Regulatory Outlook: Summer calls to action

Osborne Clarke

Advertising and marketing

The UK Tobacco and Vapes Act 2026, having received Royal Assent in April, prompted the government to launch a consultation on proposals to regulate packaging, device appearance and the display of vapes, nicotine and tobacco products by retailers. It closes on 2 October 2026. Of particular interest to businesses marketing and advertising automated vehicles (AVs) will be the new restrictions taking effect on 7 January 2027 that will prohibit the use of AV terminology in marketing unless the vehicle in question is an authorised automated vehicle (as defined in the Automated Vehicles Act 2024). On the regulatory front, the UK Advertising Standards Authority (ASA) continues to take a proactive approach to regulation, deploying its AI-based Active Ad Monitoring System to scan online advertising for non-compliant ads. Its recent review of environmental claims at scale and ongoing monitoring of gambling ads offer some examples of its approach, but businesses can expect the ASA to widen its net to include other sectors as well.

Artificial Intelligence

The EU has now finalised its Digital Omnibus on AI, bringing targeted amendments to the EU AI Act. As a result, businesses have a revised implementation timetable. The most imminent deadline is 2 August 2026, when requirements for deployers of AI to label AI deepfakes come into effect. Hot on its heels is 2 December 2026, the deadline for complying with watermarking obligations under Article 50(2) for AI-generated content created by AI systems placed on the market or put into service before 2 August 2026, as well as a new ban on AI nudification apps.

In the UK, businesses eyeing the government's AI Growth Labs (regulatory sandboxes allowing businesses to test innovative AI products and other emerging technologies safely in a real-world setting through the temporary relaxation of existing rules) should watch out for the Regulating for Growth Bill announced in the King's Speech. It will create sandbox powers, expected in November.

Bribery, fraud and anti-money laundering

Section 250 of the Crime and Policing Act 2026, which extends the identification doctrine to all criminal offences committed by a senior manager acting within their actual or apparent authority, came into force on 29 June 2026. This represents a significant expansion of corporate criminal liability. Unlike the previous position under the Economic Crime and Corporate Transparency Act 2023, which was limited to specified economic crimes, firms can now be held liable for any crime committed by their "senior managers". Organisations should use the summer break to assess who their "senior managers" are across the business, update risk registers to cover all criminal offences (not just economic crime) and strengthen due diligence processes for senior management, including ongoing monitoring of individuals in senior roles to identify potential issues or risks early.

Competition

Both the European Commission and the Competition and Markets Authority (CMA) are currently reviewing aspects of their merger assessment guidelines. For its part, the Commission is conducting a comprehensive review of its merger guidelines with the aim of consolidating both its 2004 horizontal and 2008 non-horizontal guidelines. It expects to finalise its review process in Q4 2026 after a public consultation closed in June. Meanwhile, the CMA is reviewing its approach to "rivalry enhancing efficiencies" following updates to its wider jurisdiction and procedure guidance in 2025. A consultation on this closed on 1 July.

The changes being considered represent an increasing openness to examine potential efficiencies arising from a merger. Businesses active in M&A or considering exit strategies should be mindful of these potential changes, particularly in so far as they encourage putting forward the beneficial effects of a merger.

Consumer law

The CMA has made clear that it will not hesitate to use its new direct enforcement powers under the Digital Markets, Competition and Consumers Act 2024 (DMCCA) to tackle breaches of consumer law, with its focus spanning from drip pricing and automatic opt-in charges to simple failures to respond to statutory information notices. Notably, the

CMA's current approach appears to have shifted to imposing fines over accepting undertakings, suggesting a possible move to making decisions that will act as deterrents. Businesses with consumer-facing subscription models should prepare for the upcoming subscription contracts regime under the DMCCA. Although the regime is not expected to take effect until spring 2027, the CMA's stance on enforcement sends a clear message that businesses should get ahead on compliance so that they are ready when the new rules come into force.

Cyber security

The Cyber Security and Resilience Bill passed its third reading in the House of Commons on 16 June 2026 and has now proceeded to the House of Lords for further consideration. With Royal Assent expected before the end of 2026, businesses should not wait to begin preparing for the new framework. The bill represents a significant overhaul of the NIS Regulations, expanding the scope of regulated organisations by bringing managed service providers, data centre operators, large load controllers and designated critical suppliers within scope, with tightened incident reporting requirements and higher maximum penalties for infringements. Organisations that are likely to fall within scope, as well as those that supply goods or services to in-scope entities, should begin preparing for these changes by conducting a gap analysis against existing tools and resources such as the National Cyber Security Centre's Cyber Assessment Framework.

Data law

The UK government is gathering evidence on various topics relating to data policy, covering smart data schemes, data regulation and AI, and international data flows, meaning that further data regulation reform might be in the pipeline.

In the meantime, the UK Information Commissioner's Office (ICO) is consulting on its draft corporate strategy, designed to "provide a bridge" from the ICO to its future Information Commission governance model. The transition is anticipated to take place in the autumn. Central to the draft strategy is its impact-driven regulatory approach, meaning that the ICO intends to focus its efforts directly on areas of highest risk and systemic importance, while investing proportionately less resource in routine or lower-risk work. The ICO's four regulatory priorities are: protecting children, promoting trust and transparency in AI, public services' use of personal data and building cyber resilience.

Having already published a raft of guidance reflecting the changes introduced by the Data (Use and Access) Act 2025, the ICO has further guidance in the pipeline, for example an update to controllers and processors detailed guidance. The regulator is also starting work on a new statutory code of practice on AI and automated decision-making, promising more detail on timings "in due course".

Digital regulation

The protection of children online continues to dominate the agenda. A social media ban for under 16s and measures aimed at protecting 16 and 17-year olds, including restrictions on infinite scrolling and AI chatbots, as well as overnight curfews, all featured in the UK government's announcements that followed the conclusion of its "Growing up in the online world" consultation.

The EU is also considering introducing its own child safety measures, with a proposal expected after the summer, once the European Commission has reviewed the recommendations of its expert panel on child safety. Among those recommendations is a harmonised, EU-wide ban on social media and other digital services for children under 13, unless supervised by parents. The UK and the EU are both focused not just on social media platforms, but on all digital services that are potentially harmful to children.

In the UK, the amendments made to the Online Safety Act 2023 (OSA) by the Crime and Policing Act 2026 are gradually coming into effect through secondary legislation and amendments to Ofcom's Codes of Practice. In the autumn, Ofcom is also expected to publish its statement on additional safety measures to strengthen its codes, on which it consulted at the end of last year. In addition, Ofcom has commenced the third phase of its implementation of the OSA relating to categorised services, with the regime expected to start coming into effect in the autumn.

On the media front, Ofcom is progressing in its implementation of the UK Media Act 2024. It is currently consulting on its draft Tier 1 standards code for video-on-demand services and its code on accessibility requirements for Tier 1 services. The new listed events regime will come into effect on 1 January 2027, while Ofcom's statement and final code of practice on prominence and accessibility on connected TV platforms is expected over the summer. Meanwhile, the UK government has published a green paper, "Watch this space", which is open for consultation until 31 August 2026, setting out what it calls a "new strategic direction for the government's media policy".

Employment, contingent workforce and immigration

The next wave of Employment Rights Act 2025 reforms comes into force in October 2026 and January 2027. These cover strengthened sexual harassment obligations requiring employers to take all reasonable steps to prevent harassment including by third parties; new trade union access rights including a duty to inform workers of their right to join a trade union; extended employment tribunal time limits; and restrictions on contractual variations (fire and rehire) from January 2027, with several reforms still awaiting the outcome of consultations. Businesses should be using the summer to audit and update employment contracts, policies and manager training programmes and to track the outstanding consultations that will finalise the remaining detail.

From 1 October 2026, the right to work regime will expand significantly beyond traditional employment. Under the Border Security, Asylum and Immigration Act 2025, businesses that engage workers under workers' contracts, individual sub-contractors supplied through intermediaries, or workers sourced via online matching service platforms will, for the first time, fall within the scope of the right to work scheme. Businesses should act now to:

- Map their supply chains. Identify who holds the direct contractual relationship with each worker and where extended liability exposure may arise.
- Audit existing contracts. No standard-form supply chain contract currently contains all five terms required to establish a statutory defence; contracts at every tier must be updated before 1 October 2026.
- Implement identity verification. This is an entirely new requirement; technology solutions must be procured and operational in time.
- Review onboarding processes. Right to work check procedures must be assessed against the requirements of the draft Code of Practice.

Environment

The Energy Savings Opportunity Scheme (ESOS) has been subject to a number of amendments, effective from 22 July, following introduction of the Energy Savings Opportunity Scheme (Amendment) Regulations 2026 (SI 2026/701). Companies that are obliged under ESOS should ensure that they are prepared to comply with the more stringent obligations. Companies previously using Display Energy Certificates or Green Deal Assessments for their ESOS compliance should plan to replace these compliance routes, while those businesses that are ISO 50001 Certified will now be excluded from ESOS compliance obligations. Companies should also be aware of the fuller reporting requirements on energy saving measures within the submission of ESOS reports; including a third progress update within the last year of the compliance phase, a review of the current action plan, and more information required about assessors (including a notification and submission of their contact details to the relevant professional body).

ESG

The EU Deforestation Regulation applies to large and medium companies from 30 December 2026, covering cattle, wood, cocoa, soy, palm oil, coffee and rubber and their downstream products, and businesses with exposure to these commodities should be finalising their traceability systems and supplier due diligence programmes, drawing on the Commission's updated guidance published in May 2026 ahead of the regulation coming into application.

Changes are on the horizon with the Commission proposing amendments to the product scope for certain downstream derived products, so businesses should check whether their specific products are affected, and with the UK government having signalled a consultation on a GB deforestation regime later this year, how closely the two regimes will align remains to be seen.

Fintech, digital assets, payments and consumer credit

The government has introduced final rules for the UK's new cryptoasset regulatory regime. The regulations amend existing legislation to bring activities relating to in-scope cryptoassets fully within the regulatory perimeter, effective from 25 October 2027. Many cryptoasset firms will need to seek authorisation by the UK Financial Conduct Authority (FCA) for the first time, or risk committing a criminal offence.

For firms requiring authorisation to undertake the new cryptoasset regulated activities, the application period will be open from 30 September 2026 to 28 February 2027. Where a firm applies during this window, the FCA expects to determine its application before the new regime commences, so it will be important to engage with the application process early to help avoid delays.

Firms already registered with the FCA under the Money Laundering Regulations 2017 will need to go through the process to become authorised, as there will be no automatic conversion of money laundering registration to full authorisation.

The FCA has released an overview of its cryptoasset regime policy publications, which also sets out next steps for firms.

Food law

The UK-EU summit at which the agrifood SPS agreement was due to be finalised was postponed following Keir Starmer's resignation. A rescheduled summit is now expected in the autumn. Defra has published guidance to support businesses in preparing for the agreement by the anticipated mid-2027 implementation timetable. It covers sector-specific areas including food production, plants and animals, pesticides and biocides, food manufacturing, processing and standards, food hygiene, food safety and labelling. The guidance will be updated once the final details of the agreement are confirmed, but agrifood businesses should engage with it now and begin mapping which product lines, supplier relationships and compliance processes will need to change when the agreement, which will require dynamic alignment with EU rules, comes into force.

Health and safety

The Terrorism (Protection of Premises) Act 2025, known as Martyn's Law, is expected to come into full effect in spring 2027. The Home Office's statutory guidance has been published and the SIA has consulted on its draft enforcement guidance, with the final version expected this autumn. Businesses responsible for publicly accessible premises or events should be confirming whether they are in scope of the standard or enhanced requirements of the Act and reviewing the Home Office's guidance alongside the newly published regulations on notification requirements this summer to ensure sufficient time to implement any required measures ahead of commencement.

Modern slavery

Any company doing business in the EU needs to be aware of the Forced Labour Regulation, which comes into full effect from 14 December 2027. Although this is still over a year away, the far-reaching work that may be required to achieve compliance means businesses should be reviewing the European Commission's newly released guidelines now to consider what steps are necessary and ensure minimum disruption to their trade.

Meanwhile, in the UK, the Immigration and Asylum Bill has been introduced to Parliament, and includes proposed changes to the reporting regime under section 54 of the Modern Slavery Act 2015. The bill's principal proposals cover mandatory prescribed content for modern slavery statements, the extension of reporting obligations to public bodies and a financial penalty regime for non-compliance of up to the greater of £1 million or 1% of total turnover.

Products

Since 19 July 2026, the EU's Ecodesign for Sustainable Products Regulation prohibits large companies from destroying unsold clothing and footwear, with limited exceptions, and requires supporting documentation to be retained for five years and made available to authorities on request. Businesses should check whether their inventory management practices comply with the new rules, and should also turn their attention to the EU Packaging and Packaging Waste Regulation's ban on perfluoroalkyl and polyfluoroalkyl substances (PFAS) in food-contact packaging, alongside requirements for manufacturers to produce declarations of conformity and new labelling requirements, which follows on 12 August 2026 and is now fast approaching.

The EU Cyber Resilience Act's vulnerability and incident reporting obligations apply from 11 September 2026, ahead of the full Act coming into force on 11 December 2027. Manufacturers, importers and distributors of products with digital elements sold into the EU, or into Northern Ireland, should be actively progressing their CRA compliance programmes, particularly around vulnerability reporting systems and conformity assessment readiness for the 2027 application date.

Regulated procurement

It has been over a year since the Procurement Act 2023 came into force and suppliers should be using the summer to check compliance in some of the areas where difficulties are most commonly arising in practice. Suppliers should ensure that all information provided on the Central Digital Platform is accurate and complete, as failing to declare a relevant exclusion ground is itself an exclusion ground. The poor performance ground under the Act is broader than its predecessor and can be triggered without any formal breach of contract, where a supplier has simply failed to improve after being given a proper opportunity to do so.

Sanctions

The Sanctions (EU Exit) (Miscellaneous Amendments) Regulations 2026 came into force on 13 May 2026, amending the UK sanctions framework. A key development for exporters is the introduction of new sanctions end-use controls, which create a new licensing requirement for certain exports where the UK government determines there is a risk of sanctions circumvention. Businesses that export goods which could potentially be diverted, particularly those with

exposure to Russia-adjacent supply chains, should familiarise themselves with the official guidance, review internal due diligence procedures and ensure that processes are in place to submit a licence application to the Office of Trade Sanctions Implementation promptly if required, minimising potential delays and seeking legal advice where necessary.

Telecoms

The revised Telecommunications Security Code of Practice was issued on 14 July 2026 and expands guidance across a range of compliance areas including supply chain accountability, cloud providers, privileged access workstations, and security testing.

Practical steps that providers can take now:

- Confirm your tier classification and align your compliance plan, resourcing and timelines accordingly.
- Run a gap assessment against the revised code taking account of the new M22/M23/M24 measures (which have deadlines from March 2028 to December 2029) and expanded PAW expectations (which inherit the existing 31 March 2027 deadline).
- Review and remediate supply-chain controls and contracts, tightening security obligations, audit rights and oversight with a particular focus on managed services and cloud. Keep in mind the deadline of 31 March 2027 for all existing contracts to meet the relevant requirements.
- Validate board-level accountability in practice and ensure the designated person/committee has demonstrable security competence, not just a formal appointment.
- Update operational security runbooks, including restart/patching approach (including risk-based restart rationale) and incident response (socialise, rehearse, and test regularly).

For more detail, please see our June Regulatory Outlook.