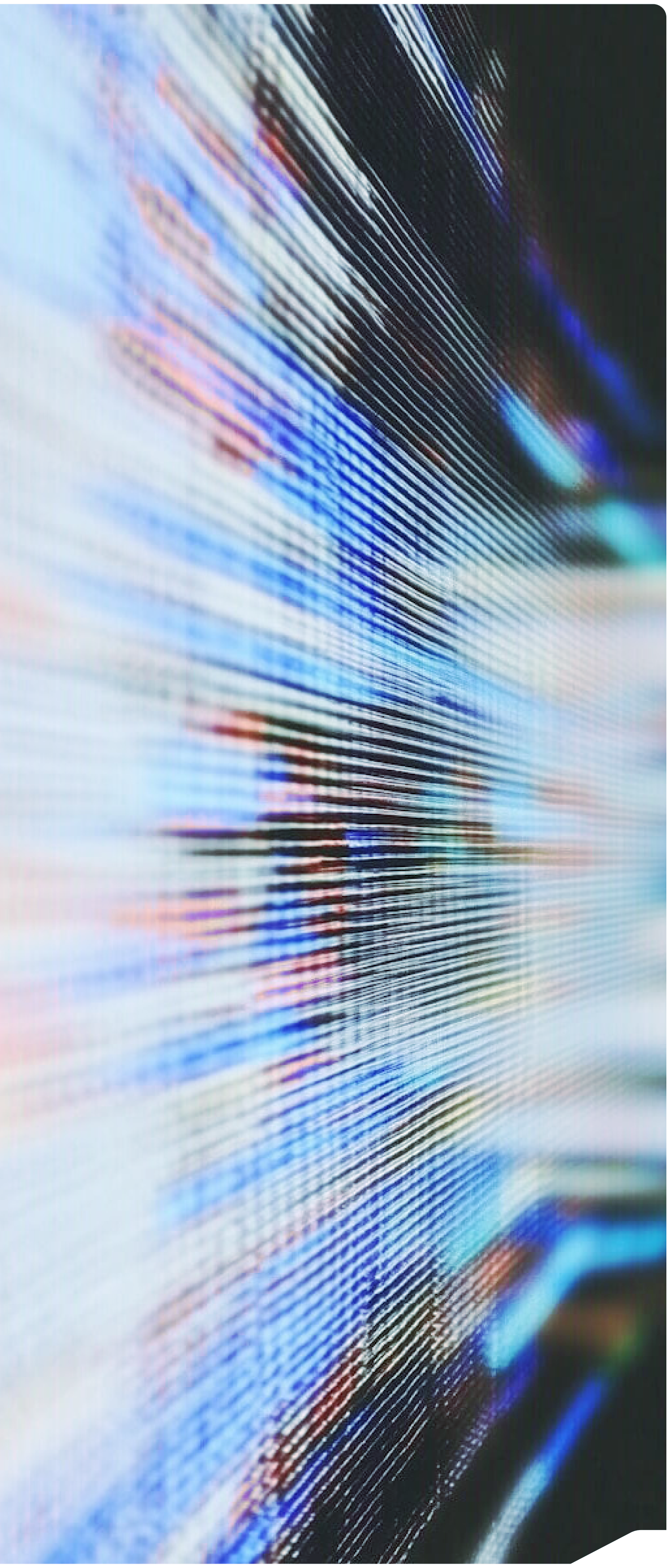
Within life sciences and healthcare, regulatory frameworks for AI-enabled technologies are increasingly being shaped around patient trust and tackling bias, but in different ways. The EU's approach is anchored in the AI Act, which classifies medical devices as "high risk" – meaning more stringent obligations around human oversight and data quality. While the US lacks a single regulatory framework, FDA initiatives such as its AI/ML-Based Software as a Medical Advice Action Plan are embedding trust and transparency into AI products and tools. Similarly, the UK's Software and AI as a Medical Device Change Programme includes a workstream on "Assurance of Trust" focussed on transparency and explainability for patients and clinicians as well as bias detection and mitigation.

Safety and Democracy

Themes such as addictive design, the protection of minors online and election integrity are also gaining traction across jurisdictions.

The EU's proposed DFA, as well as laws and initiatives such as KOSPA and the UK's Children's Code, aim to comprehensively tackle the challenges arising from online practices such as dark patterns and addictive design, particularly where minors are at risk. Following the publication of its guidance on how to protect children from harmful content online, UK regulator Ofcom has made clear that it is getting ready to take early enforcement action against services that do not comply.

The EU's DSA Elections Toolkit promotes transparency in political ads and content moderation with the aim of safeguarding democratic processes from digital interference. Comparable initiatives in India, the US and Southeast Asia vary widely in enforcement and scope – underscoring how shared risks still yield distinct national responses.



Preparing for the Next Phase

Digital regulation has not reached its peak – rather, it is entering a new chapter that is shifting in tone and focus.

Looking back, the very first wave of digital regulation, established in the lead-up to the new millennium, was characterised by a reactive, sector-neutral approach, largely aimed at supporting the growth of the internet in the dotcom era. This laid the foundations for the most recent wave, which created landmark digital frameworks and increased platform accountability.

The new chapter we are now entering will test the bandwidth of digital regulation teams in three key ways:

- First, digital regulation enforcement risk has significantly increased, with more laws, higher fines, and regulators that are more active and better resourced. Organisations will face more regulatory enquiries and challenges and may need to recalibrate risk-based stances.
- Second, the simplification-driven regulatory changes emerging in many jurisdictions will need to be assessed and absorbed.
- Third, the new wave of digital regulation – more values-led and increasingly centred around consumer welfare, digital fairness and societal impact – is driving fresh lobbying and readiness.

As a result, organisations will need deeper and more nuanced thinking from their legal teams. Legal must adopt a more integrated and strategic role, shaping governance and compliance structures as well as educating product, commercial and technical teams on evolving regulatory requirements.

Crucially, as regulatory enforcement gathers pace, and with private enforcement gradually gaining traction, now is not the time to dial down on resources. Investment in legal and regulatory infrastructure will be critical to tracking jurisdictional divergences as well as highlighting conflicting enforcement priorities across key markets.

Visit **Osborne Clarke's Digital Regulation Timeline** to monitor developments.

Contributors

We would like to thank these individuals for having shared their insight and experience on this topic.

John Davidson-Kelly

Partner

Osborne Clarke UK

+44 207 105 7024

Email John

Full bio

Konstantin Ewald

Partner

Osborne Clarke Germany

+49 221 5108 4160

Email Konstantin

Full bio

Tamara Quinn

Director – AI, Data & IP Knowledge

Osborne Clarke UK

+44 207 105 7066

Email Tamara

Full bio

Paula Margolis

International Key Client Knowledge Lawyer

Osborne Clarke UK

+44 207 105 7177

Email Paula

Full bio

Rafael Garcia del Poyo

Partner

Osborne Clarke Spain

+34 91 576 44 76

Email Rafael

Full bio

Henrik Bergström

Partner

Osborne Clarke Sweden

+46 72383 5301

Email Henrik

Full bio

Claire Bouchenard

Partner

Osborne Clarke France

+33 1 84 82 45 30

Email Claire

Full bio

Osborne Clarke

Osborne Clarke is the business name for an international legal practice and its associated businesses.

Full details here: osborneclarke.com/verein

These materials are written and provided for general information purposes only. They are not intended and should not be used as a substitute for taking legal advice. Specific legal advice should be taken before acting on any of the topics covered.

Publication number OSB.DRW.003 06/25