Ashurst

What's Ahead

2026 Technology industry in the EU & UK

Outpacing change

Introduction

In 2026, businesses in the technology sector face a rapidly evolving landscape in the EU and UK. Global disruption and regulatory divergence, unprecedented investment in infrastructure fuelled by AI, heightened merger scrutiny, and a surge in private legal actions are shaping a complex environment where innovation, compliance, and risk management must be carefully balanced.

Here is our take on key themes for 2026:

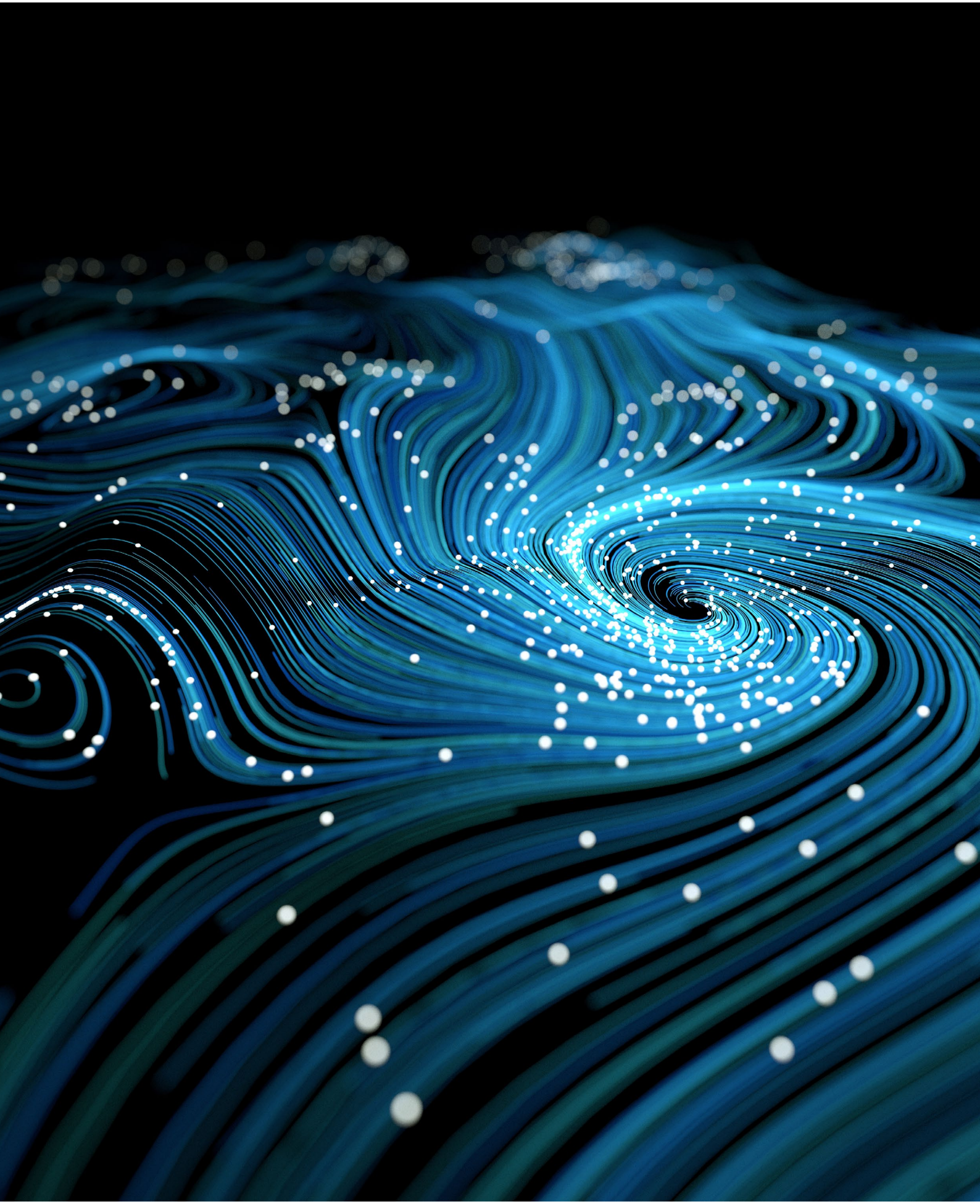
1. **Continuing intensive regulatory reform:** between the EU Digital Markets Act (**DMA**), EU Digital Services Act (**DSA**), AI Act, Data Act, Data Governance Act (**DGA**), Network and Information Systems 2 Directive (**NIS2**), Digital Operational Resilience Act (**DORA**) and Cyber Resilience Act in the EU and the Digital Markets, Competition and Consumers Act (**DMCC Act**) and Online Safety Act (**OSA**) and Data (Use and Access) Act (**DUUA**) in the UK, the regulatory landscape in the EU and UK is continually evolving. In addition, the European Commission has acknowledged the need for a more simplified digital regulatory framework to avoid the unintended consequences identified in the Draghi report. It continues to consult on its Digital Omnibus Package unveiled in November last year (see our November 2025 update).

2. **More aggressive enforcement and higher penalties:** by the European Commission, EU Member States' national competition authorities (**NCAs**) and the UK Competition and Markets Authority (**CMA**). Armed with greater resources, expertise, and enforcement powers, we are seeing more investigations, pursuit of novel theories of harm, intrusive remedies and substantial penalties. The European Commission recently imposed significant fines against Google, TikTok and X (formerly Twitter) and continues to investigate Meta's AI policy on WhatsApp, Google's use of web publisher's content for AI Overviews, and whether the DMA should be expanded to cover cloud services.

3. **More private actions:** recent years have seen a significant increase in private proceedings, including class actions, alleging breaches of competition, consumer, and privacy laws.

4. **Greater coordination between domestic and international regulators:** the increasing intersection of competition, consumer protection, privacy, online safety and data issues is driving greater cooperation between regulators worldwide. In the UK, the Digital Regulation Cooperation Forum (**DRCF**) brings together four regulators (the CMA, the Financial Conduct Authority (**FCA**), the Information Commissioner's Office (**ICO**) and Ofcom) to *"protect and empower people in their use of digital services while unlocking economic growth throughout the UK digital economy"*.

5. **Intensified scrutiny of AI including algorithms, automated decision making and generative AI:** with the EU AI Act being the first legal framework for AI in the world and regulators across Europe providing guidance on how they will assess the compatibility of AI systems with competition and consumer law.



AI	
1	**EU AI Act:** the Act officially entered into force on 1 August 2024, however, its roll-out has been subject to significant delays. The European Commission has proposed delaying the entry into force of certain elements from August 2026 until 2027. For example, rules relating to human oversight of high-risk AI systems posing *"serious risks to health, safety or fundamental rights"* and transparency rules have been delayed until at least December 2027, as part of the EU's Digital Omnibus package (see our November 2025 update). In 2026, we expect to see publication of the first harmonised standards under the EU AI Act, and guidelines on technical requirements for high-risk AI systems. The Act will apply to operators of high-risk AI systems, placed on the market before this date; however, this only applies to systems which are subject to significant changes in their designs from this date onwards. Providers of general-purpose AI (**GPAI**) models placed on the market before 2 August 2025 must take the necessary steps to comply by 2 August 2027.
2	**Legislative proposals for the EU Cloud and AI Development Act:** have been tabled, with the initial draft due to be presented to the European Parliament in Q1 2026.
3	**Opinion on the Digital Omnibus on AI:** in January 2026, the European Data Protection Board and the European Data Protection Supervisor issued a joint opinion on the proposed Digital Omnibus on AI, aimed at simplifying parts of the AI Act. While acknowledging the benefits of administrative simplification, they warn against reforms that could weaken fundamental rights protections, particularly those related to personal data under the GDPR. Key concerns include preserving the AI Act's transparency obligations despite a possible delay of broader compliance deadlines to 2027, maintaining mandatory registration for systems self-assessed as non-high risk to prevent regulatory under-classification, and limiting the proposed ability to process sensitive data for bias mitigation strictly to cases of demonstrable necessity. Entities are therefore advised not to suspend *"high-risk"* compliance preparations for August 2026: transparency duties may still apply this summer, rigorous risk-classification processes should remain in place, and any use of sensitive data in model training must be carefully justified and documented.
4	**UK approach:** the UK is maintaining its non-statutory approach to AI regulation. The CMA, Ofcom, ICO and FCA continue to work together and align on policy as the DRCF to oversee implementation of AI in their respective sectors. The CMA has published guidance on how it considers competition and consumer law applies to AI systems and agents (see our March 2026 update). The UK government sees AI as a key driver for the UK economy (see, for example, the AI Opportunities Action Plan and the push towards AI Growth Zones) and has urged regulators to put in place frameworks which encourage more innovation as well as providing safeguards. It is also promoting AI within the public sector with its AI Playbook. Meanwhile, the rapid adoption of AI in the UK, like elsewhere, faces various challenges in the supply chain, including a global shortage of memory chips and a lack of industry skills. However, the clear aim of the government is to provide an attractive regulatory environment for AI innovation.
5	**UK courts' approach:** in 2025, courts in England and Wales continued to criticise inaccurate use of GenAI tools in legal proceedings. For example, in *R (Ayinde) v Haringey LBC* [2025] EWHC 1383 (Admin), the court set out examples of hallucinated cases put before the courts and tribunals. Consequences of inaccurate use or misuse of AI in litigation have included orders for wasted costs, referrals for misconduct and warnings of potential contempt. The Law Society and the Bar Council have issued updated guidance regarding practitioners' use of AI and duties to the court.

Key cases to watch

- **Getty Images v Stability AI**
  The much-anticipated High Court decision was published in November 2025. This case is one of the first IP claims against an AI developer to reach trial. The key issues narrowed as the case progressed, and the Court was primarily left to determine the issues of secondary infringement of UK copyright and trademark infringement. The Court found that the importation of a pre-trained generative AI model into the UK does not amount to secondary infringement of UK copyright. This is good news for AI developers based outside of the UK, but less so

6	**UK Civil Justice Council has set up a working group:** to consider rules governing the use of AI in preparing court documents. Proposals are expected to include mandatory disclosure of AI use, certification of human oversight, and limits on AI generated expert evidence, likely prompting closer scrutiny of litigation drafting practices throughout 2026.
7	**AI governance uplift – literacy and serious-incident reporting:** AI literacy is a mandatory, role and context specific obligation for providers and deployers, explicitly addressing generative AI risks such as hallucinations and bias. Draft guidance and a template define **"serious AI incidents"** (e.g., deaths, major health impacts, critical infrastructure disruption, significant fundamental rights harms) and set reporting windows of 2 to 15 days. Organisations should adopt integrated incident playbooks that align AI Act duties with parallel regimes, notably NIS2, DORA, and the GDPR.
8	**Report on the AI Act as a prelude to the Digital Omnibus and Omnibus AI regulations:** the European Parliament's report on the interplay between the AI Act and core EU digital laws (GDPR, DSA, DMA, Data Act, and DGA) highlights tensions, risks of fragmentation, and legal uncertainty. Its release coincides with the European Commission's Digital Omnibus and Omnibus AI initiatives, which aim to streamline and rationalise digital law, raising questions about the balance between simplification and the substance of the EU's regulatory model.
9	**Report to the European AI Office:** the new AI Act Whistleblower Tool was launched on 24 November 2025 to enable individuals and professionals to report suspected violations of the AI Act to the European Artificial Intelligence Bureau. Whistleblowers can complete an anonymous questionnaire covering when and where the infringement occurred, their relationship to the company involved, a description of the incident, and other relevant information. Using a secure inbox, whistleblowers can then maintain anonymous, ongoing communication with the AI Office to provide additional details and receive follow up updates.
10	**AI & copyright:** in the UK, tensions between the creative industries and AI developers remain, with creators seeking greater transparency and control, and developers calling for more freedom. A government consultation on the issue coincided with parliamentary scrutiny of the Data (Use and Access) Bill and a lengthy *"tug of war"* between the Commons and the Lords on the level of copyright protection. The DUUA provides various steps towards resolving the issue, including setting up expert working groups to explore solutions and inform policy. A report, with government proposals on various issues, is expected in 2026.
11	**Revised EU Product Liability Directive:** entered into force on 8 December 2024 and will apply to products placed on the EU market as of 9 December 2026. The Directive significantly expands liability exposure for AI systems, software and digital products, while also enabling claims for data loss and extending potential liability to online marketplaces where no EU-based manufacturer can be identified. Conversely, in September 2025, the Law Commission announced a review of the existing product liability regime in the UK, particularly in relation to digital products and emerging technologies such as AI, to determine what reform might be required to ensure that the product liability regime is fit for purpose. A formal public consultation on the proposals for reform is currently planned for the second half of 2026.

for owners of UK copyright. The judge also dismissed the infringement claim under section 10(3) of the Trade Marks Act, citing a lack of evidence that the appearance of Getty/iStock watermarks in AI-generated outputs amounted to detriment to distinctive character or reputation, or unfair advantage.

- **The deal between OpenAI and Disney**
  Disney has signed a three-year licensing agreement with OpenAI, a USD 1 billion investment that allows Disney's characters to be used in ChatGPT and the video generation tool Sora. The three-year license comes with only a year of exclusivity for OpenAI. Disney will then have the possibility to license its brand to other AI platforms.

Data & Privacy

1	**UK Data (Use and Access) Act:** 2025 saw a shift in the UK legislative landscape with the DUAA getting Royal Assent after much debate in Parliament. The Act is being implemented in stages (see our February 2026 update) and in-house legal teams will need to monitor its progress. The Act introduced amendments to UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003, impacting areas such as scientific research, direct marketing, automated decision-making and data transfers. The ICO's expanded investigatory remit under the DUAA, including a new power to compel interviews, documents and reports by an approved person, is a shift from reactive to more proactive oversight (see our October 2025 update). Key areas for businesses to focus on include their complaints procedures, marketing practices and cookie policy. The ICO is planning to publish updated guidance on what the DUAA changes mean in practice. The government's Modern Industrial Strategy recognises data as one of the UK's unrealised assets and the DUAA sets out a framework for smart data schemes, which aim to promote secure, consent-based data sharing with resulting economic benefits for businesses and consumers. Smart data has already transformed open banking in the UK and is likely to be expanded to cover energy. The DUAA also paves the way for digital ID, facilitating access to vital government services and reducing identity fraud, although opinion is divided about this move.
2	**Changes at the ICO:** from April 2026, the ICO will become the Information Commission. Although its functions are unlikely to change significantly, it will gain new investigatory powers under the DUAA: in particular, to compel the production of documents, to require controllers or processors to provide a report on a specified matter, and to compel individuals to attend interviews and answer questions. This marks a significant change as it shifts the investigative burden and costs onto organisations while potentially allowing the ICO to investigate more cases. 2025 also saw some noteworthy enforcement action from the ICO (in particular, a £14 million fine for Capita) and it is likely that this robust and targeted approach will continue.
3	**Biometric data:** increased use of biometric data means increased regulatory scrutiny. The ICO has published its AI and biometrics strategy with a focus on three cross-cutting issues: transparency and explainability; bias and discrimination; and rights and redress. Any organisation using biometric processing should familiarise itself with the strategy and the ICO's thinking. The regulator is also prioritising guardrails for the use of facial recognition technology, by police forces in particular. However, the Home Office believes that the use of biometric data for law enforcement merits a separate legal framework and has launched a consultation, indicating that new legislation is likely.
4	**EU Data Act:** entered into force on 12 September 2025. It sets rules for accessing and using data from connected products and related services, with safeguards for trade secrets. It also sets requirements for manufacturers to provide usable interfaces; data holders must allow third party access on fair, transparent terms and cloud and edge providers must enable switching with no more than two months' notice and support data export within 30 days. The Act covers IoT manufacturers and service providers, cloud and edge providers, data holders controlling usage data, and businesses building services on such data.
5	**EU model contractual terms for B2B data sharing and standard contractual clauses on cloud agreements:** these templates are recommendations from an expert group that aim to facilitate the practical implementation of the EU Data Act. Here is the final report of the expert group.

Key cases to watch

- **Prismall v Google/DeepMind**
  The claimant brought an opt-out representative action on behalf of 1.6 million individuals for loss of control damages in respect of misuse of private information related to the sharing of patient-identifiable data by the Royal Free Hospital with Google/DeepMind. The High Court struck out the claim in 2023, finding that while medical information is generally private, it did not necessarily give rise to a reasonable expectation of privacy. The Court of Appeal dismissed the appeal in late 2024, noting that *"a representative class claim for MPI is always going to be very difficult"*, given that some of the medical data may be trivial or anodyne, or indeed may have been shared publicly e.g. on social media.

- **Facebook user class action**
  Liza Lovdahl Gormsen has been successful in her request to amend her claim to include *"user damages"* (compensation based on what Meta would have paid Facebook users for their data in a hypothetical negotiation). Meta sought to reject this, arguing that such damages are not recoverable for competition law infringements. However, the CAT found that a claim for user damages has a real prospect of success and should be considered at trial, scheduled for September 2027.

- **Farley and Others v Paymaster (1836) Limited (t/a Equiniti)**
  The Court of Appeal's August 2025 decision found no de minimis threshold of seriousness for data protection claims (as distinct from misuse of information claims). However, a claimant must still establish, on an objective standard of reasonableness, that they suffered non-material damage. The Supreme Court granted permission to appeal in December 2025. It remains to be seen, either later this year or next, whether this judgment will be overturned so as to conclude that a threshold of seriousness applies in data protection cases.

- **French data protection authority (CNIL) fined Free Mobile €27 million and Free €15 million**
  for GDPR and security failures on 13 January 2026 following a breach that exposed data from millions of subscribers (identification, contact, and IBAN details). The decision sanctions the failure of proper breach notification to individuals, proportionate security under Article 32 GDPR (an obligation of means, with consistent risk-based measures), and sanctions excessive data retention, requiring defined retention periods with effective deletion / archiving.

Online Safety	
1	**UK Online Safety Act 2023:** most provisions of the UK's OSA are now in force. As anticipated, it has had most impact on social media, messaging and search platforms and Ofcom, as regulator, believes that over 100,000 services are now within its scope. The OSA focuses on limiting illegal content and protecting children from harm and has significant crossover with data protection law – in fact it requires Ofcom to consult with the ICO in producing codes of practice. Ofcom is given considerable information-gathering and enforcement powers, culminating, where relevant, in hefty fines. With online safety as a key focus area of its 2026/7 Plan of Work, we expect Ofcom's enforcement programme to ramp up, supported by more guidance for providers and a super-complaints procedure. The UK has not, as yet, followed the Australian approach of a social media ban for under-16s but the recently-announced consultation on children's use of mobile phones and social media may signal legal or regulatory changes ahead.
2	**Media literacy:** improving media literacy is seen as vital for enabling online audiences to make safe choices and identify trustworthy news sources. As well as boosting online safety in parallel with the UK OSA, the aim is to limit the spread of misinformation and disinformation. Ofcom has published a three-year Media Literacy Plan for platforms and other bodies, and further recommendations are promised in spring 2026.
3	**EU Digital Services Act:** during 2025, the European Commission ramped up DSA enforcement and we expect to see this continue in 2026, with a particular focus on age assurance and age verification. On 14 July 2025, the European Commission also published guidelines on the protection of minors under the Digital Services Act, which apply to all online platforms accessible to minors, with the exception of micro and small enterprises.

Key cases to watch

- **AVS Group Ltd**
  In December 2025, Ofcom fined AVS Group Ltd (a provider of adult services) £1 million for failing to implement robust age checks for users, and a further £50,000 for failing to respond to information requests.

- **Unnamed forum**
  Ofcom's first investigation under the OSA examined a suicide discussion forum. A provisional notice of contravention has been issued and a final decision is expected soon.

- **X fined €120 million**
  In December 2025, the European Commission fined X (formerly Twitter) for breaching its transparency obligations under the DSA. The breaches identified included the *"deceptive design of its 'blue checkmark', the lack of transparency of its advertising repository, and the fairly to provide access to public data for researchers"*.

- **First fine under the OSA**
  The online discussion forum 4chan was fined £20,000 for failing to respond to information requests. 4chan has stated that it plans to ignore the fine, so daily penalties are accruing.

- **Investigation into X**
  Ofcom is urgently investigating reports that the Grok AI chatbot account on X is being used to create and share naked and sexualised images. X faces similar action by the European Commission and other national regulators (including an investigation by the UK ICO announced in February 2026).

- **European Commission preliminarily finds TikTok and Meta in breach of DSA transparency obligations**
  In October 2025, the European Commission preliminarily concluded that TikTok and Meta had both breached their obligation to grant researchers adequate access to public data under the DSA. The European Commission also preliminarily found that (in relation to both Facebook and Instagram) Meta had breached its obligations to provide users with simple mechanisms for notifying illegal content and to allow them to effectively challenge content moderation decisions. The companies now have the chance to review the documents on the European Commission's file and respond to the preliminary findings. If the European Commission's views are ultimately confirmed, it may issue a non-compliance decision (with the potential for fines of up to 6% of the provider's annual worldwide turnover).

Cybersecurity	
1	**Cyber threats in the UK:** how to prevent, and deal with, cyber threats is a topic on every board's agenda following several high-profile cyber-attacks on UK household names. New legislation is on the horizon (the Cyber Security and Resilience (Network and Information Systems) Bill) which will expand the scope of the NIS Regulations, bringing data centres and other operators of essential services within their scope (see our February 2026 update). Enhanced reporting requirements, and strengthened enforcement powers for regulators, are also planned. The National Cyber Security Centre (**NCSC**) and the Department for Science, Innovation and Technology (**DSIT**) have published the Government Cyber Action Plan (January 2026) focusing on cyber resilience in the public sector, with a new Government Cyber Unit to coordinate risk management and incident response. Meanwhile, ministers have written to leading UK businesses urging action against hostile cyber activity. One recommendation is to follow the Cyber Governance Code of Practice covering key areas of risk management, strategy, people, incident planning, response and recovery, and assurance and oversight. It is likely that threats to critical infrastructure and supply chains will increase and become more sophisticated. At the same time, cybersecurity and privacy will converge. Faced with a rapidly-growing and complex threat landscape, organisations must keep their security measures under constant review.
2	**NIS2 Directive:** the NIS2 Directive extends the relevant sectors and increases the number of regulated entities significantly. The Directive strengthens the resilience and security of providers of essential and important services across the EU by imposing binding requirements on cybersecurity, risk assessment and risk mitigation measures (including supply-chain risk management) and incident reporting. Regulated entities will need to revisit their governance structure, as well as assess their supply chain contracts with technology, network and other suppliers to ensure they provide the required level over risk protection. After the implementation deadline for NIS2 elapsed in October 2024, Germany finally adopted the national implementation in December 2025. While France was initially expected to conclude its parliamentary process in Q1 2026, delays in the parliamentary debates have pushed back the timetable, with the implementation into French law now expected to take place around July 2026.
3	**New adjustments proposed by Digital Omnibus about cybersecurity:** the Digital Omnibus establishes a unified point of contact for incident notifications, replacing sector-specific regimes and proposes the creation of a single-entry point to respect the mandatory incidents notifications of NIS2, the GDPR and DORA. It also envisions deploying data labs, legal helpdesks, and related tools to mitigate the risk of sensitive data leaks.
4	**Reporting requirements of the EU Cyber Resilience Act:** the CRA is designed to protect individuals and professionals against cyberattacks by creating cybersecurity requirements for products containing digital elements, such as hardware. While most of the obligations of the CRA will apply from 11 December 2027, businesses must comply with the mandatory reporting requirements for actively exploited vulnerabilities from 11 September 2026 and the Single Reporting Platform will be operational from the same day.
5	**Digital Operational Resilience Act, key requirements & compliance guide:** DORA entered into force in 2025 to make sure that financial entities (banks, investment firms, insurance companies etc) increase their level of operational resilience notably in relation to their ICT providers. DORA, therefore, requires an internal control and governance frameworks, transparent organisational structures, continuous monitoring controls, business impact analyses and incident response protocols to detect disruptions and activate immediate procedures, as well as contract remediation with ICT providers to ensure the contracts contains the mandatory provisions required by DORA.

Consumer Law

1	**CMA's enforcement powers:** under the UK Digital Markets, Competition and Consumers Act 2024 (**DMCC Act**) which came into force in April 2025, the CMA can now directly enforce UK consumer protection laws through administrative proceedings, akin to its powers to enforce competition law and fine companies up to 10% of their global turnover and individuals up to GBP 300,000. In November 2025, the CMA launched its first consumer investigations into eight companies focused on online pricing and marketing practices (see our November 2025 update). The CMA has separately issued 100 advisory letters to businesses across the following sectors: holiday and package travel, rail, bus and coach travel, parking and airport parking, live event tickets, cinema tickets, food and drink delivery services, letter and parcel delivery, and fashion. The CMA has confirmed that it will continue to take necessary action to address any consumer protection law breaches, focusing in particular on egregious practices affecting areas of essential spend, as well as continuing to support businesses with compliance through guidance and outreach activities.
2	**Unfair commercial practices:** in the UK, the DMCC Act restated consumer protections against unfair commercial practices in primary legislation. The DMCC Act grants the Government the power to amend the list of banned practices through secondary legislation and the CMA has been active in publishing updated and new guidance. In April 2025, the CMA published its guidance on unfair commercial practices including examples and a summary of the changes made by the DMCC Act. In November 2025 the CMA published further guidance focusing on price transparency. We also expect increased enforcement in EU Member States to continue, particularly in France and Italy.
3	**Fake reviews and pricing practices in the UK:** the DMCC Act includes specific banned practices to tackle fake reviews and various misleading or illegal pricing practices such as drip pricing (see our February 2026 update). In 2025 the CMA also secured undertakings from Ticketmaster regarding the way prices and tickets were advertised during the sale of Oasis tickets. In 2025, the CMA secured commitments from Google and Amazon to tackle fake reviews appearing on their platforms. In July 2025, following a sweep of more than 100 websites, the CMA sent advisory letters to 54 firms advising them to implement measures to prevent fake reviews on their sites.
4	**Subscription traps in the UK:** new obligations are expected to come into force in Autumn 2026 which will clarify and strengthen pre-contractual information given to consumers and nudging obligations to avoid so called subscription *"traps"*. Businesses should prepare for these changes and ensure any subscription style contracts are compliant before the regime goes live.
5	**Online choice architecture:** following the publication of its Online Choice Architecture paper in 2022, the CMA has undertaken a number of investigations into misleading practices such as the use of urgency or scarcity claims, countdown timers and pre-ticked boxes. Its ongoing investigations under the direct enforcement regime include investigations into homeware retailers in relation to the use of time-limited sales and automatic opt-ins for additional services.
6	**AI and consumer law:** the CMA continues to grapple with how consumer regimes can deal with the rapid expansion in both capabilities and adoption of AI tools and agentic systems. The CMA has made clear that existing consumer protection law applies in full to AI-powered systems. Businesses remain responsible for what their AI agents do, in the same way as they are responsible for actions of their employees (see our March 2026 update).
7	**Product safety:** the UK Product Regulation and Metrology Act 2025 received Royal Assent on 21 July 2025. As part of this, the UK Government has noted its intention to hold online marketplaces to account for dangerous products sold through their platforms. Secondary legislation to this effect is expected although timings as to when remain unclear.
8	**EU Digital Fairness Act:** the European Commission is preparing a proposal to introduce the Digital Fairness Act by the end of 2026. This Act is aimed at strengthening online consumer protection by addressing manipulative digital practices such as dark patterns; misleading influencer marketing; subscription contracts; online choice and addictive design features; and unfair personalisation practices aimed at the protection of minors.

9	**EU "right to repair":** the EU's *"right to repair"* directive entered into force in July 2024 and all EU Member States must implement the new rules into national law by the end of July 2026. The new rules require manufacturers to publish details regarding their repair services and the prices for repair. By July 2027, the European Commission must also launch an EU-wide platform which links consumers with repairers, including a search function to find sellers of goods subject to refurbishment and purchasers of defective goods for refurbishment.
10	**Supply Chain Sustainability Due Diligence Law:** the Corporate Sustainability Due Diligence Directive (**CS3D**) requires companies to address their negative impact on the environment and human rights across their supply chains. In February 2026, the Council gave its *"green light"* to a simplification of the sustainability reporting and due diligence requirements. The Omnibus I Directive significantly reduces the scope and regulatory burden of the CS3D, focusing the rules on very large companies (companies with over 5,000 employees and €1.5 billion turnover), allowing risk-based prioritisation in value chains, removing climate planning and EU civil liability provisions, and delaying national transposition to July 2028 and company compliance to July 2029.
11	**Green claims:** "green washing" remains a focus of both UK and EU regulators. In the UK, the CMA has published guidance confirming that businesses across the supply chain can be liable for misleading green claims and confirming that where a business holds evidence substantiating a claim, the CMA expects it to proactively share that evidence with others in the supply chain who rely on the claim (see our January 2026 update). In the EU, in 2024 reforms to the EU Directive (EU) 2024/825) introduced a specific prohibition targeting greenwashing to explicitly prohibit misleading environmental (green) claims being made by businesses. This reform is a cornerstone of the EU's strategy to empower consumers for the green transition, targeting misleading environmental claims, greenwashing, planned obsolescence, and the misuse of sustainability labels. Member States are required to transpose the Directive by 27 March 2026 and apply its provisions from 27 September 2026.

Key cases to watch

- **Emma Sleep**
  In November 2022, the CMA launched an investigation into Emma because of concerns that some of its online sales practices (e.g. discounts and urgency claims, including countdown timers and high demand prompts) may mislead customers. The CMA launched court action in October 2024 and commented that Emma had been given *"sufficient opportunity to alter the way it does business to address"* the CMA's concerns. In August 2025, the case was listed to be heard in the High Court starting on 3 June 2026. This case was initiated before the CMA's direct enforcement powers came into force in April 2025.

- **First investigations opened by the CMA**
  The focus of these initial investigations is on online pricing and sales practices (including the use of drip pricing and presentation of mandatory fees, time-limited promotional sales, and pre-selected default options) by eight companies in the secondary ticketing, driving schools, gyms and fitness and homeware retailers sectors.

Ex Ante Regulation	
1	**EU:** the DMA is designed to ensure fair and contestable markets, which should deliver a competitive and level-playing field in the digital sector. It enables the European Commission to designate companies as gatekeepers. The first designations were announced in September 2023, with Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta and Microsoft being designated as gatekeepers in relation to core platform services. Since then, the European Commission has continued to update the list of designated gatekeepers, adding Booking.com in May 2024, and has been monitoring compliance with a number of investigations into non-compliance. In 2025, the European Commission also issued investigations into whether Amazon and Microsoft should be designated in respect of their cloud computing services. The DMA's obligations cover a wide range of conduct such as prohibitions on combining personal data across services without consent, restrictions on self-preferencing, requirements to enable effective interoperability and data portability, protections for business users, limitations on pre-installation and bundling practices, and reporting obligations for planned acquisitions.
2	**First fines under the DMA:** in April 2025, the European Commission fined Apple €500 million for breaching its anti-steering obligations under the DMA and Meta €200 million for breaching the DMA obligation to give consumers the choice of a service that uses less of their personal data. Under the DMA, gatekeepers must obtain users' content to combine their personal data between services and users who do not consent must have access to a less personalised but equivalent service. In the same announcement, the European Commission confirmed that it had closed its investigation into Apple's user choice obligations *"thanks to early and proactive engagement by Apple on a compliance solution"*.
3	**EU Member States:** while the European Commission is the sole regulator which can enforce the DMA, the DMA envisages cooperation with NCAs in the EU Member States. The European Commission has indicated that NCAs may investigate alleged non-compliance and report their findings to the European Commission. Depending on how the NCAs perceive their role, we may see more antitrust investigations being opened. In addition, the DMA only regulates specific activities and conduct so competition enforcement will continue in parallel. Member States such as Germany have continued strong against digital platforms under national rules.
4	**UK:** the DMCC Act implements the UK Government's digital markets strategy. The DMCC Act established a new ex ante regime for firms designated to have Strategic Market Status (**SMS**), with the ability to impose binding conduct requirements on designated firms. The DMCC Act also gave the CMA a new enforcement toolkit in relation to SMS firms, including the ability to impose penalties of up to 10% of annual global turnover (or 5% of daily turnover) for SMS firm's breaches of conduct requirements, as well as the ability to seek director disqualification. SMS firms are also subject to a mandatory and suspensory reporting regime for transactions where the deal consideration exceeds £25 million. Following designation decisions issued in 2025, in 2026 the CMA consulted on proposed conduct requirements on Google in respect of its general search and search advertising services, and accepted undertakings from Google and Apple in respect of their mobile platforms. The CMA's CEO, Sarah Cardell, has also recently reported that a further SMS investigation is expected by end of Q1 2026. Further information is available in our August 2024 update and in our April 2025 podcast.

Key cases to watch

- **A further SMS investigation and potentially new conduct requirements in the UK**
  In January 2026, the CMA's CEO, Sarah Cardell, informed the House of Lords Industry and Regulators Committee that the CMA will propose opening its fourth SMS investigation by the end of March 2026. Ms Cardell did not confirm which company it is proposing should be investigated. She also told the committee that the CMA would announce *"first proposals"* in relation to the three existing designations.

  In the same month, the CMA published its proposals for conduct requirements relating to Google's general search services. The proposed conduct requirements relate to: (i) ensuring publishers have more choice and transparency over how their content is used in Google's AI Overviews, (ii) making sure Google's approach to ranking results is fair and transparent for businesses, (iii) making it easier for people to switch the search services they use by making default choice screens on Android mobiles a legal requirement and introducing choice screens on the Chrome browser and (iv) making it easier for people and businesses to make use of Google search data (data portability).

  In February 2026, the CMA published proposed commitments from Apple and Google intended to *"improve certainty, transparency and fairness"* for UK businesses dependent on app stores to serve their customers. The proposed commitments relate to (i) making sure Apple and Google review and rank apps to be distributed on their app stores in a fair, objective and transparent way and do not discriminate against apps which compete with their own (or give preferential treatment to their own apps), (ii) data collection and (iii) interoperability. Subject to comments from stakeholders, the commitments will apply from 1 April 2026.

- **European Commission market investigations on cloud computing services**
  In November 2025, the European Commission opened three market investigations on cloud computing services under the DMA. Two investigations are focusing on whether Amazon and Microsoft should be designated as gatekeepers for their cloud computing services (Amazon Web Services and Microsoft Azure). The European Commission is aiming to complete these investigations within 12 months.

  The third investigation is assessing whether the DMA can effectively tackle practices that may limit competitiveness and fairness in the cloud computing sector in the EU. As part of this, the European Commission will consider obstacles to interoperability between cloud computing services, limited or conditioned access for business users to data, typing and bundling services and potentially imbalanced contractual terms. The European Commission will publish a final report within 18 months which may propose updating the DMA obligations in respect to cloud services.

Competition & Foreign Investment	
1	**Closer scrutiny of transactions:** both the EU DMA and UK DMCC Act impose enhanced transaction reporting obligations for designated companies to inform regulators of a wider range of transactions. Investments may also be caught by national foreign investment regimes. These factors coupled with the heightened interest in mergers in the digital sector by competition regulators worldwide mean that companies will need to carefully consider the potential impact on deal timelines. Regulators are continuing to make use of call-in powers for transactions falling below notification thresholds. Following the Illumina v Commission ruling, the European Commission can generally only review below-threshold transactions if the referring Member State would have jurisdiction to review the transaction in question (see our September 2024 update). Companies should also be mindful of the risk of regulators reaching different conclusions on remedies.
2	**Foreign investment:** in addition to merger control, investment in digital activities may be reviewed under national foreign investment regimes, with semiconductors, digital infrastructure and AI being areas of particular interest from a national security perspective. Several jurisdictions (including the EU and USA) are also contemplating restrictions on outbound investment, with the EU proposals focusing on investments in advanced semiconductors, AI, quantum technologies and biotechnologies. As of the date of publication, nearly all EU Member States have established active FDI regimes, with Croatia, Greece, Bulgaria, and Ireland, launching or significantly updating their regimes in 2025, and Cyprus set to implement its regime in April 2026.
3	**EU Technology Transfer Block Exemption (TTBER):** provides a safe harbour under EU competition law for technology licensing agreements that meet certain criteria. In September 2025, the European Commission published a draft of the new TTBER and new Technology Transfer Guidelines. The revised Regulation and guidelines provide more clarity on the application of the TTBER's market share thresholds for technology markets and extend by one year the grace period for which the block exemption continues to apply where the parties' market shares subsequently rise above the TTBER market share thresholds. The draft guidelines also provide more clarity on the treatment of technology pools, as well as new guidance on licensing negotiation groups and data licensing. The consultation closed in late October 2025. The current TTBER is due to expire on 30 April 2026. The UK block exemption is also due to expire on 30 April 2026 and the UK Government consulted on a draft regulation in January 2026.

Key cases to watch

- **European Commission investigation into use of online content for AI purposes**
  In December 2025, the European Commission opened an investigation under Article 102 of the Treaty on the Functioning of the European Union to assess whether Google has breached EU competition law by using web publishers' content (and content uploaded to YouTube) for AI purposes. The investigation will consider whether Google has distorted competition by imposing unfair terms and conditions on publishers and content creators, or by granting itself privileged access to this content, and has therefore disadvantaged developers of competing AI models.

- **European Commission investigation into AI providers' access to WhatsApp**
  In December 2025, the European Commission opened an investigation to consider whether Meta's new policy on AI providers' access to WhatsApp may infringe competition law. In October 2025, Meta announced a new policy which prohibits AI providers from using a tool which allows businesses to communicate with customers via WhatsApp when AI is the primary service offered. AI tools can still be used for ancillary or support functions. The European Commission is considering whether this policy may prevent third party AI providers from offering their services through WhatsApp while Meta's own AI service will still be accessible to users on WhatsApp. In March 2026, Meta suspended the policy change for 12 months and introduced a fee for AI agents wanting to use the platform. The European Commission is now considering whether this change impacts the need for it to act urgently.

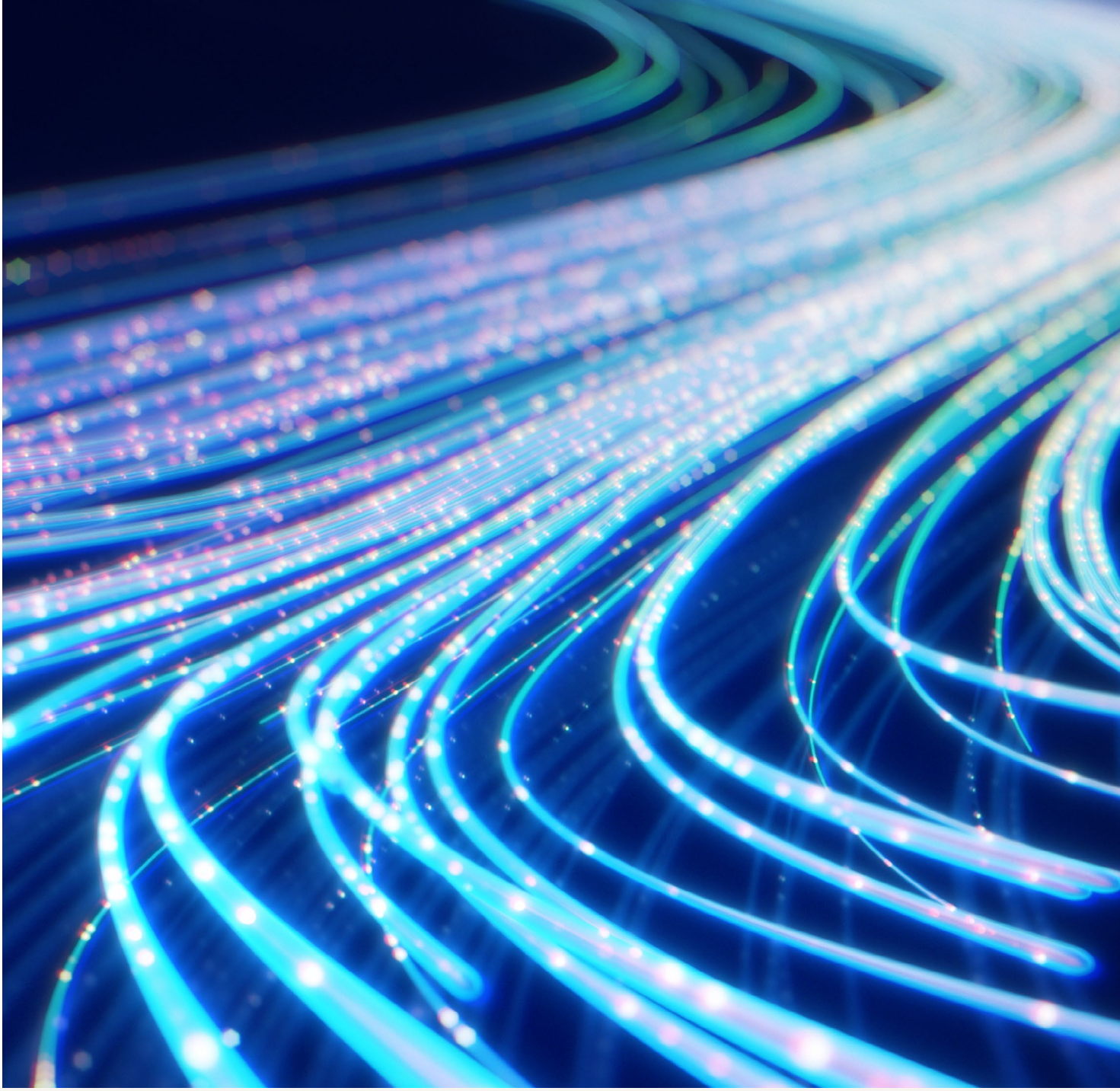
- **Google Adtech decision**
  In September 2025, the European Commission found that Google had abused its dominant position in the display advertising technology (Adtech) industry and fined Google €2.95 billion. The European Commission concluded that Google abused is dominant position on both sides of the Adtech supply chain *"by favouring its own online display advertising technology services to the detriment of its competitors, online advertisers and publishers"*. The European Commission found that advertisers *"faced higher marketing costs which they likely passed on to consumers in the form of higher prices for products and services"* and Google's conduct also reduced revenues for publishers which may have led to lower service quality and higher subscription costs of consumers.

Competition Litigation	
1	**Litigation funding reform in the UK:** on 17 December 2025, the UK Government confirmed its acceptance of the Civil Justice Council's two primary recommendations. The Government will introduce legislation to clarify that funding agreements are not damages based agreements (**DBAs**) and therefore do not need to comply with the 2013 DBA regulations (reversing the Supreme Court's PACCAR ruling with prospective effect) and provide for *"proportionate regulation"* of funding agreements *"when parliamentary time allows"*. The UK and EU approaches are diverging, with the European Commission confirming in late November 2025 that it will not progress the regulation of third-party funding in the EU.
2	**Efficiency drive at the CAT:** with the appointment of Mrs Justice Bacon as the new President of the CAT, 2025 marked the start of reforming certain CAT procedures in the interests of efficiency. By way of example, the CAT published a new Practice Direction in December 2025 setting out fresh expectations in relation to expert evidence (see our December 2025 update). The new principles include an emphasis on the early identification of experts to avoid duplication, the independence of experts and the expectation of *"plain-English"* expert reports that can be understood by non-experts. There is a page limit on expert reports as per a practice direction handed down in November 2025.
3	**Closer scrutiny at certification stage in the CAT:** the coming year is likely to be marked by tighter gatekeeping for collective proceedings claims at the pre-certification stage, following some high-profile refusals to certify collective proceedings *(Riefa vs Apple)* and substantive dismissals *(Le Patourel v BT)*. In addition, following the Supreme Court decision in the FX collective action *(Evans)*, the merits of a claim may now play a more determinative role in deciding whether a claim can proceed on an opt-out basis.
4	**Claims under the DMCC Act:** in 2026, there is the potential for the first claims and/or appeals to arise under the DMCC Act. The Act grants the CAT new powers to award exemplary damages and declaratory relief in private competition law claims (though exemplary damages remain unavailable in collective proceedings).
5	**Call for evidence on UK opt-out collective action regime:** marking a decade since the opt-out collective action regime was introduced by the Consumer Rights Act 2015, the Department for Business and Trade launched a consultation in August 2025 to review the operation and impact of the regime. This sets out 31 questions covering, among other things, litigation funding, certification, distribution of damages and alternative means of resolving disputes. The outcome is expected in 2026.

Key cases to watch

- **Umbrella Interchange Fee litigation**
  A decision by the Court of Appeal on whether to grant permission to appeal, following a hearing in March 2026, is anticipated shortly in the Umbrella Interchange Fee proceedings. The application relates to the CAT's Trial 1 judgment on infringement, which found that liability could arise even where interchange fees were set within the levels permitted under the Interchange Fee Regulation. Mastercard has also indicated that it intends to seek permission to appeal the CAT's Trial 2 judgment on pass-on, which was handed down by the CAT in February 2026. Trial 3, which will consider the question of exemptibility, is currently listed for hearing in October 2027.

- **Appeal in Kent v Apple**
  In October 2025, the CAT ruled that Apple abused its dominant position by *"imposing exclusionary practices"* and charging *"excessive and unfair"* fees on purchases of apps, app subscriptions and in-app purchases made by UK iPhone and iPad users. As a result, £1.5 billion in compensation will be handed out to nearly 36 million UK consumers and businesses. Apple appealed the judgment, but this was rejected by the CAT. Apple has now applied for permission to appeal at the Court of Appeal.



- **Coll, Rodger and Epic proceedings against Google**
  The CAT has ordered that the three separate proceedings in Coll, Rodger and Epic should be consolidated in the interests of efficiency and to avoid inconsistent outcomes. Trial is expected to commence in October 2026. Each action challenges Google's app distribution and in-app payment practices, raising overlapping factual and economic issues. Ms Coll seeks damages for UK consumers, Professor Rodger for UK app developers, and Epic was seeking injunctive relief but reached a settlement in March 2026.

- **Alex Neill Class Representative Limited v Sony**
  A ten-week trial started on 2 March 2026 in the claim filed by Alex Neill against Sony, seeking compensation on behalf of 8.9 million UK users of PlayStation. This is a standalone claim, which has been certified by the CAT on an opt-out basis.

Key Contacts

Antitrust, Regulatory & Trade

Nigel Parr
Partner
T +44 20 7859 1763
nigel.parr@
ashurst.com

Rafael Baena
Partner
T +34 91 364 9895
rafael.baena@
ashurst.com

Anna Morfey
Partner
T +44 20 7859 3006
anna.morfey@
ashurst.com

Gabriele Accardo
Partner
T +39 02 85423430
gabriele.accardo@
ashurst.com

Christopher Eberhardt
Partner
T +44 20 7859 3269
christopher.eberhardt@
ashurst.com

Fiona Garside
Expertise Counsel
T +44 20 7859 2712
fiona.garside@
ashurst.com

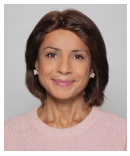
Digital Economy Transactions

Amanda Ludlow
Partner
T +44 20 7859 1294
amanda.ludlow@
ashurst.com

Nicolas Quoy
Partner
T +33 (1) 53 53 54 33
nicolas.quoy@
ashurst.com

Alexander Duisberg
Partner
T +49 89 24 44 21 149
alexander.duisberg@
ashurst.com

Rhiannon Webster
Partner
T +44 20 7859 3070
rhiannon.webster@
ashurst.com



Fiona Ghosh
Partner
T +44 20 7859 1520
fiona.ghosh@
ashurst.com

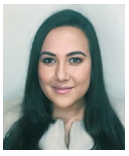
Patricia Wade
Expertise Counsel
T +44 20 7859 1031
patricia.wade@
ashurst.com

Dispute Resolution

Tim West
Partner
T +44 20 7859 2858
tim.west@
ashurst.com

Martin Eimer
Partner
T +49 69 97 11 26 00
martin.eimer@
ashurst.com

Jon Gale
Partner
T +44 20 7859 1630
jon.gale@
ashurst.com



Sarah-Jane Dobson
Partner
T +44 20 7859 1519
sarah-jane.dobson@
ashurst.com

Max Strasberg
Senior Associate
T +44 20 7859 3967
max.strasberg@
ashurst.com

India Case
Senior Associate
T +44 20 7859 3161
india.case@
ashurst.com

Ashurst

ashurst.com

Design Ref: R016793 Mar 26