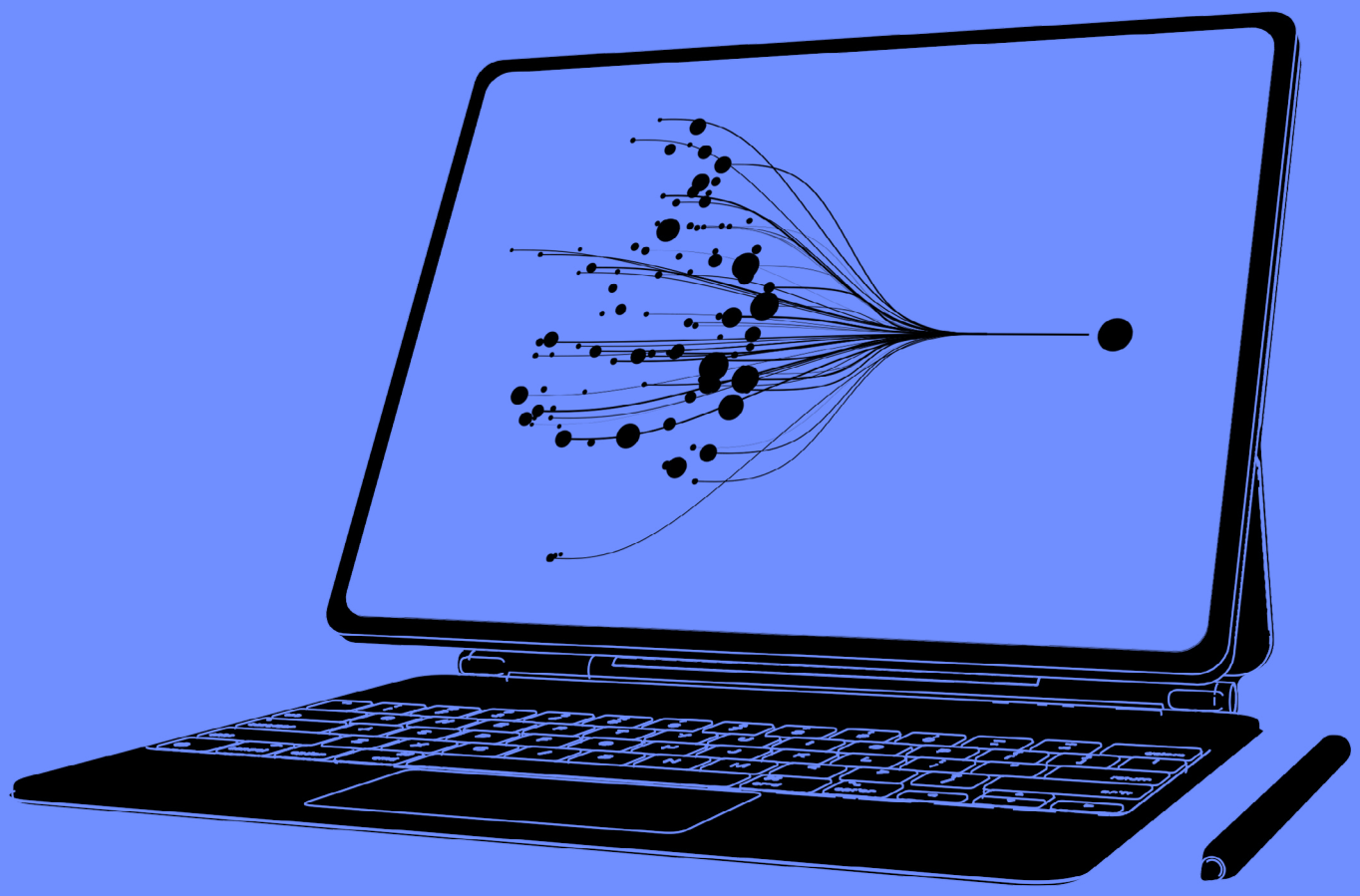
FRESHFIELDS

Data law trends 2026

Exploring the interface of law, AI, and global data.



Contents

Executive summary

The 2026 Data Law Trends report reveals a world in which businesses confront an increasingly complex, multi-polar regulatory environment.

Data law has become a global fault line: divergent rules, intensifying enforcement and competing agendas across jurisdictions are fracturing what businesses once considered predictable.

From the expansion of AI oversight to new limits on data transfers, child privacy regulations and cybersecurity guardrails, the legal landscape is evolving rapidly – and no market is immune.

Where change is accelerating, old assumptions no longer hold. Many businesses are discovering that yesterday's compliance playbooks won't work in today's multi-polar environment. Data laws are shaping everything from risk management to growth opportunities, and staying ahead of these shifts is critical.

> In 2026, data law has become a geopolitical and commercial chessboard for nations and businesses alike. Success now depends on mastering a fragmented global landscape. This report provides the strategic foresight needed to turn divergence and complexity into a competitive advantage.
>
> **Giles Pratt and Christoph Werkmeister**
> Global Co-heads of the Freshfields data privacy and security practice.

This year's developments build on last year's momentum but come with new urgency. Enforcement is more aggressive, regulatory silos are breaking down and issues – from algorithmic fairness to cross-border data flows and content safety – are broader than ever.

Inside, you will find:

1. **The global surge in data privacy mass claims**
2. **An increasingly fractured global rulebook for data, cyber, and AI**
3. **Why businesses must rethink their approach to young people's data**
4. **Rising risks and shifting rules for international data transfers**
5. **AI now a board-level imperative for public companies and investors**
6. **Regulatory convergence grows across sectors and borders**
7. **The fragmented global landscape for anonymization**

This report is your early warning system, your trend-map and your strategic briefing rolled into one. It helps you see what's coming, understand what matters and respond effectively.

The next chapter of data law is being written.

Your guide to navigating it starts here.

1.

The global surge in data privacy mass claims

In brief

Navigating the complex landscape of data-related litigation has never been more critical. Across major jurisdictions – including Germany, the Netherlands, England and Wales, and the US – the rules of engagement are changing rapidly. What were once straightforward claims are now sophisticated collective actions and bundled proceedings, driven by new regulation and innovative funding models.

Businesses face a heightened risk of multi-pronged attacks seeking not only large damages, but also injunctions that can disrupt core operations. Understanding these shifting trends is essential for proactive risk management, robust defense strategies and limiting legal exposure.

The global picture

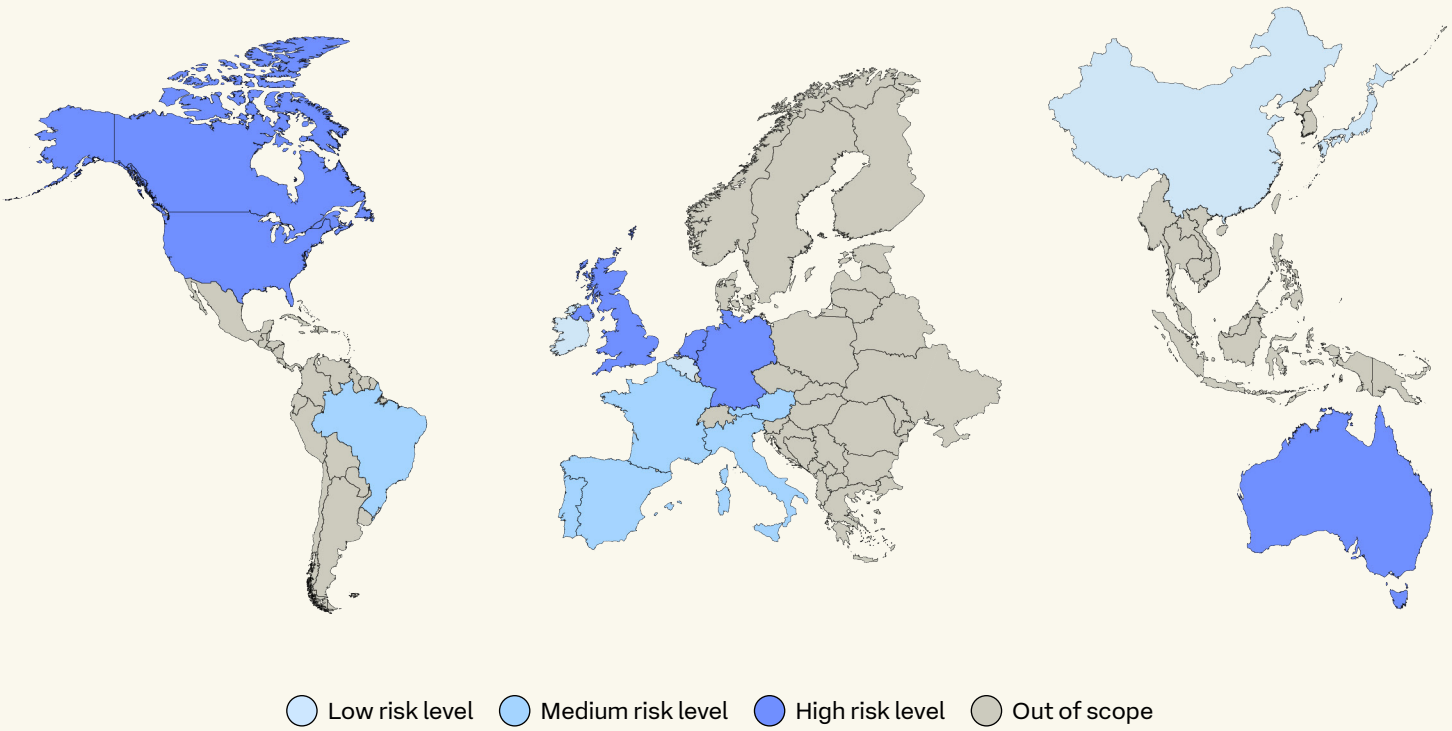
Few threats have escalated with the speed, scale and financial menace of mass data privacy litigation. Once a niche concern, collective privacy claims have become a primary driver of complex, high-stakes legal battles – threatening not just balance sheets but entire business models, as individually low value claims by thousands or millions of data subjects can quickly turn into millions or billions in potential damages.

This development reflects a convergence of factors, including:

- an expanding patchwork of laws codifying enforceable data rights for individuals (e.g. under the EU General Data Protection Regulation (GDPR), UK GDPR and various US state laws);
- the emergence of a sophisticated and well-capitalized ecosystem of claimant law firms and third-party litigation funders;
- increased public awareness and concern regarding data rights;
- new collective action mechanisms, such as the Netherlands' Act on Collective Damages Claims (WAMCA) and the EU's Representative Actions Directive (RAD); and
- the rise of 'non-attack' claims – lawsuits arising not from breaches but from routine data processing activities such as the use of ad-tech and tracking cookies.

Risk of class and collective actions

This heatmap highlights certain high-, medium- and low-risk jurisdictions for class and collective actions (including data breach, tech and other litigation), based on Freshfields' experience and our 2025 Class and Collective Action Guide.



This chapter focuses on four high-risk jurisdictions: Germany, the Netherlands, England and Wales and the US.

Germany: A new era for collective actions

Germany is experiencing a rise in collective actions, particularly in GDPR and technology-related claims. Consumer organizations are not only seeking damages, but also pursuing injunctions to halt data processing activities – forcing businesses to mount rapid and robust defenses. While legal insurers remain cautious about funding individual claims, a trend toward higher GDPR damage awards may change that. Litigation funders are also entering the field, acquiring claims from thousands of individuals and pursuing them in bundled proceedings, often through special purpose vehicles (SPVs).

At the same time, defendants are developing novel strategies to challenge the standing of consumer organizations and SPVs, offering new options to manage business-critical litigation risks.

A key issue to watch is the Court of Justice of the EU's (CJEU) guidance on whether 'loss of control' constitutes a basis for damages under the GDPR.

Its clarification will shape both the prerequisites for and the quantum of damages, with major implications for corporate risk management.

Practical implications: Businesses must be prepared for multi-pronged attacks – claims for damages and injunctions, brought, often in parallel, by consumer organizations, commercial SPVs and individual claimants. A robust response strategy is crucial to minimize risk and operational disruption. Monitoring CJEU developments is equally critical.

> In Germany, legal strategy is no longer just about defending against damages – it's about disrupting professional plaintiffs' business models to guard against an increasingly aggressive data litigation landscape.
>
> **Martin Mekat**
> Partner

The Netherlands: The go-to jurisdiction for mass claims

The Netherlands remains a magnet for class actions, with nearly 100 active cases on the docket. The Dutch WAMCA is widely regarded as claimant- and funder-friendly, offering an opt-out system and monetary damages. Success fees for litigation funders – sometimes up to 25 percent of a claim's value – make the regime especially attractive.

That said, legal uncertainties remain. The interplay between WAMCA and the EU RAD is unresolved, and questions around additional national admissibility rules and opt-out damages under the GDPR are before the CJEU in a major case against Amazon. Recent judgments suggest closer scrutiny of claimant organizations, but pending legislative amendments may tilt the balance back toward plaintiffs.

Practical implications: The Netherlands remains a high-risk jurisdiction for data and tech businesses. Because of the opt-out mechanism, a single action can create massive exposure. Businesses should closely monitor forthcoming CJEU decisions and the legislative review of WAMCA to anticipate shifts in the legal landscape.

> The Netherlands consolidates its position as a premier venue for mass claims in the EU. The key challenge for defendants is the sheer scale and financial exposure that the WAMCA's opt-out system brings.
>
> **Mark Egeler**
> Partner

England and Wales: Adapting to new challenges

Following the Supreme Court's 2021 *Lloyd v Google* decision, bringing data-related opt-out representative claims in England and Wales has become more difficult: 'loss of control' was found not to be enough for a damages claim, and claimants must show actual financial loss or distress.

The Court of Appeal reinforced this in *Prismall v Google* (2024), reiterating the high threshold for claimants in an opt-out representative claim to meet the 'same interest' requirement. In a misuse of private information claim, this meant each claimant had to demonstrate a reasonable expectation of privacy over the affected data.

It is also worth noting the Court of Appeal's August 2025 decision in *Farley and Others v Paymaster*, which found no *de minimis* threshold for data protection claims (as distinct from misuse of information claims). Instead, a claimant must establish that any harm alleged was 'well-founded' by reference to the facts known – or that should have been known – to them at the time.

It is clear, therefore, that data mass claims remain a real prospect. Claimant firms continue to advertise that they have recruited thousands of clients after data breaches, while recent high-profile cyberattacks have driven more activity. The *Lloyd* decision has pushed claimant firms and funders toward Group Litigation Orders and collective proceedings in the antitrust space to bundle claims. Courts are also showing procedural flexibility, including through the use of the 'lead claimant' model.

Additionally, the Supreme Court's 2023 judgment in *R (PACCAR) v Competition Appeal Tribunal* made litigation funding more difficult, ruling that funding agreements based on a percentage of damages are unenforceable. However, funders are adapting. In July 2025, the Court of Appeal held that 'multiple of investment' litigation funding agreements are enforceable, and in August 2025, it overruled a lower court to breathe fresh life into another mass claim – illustrating the fast-moving funding environment.

Practical implications: While the *Lloyd v Google* ruling made mass data breach claims by way of opt-out representative action more difficult, it did not shut them down. Claimant firms are finding creative paths forward, even where claims are low in value. Businesses should be prepared for more innovative forms of case management and funding arrangements.

> Data breach actions remain a focus for claimant firms, with recent rulings driving a push toward more creative forms of case management. There are potential gains to be made by embracing novel approaches that may offer a cheaper and quicker route to resolving mass data breach claims.
>
> **Cat Greenwood-Smith**
> Partner

United States: Expansion of privacy class actions

The US is poised for a surge in data breach class action litigation, driven by three main trends:

First, federal courts are providing expansive interpretations of state privacy laws, particularly the California Consumer Privacy Act (CCPA), allowing lawsuits over common tools such as cookies and pixels. This is a crucial development since the CCPA applies to certain companies, regardless of location, that collect or process California residents' personal information – and it remains the only comprehensive state privacy law granting a private right of action for data breaches.

Second, healthcare-sector lawsuits are increasingly moving past early dismissal stages, raising settlement pressure given the strong jury appeal of sensitive health data. New state health privacy laws, such as Washington's, are also creating new avenues for claims, including private rights of action.

Third, recent securities class actions against tech companies have resulted in multimillion-dollar settlements, with plaintiffs alleging failures to disclose – or misleading statements about – data breaches. This trend is reinforced by heightened scrutiny from the US Securities and Exchange Commission (SEC).

Practical implications: Regardless of where they are based, businesses with US customers face risk from the patchwork of state privacy laws. Even everyday web technologies may trigger litigation. Robust data breach response plans and careful disclosure practices are essential to reduce exposure.

> In the US, the playbook for data breach litigation is being rewritten. Companies must now look beyond traditional data theft and recognize that even everyday web technologies are being used as a new tool for sophisticated class actions.
>
> **Tim Howard**
> Partner

Looking ahead

The global data litigation landscape is becoming more aggressive and complex. Businesses cannot afford to be reactive – proactive, multi-jurisdictional strategies are essential.

In Europe, forthcoming CJEU rulings on GDPR damages will be crucial. In the US, state laws and expansive court interpretations are rewriting the playbook. Global businesses must monitor these developments closely and build resilient, cross-border strategies to manage the risks.

2.

An increasingly fractured global rulebook for data, cyber, and AI

In brief

The global landscape for data, cyber and AI is shifting fast. Deregulatory moves under the Trump 2.0 administration are in direct tension with the EU's enforcement-driven digital strategy.

The US is betting on an innovation-first model, while the EU AI Act is reshaping how companies operate. Meanwhile, the UK and countries across the APAC region are pursuing their own, often divergent approaches.

For businesses, the result is a fractured environment where policies have areas that align and conflict across AI governance, data transfers, cybersecurity and consumer protection. Navigating these crosscurrents is now critical to managing risk – and unlocking opportunity – in the digital economy.

Trump's AI reset: Innovation first

Since retaking office in January 2025, the Trump administration has made clear its commitment to AI innovation and desire to remove regulatory barriers and boost investment in US-based AI companies.

The day after his inauguration, President Trump announced a US$500bn private sector investment project in AI infrastructure. The following month, Vice President J.D. Vance spoke at the AI Action Summit in Paris, outlining the administration's plans to clear the way for AI innovation and move away from the Biden administration's focus on AI safety.

The actions taken by President Trump in the immediate weeks following inauguration confirmed this shift, including the signing of a flurry of AI-related executive orders to enact an innovation-forward approach and the revocation of some of Biden's executive orders focused on AI safety.

The release of an unprecedented American AI Action Plan and additional related executive orders in July 2025 affirmed the administration's new direction.

Despite the federal government's change in approach, some US states are maintaining a focus on AI safety regulation. For example, California recently passed the 'Transparency in Frontier Artificial Intelligence Act' — a new AI law that is narrower in scope than the EU AI Act but imposes overlapping requirements related to AI transparency, governance and incident reporting.

The Trump administration's new approach to AI innovation has also led to recent policy and personnel changes at US federal agencies. For example, in January 2025, the Equal Employment and Opportunity Commission removed Biden-era AI guidance on the application of federal anti-discrimination law to the use of AI for employment decisions.

The Department of Labor similarly signaled its 'AI & Inclusive Hiring Framework' may no longer reflect current policies. In May 2025, soon after the US Copyright Office published a report assessing the legality of the use of copyrighted material to train AI models, the Trump administration fired the head of that agency, which could be construed as a rejection of the report's conclusions.

US AI and free speech

At the same time the AI Action Plan was released, President Trump signed an executive order entitled 'Preventing Woke AI in the Federal Government,' which signaled the Trump administration's other top priority alongside American-led AI innovation: ensuring this AI is free from 'ideological bias.' While this executive order echoed themes of deregulation ('the Federal Government should be hesitant to regulate the functionality of AI models in the private marketplace'), it also emphasized the obligation on federal agencies to ensure they are only procuring AI technologies that are 'truth-seeking' and developed with 'ideological neutrality.'

This focus on 'ideological neutrality' in technology is not new for President Trump. On his first day back in office, he made clear his aggressive stance on countering perceived censorship on online platforms when he signed an executive order entitled 'Restoring Freedom of Speech and Ending Federal Censorship.'

Also concerning speech issues, combatting AI-washing, AI-generated deepfakes and other AI-related consumer harms has been a continued focus of federal agencies like the US Federal Trade Commission (FTC) and the US Securities and Exchange Commission, and by Congress.

For example, in 2024, the FTC announced a crackdown on deceptive AI practices; in line with this AI-washing focus, the FTC issued an order in April 2025 alleging a marketing content company had made false claims about its AI capabilities. In May 2025, Congress passed the 'TAKE IT DOWN Act' to criminalize non-consensual publication of intimate images, including deepfakes.

> AI and other tech companies face strong crosswinds from the Trump administration. Many see opportunity in the Trump administration's removal of AI regulations. However, companies must take care to ensure they do not run afoul of rules the Trump administration has set for 'ideological neutrality,' and can continue to expect scrutiny of their products, including by the Federal Trade Commission and state Attorneys General.
>
> **Beth George**
> Partner

Continuity in US cyber and child safety

While the Trump administration has diverged from the Biden administration in notable ways when it comes to its approach to AI, it has continued the efforts of the prior administration in other areas of tech regulation.

> The expansion of AI solutions presents unique security risk exposures that merit analysis and the development of relevant mitigation strategies.
>
> **Brock Dahl**
> Partner

For example, the US Department of Justice and a member of the FTC have signaled that their agencies will enforce rules from the prior administration regulating US data transfers to foreign adversaries, including under the new Data Security Program initiated under a Biden-era executive order and the Protecting Americans' Data from Foreign Adversaries Act passed in 2024. In June 2025, President Trump signed an executive order maintaining certain federal cybersecurity efforts by President Biden (including federal efforts around post-quantum cryptography, Border Gateway Protocol, and advanced encryption).

Lastly, the new FTC chairman has stated that the agency remains focused on protecting children online, particularly related to social media.

For example, in June 2025, FTC regulations related to the Children's Online Privacy Protection Act came into effect after they were proposed during the Biden administration.

The UK bets on balance

> The UK is forging a distinctive path in digital governance: while the Online Safety Act introduces strict obligations on platforms, particularly to protect children, our flexible, pro-innovation approach to AI and data signals a clear ambition for the UK. Businesses should prepare for a dual landscape of compliance and opportunity, balancing regulatory risk with data-driven growth.
>
> **Rachael Annear**
> Partner

The UK is positioning itself as a distinct 'third pillar' in global digital governance. While it is not always straightforward to definitively characterize the UK as occupying a true middle ground between the EU and US, the UK's approach aims to balance competing pressures. It is selectively aligning with more prescriptive EU rules where legal certainty and cross- border data flows require it, while championing innovation-led, agile supervision at home.

This third pillar strategy has begun to deliver results, with US companies including Microsoft, Nvidia and Google pledging over £150bn of investment in the UK during President Donald Trump's visit to the UK in September 2025.

This third pillar is most apparent in the UK's divergence from the EU on AI and data regulation. The UK government has rejected repeated calls for a specific, EU-style AI bill.

Instead, the UK published a policy paper in March 2025 outlining a new approach for regulators to support growth, stating that the UK should 'cut red tape' and 'create a more effective system.'

Read Chapter 3 of this report to learn more about the UK's Online Safety Act and why UK and global businesses must rethink their approach towards young people's data.

The UK's digital divergence

This pro-innovation approach avoids prescriptive legislation, while still ensuring there is regulatory oversight. In addition, the government's Data (Use and Access) Act 2025 (DUAA), which became law on 19 June 2025, illustrates a targeted intention to depart from the EU's General Data Protection Regulation (GDPR) framework in specific areas.

Positioned as a more flexible and innovation-friendly model, the DUAA seeks to streamline compliance obligations and introduce mechanisms that support data-driven growth, with particular emphasis on easing burdens for small and medium-sized enterprises and fostering responsible AI development; for example, by allowing the use of certain cookies without explicit consent in specific low-risk situations.

However, this pro-innovation approach is not without its challenges. The UK government abandoned its plans to introduce a broad copyright exemption for text and data mining following intense backlash from creative industries. While the DUAA requires the government to prepare and publish a report on the use of copyright works in the development of AI systems and an assessment of the economic impact of AI and copyright, the issue remains unresolved, leaving the UK with a clear policy choice: liberalize copyright to align with the US approach or strengthen protections and transparency obligations for rights holders, more akin to the EU AI Act.

Online safety is another area where the UK is pursuing blended alignment and divergence. The Online Safety Act (OSA) became law in October 2023, although its obligations have only recently begun to take effect – platforms having gained a legal duty to protect users from illegal content from 17 March 2025 and a duty to protect children online from 25 July 2025.

The OSA bears notable similarities to the EU's Digital Services Act (DSA); both regimes adopt a prescriptive structure, including proactive content moderation, risk assessments and transparency reporting, with significant penalties for non-compliance, and an emphasis on platform accountability. At the same time, the UK has given special prominence to child safety, introducing obligations that go beyond the EU model.

UK chooses to converge, diverge, compete

In other areas, the UK has moved to align more closely with the EU, while allowing room to differentiate where it wants to maintain an edge. For example, the policy statement for the proposed Cyber Security and Resilience Bill commits to modernizing the UK's cyber resilience framework and ensuring it 'aligns where appropriate' with the EU's updated Network and Information Security Directive, NIS2.

In the consumer protection space, there are also clear parallels between the EU's proposed Digital Fairness Act and the UK's Digital Markets, Competition and Consumers Act 2024 (DMCCA). The new powers granted to the Competition and Markets Authority under the DMCCA allow it to take direct enforcement action against companies using deceptive 'dark patterns' in interface design or hosting fake reviews, tackling many of the same digital fairness issues identified in the EU.

This pattern of selective alignment and strategic divergence signals how the UK is pursuing a dual objective: mirroring Europe's pro-regulatory instincts where it serves domestic priorities, while prioritizing competitiveness and practical interoperability with global markets, including the US, in high-growth areas like AI.

The EU's next phase: From rules to rollout

The EU is currently navigating a complex period in digital governance, marked by a drive towards both regulatory coherence and simplification. While often perceived as having a rigid framework, recent developments indicate a more overtly nuanced approach, acknowledging the impact of extensive legislation on innovation and economic competitiveness.

Following the 2019-2024 institutional term – a period of intense legislative activity that produced landmark regulations such as the Data Act, DSA, Digital Markets Act (DMA) and AI Act – the EU is now exploring simplification initiatives (e.g. discussions about 'targeted changes' to the GDPR, AI Act and cybersecurity laws as part of the upcoming Digital Omnibus Package) and focusing more on technical implementation (e.g. the General-Purpose AI (GPAI) Code of Practice). These efforts aim to reduce administrative burdens, streamline compliance procedures, and eliminate overlapping requirements across different digital laws.

The EU's focus is on making the existing framework more efficient, particularly for SMEs, rather than a wholesale deregulation.

> Following a wave of major digital legislation, the EU now appears to be slowly shifting its focus from (only) creating new rules to refining existing ones. The goal is to make compliance simpler and reduce burden on businesses by increasing efficiency and providing more practical and detailed technical guidance. Businesses should therefore pay even closer attention to the publication of secondary legislation and official guidelines.
>
> **Theresa Ehlen**
> Partner

Most prominently, over the past year, the AI Act has moved firmly into its implementation phase following its entry into force on 1 August 2024. Significant milestones were the February and August 2025 deadlines to implement certain measures, which saw the prohibition of AI systems posing an unacceptable risk, such as those used for social scoring, as well as the application of the rules on GPAI models.

The newly established European AI Office has been central to guiding this rollout, in particular with regard to the finalization of the GPAI Code of Practice. Concurrently, Member States have been actively designating national competent authorities to oversee the application of the regulation, with Italy being the first Member State to pass a comprehensive law regulating the use of AI. While progress is evident, the implementation has not been without its challenges, sparking ongoing discussions around the complexities of compliance and the harmonization of the AI Act with existing digital legislation.

Despite its current focus on technical implementation and simplification of existing EU digital rules, we would not expect that the EU's legislative momentum is likely to fade anytime soon. In fact, new digital proposals such as the Digital Fairness Act and the Digital Networks Act are currently under consultation:

- The Digital Fairness Act is the EU's attempt to regulate unethical techniques and commercial practices on the internet. These include deceptive or manipulative interface design (such as 'dark patterns'), addictive design of digital products and unfair personalization practices. Rather than creating entirely new rules, it will update existing EU consumer laws to address these emerging digital challenges.
- The Digital Networks Act seeks to create a genuine single market for telecoms, simplifying regulations to encourage investment in secure, high-speed networks such as fiber and 6G. The draft act also aims to address the economic relationship between network operators and large tech companies that generate significant data traffic. The ultimate goal is to improve access to secure, fast and reliable connectivity in order to facilitate the transition to cloud-based infrastructure and AI.

EU enforcement meets geopolitics

However, the enforcement of existing EU digital rules, in particular on US and Chinese tech companies, presents a challenge for EU regulators. Especially under the second Trump administration, the US government demonstrates a readiness to defend US tech interests, characterizing EU fines as tariffs and threatening retaliatory trade measures. This could lead to increased geopolitical friction and putting pressure on the EU to balance its regulatory ambitions with broader transatlantic relations.

The EU Commission, while affirming its commitment to enforce the EU's digital rulebook fairly and without bias, could therefore be confronted with demands from Member States to suspend supervisory proceedings against US technology companies in return for the lifting of retaliatory tariffs (if that has not already happened de facto). So far, however, the EU has resolutely defended its position that EU digital laws such as the DSA and DMA are non-negotiable. We would therefore not expect any changes to this position in the short-to-medium term.

APAC charts its own course

> Asian governments are taking a considered and thoughtful approach to AI regulation, forging their own individual pathways between hard law approaches and voluntary frameworks.
>
> **Richard Bird**
> Partner

Unlike the data privacy landscape, where GDPR's impact on regulation in APAC is indisputable, the extent of the EU AI Act's influence on the region's emerging AI regulations is less clear at this stage. Overall, the picture is diverse across the region; reflecting the different economic priorities, political systems and technological maturity of its many constituent countries, and the emergence of several distinct, locally tailored models. And while some Asian governments had initially leaned towards adopting elements of the EU's risk-based model, the predominant direction of travel has now shifted towards lighter-touch approaches.

China was one of the very first countries to specifically regulate AI, reflecting its policy priorities to ensure control over the content of GenAI outputs, coupled with targeted consumer protection interventions such as mandating the labeling of AI-generated synthetic content and provision of opt-outs from recommendation algorithms.

China had also been understood to be developing a comprehensive AI law, but this no longer features in the 2025 legislative plan. Instead, the 2025 plan lays down an objective of 'promoting legislation for the healthy development of artificial intelligence' – an apparent pause that perhaps comes as a response to the unexpected recent technological breakthroughs in this area by the likes of DeepSeek.

For AI developers, the recent Beijing Free Trade Zone (FTZ) negative list for cross-border transfers of 'important data' creates a narrow but valuable channel for the export of certain types of training datasets without requiring prior approval, which has also since been adopted by other FTZs.

Other countries in Asia, such as Japan, Vietnam and South Korea, have also recently enacted laws to regulate AI, and preparatory legislative work has begun in Thailand as well. Both the Vietnamese and Korean laws introduce a concept of high-risk AI seen in the EU AI Act, but South Korea has emphasized that its AI law is more business friendly than its European counterpart's, and Japan's law does not impose any financial penalties for breach. These are all measures clearly intended to avoid stifling innovation.

Ultimately, these laws mostly set out high-level principles which require further implementing regulations or guidelines to be issued. The practical implications of these laws, as well as the enforcement risks, is therefore unclear as of now. Vietnam has recently also published for public consultation the draft of a comprehensive AI law that is modeled on the EU AI Act and will supersede the provisions on AI in the existing law.

Also focused on promoting the adoption of AI and avoiding overregulation are Hong Kong and Singapore. Both Hong Kong and Singapore have thus far favored guidelines that promote the adoption of good governance practices and internal controls over regulation. Singapore has also been working closely with businesses and other stakeholders to create a trustworthy ecosystem for AI development and adoption (e.g. through AI testing tools) and has played a leading role in formulating APAC governance and ethics guidelines.

Looking ahead

Global rules on data, cybersecurity and AI are fragmenting fast. Divergent approaches in the US, EU, UK and APAC mean businesses need strategies that are proactive, flexible and geopolitically aware.

Key takeaways for clients:

1. **Track divergence:** Monitor policy shifts closely – from the US's deregulatory stance to the EU's prescriptive frameworks – while noting areas of continuity such as cybersecurity, child safety and AI-washing.
2. **Strengthen governance:** Reinforce internal data classification, processing and transfer frameworks to withstand scrutiny across jurisdictions.
3. **Stay adaptable:** Build global principles for AI, data and cyber governance, but tailor controls to meet regional demands like the EU AI Act or UK OSA.
4. **Factor in geopolitics:** Assess how enforcement may be shaped by broader political tensions, adding complexity to compliance and trade.
5. **Keep ethics central:** Regulators remain focused on responsible AI, deceptive practices and child safety. Embedding these principles into products and disclosures reduces legal and reputational risk.

The landscape will only grow more complex. Businesses that anticipate change, integrate ethics and build resilience into governance will be best placed to manage risk and seize opportunity.

3.

Why businesses must rethink their approach to young people's data

In brief

Governments around the world are accelerating efforts to regulate the digital experience of young people, from targeted age gating laws to sprawling content regulations like the UK's Online Safety Act (UK OSA). The global regulatory tapestry is increasingly complex. While there's growing support for age-appropriate design codes (AADCs) and a wave of new policy proposals, we're also seeing more deliberate divergence in legal approaches, and new attempts to apply existing laws to novel issues.

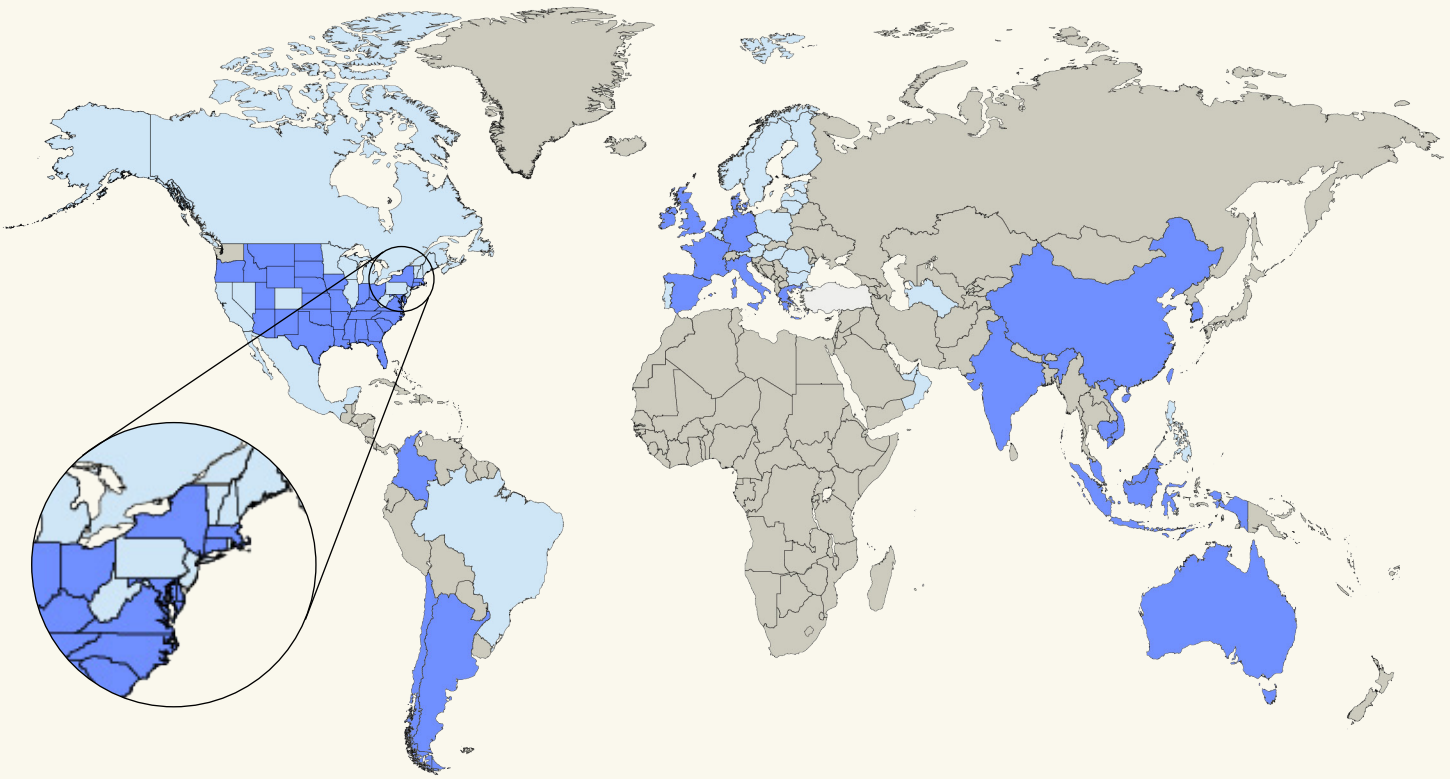
We predict this tapestry will only get more complicated before it gets simpler. Not only will current AADCs, age assurance rules and content moderation laws amplify compliance cost and enforcement risk for companies in the short term, but strategic competition between governments to set the agenda will drive even more divergence. Privacy and free speech concerns may provide some friction, but broad-based support to improve the online experience of children seems set to drive ongoing change.

Age assurance rules are expanding, but diverging

A global trend is accelerating to regulate minors' access to online services and content through age assurance measures. A key driver of complexity is the differing focus and technical requirements of these laws.

The UK OSA requires providers to restrict children's access to various services that allow certain 'harmful' content (e.g. pornography and suicide content). In the US, there are similar efforts in various states to restrict children's access to specific harmful content – although current efforts are largely focused on pornography.

Mandatory/recommended online age-gating measures



Data collected August 2025

Several US states have also enacted or proposed laws focused on service/feature access, for example requiring parental consent for minors to use social media services and restricting platforms' use of algorithmic feeds. Australia has similarly taken action, with its 'social media ban' for children set to take force in December 2025.

In September 2025 the European Commission announced that an expert panel will deliver comprehensive advice on a social media ban for children under 16 by the end of the year. The European Commission president, Ursula von der Leyen, explicitly referenced Australia as a pioneer that Europe would be closely watching.

> The European Commission is also aiming for a harmonized approach to age assurance across the EU by providing a blueprint for an age verification solution that may voluntarily be adopted by EU Member States.

Theresa Ehlen
Partner

Despite political momentum, important privacy, free speech and feasibility concerns remain – especially when biometric checks or digital IDs are involved. Jurisdictions are seeking to address these issues in different ways. The European Commission has recently funded a tender for the envisioned EU-wide age verification solution.

In parallel, several EU Member States have begun rolling out or testing national age verification tools, often tied to digital identity systems. In the UK, Ofcom and the Information Commissioner's Office (ICO) are maintaining an ongoing dialogue and have issued guidance on their aligned approach. The UK government has also signaled an intention to actively enable innovation at the intersection of identity verification and privacy, through reforms to the UK Data Protection Act under the Data (Use and Access) Act, which establishes a comprehensive framework for digital verification services.

The US Supreme Court's decision in *Free Speech Coalition v Paxton* is likely to embolden further laws, as it confirmed a more permissive constitutional review standard for age verification requirements relating to access to pornographic material.

With these initiatives advancing, businesses – especially platforms for young people – face a rapidly evolving challenge: navigating fragmented age assurance laws that demand different platform designs, accessibility standards and infrastructures across jurisdictions.

Age-appropriate design codes – an increasingly popular policy tool

AADCs are emerging as a powerful policy instrument, setting clear requirements for how online services should handle young users' data. Common features include requiring high privacy settings by default, greater transparency, age assurance mechanisms and restrictions on profiling and targeted advertising. However, the scope of protection, age thresholds and enforcement mechanisms differ significantly between schemes.

In the US, an increasing number of states are advancing their own AADCs, modeled in part on the UK ICO's Children's Code – which was recently put on a statutory footing. These efforts are encountering significant First Amendment challenges. Critics argue that such laws may infringe on free speech rights by requiring platforms to restrict or alter content based on user age, effectively compelling speech or imposing broad limits on lawful expression.

Beginning in 2023, the European Commission sought to leverage the EU's Digital Services Act (EU DSA) tool of voluntary codes of conduct to bring platforms behind AADCs. A special group began developing a new EU code of conduct on age-appropriate design ('BIK+ Code'). As of this year, the European Commission appears focused on setting its own approach rather than following other countries. In its guidelines on the protection of minors, the Commission set out its interpretation of Article 28 EU DSA, including requirements for engaging design features and safeguards applied to AI chatbots integrated into online platforms.

Elsewhere, countries are using the AADC concept to inform local approaches. Australia is developing a legally binding Children's Online Privacy Code modeled directly on the UK framework. In contrast, Singapore has strengthened existing protections by interpreting its data privacy laws through advisory guidelines for children's data.

With the world's largest youth population, the Indian government's draft Digital India Act is expected to contain specific and stringent rules regarding the processing of children's data, although the draft is currently on hold.

While current free speech challenges in the US may temporarily slow momentum, a broader global push may ultimately establish de facto global standards that minimize the significance of those laws not coming into force.

Expansive content regulations are likewise focused on children's safety

Alongside rules for age assurance and design, a parallel trend sees governments implementing expansive content moderation regimes, with children's safety often cited as the central justification for broad new duties.

> Frameworks like the UK OSA and the EU DSA create comprehensive new obligations for online services, but their differing approaches introduce another layer of regulatory fragmentation.
>
> **Rachael Annear**
> Partner

The UK OSA is arguably the most prescriptive. It requires services with a UK user base to have systems and processes in place to reduce illegal content and, crucially, material deemed 'harmful to children.' This creates stringent obligations on platforms to conduct robust risk assessments and adopt measures such as notice-and-takedown frameworks and, in certain cases, automated content moderation tools.

The EU DSA takes a different, though equally comprehensive, approach. Rather than defining specific categories of 'harmful' content, it focuses on process and systemic risk. Platforms must swiftly remove illegal content once identified and, under Article 28(1) EU DSA, implement special protection measures for minors, including a ban on targeted advertising based on their data.

Recent guidelines from the European Commission on how services should approach the protection of minors under Article 28(1) have added significantly more depth to compliance expectations. These efforts are likely to be reinforced by renewed initiatives to pass new EU laws targeting child sexual abuse material.

As enforcement under these laws ramps up – and as other jurisdictions study the UK OSA and EU DSA as potential models – businesses face the likelihood of yet another layer of regulatory divergence.

Current enforcement trends paint a complex picture

Across Europe and the US, enforcement of child safety and privacy laws has predictably ramped up as more laws have come into force, regulators have received boosted funding, and the public and lawmakers have pressed more aggressively for action.

In the EU and UK, while a number of large services have implemented new or upgraded age assurance measures, child-focused regulatory actions have increased sharply. The Irish Data Protection Commission issued billions of euros in fines between 2022 and 2024, with a notable uptick in cases involving minors.

Italy's Garante temporarily blocked access to a well-known AI service in 2023, in part due to concerns about the platform's lack of age verification. Similarly, Coimisiún na Meán (CnaM), Ireland's media regulator, recently opened an investigation into X for allegedly failing to apply age assurance under the Irish Online Safety Code in relation to pornographic material on the platform. This aligns with the broader strategy CnaM announced in April 2025, which placed issues affecting children at the center of its regulatory agenda for the coming years.

In the US, enforcement is more fragmented, involving actions by federal and state regulators as well as private litigants. In early 2025, the Federal Trade Commission reached a US$20m settlement with Cognosphere, LLC over allegations that its mobile game was deceptive and failed to obtain required parental consent for minors' use. Last year, the Texas Attorney General launched a data privacy and enforcement initiative, and his office has since announced investigations into multiple tech platforms related to children's data. Multiple private class actions against TikTok and its parent company over children's use of the platform have been consolidated into an ongoing multidistrict litigation in federal court in California.

> In the future, enforcement will be shaped by overlapping laws – privacy, consumer protection and content moderation – creating legal complexity.
>
> **Theresa Ehlen**
> Partner

A common challenge in enforcement will be evidentiary – particularly proving causation between platform design and harm to minors when alleged harms are primarily psychological. The ongoing ramp-up in enforcement warrants close attention to how regulators and private plaintiffs apply new and existing regulations.

Looking ahead

As we move forward, we anticipate that more jurisdictions will introduce laws aimed at regulating children's online experiences. As these regulations evolve, we expect:

1. **Escalation of enforcement action** – regulators, fueled by increased funding and public demand, will increasingly use a combination of privacy, consumer protection and content moderation laws to impose stricter operational requirements on platforms and issue larger penalties.
2. **Divergence in jurisdictional approaches** – regions are pursuing individual courses of action, with policy goals at times prioritized over the creation of a unified international standard.
3. **Heightened compliance costs** – companies, particularly those with younger audiences, will face pressure to invest in age assurance infrastructures and adapt platform designs to meet diverging legal requirements across jurisdictions.

The regulation of children's digital experience is shifting from a patchwork of isolated efforts to a more systematic, yet highly divergent, global framework. While the shared goal is child safety, the way it is being implemented is creating jurisdictional and legal conflicts. Much of the burden of navigating this complexity falls on companies – service providers must proactively embed robust compliance and assurance frameworks directly into product development and design from the outset. Within this fragmented ecosystem, a strategic rather than reactive approach to child safety is no longer optional – it is paramount.

4.

Rising risks and shifting rules for international data transfers

In brief

Are we witnessing a fundamental restructuring of global data flows? The international data transfer landscape is now defined by a tangle of divergence and reform: some jurisdictions push for interoperability, while others tighten their grip on cross-border transfers.

The EU's approach is marked by tension. Progress on adequacy decisions – including the (temporary) confirmation of the EU-US Data Privacy Framework – contrasts with a strong push for data sovereignty, driving heightened scrutiny for transfers to countries such as India and China.

The UK's Data (Use and Access) Act 2025 (DUAA) introduces a new data protection test for transfers that requires a risk-based comparative assessment. In the US, Executive Order 14117 and Protecting Americans' Data from Foreign Adversaries Act (PADFAA) have redefined export restrictions on bulk transfers and data brokerage. Meanwhile, China continues to provide clearer guidance on its data export mechanisms—including the Free Trade Zone 'negative lists' – even as enforcement against non-compliance begins to pick up pace. Vietnam has taken steps to implement controls over data transfers that concern national security and other state interests, while South Korea has recently imposed substantial penalties for unlawful data transfers.

EU: Stability and stricter scrutiny

The EU's international data transfer regime is increasingly defined by two conflicting realities. On the one hand, stability comes from developments such as the (temporary) confirmation of the EU-US Data Privacy Framework by the General Court and progress towards new adequacy decisions – for the UK and potentially Brazil. On the other hand, transfers of personal data to countries without an EU adequacy decision are facing a harsher climate, as regulators adopt a stricter stance. High-profile enforcement – including the Irish data protection authority's fine against

TikTok over transfers to China and the European Data Protection Supervisor's decision to block transfers to India – underlines this trend. Looking ahead, 2026 may bring fresh scrutiny of the EU-US Data Privacy Framework, given the low procedural barriers for challenging adequacy decisions identified by the General Court, and ongoing legislative shifts in the US.

An EU adequacy decision can increase digital trade by up to

↗14%

(CEPR, 2023)

Despite this, organizations should not adopt an unworkable strategy of excluding every hypothetical risk of governmental access from General Data Protection Regulation (GDPR)-covered transfers. Experience with supervisory authorities shows that the use of the approved standard contractual clauses, backed by a well-documented transfer impact assessment, can still be considered robust – especially where the risk of governmental access is minimal and transfers are shielded by strong technical and organizational measures. Encouragingly, the European Commission is exploring ways to ease GDPR compliance burdens regarding data transfers. Its multi-stakeholder expert group has acknowledged that transfer impact assessments are 'burdensome, costly and time-consuming.' In addition, a recent judgment of the Court of Justice (*SRB v. EDPS*) – signaling a broader interpretation of what is understood as 'anonymized' data – could have welcome spillover effects, particularly on the requirement for additional technical and organizational measures to safeguard transferred personal data (see also Chapter 7 on anonymization).

UK: Risk-based test signals divergence

The EU GDPR has not applied in the UK for almost five years, yet so far there has been little divergence between the EU and UK approaches. The DUAA may change that, especially in relation to international personal data transfers once its key provisions come into force.

A centerpiece of the DUAA is a new 'data protection test.' This applies both to: (i) the Secretary of State, when making adequacy decisions; and (ii) businesses, when exporting data to third countries using standard contractual clauses or other safeguards. The test requires an assessment of whether the third country or organization offers protection that is 'not materially lower' than UK standards.

For businesses, this means that reliance on alternative transfer mechanisms will be sufficient if they can show that protections for a data subjects are not materially lower than under UK law. When in force – likely by 2026, if not earlier – the new test will move the UK away from the EU's binary 'adequate/inadequate' model, replacing it with a risk-based, comparative approach. The DUAA also introduces continuous monitoring of third-country regimes, replacing the previous four-year adequacy review cycle.

Data autarky, where all economies restrict their data flows (full fragmentation), would lead to

global GDP losses of

↘4.5%

reductions in exports of

↘8.5%

(OECD, 2025)

In practice, this gives the UK government discretion to adjust or withdraw transfer permissions at any time, in response to changing legal or geopolitical conditions. It remains unclear, however, whether this discretion will result in real divergence from the EU's adequacy list, or in the creation of 'UK-only' adequacy decisions.

US: National security drives new restrictions

In the US, the legacies of Executive Order 14117 and PADFAA continue to shape the regulatory landscape in 2026. While distinct, both frameworks share a common goal: preventing foreign adversaries from accessing sensitive US data in the name of national security. PADFAA specifically prohibits data brokers from transferring sensitive personal data to designated 'foreign adversaries.' Executive Order 14117, by contrast, is a broader presidential directive that created a Department of Justice program restricting bulk transfers of sensitive personal and government-related data to 'countries of concern' such as China and Russia.

> New US transfer restrictions have implications for transaction structures and business models. Companies should establish clear protocols for assessing commercial activities involving transfers of certain categories of US personal data.
>
> **Brock Dahl**
> Partner

Initially established under the Biden administration, both frameworks have been retained – and in some areas expanded – under the Trump administration. The focus remains firmly on national security, with regulation aimed at data brokers, vendor relationships and industries handling genomic, biometric, health, and geolocation data.

These measures are fundamentally reshaping US data transfer risk. Organizations with US operations or reliance on US vendors must assess their data flows to identify areas likely to attract increased scrutiny. Agility will be essential as regulatory classifications shift quickly. Sectors such as healthcare, telecoms and finance face particularly acute compliance burdens. As US enforcement agencies operationalize these rules and regulations, companies should expect increased scrutiny and prepare for a heavier compliance and governance workload around international data exports.

China: Free Trade Zone reforms ease rules – but enforcement ramps up

China has made progress in detailing its outbound data transfer regime, most notably through the introduction of 'negative lists' applicable to designated Free Trade Zones (FTZs), including those in Beijing and Shanghai. Under this model, within certain sectors (e.g., life sciences, automotive, retail and hospitality, and AI) data categories that are explicitly listed as 'negative' are subject to security assessments for government approvals, standard contracts, or certification prior to export (including highly-sensitive 'important data' and high volume of personal data). All sectors (including these) are subject to general 'reference rules' that apply universally, and which impose additional controls on data such as high-value, sensitive data related to the competitiveness or safety standards or related to supply chains that impact national security. Outside of this framework, non-personal data can be freely exported.

Volume thresholds that trigger additional controls within FTZs are set higher than those prescribed by national regulations. For example, Shanghai's Negative List only requires a standard contract filing for international transfers of certain non-sensitive personal data of between one and ten million individuals (after which a security assessment must be completed), such as loyalty program data in retail and hospitality. National regulations, by contrast, set the limit at 100,000 to one million individuals.

> The past year has been a mixed blessing for international companies operating in China: much-needed further clarity, but coupled with elevated levels of enforcement.
>
> **Richard Bird**
> Partner

The result is a two-tier compliance environment: FTZs may provide meaningful clarity (and flexibility) in sectors such as life sciences, AI and automotive, but other sectors will continue to face uncertainty and tougher restraints. FTZ rules are also likely to evolve in line with geopolitical and sector-specific needs.

At the same time, China is moving from rulemaking to enforcement. In September 2025, regulators fined the Shanghai subsidiary of a multinational for transferring customer data to its French headquarters without implementing an approved data transfer mechanism or obtaining proper consents. The case also highlights the risks of underlying non-compliance surfacing through an authority's investigation of a reported data breach.

Continuing developments in other APAC countries

Vietnam has taken steps to implement a new legal system for data control – according to its Law on Data (in effect since 1 July 2025) and its implementing decree, 'core data' and 'important data' that may affect national security, public benefits and legitimate interests of relevant individuals and organizations cannot be exported without government approval (for core data) and the filing of an impact assessment (for important data). As an initial step for implementation, the government has released a list of 26 types of 'core data' and 43 types of 'important data,' but some of these appear highly broad and ambiguous—such as 'data on organizations and citizens that has not been made public.'

9.2%

of world by population outside the EEA live in countries covered by full or partial EU/EEA GDPR adequacy decisions.

(Freshfields data, population figures from CIA World Factbook)

South Korea continues its strict enforcement against unlawful cross-border data transfers. Two Chinese e-commerce platforms were recently fined the equivalent of US$930,000 and US$1.43m. Additionally, Deepseek was ordered to implement corrective measures to rectify future transfers of personal data abroad – as a condition for being permitted to return to South Korean app stores.

Looking ahead

The international data transfer landscape is becoming ever more complex as regulatory priorities diverge. To manage risk and protect business continuity, companies need a proactive and strategic approach – keeping a global perspective, monitoring developments and re-evaluating data transfer practices.

For EU transfers, it remains prudent to rely on established mechanisms and well-documented transfer impact assessments backed by strong technical safeguards. At the same time, organizations should watch national divergence closely – from the UK's new 'not materially lower' test to the US's expanding national security-based restrictions.

The year ahead is likely to bring further change, including continued challenges to the EU-US Data Privacy Framework and the full roll-out of the UK's new transfer regime. Forward planning will be essential to stay compliant and keep operations running smoothly.

5.

AI now a board-level imperative for public companies and investors

In brief

AI has moved from a technical consideration to a board-level imperative for public companies worldwide. The opportunities and risks it presents carry profound implications for strategy, operations and investor relations and demand active oversight. As 2026 approaches, boards must not only manage AI but also be ready to articulate their approach clearly and convincingly to the market.

AI is reshaping business operations

> AI is not just a tech issue, it's a core tool and risk that demands board attention across industries.

Alejandra Lynberg
Senior Associate

This wave of adoption spans not only generative AI – such as the large language models popularized by platforms like ChatGPT – but also more established applications, including automated and algorithmic decision-making. As a catalyst for efficiency and innovation, successful AI adoption can create new paths for growth. But when competitors or new entrants move faster, it can just as easily upend incumbents.

These twin dynamics have made AI a core concern for public company boards. Their role is to steer organizations through this technological transformation and to ensure risks and opportunities are disclosed in ways that stand up to scrutiny from investors and regulators alike.

From risk disclosure to growth story

The impact of AI is so significant that it is changing how companies explain their use of the technology to investors, including in annual reports. Across the UK, US, and EU, public companies have materially increased AI-related disclosures.

AI now a board-level imperative for public companies and investors

In the UK, the number of statements on AI in annual reports rose by 12% last year. In the US, the proportion of S&P 500 companies disclosing board oversight of AI or board-level AI competency jumped more than 84% over the past year.

Much of this reporting has focused on risk. In the UK, the Corporate Governance Code requires boards to assess and manage business risks. Similarly, in the US, Securities and Exchange Commission (SEC) regulations compel disclosure of material risks. AI is increasingly treated as one of those material factors. In the EU, direct AI risk disclosure is still emerging, but the Corporate Sustainability Reporting Directive is already pushing companies to report on technology-related risks and opportunities – including AI's potential to cut energy use, or conversely, drive higher demand. Member States such as Germany have additional specific regulations, such as the German Corporate Governance Code, the Stock Corporation Act, as well as the German Commercial Code and the German Accounting Standard.

The trend is visible in the numbers:

41% FTSE 100 companies now identify AI as an emerging risk in annual reports,

9% identifying it as a principal risk.

(Freshfields data, August 2025)

In the US, Fortune 500 companies mentioning AI as a risk factor rose from

2022 **9%**

2024 **↗56%**

('The Rise of Generative AI in SEC Filings,' 2024)

Investor communication is expanding beyond AI-related risks. Companies are also outlining how AI is being integrated into operations, how it is affecting costs and resourcing, and whether they are making strategic investments in the technology in annual reports.

> AI governance is developing swiftly. A company's success will increasingly depend on combining structured oversight with AI competency, strong governance frameworks, and a clear focus on delivering value while managing risks.
>
> **Rachael Annear**
> Partner

Investor activism takes aim at AI

Proxy advisors are pushing for enhanced disclosures on how companies are implementing AI, the risks it creates and the role of boards in overseeing it – pressure now visible across jurisdictions. For example, in the US, shareholder activists are demanding more transparency. The trade union federation AFL-CIO has submitted proposals at Apple, Netflix, Comcast, Warner Bros and Walt Disney, seeking detail on how AI is being used. At Apple's 2024 AGM, 37.5% of investors backed the AFL-CIO's call for AI ethics disclosures – a level of support that signals growing momentum.

AI-washing: the next enforcement flashpoint

As companies set out their AI strategies, they must navigate the risk of 'AI-washing' – exaggerating AI capabilities to gain a competitive advantage or appeal to investors. This practice is now firmly on the enforcement radar globally. Companies making statements about AI – whether in marketing or mandatory disclosures – must ensure their accuracy.

In the US, the SEC has already acted. In 2024, two investment advisers settled the first AI-washing enforcement cases for false or misleading claims, paying US$225,000 and US$175,000 respectively, alongside censures and cease-and-desist orders. In 2025, the SEC's Cybersecurity and Emerging

Technologies Unit declared AI-washing a core enforcement priority, targeting misleading representations by both public companies and startups – particularly the practice of rebranding rule-based automation as 'AI' or overstating capabilities of predictive analytics and chatbots.

> We will see increased scrutiny of regulators in the field of AI. For example, the US SEC is closely monitoring AI use in companies, financial services, trading and corporate disclosures. It has also refocused and renamed the Crypto Unit of their Division of Enforcement as the Cyber and Emerging Technologies Unit, which now prioritizes AI-related investigations and actions.
>
> **Beth George**
> Partner

Europe and the UK are moving in the same direction. While AI-washing is not yet addressed in a single statute, a combination of the EU AI Act, consumer protection laws and national advertising standards provides a strong enforcement toolkit. Companies making unsubstantiated AI claims risk fines, reputational damage and even civil or criminal liability, depending on jurisdiction. Under the EU AI Act, providers of high-risk AI systems must meet stringent transparency requirements, conduct conformity assessments and notify deployers. Misrepresentation can trigger fines of €7.5m or up to 1% of global turnover, whichever is higher.

AI oversight moves into the boardroom spotlight

Investor scrutiny is increasingly focused on how boards oversee AI integration and deployment. This expectation is being formalized in regulatory and advisory frameworks across all three regions.

In the UK, the Financial Reporting Council's guidance highlights controls over new technologies – including AI – as potentially 'material' for the purposes of a board's declaration on the effectiveness of a company's material controls. In the US, influential proxy advisors such as Glass Lewis now explicitly expect disclosures on board-level AI governance. In the EU, authorities including the European Securities and Markets Authority are issuing similar recommendations on AI oversight by corporate management.

Despite this pressure, governance structures remain in flux. Among FTSE 100 companies, only 7% of boards retain full oversight of AI, 19% delegate responsibility to the audit or risk committees, and 16% have dedicated AI committees. The remainder either assign AI to general committees or leave governance undefined. The picture is similar in the US, however, in 2024, 89% of S&P 500 companies had not expressly disclosed the assignment of AI oversight to either the full board or a committee.

> As is often the case in the field of AI, the process of board disclosures and AI oversight requires iterative risk assessment and management. Regulators and investors worldwide expect ongoing reviews that produce updated policies and procedures, training and disclosures.
>
> **Giles Pratt**
> Partner

In the EU, there are not yet reliable figures on how AI oversight is distributed within companies. The AI Act itself does not mandate a particular governance model, leaving companies free to appoint internal or external officers – such as AI, IT security or compliance officers. Ultimately, members of the management and supervisory board must have the expertise to critically assess and guide strategic decisions on AI. They are under a duty to examine the potential applications of AI models and, where appropriate, adjust corporate strategy in response to new developments. The high degree of regulatory scrutiny around AI means that boards must address not only traditional product- and sector-specific requirements, but also obligations under data protection law and the fast-emerging body of AI regulation.

Three pillars of effective AI governance

To manage risk and capture opportunity, forward-thinking boards are adopting comprehensive AI governance strategies built around three priorities:

> Boards must lean into scrutinizing how their businesses use AI to mitigate risks, capture value, and give investors confidence in relation to corresponding processes.
>
> **Zofia Aszendorf**
> Senior Associate

1. Navigating regulation: The global AI regulatory landscape is fragmented. Boards must contend with the EU's risk-based AI Act, a growing patchwork of US state laws and the divergent approaches in jurisdictions such as the UK, South Korea and China. This complexity requires boards to work closely with their compliance and legal teams to ensure oversight keeps pace with evolving risks.
2. Building strong governance: Effective oversight starts with a clear internal framework that applies across markets. Boards need timely, relevant information – spanning product development, AI deployment, governance and compliance – to challenge management and hold AI operations to account.
3. Scrutinizing high-risk use cases: Boards should give particular attention to the AI applications most likely to create legal, operational or reputational risks.

> Companies are recognizing the growing need for structured AI oversight at the board level — and rightly so. It has become a strategic necessity, not just an add-on.
>
> **Theresa Ehlen**
> Partner

Looking ahead

As AI becomes more deeply embedded in business operations, boards will face intensifying pressure – both to manage the risks it creates and communicate a compelling and credible narrative to the market.

For companies with disclosure obligations, the task is to find clear and defensible ways to meet rising expectations from investors and regulators. Public companies should consider:

- substantiating all public AI claims, with proper documentation of how AI is actually deployed in the business and its services;
- strengthening disclosure and marketing review procedures, for example by creating cross-functional panels bringing together legal, product and marketing expertise;
- enhancing internal governance and compliance processes, including adopting and adhering to an AI governance framework; and
- planning for transparency and auditability, to comply with requirements under the EU AI Act and consumer protection laws.

6.

Regulatory convergence grows across sectors and borders

Regulatory convergence grows across sectors and borders

In brief

Digital technology is blurring the boundaries between privacy, competition, consumer welfare, cybersecurity and finance regulation – creating pressures that traditional governance structures struggle to absorb. Across Europe, the UK and the US, regulators are increasingly collaborating across sectors and jurisdictions to address risks that cut across multiple domains.

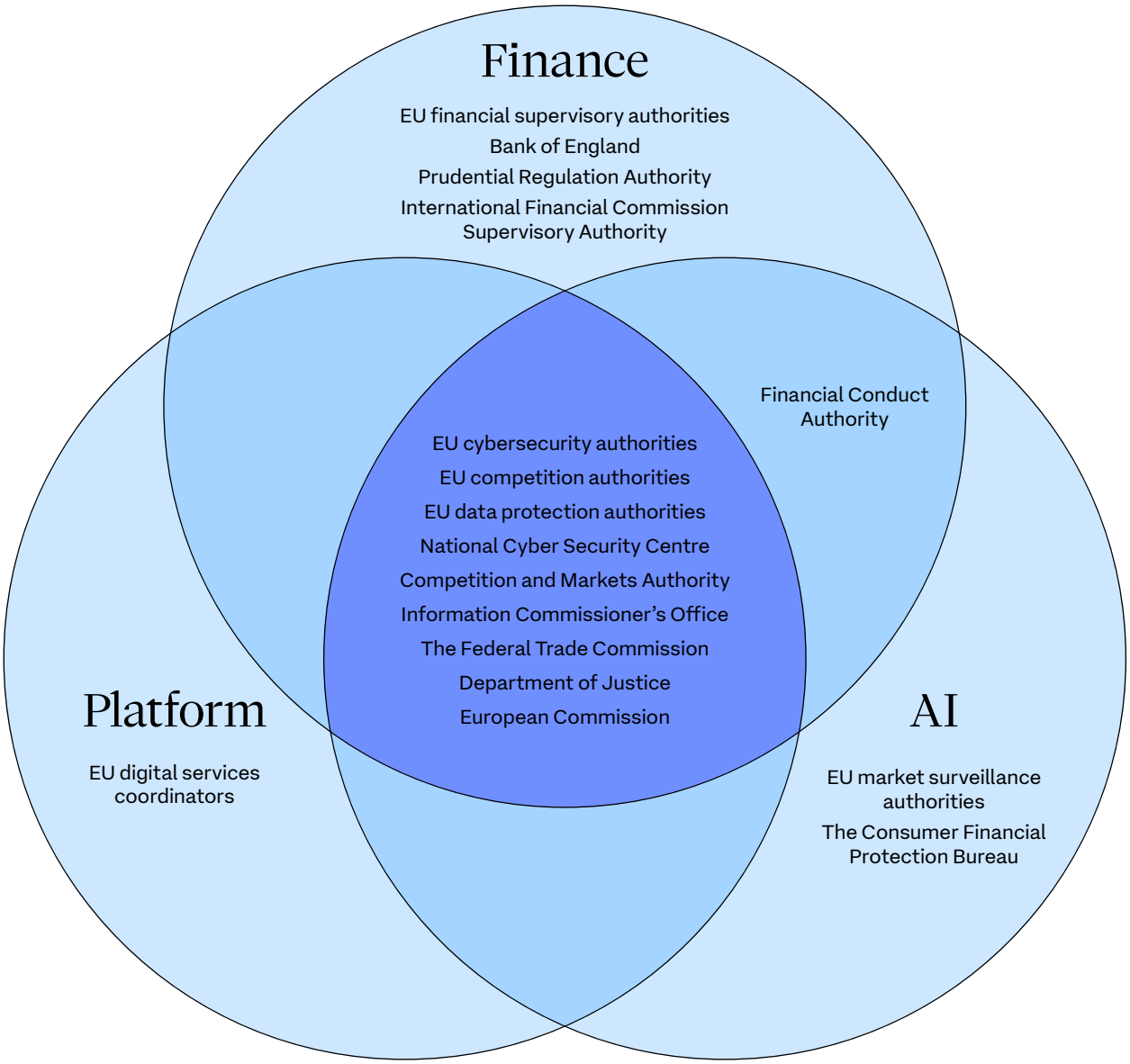
Companies that treat regulation as an interconnected system – rather than a checklist of siloed obligations – will be better placed to stay compliant in 2026. This chapter explores that convergence through three high-impact areas: digital platforms, finance and AI.

> Global compliance isn't about ticking boxes – it's about connecting dots.

Mark Egeler
Partner

Regulators across domains are increasingly eyeing the same decisions: platform design, data sharing and AI behavior. Privacy, competition, cybersecurity, finance and consumer-rights authorities now intersect and co-investigate. In practice, this means a single change – in algorithm, contract or interface – can trigger scrutiny from multiple agencies. The Venn diagram below illustrates how these oversight domains overlap and converge.

Mapping the intertwined global enforcement landscape



Platforms: Market power, privacy and safety under joint scrutiny

Europe

The EU's Digital Markets Act (DMA) addresses gatekeeper power, yet its first major fines centered on consent for data combination and user choice. Here, a competition tool was used to enforce privacy-style rules – illustrating a wider trend where competition enforcement is shaping data governance.

Meanwhile, the Digital Services Act (DSA) requires transparency in recommender algorithms, forcing content moderation, consumer protection and data governance teams to collaborate. National data protection and consumer agencies are embedded in the supervision structure, ensuring cross-disciplinary oversight from day one. The European Data Protection Board and national consumer authorities are also increasingly issuing joint opinions and coordinating enforcement strategies, particularly where algorithmic profiling affects both privacy and consumer rights.

United Kingdom

The Digital Markets, Competition and Consumers Act, in force since January 2025, gives the Competition and Markets Authority bespoke powers over large digital companies with substantial and entrenched market power, while the Online Safety Act empowers Ofcom to act against companies that fail to remove online harmful content. Both bodies participate in the Digital Regulation Cooperation Forum alongside the Information Commissioner's Office (ICO). The forum already issues joint statements and guidance – illustrating how design choices with competition implications are simultaneously screened for their privacy and safety impact.

United States

No single federal statute mirrors the DMA or DSA, yet practice shows similar convergence. The Federal Trade Commission (FTC) can challenge unfair data practices, consumer protection concerns and anticompetitive conduct, often in parallel. State privacy laws, consumer protection lawsuits and Department of Justice (DOJ) antitrust litigation also frequently address the same fact patterns, prompting informal inter-agency coordination.

Takeaway: For platform operators, changes to terms of service, ranking algorithms or user interactions must now withstand scrutiny from competition, privacy, consumer and safety regulators – sometimes within a single investigation.

> The same product change can trigger review by multiple regulators.
>
> **Christoph Werkmeister**
> Partner

Finance: Open data, shared risks, coordinated regulators

Europe

The Digital Operational Resilience Act took effect in January 2025, complementing the NIS2 cybersecurity directive in protecting critical infrastructure. Both regimes extend deep into the supply chain, placing cloud and software vendors serving banks under dual cybersecurity scrutiny. Their significant overlap encourages integrated audits to avoid duplicate penalties for the same incident.

Meanwhile, competition-driven open finance initiatives require financial institutions to share customer data with third-party apps. However, this mandate depends on General Data Protection Regulation (GDPR)-level consent and security, requiring privacy and competition authorities to align on how data can be shared.

United Kingdom

The Financial Conduct Authority and the ICO run joint services, including sandboxes and AI labs, allowing FinTechs to test new data driven services once rather than twice. They have also issued coordinated guidance on AI credit scoring and consumer data rights. The Bank of England, Prudential Regulation Authority and National Cyber Security Centre share incident reporting templates – a sign that operational resilience audits are now multi-agency by design.

Regulatory convergence grows across sectors and borders

United States
The Consumer Financial Protection Bureau (CFPB) is finalizing an open banking rule under Dodd Frank §1033, while banking regulators are developing third-party risk standards that reference Cybersecurity and Infrastructure Security Agency cyber guidance. Privacy obligations stem from the Gramm-Leach-Bliley Act, but enforcement can involve the FTC and state attorneys general. Therefore, a single data breach at a financial institution can trigger investigation across multiple regulators – who increasingly coordinate.

> Open finance means open scrutiny – by privacy, cyber and conduct watchdogs alike.
>
> **Rachael Annear**
> Partner

Takeaway: Finance firms face oversight from data, prudential, conduct and cyber authorities that increasingly read from the same playbook. Controls, contracts and reporting lines must satisfy them all at once.

AI: Horizontal rules, converging enforcement

Europe
The EU AI Act is explicitly 'horizontal' in scope, but fragmented in execution. Sector-specific AI – like in finance or healthcare, for example – is policed by national regulators depending on sectoral jurisdiction, leaving room for potential inconsistencies and friction. Only general-purpose AI models fall under the new European AI Office, which leads cross-border investigations and coordinates enforcement. The AI Office has called for joint enforcement protocols, particularly for biometric identification, profiling or automated decision-making. It has also signaled plans to work closely with GDPR authorities to avoid duplicative sanctions and ensure consistency where AI systems overlap with other frameworks, such as the DSA.

United Kingdom
Instead of a single AI statute, the UK embeds five high-level principles – safety, transparency, fairness, accountability and contestability – into existing laws. Each sectoral regulator must interpret them and cooperate with peers under a forthcoming statutory duty. The Digital Regulation Cooperation Forum is already producing joint guidance on issues such as children's data and algorithmic discrimination.

United States
Congress continues to debate comprehensive AI legislation, but regulatory agencies are not waiting. The FTC is pursuing deceptive or biased practices related to the marketing and deployment of generative AI under its unfair practices authority. The Equal Employment Opportunity Commission (EEOC) focuses on bias in algorithmic employment decisions, while financial regulators examine AI-driven credit decisions. These agencies are coordinating more closely, formalized in a 2023 interagency memorandum of understanding on AI oversight signed by the FTC, DOJ, EEOC and CFPB.

> Deploying AI without an integrated governance framework creates significant legal risk.
>
> **Beth George**
> Partner

Takeaway: Deploying AI can trigger parallel investigations into data provenance, fairness, sector specific risks and consumer deception. Governance teams must map which regulator leads on each risk – while assuming information-sharing among agencies.

Five ways to stay ahead in 2026

> Continuing to address regulatory challenges in silos invites increased regulatory scrutiny and amplifies operational risk.
>
> **Vera Ibes**
> Principal Associate

1. **Adopt a 'one dossier' mindset.** Build evidence, risk assessments and audit trails that address privacy, competition, consumer and sectoral questions together – not in silos.
2. **Establish cross-disciplinary teams.** Legal, compliance, data science and product leaders should engage regulators jointly, rather than through fragmented briefings.
3. **Use global heat maps.** Track how the same issue – such as consent for data reuse – triggers different frameworks in the EU, UK and US. Align policies to the highest common standard where feasible.
4. **Plan for coordinated enforcement.** Expect regulators to synchronize remedies even if deadlines differ. Early dialogue can reduce the risk of conflicting orders.
5. **Safeguarding organizational credibility holistically.** Customers and regulators do not distinguish between privacy breaches, unfair practices or biased algorithms. A failure in one area can undermine trust in all.

Looking ahead

Regulatory domains are no longer siloed – they increasingly overlap, creating a network of converging expectations. The intersections – privacy with competition, cybersecurity with financial conduct – mark the new frontier of compliance.

Organizations that map these overlaps and develop integrated response strategies will be more resilient, more credible with regulators and better positioned to thrive.

7.

The fragmented global landscape for anonymization

In brief

Around the world, anonymization is coming under intense legal and regulatory pressure. As organizations increasingly want to leverage data to power AI, analytics and global collaborations, the rules on what truly counts as anonymized data are shifting fast – and expectations are rising. Courts and regulators are challenging outdated or over-broad claims that data can no longer be linked to individuals, pushing companies to adopt more robust, context-sensitive approaches. Recent decisions in Europe and stepped-up actions from regulators like the US Federal Trade Commission (FTC) make clear that half-measures don't work – and carry real legal and reputational risks. In this environment, effective anonymization is no longer a technical detail; it's a baseline.

> Using inadequate anonymization methods or overstating anonymization processes carries significant compliance and reputational risks.

Giles Pratt
Partner

Fragmented global standards for anonymization

Anonymization is essential for organizations seeking to use personal data for innovation and secondary purposes while minimizing privacy risk and compliance obligations, including under additional sector-specific regulation. But for multinationals, the absence of global alignment creates a patchwork of obligations that increases legal risk, drives up compliance costs and complicates cross-border data use.

The trend – especially in the EU – is towards a more nuanced, context-specific test of when data is truly anonymized, with recent court pronouncements adding further layers of complexity.

- **EU:** The EU's General Data Protection Regulation (GDPR) doesn't define 'anonymization,' but Recital 26 makes clear that anonymous information falls outside its scope. The key question is whether data 'relates to an identified or identifiable natural person.' Courts initially took a strict view, asking whether anyone could, in principle, identify the individual. Recent case law, including *SRB v EDPS* (Court of Justice of the EU (CJEU) case C-413/23 P), signals a shift towards a more pragmatic understanding. Whether information is considered personal data must be assessed in context, based on the means reasonably available to the respective actor (data provider or recipient), rather than to hypothetical others.
- **UK:** The UK GDPR and the Data Protection Act 2018 also stop short of defining 'anonymization.' The line is instead drawn by reference to the definition of personal data. The Information Commissioner's Office provides practical guidance, describing anonymization as 'the techniques and approaches you can use to prevent identifying people that the data relates to,' and referring to 'effective anonymization' when the UK GDPR threshold is met through robust technical and organizational measures.
- **US:** In the US, 'deidentification' is the term typically used, and definitions vary across a patchwork of state and sectoral laws. The California Consumer Privacy Act defines deidentified data as data that cannot reasonably be linked to a consumer, provided the business: (i) takes reasonable measures to prevent reidentification; (ii) publicly commits not to reidentify the data; and (iii) requires recipients to uphold deidentification requirements. Additional frameworks, like the Health Insurance Portability and Accountability Act (HIPAA), add complexity, offering both a 'Safe Harbor' method (removal of 18 identifiers) and an 'Expert Determination' method (statistical assessment of reidentification risk).
- **APAC:** Standards for anonymization vary significantly across the region:
  - **China:** The Personal Information Protection Law (PIPL) distinguishes between anonymization (irreversible, non-restorable data) and de-identification (reversible, potentially identifiable when combined with other data). A national anonymization standard is under development.
  - **Japan:** Data is considered anonymized if it cannot be restored using methods available to ordinary people or businesses, assessed case-by-case and in context.
  - **Singapore:** Guidelines allow both reversible and irreversible anonymization, with emphasis on assessing the likelihood of reidentification in practice.
  - **Hong Kong:** Focuses on practical risk: could an individual reasonably and practically be re-identified, including using other publicly available information?
  - **South Korea:** The Personal Information Protection Act now delineates anonymized and pseudonymized data, and detailed guidelines on pseudonymization have been published.
  - **Regional Guidance:** In June 2025, the Technology Working Group of the Asia Pacific Privacy Authorities published its Guide to Getting Started with Anonymization, aiming to align approaches across the region. It defines anonymization as rendering personal data unidentifiable (alone or in combination with other data) using reasonable and state-of-the-art measures, and recommends best-practice techniques such as suppression, masking, generalization, noise addition, sampling and swapping, drawing on international standards such as ISO/IEC 20889 and risk-assessment methods like k-anonymity.

> Standards for anonymization vary across the globe. Special care needs to be taken with aggregations of data from multiple country sources.
>
> **Richard Bird**
> Partner

Rising regulatory enforcement around misleading anonymization claims

Regulators are increasingly targeting misleading or overstated claims of anonymization. In the US, the FTC has shown particular interest in pursuing companies that rely on weak deidentification measures or misrepresent their practices. Its guidance, 'No, hashing still doesn't make your data anonymous,' makes clear that techniques such as hashing – which converts personal data into unique strings – fall short of true anonymization. Such methods can still leave individuals re-identifiable, particularly when hashes are matched or combined with other information. The FTC has already brought enforcement actions against companies on this basis.

Internationally, regulators are scrutinizing purported anonymization that fails to meet legal or technical standards, with growing attention on whether datasets can be realistically reidentified given advances in analytics and the availability of external data.

Best practice is moving towards comprehensive risk assessment and stronger governance of anonymized datasets. Keeping detailed records, testing reidentification risk on an ongoing basis and updating governance to reflect evolving guidance and technology are now critical.

Anonymization as a strategic enabler of AI and global data flows

For global organizations, anonymization is no longer just a compliance exercise; it is a strategic tool for responsible innovation in AI, machine learning, advanced analytics and cross-border data collaborations.

Properly anonymized datasets – where individuals cannot reasonably be reidentified – usually fall outside the scope of data protection regimes such as the EU GDPR, and cross-border data transfer frameworks (including Standard Contractual Clauses, Cross-Border Privacy Rules, and adequacy decisions). That exemption reduces compliance pressure and clears the way for international data-driven initiatives. Although anonymization does not exclude the application of frameworks like the EU AI Act, it simplifies AI compliance significantly.

But advances in technology – from the growing sophistication of AI to the sheer volume of external data now available – have raised the bar. Traditional techniques are increasingly vulnerable to reidentification, making anonymization a dynamic, context-specific discipline rather than a one-off fix. New approaches are emerging, from synthetic data generation to privacy-enhancing technologies (PETs) and federated learning. These solutions allow organizations to train AI models and extract value from data while keeping privacy risks – and regulatory exposure – in check.

> Anonymization is a strategic enabler for global data innovation.
>
> **Mark Egeler**
> Partner

Sector-specific relevance and compliance use cases

Anonymization plays a decisive role across industries, balancing innovation with legal limits:

- **Healthcare/Pharma:** Anonymized patient data underpins secondary research and collaboration despite strict rules on clinical trial and health information.
- **Financial Services:** Institutions anonymize transactional data to power AI-driven fraud detection, risk modeling and market analytics, while staying within strict privacy boundaries.
- **Technology & Media:** These sectors rely on behavioral analytics for product development but must draw a clear line between pseudonymization and full anonymization to remain compliant, particularly under the GDPR and emerging AI regulations.

In each case, the ability to robustly demonstrate that data is genuinely anonymized not only reduces legal risk but also opens the door to new forms of data use.

> Robust anonymization unlocks data's value and safeguards trust.
>
> **Satya Staes Polet**
> Partner

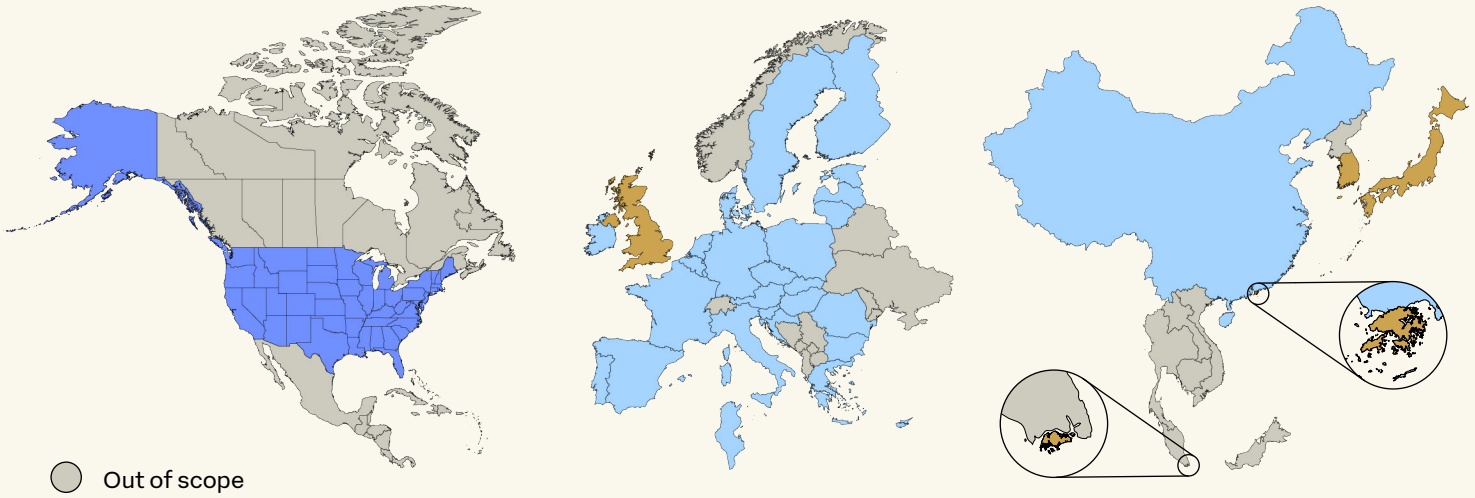
Looking ahead

Effective anonymization is no longer a one-off technical fix but an ongoing governance priority – central to unlocking AI, advanced analytics and cross-border data flows while keeping pace with fast-changing laws. Here's what organizations should do now:

1. **Re-evaluate processes:** Regularly test anonymization and deidentification methods against new laws, court rulings and technological advances. Ensure that your approaches – whether hashing, aggregation, masking or more advanced techniques – meet current standards and withstand scrutiny.
2. **Build strong governance:** Treat anonymization as a dynamic process. Put in place governance frameworks, continuous reidentification risk assessments and periodic audits. Document your methodologies and decision-making – regulators increasingly expect you to show your work.
3. **Adopt new tools:** Explore synthetic data, federated learning and other PETs to balance utility with protection. Combine technical and organizational controls for maximum effect.
4. **Train and align:** Make sure staff understand the distinction between anonymization and pseudonymization. Update privacy policies, contracts and data-sharing arrangements, and hold partners and vendors to the same standards.
5. **Monitor enforcement trends:** Follow regulatory guidance and enforcement in your key markets. Be precise in disclosures – overstating anonymization is an emerging enforcement trigger.

Anonymization is complex, but it is also pivotal to building resilient, future-ready data strategies. Our global team helps organizations respond to regulatory change, from practical compliance assessments to detailed technical and legal reviews.

Global anonymization standards heat map



Out of scope

US

FTC enforcement (hashing ≠ anonymization)

Flexible, decentralized/sectoral

UK

ICO practical anonymization guidance

Robust risk-based/pragmatic

EU

CJEU ruling C-413/23 P (context-based test)
Growing DPA scrutiny of pseudo-anonymization

Strict, context-dependent

APAC

China PIPL distinction (anonymization vs deidentification)
APPA June 2025 regional guidance

China
Strict, context-dependent

Hong Kong, Singapore, Japan and **South Korea**
Robust risk-based/pragmatic

Key contacts

EU

Mark Egeler
Partner, Amsterdam
T +31 20 485 7680
E mark.egeler
@freshfields.com

Theresa Ehlen
Partner, Düsseldorf
T +49 211 49 79 601
E theresa.ehlen
@freshfields.com

Martin Mekat
Partner, Frankfurt
T +49 69 27 30 80
E martin.mekat
@freshfields.com

Jérôme Philippe
Partner, Paris
T +33 1 44 56 44 56
E jerome.philippe
@freshfields.com

Lutz Riede
Partner, Vienna
T +43 1 515 15 0
E lutz.riede
@freshfields.com

Satya Staes Polet
Partner, Brussels
T +32 2 504 7000
E satya.staespolet
@freshfields.com

Christoph Werkmeister
Partner, Düsseldorf
T +49 0211 4979 390
E christoph.werkmeister
@freshfields.com

Davide Borelli
Counsel, Milan
T +39 02 625 301
E davide.borelli
@freshfields.com

Philipp Roos
Counsel, Düsseldorf
T +49 211 4979-390
E philipp.roos
@freshfields.com

US

Brock Dahl
Partner, Silicon Valley and Washington, DC
T +1 650 618 9250
E brock.dahl
@freshfields.com

Beth George
Partner, San Francisco
T +1 415 400 2117
E beth.george
@freshfields.com

Timothy Howard
Partner, New York
T +1 212 230 4690
E timothy.howard
@freshfields.com

Megan Kayo
Partner, San Francisco
T +1 650 461 8297
E megan.kayo
@freshfields.com

Christine Wilson
Partner, Washington, DC
T +1 202 777 4573
E christine.wilson
@freshfields.com

Nina Frant
Special counsel,
Washington, DC
T +1 202 777 4548
E nina.frant
@freshfields.com

Key contacts

UK

Rachael Annear
Partner, London
T +44 20 7936 4000
E rachael.annear
@freshfields.com

Matthew Bruce
Partner, London
T +44 20 7936 4000
E matthew.bruce
@freshfields.com

Cat Greenwood-Smith
Partner, London
T +44 20 7716 4870
E cat.greenwood-smith
@freshfields.com

Giles Pratt
Partner, London
T +44 20 7936 4000
E giles.pratt
@freshfields.com

Rhodri Thomas
Partner, London
T +44 20 7936 4000
E rhodri.thomas
@freshfields.com

Tony Gregory
Counsel, London
T +44 20 7936 4000
E tony.gregory
@freshfields.com

APAC

Richard Bird
Partner, Hong Kong
T +852 2846 3400
E richard.bird
@freshfields.com

Cédric Lindenmann
Counsel, Singapore
T +65 6636 8000
E cedric.lindenmann
@freshfields.com

MENA

Kim Rosenberg
Partner, Dubai
T +971 4 5099 100
E kim.rosenberg
@freshfields.com

FRESHFIELDS

2025, 546615

freshfields.com