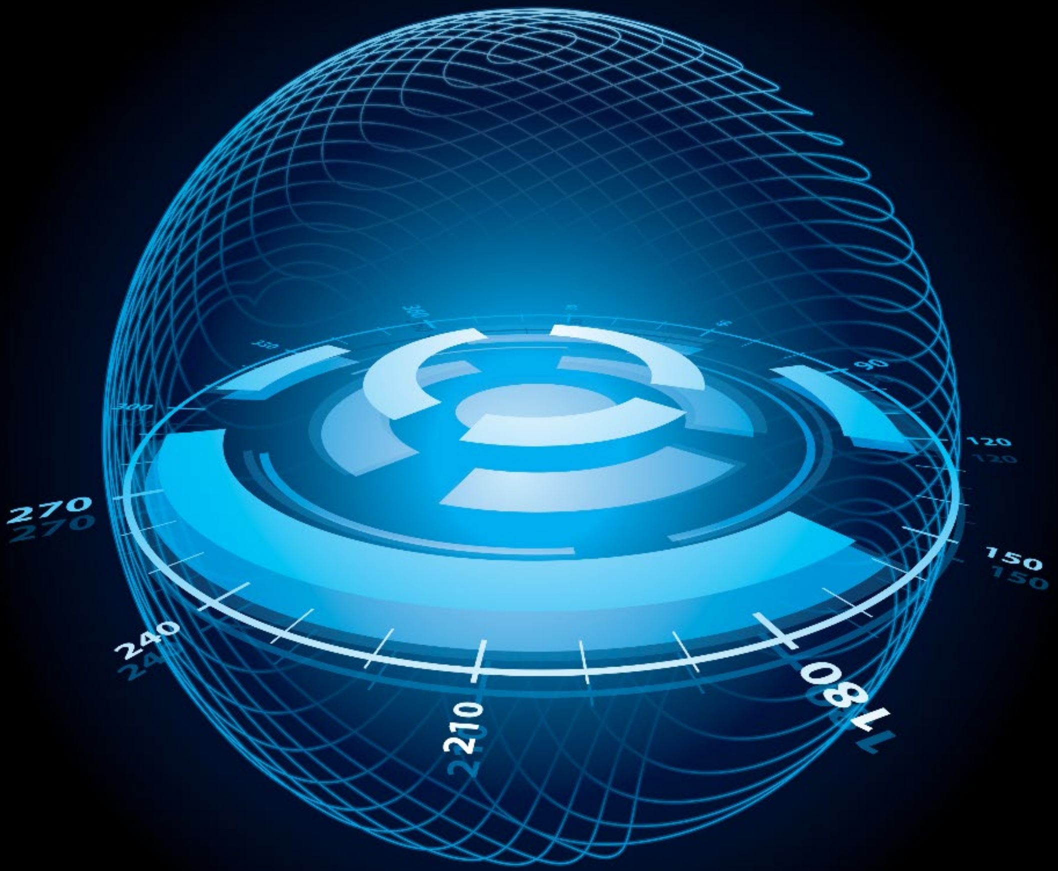
Deloitte.

CENTRE *for*
REGULATORY
STRATEGY
EMEA



Digital Regulatory Outlook 2026

Balancing competitiveness, safety and sovereignty in a dynamic digital era

January 2026

Contents

Global Introduction

Trends relevant to information integrity, competitiveness, trade and sovereignty demand an agile response

PAGE 3

Navigating the Outlook

Relevance to different companies across the digital ecosystem and in-scope policy & regulation

PAGE 8

1. Online Safety Regulatory Priorities

Protection of minors, fraud, disinformation and Trust & Safety implications

PAGE 10

2. Online Safety Supervisory Trends

Transparency, civil society, risk assessments and regime funding

PAGE 16

3. Media

A pivotal year for regulation of the sector

PAGE 20

4. Consumer Fairness

The rubber hits the road in the UK

PAGE 24

5. Competition

A fluid EU environment, with the first UK requirements expected

PAGE 29

6. AI

Focus on the known knowns whilst preparing for further change

PAGE 34

7. Cloud and the Data Economy

Unlocking competition and innovation, with AI as a golden thread

PAGE 39

8. Digital Networks and Sovereignty

Business roadmap required

PAGE 44

Global Introduction

> Trends relevant to information integrity, competitiveness, trade and sovereignty demand an agile response from companies across the digital ecosystem

Digital technology is fundamental to how we live, work, communicate, educate and entertain in the modern world. In 2026, we expect the fundamental question of "*what sort of digital environment do we want*" to be more prevalent in the global political and regulatory debate than ever, characterised by the following considerations:

- What sort of digital environment do we want for our **children**?
- What sort of digital environment is consistent with our broader **societal values**?
- What sort of digital environment will strengthen **competitiveness** and **create growth**?
- What sort of digital environment is **sovereign** and **secure**?

Clearly, how the appropriate authorities in different regulatory jurisdictions respond to these considerations will be informed by distinct legal, cultural, political and economic factors. This will all have an important bearing on how the current wave of digital regulation is either enforced, or evolves, during the next twelve months.

2025 already saw important regulatory developments (such as age assurance) and market developments (such as the increased use of AI chatbots). What is not in doubt is that things will not stand still. Companies that are agile and respond quickly, effectively navigating the evolving political and regulatory environment, will be well placed to stay ahead of the curve – effectively managing risks and converting opportunities.

Setting the geopolitical scene

The Digital Regulatory Outlook 2026 examines the strategic implications of regulatory developments in the **UK** and **EU** which will affect providers of both end-user services (e.g. social media) and enabling technology and services (e.g. cloud). Please see the '*Navigating the Outlook*' section for a breakdown of the affected industry sectors and the chapters that are of particular relevance to different companies across the digital ecosystem.

In an increasingly politicised regulatory environment, there are a number of geopolitical trends which we expect will have an impact on the direction of regulatory travel in the year ahead. We elaborate on these trends (relevant to information integrity, competitiveness, trade and sovereignty), along with how they are reflected in the content of our 2026 Outlook, in *Figure 1*.

Figure 1 – Geopolitical trends affecting digital regulation during 2026

TREND	DESCRIPTION
Information integrity	Responding to disinformation and misinformation concerns, as well as the debate around the dividing line between content moderation, age assurance and freedom of speech, makes information integrity a key factor influencing the regulatory environment. This is of particular relevance to online safety, which we cover in *Chapters 1 & 2*, as well as media, which we cover in *Chapter 3*.
Competitiveness	Leveraging AI, Cloud and Data is central to government competitiveness and growth agendas across the globe. The impact that regulation may have on that agenda is therefore a key question for companies to respond to. This applies both in terms of the introduction of new regulation designed, at least partially, with competitiveness and economic growth in mind (such as conditions for digital network deployment, something that we cover in *Chapter 8*), as well as the streamlining or simplification of regulation (as exemplified by recent proposals set out in the **EU Digital Omnibus**, something that we cover in *Chapters 6 & 7*).
Trade	The interdependency between trade and digital regulation is not new, given, for example, the inclusion of data flow provisions in trade deals. In addition, we have seen continued activity in relation to stand-alone **Digital Trade Agreements**. However, what has been apparent in the last twelve months is how the digital regulatory agenda (for example relevant to the online safety and competition developments that we cover in *Chapters 1, 2 & 5*) has been a notable reference point in trade deal dialogues. This remains something for companies to be mindful of during 2026.
Sovereignty	Ongoing conflicts, combined with changes to the existing geopolitical order, mean that sovereignty is now ingrained in the digital regulatory landscape. This has a particular bearing on the deployment of the networks (in particular submarine, satellite and terrestrial) that are essential to the maintenance of the global digital environment (something that we cover in *Chapter 8*).

Evolution in the global digital regulatory agenda

Whilst this Outlook covers **UK** and **EU** regulatory developments during 2026, many of the regulatory topics high on the European regulatory agenda are also being considered by policymakers in different countries around the globe. To set the European regulatory developments in the appropriate global context, we provide a snapshot of certain related regulatory initiatives taking place internationally.

We do this by reference to three priority regulatory topics, namely AI, protection of minors and data.

AI

No topic currently combines all the geopolitical themes highlighted above more than AI. In very broad terms, in the year ahead we expect that there will be a continued emphasis on how AI policy can stimulate competitiveness, economic growth and innovation on the one hand (increasingly in a 'sovereign' manner), balanced by regulatory 'checks and balances' on its deployment and use on the other.

In the **US**, important developments are evolving at both the federal and state levels. Prioritised implementation of the **AI Action Plan** will continue, with the development of a potential sandbox regulation at federal level a notable development to look out for. At state level, certain lawmakers (for example California and Colorado) have already taken steps to address AI risks, including in areas like employment, privacy and consumer protection. Clearly, this activity also needs to be set in the context of the recent **Executive Order** relevant to the enforcement of these rules.

In the **UK**, the Government has proposed an **'AI Growth Lab'**, which would enable the deployment of AI-enabled products and services by modifying or disapplying specific regulatory requirements under close supervision, with the possibility of successful modifications being made permanent. 2026 will also see the UK DRCF's new **Thematic Innovation Hub** progress in earnest, with its initial focus on Agentic AI, building on experiences from its **AI & Digital Hub Pilot.**

AI is a central element of the **EU**'s competitiveness agenda, in the form of the **Apply AI strategy**. Continuing on the sandbox theme, the EU Digital Omnibus proposes to expand the AI Office's power to establish specific regulatory sandboxes. Despite Digital Omnibus proposals for certain delays to **AI Act** timelines (alongside a number of targeted changes), the Commission remains committed to the broad goal of regulating risks associated with AI, with key requirements still incoming.

Finally, in the Asia Pacific region, **South Korea's AI Framework Act** (at the time of writing, due to take effect in January 2026) includes more stringent obligations for 'high impact' AI. The **Japan AI Act** (passed in May 2025), while non-prescriptive, lays the foundation for introducing more prescriptive obligations in the future. In addition to the recently passed AI law in **Vietnam**, due to come into effect in March 2026, attention will also be on the draft AI law under consideration in **Thailand.**

Protection of minors

In 2026, following early moves in 2025, the global debate around an enforced minimum age for social media access is expected to gain momentum. This is particularly relevant to the debate around information integrity.

At the start of 2026, all eyes are on **Australia**, given the new law requiring social media companies to limit account creation to those aged 16 and over, which came into force in December 2025. This looks set to be an important early test of the adequacy of age assurance techniques in a large-scale, real-world setting. The question of age limits for social media is also a priority topic in the **EU** in 2026, further to its inclusion in President von der Leyen's annual 2025 **State of the Union** speech, and various Member States are expected to take forward proposals in this respect. It is also a live issue in the **UK**.

In the **US**, certain States have already introduced age limits for social media use, with different models in play (with one key area of differentiation being whether or not the responsibility lies at app store level). Further activity is expected during 2026, with the passage of the **App Store Accountability Act** being closely monitored at Federal level.

There are also expected to be other notable global developments on the topic in the year ahead. In **India**, for example, further implementation of the **Digital Personal Data Protection Act** is expected, given its requirement for parental consent for the processing of children's data. **Singapore** has recently introduced its new online safety rules, accompanied by the creation of a new Online Safety Commission responsible for enforcement. In **Brazil**, the **Digital Statute of the Child and Adolescent**, enacted in September 2025, establishes a range of new rules relevant to the protection of children and adolescents online, including a requirement for in-scope services to introduce effective age verification mechanisms, prohibiting self-declaration as an appropriate approach.

Attention will also be on initiatives such as the Global Online Safety Regulators Network **(GOSRN),** a global forum dedicated to supporting collaboration between online safety regulators. This includes European authorities such as those from the **UK**, **Ireland** and **France** and also the **South African** Film and Publication Board, the **Korean** Communications Standards Commission and the **Australian** eSafety Commissioner. In December 2024, GOSRN stated that "*Ultimately, the success of the Global Online Safety Regulators Network depends on our common commitment to develop regulatory coherence across jurisdictions and to promote compliance with rights-respecting online safety regulation.*" Such frameworks are also being complemented by further Memoranda of Understanding, such as the joint communication that the European Commission, Ofcom and the Australian eSafety Commissioner recently signed in which they agreed to work together to advance child safety on online platforms.

Data

Regulatory initiatives relevant to the Data Economy highlight trends relevant to growth, trade and sovereignty in somewhat equal measure.

The concept of Data Sovereignty is not a new one, to date typically associated with the geographic region where data is stored. It remains relevant in the context of the now broader digital sovereignty discussion, with the recent **EU Data Union Strategy** containing a specific pillar designed to safeguard the EU's data sovereignty through a strategic international data policy, which includes activity to link EU data-sharing ecosystems with those of like-minded third countries. It is also relevant in the context of the data that is used to train AI models. This is likely to be a feature of ongoing discussions on AI sovereignty in different global regions.

Data will also remain central to the growth agenda during 2026. In the **UK** for example, the new **Data (Use and Access) Act** seeks to capture the economic benefits of smart data, endeavouring to replicate the economic benefits of Open Banking. Last year, the UK Government stated that it would invest £36 million to support new Smart Data schemes, referring to *"the success of Open Banking, where 82 firms alone have raised over £2 billion in private funding since 2018"*. And in the **EU**, promoting innovation and economic growth is also a feature of new Data Union Strategy. The existing data sharing framework established under the **Data Act** is a key element of this, as well as proposed measures to simplify the regime as introduced via the Digital Omnibus.

Finally, data remains central to the global trade discussion. Incorporating data provisions into trade agreements is certainly not new, and it remains a central element of the current wave of digital trade agreements, with the **EU** finalising a 'first of its kind' digital trade agreement with **Singapore** and concluding negotiations for a similar pact with **Korea** during 2025, for example. The discussion on the **ASEAN Digital Economy Framework Agreement** (comprised of **Thailand**, **Indonesia**, **Malaysia**, the **Philippines**, **Singapore**, **Brunei**, **Laos**, **Vietnam**, **Myanmar** and **Cambodia**) also shows how other global regions are responding.

Ensuring a joined-up companywide response

In such a fluid environment, ensuring an effective response to regulatory developments will require input from numerous internal teams, including External Affairs, Compliance, Strategy, Commercial and Technology. It will therefore be more important than ever to effectively scan the regulatory horizon and ensure internal alignment so that companies can explore the cumulative strategic and operational impact and respond in a joined-up way.

Taking three short examples from the digital ecosystem:

- For a **social media company**, implementing effective age assurance processes is not solely a responsibility for Trust & Safety professionals. It requires a coordinated effort across the organisation, requiring input from business areas such as External Affairs, Legal, Technology & Engineering, Product and Marketing. This is especially important to ensure that required checks and balances are incorporated as part of a broader age-appropriate design.
- For a **telecoms company**, developments in sovereignty raise clear strategic implications. A company's response should map out risks and opportunities relevant to network and service deployment across its geographic footprint, for example in relation to cloud, satellite and submarine cable infrastructure. This should take into account political, regulatory and commercial considerations, prioritising where the greatest risks, dependencies – and also opportunities – arise.
- For a **Public Service Broadcaster**, discoverability and findability of trusted public service/general interest content in an era of disinformation also requires agility. This is relevant across broadcast TV, multiple third-party digital platforms, and across a variety of devices and environments where such content is now consumed, including connected TVs, smart devices and in-car infotainment systems.

We explore the regulatory implications of these trends, and much more, in this year's Digital Regulatory Outlook, highlighting the topics that we expect to shape the digital regulatory landscape in the **UK** and **EU** in the year ahead, and how companies can respond.

> *"The tide on online safety is beginning to turn for the better. This year has seen important changes for people, with new measures across many sites and apps now better protecting children from harmful content. But we need to see much more from tech companies next year and we'll use our full powers if they fall short"*
>
> **Oliver Griffiths, Ofcom's Online Safety Group Director, 4 December 2025**

> *"Transparent ad practices can build trust in the online environment. Transparency is essential in uncovering scams, ensuring the integrity of information and keeping young users and children safe from lurking harm. The message is clear: our aim is compliance. When platforms engage constructively with the Commission, we are ready to accept solid commitments."*
>
> **Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy, 5 December 2025**

Navigating the Digital Regulatory Outlook: company relevance

Application to different companies across the digital ecosystem

END-USER SERVICES

COMPANY CATEGORY	MOST RELEVANT CHAPTERS
Social Media and Interpersonal Communications	Online Safety Media Consumer Fairness AI
Dating	Online Safety Media Consumer Fairness AI
Gaming	Online Safety Media Consumer Fairness AI
Media and streaming	Online Safety Media Consumer Fairness
Transactional (e.g. online marketplaces, e-commerce websites, gig economy platforms)	Online Safety Consumer Fairness Competition
AI services (e.g. AI chatbots, agentic AI)	Online Safety AI Cloud and Data

ENABLING TECHNOLOGY AND SERVICES

COMPANY CATEGORY	MOST RELEVANT CHAPTERS
User interfaces (e.g. Operating Systems, App Stores, Internet browsers)	Media Consumer Fairness Competition AI
Devices (e.g. Smart TV, mobile, smartwatch)	Media Consumer Fairness Competition AI
Intermediary services (e.g. cloud, data storage, data centres, quantum)	Online Safety AI Cloud and Data
Compute (Cloud, data storage, data centres, quantum)	Cloud and Data Digital Networks and Sovereignty
Connectivity (e.g. fixed, mobile, internet routing, satellite)	AI Digital Networks and Sovereignty

N.B. One service may fall into multiple categories. For example, a video game may include social elements and transactions. Similarly, an AI chatbot may support productivity, provide information and offer access to media content.

Navigating the Digital Regulatory Outlook: in-scope policy & regulation

Key UK and EU regulatory and policy initiatives considered

	KEY INITIATIVES CONSIDERED*	
CHAPTER	**UNITED KINGDOM**	**EUROPEAN UNION**
1. Online Safety Regulatory Priorities	• Online Safety Act **(OSA)** • Ofcom-ICO joint statement on age assurance • UK Government Violence Against Women and Girls strategy	• Digital Services Act **(DSA)** • European Digital Identity Wallets • European Democracy Shield • Digital age of majority (potential proposal) • Payment Services Directive 3
2. Online Safety Supervisory Trends	• OSA categorised services regime and transparency reporting • OSA additional safety measures • Ofcom technology notices • Guidance on OSA super-complaints • OSA fees and penalties regime	• Harmonised DSA transparency reports • DSA vetted researcher access to data • DSA guidelines on trusted flaggers • Delegated act on user number calculation for the purposes of fees under the DSA
3. Media	• Media Act VOD Code • Media Act Code of Practice on prominence and accessibility on connected TV platforms • UK Government response to Ofcom's PSM review	• Audiovisual Media Services Directive review • New customisation right under the Media Freedom Act
4. Consumer Fairness	• Digital Markets, Competition and Consumers Act **(DMCCA)** • Secondary legislation for DMCCA subscription contract requirements • CMA strategy 2026 to 2029	• Digital Fitness Check (2024) • Digital Fairness Act proposal • EU Consumer Protection Network principles to promote transparency & fairness in video games
5. Competition	• Consultations on Conduct Requirements in search and mobile under the DMCCA • Potential further SMS designation investigations under the DMCCA • CMA revised merger remedies guidance	• Digital Markets Act **(DMA)** • DMA Review • Guidelines on DMA/GDPR interplay • Merger guidelines review
6. AI	• UK Government impact assessment and report on copyright • OSA • DMCCA	• AI Act • Digital Omnibus • DSA • DMA
7. Cloud and the Data Economy	• Data (Use and Access) Act **(DUAA)** • Secondary legislation for smart data schemes under DUAA • UK fuel finder scheme	• Data Act • Automotive data sharing guidance • Digital Omnibus • Cloud and AI Development Act
8. Digital Networks and Sovereignty	• DSIT has stated that is working to develop a comprehensive definition of digital sovereignty	• Digital Networks Act • Cloud Sovereignty Framework • Cloud & AI Development Act • Space Act

** The Digital Regulatory Outlook typically focuses on regulation which aims to benefit consumers, protect users or promote competition. This list is non-exhaustive. Details on the regulatory initiatives set out in this Outlook are up to date as of 16 January 2026.*

1. Online Safety Regulatory Priorities

Protection of minors, fraud, disinformation and Trust & Safety implications

EXECUTIVE SUMMARY

Online safety regulations, including the EU Digital Services Act ***(DSA)*** *and UK Online Safety Act* ***(OSA)*** *are now an established element of the European digital regulatory landscape. There is much for platforms to focus on, however we see priorities relevant to the protection of minors, prevention of fraud, and combatting of disinformation that should be particularly high on the agenda during 2026. In this context, Trust & Safety* ***(T&S)*** *functions are set to play a pivotal role in responding to the evolving regulatory landscape and complex risk environment.*

The past year has been characterised by significant regulatory activity in both the **UK** and **EU** relevant to the protection of users, in particular vulnerable users such as children, online. In both jurisdictions this activity has included enforcement activity, notably the first fine under the DSA, issued in late 2025.

We expect online safety to continue to be a central regulatory priority throughout 2026. Whilst there are many dimensions to this activity, we focus on three specific topics which we think should be high on platforms' agenda, namely the protection of minors, fraud and disinformation. We then consider how T&S functions can effectively respond.

Protection of minors

In the **UK**, Ofcom is expected to prioritise supervising platforms, monitoring their compliance with OSA duties by drawing on the relevant **Codes of Practice**, whilst in parallel strengthening child protection through additional safety measures (see *Chapter 2*). Relevant measures are likely to include expanding the use of Highly Effective Age Assurance **(HEAA)** to protect children from grooming, restricting user interactions on children's livestreams, and allowing users to appeal age assurance decisions. Additionally, companies should anticipate Ofcom's statutory reports on age assurance (expected by July 2026), and content harmful to children (expected by October 2026), which will no doubt provide further clarity on Ofcom's long-term approach and expectations.

In the **EU**, the protection of minors has been a key focus of several DSA investigations into platform compliance initiated by the European Commission, the first of which was opened in 2024. In 2026, the Commission will be expected to prioritise conclusion of these probes, as well as supervising

services' adherence to its **Guidelines on the Protection of Minors** under the DSA. Priority areas of focus are likely to include whether in-scope platforms have taken appropriate and proportionate steps to verify age, make improvements to content moderation, ensure safe interfaces and recommender systems, turn default settings to private and provide parental controls.

Beyond OSA and DSA-specific developments, in *Figure 2* we identify three specific areas affected services should have on their radar in relation to online child protection in both the **UK** and **EU**.

Figure 2 – priority child protection topics

Interaction between age assurance and data protection

European authorities, notably through European Data Protection Board **(EDPB)** and DSA Guidelines, underscore the importance of data protection in age assurance implementation. The **UK**'s Ofcom and Information Commissioner's Office **(ICO)** are set to issue a joint statement during 2026, expected to provide more clarity on the topic. Platforms should therefore prioritise 'least intrusive' methods and conduct Data Protection Impact Assessments **(DPIAs)** to demonstrate data minimisation. This may include leveraging double-blind methods, where user identity remains unknown to the platform and the service accessed is unknown to the verifier. This is something we wrote about in our age assurance report, which can be found here.

Alignment between age assurance and emerging digital ID frameworks

In the **EU**, the Commission is developing an **age verification app**, expected to set the compliance benchmark for how services should meet their child protection duties. The app is currently being piloted in six EU countries – Denmark, France, Greece, Italy, Spain and Cyprus – and will serve as an interim measure before the planned rollout of the European Digital Identity **(EUDI)** Wallet. EUDI Wallets are expected to become available in each Member State by the end of the year, enabling users to verify age without revealing any other personal data. In the **UK**, the Government has announced plans to roll-out a **digital ID** over the course of this Parliament. Whilst no longer expected to be mandatory to prove right to work, these IDs are expected to enable further use cases, including enabling users to verify their age online.

Introducing additional age limits

The Commission's assessment of whether, and if so how, to establish a minimum age for social media use (a '**digital age of majority'**) is ongoing and will draw on advice from a specially commissioned expert panel. So far, the Commission has indicated that the DSA would not be the legal basis underpinning this initiative. A likely scenario would see the **EU** coordinate the implementation of new rules, with Member States having flexibility to establish their own national age limits, which would clearly add to cross-border compliance complexity. In this context, a number of Member States are already taking action, with countries such as France working towards new rules. At the time of writing, a social media ban for under-16s is also the subject of significant debate in the **UK**.

Fraud

Policymakers are increasingly focusing on how online services can be misused to facilitate fraudulent activities, something which is exacerbated by the rising use of AI and deepfakes by criminals. 'Illegal content' fraud is central to both the OSA and DSA, meaning in-scope services must assess and mitigate associated risks.

In the **UK**, collaboration with the Financial Conduct Authority **(FCA)** has already informed measures set out in Ofcom's **Illegal Content Code of Practice**, finalised during 2025. This Code, among other things, recommends dedicated reporting channels for large services to enable trusted flaggers, such as the FCA and law enforcement agencies, to report fraud-related offences directly to the service. Beyond Ofcom-FCA collaboration, the DRCF has recently highlighted the cross-sectoral nature of fraud, with the intention of facilitating ongoing UK cross-regulatory dialogue into 2026.

Ofcom will consider how the largest platforms address fraudulent advertising as part of its incoming **categorised services regime** (see *Chapter 2*). Potential measures include the use of proactive technologies to identify fraudulent advertising, robust advertising onboarding and verification, user reporting mechanisms and appeals processes for takedown decisions. Ofcom is expected to set out more detail in a summer 2026 consultation, though the requirements themselves are not currently due to be in force until 2027.

In the **EU**, the DSA provides a mechanism for the designation of trusted flaggers**.** The Central Bank of Ireland has already been granted such status in Ireland for example, given its role in detecting, identifying and notifying financial scams and fraud. More broadly, the European Commission issued information requests in September 2025 to a number of large platforms and search engines requesting detail on how they identify and manage risks related to financial scams. This focused on areas including deceptive apps, fraudulent accommodation listings and malicious links to scam websites.

This issue is set to gain further prominence in 2026. The Commission has already stated that going forward it will pay particular attention to how regulated platforms verify the identities of business users and their advertising repositories, which can be used to detect fraudulent advertising and patterns in scam activity. Additionally, the European Board for Digital Services, composed of the Member States' Digital Services Coordinators **(DSCs)** and chaired by the European Commission, has launched a **joint initiative focused on financial scams** and fraud, including information sharing and coordination on enforcement strategies.

Ultimately, platforms in scope of online safety regulation face growing pressure to identify, prevent and remove fraudulent content. Firms should ensure robust reporting channels and deploy 'Know Your Business Customer' checks and other processes to identify and remove such content. Firms should also consider the feasibility of proactively identifying fraudulent content as part of their content moderation systems, given this is a likely focus for regulators.

> *"Ultimately, platforms in scope of online safety regulation face growing pressure to identify, prevent and remove fraudulent content."*

Beyond online safety regulation, **EU** lawmakers have reached a political agreement on their review of the payments regulatory framework, known as the Payment Services Directive 3 **(PSD3)** package, including introducing stricter protections for victims of impersonation fraud. Under the revised framework, platforms will be liable to compensate banks and payments firms who have reimbursed defrauded customers, if the platform was informed of the fraudulent content on their platform and failed to remove it. The final legal text, setting out how this will work in practice, will only emerge later this year. Nonetheless, this highlights the need for platforms to establish robust and timely procedures to review and remove fraudulent content.

Disinformation

Disinformation remains a critical focus in a fast-moving geopolitical environment. In the **EU**, the formalised DSA **Code of Conduct on Disinformation** now sets the benchmark for determining compliance regarding disinformation risks for signatories. Even Very Large Online Platforms **(VLOPs)** and Search Engines **(VLOSEs)** that are not signatories should consider adopting elements of this Code, as the Commission will increasingly view it as a baseline for compliance. For platforms allowing political advertising, introducing measures such as labelling will be crucial, particularly with the **Transparency and Targeting of Political Advertising regulation** now in force.

The **European Democracy Shield**, published late last year, is designed to complement the DSA by introducing measures to counter foreign interference, safeguard electoral integrity and bolster independent media. Planned measures include establishing a new independent **European Network of Fact-Checkers** and a **Centre for Democratic Resilience** to enhance coordination and information sharing, including with Member States. Digital firms, particularly signatories of the Code of Conduct on Disinformation, should anticipate increased Commission engagement and scrutiny. Areas of potential focus highlighted include strengthening recommender system transparency, demonetising disinformation and exploring new measures such as labelling AI-generated content and implementing voluntary user verification tools. Furthermore, the Commission plans to develop a DSA incidents and crisis protocol to improve coordination during crises. Whilst detail on the specifics will follow, it's worth noting that the legislation indicates that only "*extraordinary circumstances affecting public security or public health*" should trigger such protocols.

Unlike the DSA, the OSA does not impose specific duties related to disinformation, which has been a topic of significant public debate. That said, illegal content and children's protection duties may apply to some forms of disinformation, which Ofcom may consider as part of supervision and enforcement activity. In addition, Ofcom also has duties related to promoting media literacy, which can act as a mechanism to combat disinformation by enabling users to critically engage with online content. Whilst non-binding, services should watch out for Ofcom **recommendations on how online platforms should promote media literacy**, expected in spring 2026.

The evolving role of T&S

All of this activity has particular implications for T&S functions, a business function which is increasingly expanding to include compliance and legal functions, and not just content moderation or policy activities. Considered holistically, T&S can be more than a defensive function, delivering significant economic and social return on investment. To achieve this, T&S leaders should prioritise the following critical issues during the year ahead, set out in *Figure 3* below.

Figure 3 – priority issues for T&S teams in 2026

ISSUE	DESCRIPTION	IMPLICATION
AI Generated Harm	Generative AI is enabling an unprecedented proliferation of synthetic harms. Deepfakes, fabricated child sexual abuse material and AI-driven misinformation can spread at speed and scale, which risks compromising traditional detection methods and eroding public trust.	In 2026, a core challenge for platforms will involve building reliable content provenance and authentication systems, without undermining privacy or legitimate expression.
Youth safety and algorithmic exposure	The protection of minors is a key regulatory focus, with expectations likely to shift beyond content moderation towards the wider design of online services. Policymakers and parents alike will demand greater accountability for how recommendation systems shape children's experiences.	This may call for age-appropriate interfaces, transparent algorithms and meaningful user control.
Violence against women and girls (VAWG)	Women and girls are disproportionately/uniquely affected by a range of serious risks online, including intimate image abuse, misogynistic abuse and online stalking. Policymakers are increasingly prioritising this issue, with both Ofcom **guidance for companies** and a **UK Government VAWG strategy** published in late 2025, which explicitly recognises online harms as a root cause and driver of abuse. Additional safety measures proposed by Ofcom will also be relevant *(see Chapter 2)*. Ofcom is also expected to engage with companies to understand how they are using the guidance, ahead of an assessment report planned for May 2027.	Firms should carefully consider Ofcom's guidance and identify necessary action beyond existing Code requirements. Whilst voluntary, Ofcom has indicated it strongly encourages action and will follow up on how the guidance has been applied. Firms should also consider any potential implications arising from the VAWG strategy, for example the banning of 'nudification' tools.

ISSUE	DESCRIPTION	IMPLICATION
Maintaining privacy	As online safety regulation matures, so do the perceived tensions with privacy, meaning platforms will need to take measures to reassure users.	Services should prioritise transparent reporting and ensure user data remains secure whilst responding to data requests by regulators and researchers. Age verification and digital ID services will remain a hotly debated issue, meaning privacy-preserving technologies will be essential for building trust.
Safeguarding freedom of speech	Debate over the impact of safety measures on free speech will continue. In complying with regulation, platforms may face trade-offs: over-zealous action may risk suppressing lawful speech whilst under-compliance may risk enforcement action and reputational damage. Complicating this, expectations differ globally, meaning a measure deemed appropriate in one jurisdiction could be considered unacceptable from a free speech perspective in another.	Platforms will need to navigate this potential tension. This will involve tracking to enable identification of common regulatory approaches (where they exist) and tailoring approaches by jurisdiction where required.
Automation limits and moderation bottlenecks	Content moderation remains fundamentally a problem of scale. While platforms extensively rely on automated systems to manage billions of daily interactions, difficulties in discerning context and cross-cultural nuances remain.	The 'human-in-the-loop' remains indispensable, despite challenges associated with training, retention and protection from harm. Human oversight will be necessary to ensure accuracy and fair outcomes, whilst delegating low-risk, high-speed decisions to automated systems.
Rebuilding trust	Public trust in online platforms has been influenced by controversies over the years. Civil society organisations, academics and government agencies are continuously updating their research into harms-specific online safety issues, and there is a growing expectation of services to translate these insights into improved policies and safety outcomes for users.	T&S leaders should prioritise enhancing credibility and building trust through greater transparency and engagement, robust accountability and authentic user engagement. Ultimately, success will depend on the extent to which T&S functions can embed safety into organisational culture and product design.

2. Online Safety Supervisory Trends

Transparency, civil society, risk assessments and regime funding

EXECUTIVE SUMMARY

Finalisation of the UK regime will pave the way for Ofcom's use of new supervisory tools, in particular relevant to categorised services. In the meantime, we see four supervisory trends for all in-scope services to focus on. First, enhanced transparency reporting, with a new EU framework and the first UK reporting notices. Second, increased civil society activity, including by researchers and trusted flaggers. Third, improved risk assessments, with Ofcom already highlighting that 'higher standards' are required in 2026. Finally, UK firms face an April deadline to submit revenue calculations under the new fees and penalties framework, to cover the costs of Ofcom exercising its online safety functions.

Approaching finalisation of the UK Online Safety regime

A central element of the **OSA** set to progress during 2026 is the **categorised services regime.** This will ultimately impose additional duties on the largest in-scope services and is expected to become active in 2027 (with thresholds beginning at 3m **UK** users for services with a messaging functionality and 7m for other types of services). Beyond fraudulent advertising discussed in *Chapter 1*, categorised services will ultimately face a range of new obligations, depending on which category they are designated as, though new transparency obligations will apply to all (see the Transparency Reporting section).

Following a legal challenge in 2025, Ofcom has now committed to a '**representations process**' in early 2026. This will allow services meeting the categorised service threshold conditions to comment on designations, before a final register of firms who will be subject to additional obligations is published in the summer. It's worth noting that the register will be subject to change as user numbers evolve, meaning firms near the thresholds should monitor carefully.

Whilst a consultation, also expected in the summer, will provide more detail on Ofcom's plans, firms should begin to proactively consider their approach. This may require in-scope services to consider and prepare for:

- The deployment of **new features**, such as user identity verification and empowerment options, allowing users to tailor how much of certain types of content they see.
- The deployment of **new controls**, including to ensure that content and user restrictions (e.g. bans) are carried out in line with their terms of service.
- The implementation of **robust data collection processes**, given Ofcom may request evidence of these controls in future transparency notices.

Beyond categorised services, Ofcom will also further develop existing **Codes of Practice** with a statement expected by the autumn. This is expected to introduce new Code measures relevant to all in-scope services, with a particular focus on the use of proactive technologies for the early detection of prohibited content, alongside crisis response protocols, recommender system design, user sanctions and the protection of minors.

These developments raise two particular strategic implications for in-scope services:

- The **potential need for further investment** in areas such as advanced moderation, robust age assurance and comprehensive crisis protocols. Firms should ensure their safety controls and allocated resources are proportionate to their userbase and service-specific risks.
- As with new categorised services requirements, **keeping up-to-date evidence of controls** will be essential for demonstrating compliance. While Ofcom's Codes are non-binding, they act as a 'safe harbour' for compliance, meaning providers opting for alternative measures must document and justify how they meet relevant safety duties.

On a related point, Ofcom will also progress work on **Technology Notices**. Unlike Codes of Practices, these notices can impose new legal requirements on services, mandating specific, Ofcom-accredited technologies to combat specific issues like terrorism content. **Final advice on minimum standards and guidance** is expected by April 2026, followed by the establishment of an accreditation process. After that, Ofcom will need to follow a set process before imposing a Notice on a service, meaning they are unlikely to be imposed before late 2026, at the earliest.

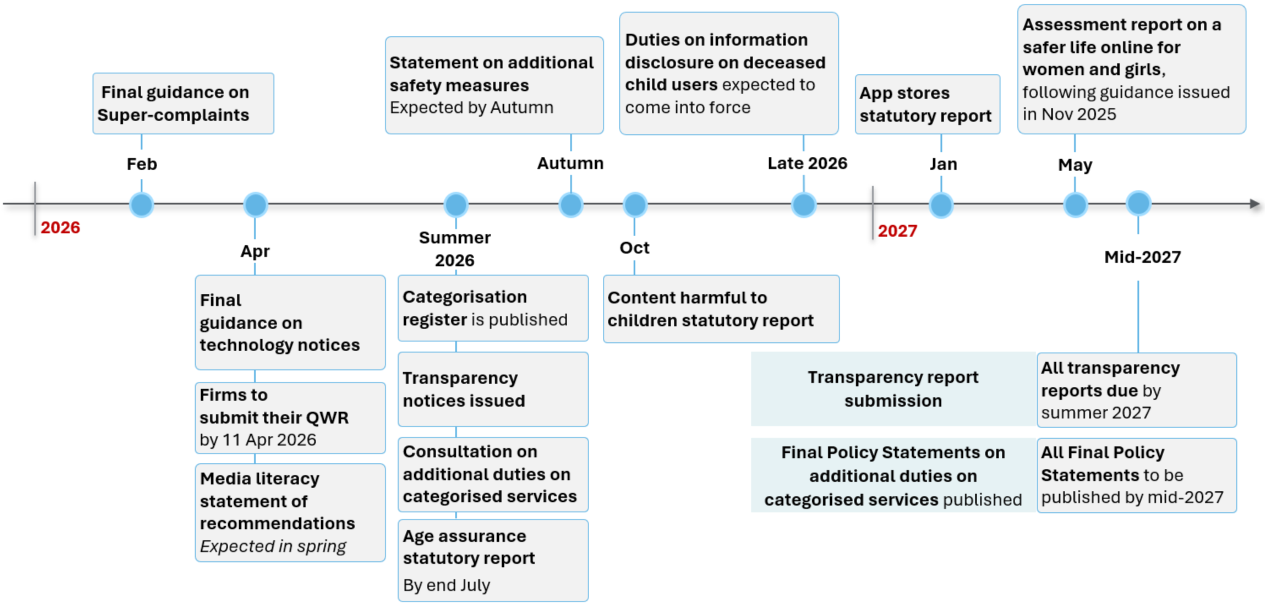
A timeline for these and other Ofcom activities discussed below is set out in *Figure 4*.

Transparency Reporting

Transparency reporting is a central feature of both the **DSA** and OSA supervisory regimes and will require particular attention in 2026.

Under the **EU's transparency framework**, all providers of intermediary services are required to report on their content moderation annually, with VLOPs and VLOSEs facing more onerous requirements and reporting twice annually. This reporting has now been harmonised for consistency, with the first VLOP and VLOSE reports under the new rules due in February 2026, covering the second half of 2025. Whilst new templates might reduce some of the burden, by limiting the need for descriptive sections of the report, the overall reporting requirement remains significant. Consequently, in-scope services should prioritise transforming the in-scope data into the required format, implementing robust processes to verify the data whilst documenting steps taken to ensure consistency in future reports. Firms should leverage lessons learned from this first set of reports to develop more efficient workflows, reducing long-term resource demands.

Figure 4 – Ofcom's timeline to finalise its online safety regime


2026
Feb
Final guidance on Super-complaints
Apr
Final guidance on technology notices
Firms to submit their QWR by 11 Apr 2026
Media literacy statement of recommendations Expected in spring
Summer 2026
Categorisation register is published
Transparency notices issued
Consultation on additional duties on categorised services
Age assurance statutory report By end July
Autumn
Statement on additional safety measures Expected by Autumn
Oct
Content harmful to children statutory report
Late 2026
Duties on information disclosure on deceased child users expected to come into force
2027
Jan
App stores statutory report
May
Assessment report on a safer life online for women and girls, following guidance issued in Nov 2025
Mid-2027
Transparency report submission
All transparency reports due by summer 2027
Final Policy Statements on additional duties on categorised services published
All Final Policy Statements to be published by mid-2027

In the **UK**, Ofcom's **transparency reporting regime** applies only to the largest services. These will be communicated through transparency notices expected to be issued to all categorised services in summer 2026, which will set out exact timings for report submission, with all reports expected by summer 2027.

Unlike the DSA's newly standardised approach, **UK** requirements will be communicated through bespoke transparency notices, considering the specifics of the platforms. For instance, a social media service popular with children may receive an information notice with more detailed questions on child safety measures, reflecting specific risks and user demographics. To provide year-to-year certainty and trend analysis, Ofcom will establish a set of 'core' information requirements that will be repeatedly requested, in addition to 'thematic' information requirements that change and are tailored to individual services. This may complicate the development of a consistent, repeatable process, requiring targeted projects to respond to new data requests, in parallel to set processes for the repeatable core requirements. This reinforces the need for effective data-gathering processes to enable an efficient response as non-standard information requests are received.

The Role of Civil Society

Alongside regulators, broader civil society organisations are expected to play an important role in the supervisory regime relevant to online safety, with **vetted researchers**, as well as **trusted flaggers**, an integral part of this.

Since October 2025, vetted researchers (a status granted by DSCs) can request non-public VLOP/VLOSE data for systemic risk research. As more researchers utilise this route, DSCs and the Commission will closely monitor compliance. Affected firms should ensure they have robust data access processes and governance, including clear procedures and responsibilities, to ensure adherence to the requirements. This will require data management and technological capabilities to extract, transform and deliver data in the requested format. Finally, it is crucial that firms keep records of steps taken to ensure auditability and transparency, alongside maintaining clear communication with researchers and DSCs via the new DSA **Data Access Portal.**

> *“Alongside regulators, broader civil society organisations are expected to play an important role in the supervisory regime relevant to online safety, with vetted researchers, as well as trusted flaggers, an integral part of this.”*

In a similar vein, we may also see early steps towards a **researcher access to data regime** in the **UK**. The decision now rests with the Government, following an Ofcom report on the topic. Whilst new rules in 2026 are unlikely, the Government response will determine whether firms should anticipate DSA-style researcher access requirements in the UK in the future.

Around 60 trusted flaggers have so far been appointed under the DSA, with DSCs playing a crucial role in awarding this status. Trusted flaggers are considered experts in detecting certain types of illegal content online. As a result, online platforms are expected to prioritise notices from trusted flaggers when they identify such content. Whilst the regime is already up and running, the Commission is developing guidelines designed to streamline the process of appointing trusted flaggers. If successful, we may see the list of trusted flaggers expand, meaning platforms should prepare for a greater volume of notices by ensuring they have the processes in place to appropriately prioritise these and respond. We may also see increasing coordination between trusted flaggers, with the planned **European Network of Fact-Checkers** discussed in *Chapter 1* being one to watch.

In the **UK**, Ofcom's **super-complaints regime** commenced on 1 January 2026, with final guidance providing further details expected in February. Like the DSA's trusted flagger system, it seeks to empower eligible expert bodies. However, in this case, these bodies will be able to formally raise issues with Ofcom regarding regulated online services that pose significant harm. This mechanism can trigger enforcement action, policy work on new Code measures, or even Government referrals if beyond Ofcom's remit. Platforms will need to ensure governance processes are in place to effectively respond to issues raised.

Risk Assessments

The completion of fit-for-purpose **risk assessments** will continue to be an area of regulatory scrutiny. In developing their approach, firms should carefully consider the findings of regulatory reviews to date. For example, Ofcom has signalled it expects 'higher standards' for 2026, highlighting the importance of separately assessing the risk of all relevant types of illegal and harmful content, providing robust, evidence-based justification for risk levels, documenting and monitoring controls to demonstrate their effectiveness in mitigating risk, and implementing appropriate governance and accountability over risk assessments.

Regime funding

Whilst the DSA framework is mostly established, one area of focus will be **regime funding**, whereby regulated firms bear the costs of regulation. Following a legal challenge, the Commission was required to revisit how user numbers are calculated for the purposes of fees via a delegated act. The Commission has previously stated that the ruling addresses a largely procedural issue rather than issues relating to fee methodology or charges. The Commission has since appealed this decision, meaning firms should monitor for the ultimate outcome.

In the **UK**, the OSA fees regime came into force at the end of 2025, with firms now required to take immediate action. In-scope services are required to calculate their Qualifying Worldwide Revenue **(QWR)** and notify Ofcom if this exceeds £250m, which will determine both fees and maximum fines (10% of QWR, if over £18m). This calculation is more complex than the DSA equivalent, involving identifying the proportion of revenue associated with relevant parts of regulated services, something we have discussed in more detail here. Firms must submit their QWR, with supporting evidence, via a planned fees portal by 11 April 2026. On top of this, the OSA includes provisions to recover pre-regime setup costs. Firms above the fees threshold will be required to cover these costs, spread over a three-to-five-year period, with further detail expected in a forthcoming Government consultation.

3. Media

A pivotal year for regulation of the sector

EXECUTIVE SUMMARY

We've written before about the convergence between the new wave of digital regulation (regulating topics such as online safety) and media regulation (regulating audiovisual media services). With users increasingly consuming audiovisual media online, 2026 is set to bring this convergence into even sharper relief. We expect this to be a pivotal year for European media regulation, with the implementation of concrete new compliance obligations in the UK, as well as broader reviews in both the UK and the EU. These developments, which raise particular issues relevant to content compliance, prominence and age assurance, will primarily affect large streaming services, Public Service Broadcasters, TV Selection Services and large digital platforms. A strategic and agile response, blending governance, commercial, technical and early warning considerations, will be essential.

Key regulatory initiatives

There are three main regulatory initiatives that will be high on the media agenda during 2026. First, Ofcom's continued implementation of the **UK Media Act**, the biggest change to the UK public service media framework in two decades. Second, the European Commission's review of the Audiovisual Media Services Directive **(AVMSD)**, designed to respond to the fast-changing media landscape in the **EU**. Third, the UK Government's response to Ofcom's recent recommendations from its Public Service Media review, in which Ofcom warned that traditional public-service TV is endangered and made recommendations for prominence on third party platforms.

In our view, the following categories of companies will be particularly affected by these developments:

- First, **Large Streaming Services**, that operate commercial video on demand **(VOD)** services.
- Second, **Public Service Broadcasters**, that produce public service content and also operate public service VOD players.
- Third, **TV Selection Services**, that provide the primary user interface for consumers to access audiovisual media services, such as smart TVs, set-top boxes and streaming sticks.
- Finally, **Large Digital Platforms**, such as social media companies and video sharing platforms.

There are a variety of issues at play which will affect companies in the abovementioned market segments in different ways. We do not cover them all here but instead focus on implications relevant to three regulatory topics (namely **Content Compliance, Prominence** and **Age Assurance**) that we expect to be central to the debate. A summary of how we expect this to play out in the year ahead is outlined in *Figure 5*.

Figure 5 – implications of the changing media regulatory landscape in 2026

REGULATORY AREA	DESCRIPTION	DEVELOPMENTS TO LOOK OUT FOR IN 2026	AFFECTED SERVICE
Content Compliance	Imposition of a range of rules to large streaming services similar to those that have existed for many years in respect of linear broadcast television.	**UK Media Act** – the Secretary of State is expected to designate the Large Streaming Services within scope of the regime by March 2026. Ofcom intends to finalise the VOD Code, setting out how services can meet their obligations, during July-Sept 2026. Compliance is then required within 12 months. **EU AVMSD** – potentially extending certain obligations to Large Streaming Services and Large Digital Platforms.	This will be immediately relevant to **Large Streaming Services** in the **UK** and should be on the agenda of these players, as well as **Large Digital Platforms**, in the **EU**.
Prominence	Obligations to ensure public service content is sufficiently discoverable in an increasingly fragmented audiovisual digital environment.	**UK Media Act** – in December 2025, Ofcom proposed the 15 Connected TV platforms for the Secretary of State to designate as being in scope of the new television selection service requirements. Designation is expected in Q1 2026. The Public Service Broadcast VOD players that will benefit from these obligations are expected to be confirmed during Q2 2026. Ofcom's Code of Practice on Prominence and Accessibility on Connected TV Platforms is expected to be finalised during Q3/Q4 2026. Other important elements of the regime (e.g. Ofcom's approach to dispute resolution and enforcement) are also due to be finalised. **UK Government response to Ofcom's Public Service Media (PSM) review recommendations** – with Ofcom highlighting that Government should urgently consider further measures to ensure the discoverability of public service content online. **EU AVMSD** – further intervention to ensure consistent and harmonised implementation of prominence rules in EU.	This will be relevant to **Public Service Broadcasters, TV Selection Services, Large Digital Platforms** and **Large Streaming Services**, both in the **UK** and **EU**.
Age Assurance	Ensuring that audiovisual content is age appropriate for the viewer watching it.	**UK Media Act** – new requirements under VOD Code to apply to Large Streaming Services. **EU AVMSD** – review of how AVMSD requirements dovetail with requirements under the DSA.	Primarily relevant to **Large Digital Platforms** and **Large Streaming Services** in both the **UK** and the **EU**.

Large Streaming Services

In-scope streaming services should prepare for new Content Compliance and Age Assurance obligations under the new **UK VOD Code**. This will have a number of different dimensions, relevant in particular to compliance with generally accepted standards, fairness & privacy and audience protection (all of which are mandatory compliance requirements for broadcasters in the 'traditional' TV environment).

In relation to compliance with **generally accepted standards**, preparation should include assessment of the following:

- How current **content compliance processes or editorial guidelines** map against the requirements of the new Ofcom VOD Code.
- The **archival content** hosted, as content that complied at one point in time may require further consideration over time (e.g. in relation to offensive or discriminatory language).
- Whether **complaints systems**, which can act as an important mechanism to alert compliance teams to potential issues, are sufficiently robust.

In relation to **fairness & privacy**, in-scope streaming services should ensure compliance systems and processes are in place to consider the privacy and potential vulnerability of individuals during the making and airing of programmes. This could represent one of the most profound impacts of the new regime as it will mean that streaming services will need to work with programme makers to meet a range of obligations around the individuals who feature in their programmes.

In relation to **audience protection**, including protections for children, designated services should review the efficacy of their current audience protection measures, which could include age assurance and parental controls, and ensure they are prepared to meet the specifications set out in Ofcom's new guidance.

In terms of indirect impact, streaming services should also map the strategic and commercial implications of changes to **prominence requirements** in both the **UK** and **EU**. In the UK**,** this should include reviewing their commercial agreements with regulated TV Selection Services (i.e. operators of connected TV platforms), given they will be indirectly affected by the regulation now in place between designated TV Selection Services and Public Service Broadcasters. Affected streaming services should also follow the direction of travel on this subject in the EU, again primarily in terms of identifying any indirect impact on the discoverability and findability of their services that might arise out of changes to the prominence regime under the AVMSD.

> *"In-scope streaming services should ensure compliance systems and processes are in place to consider the privacy and potential vulnerability of individuals during the making and airing of programmes."*

Public Service Broadcasters

The **accessibility and findability of public service content** ('general interest' content in the **EU**) is also likely to be central to regulatory activity during 2026, with these broadcasters likely to be directly affected by changes in this area.

In the **UK**, affected broadcasters should develop strategic and commercial strategies that should underpin the prominence agreements in place with the newly regulated TV Selection Services. They should also develop a fit-for-purpose strategy in respect of the data governance arrangements necessary to evidence compliance with a public service remit in an increasingly fragmented media environment.

TV Selection Services

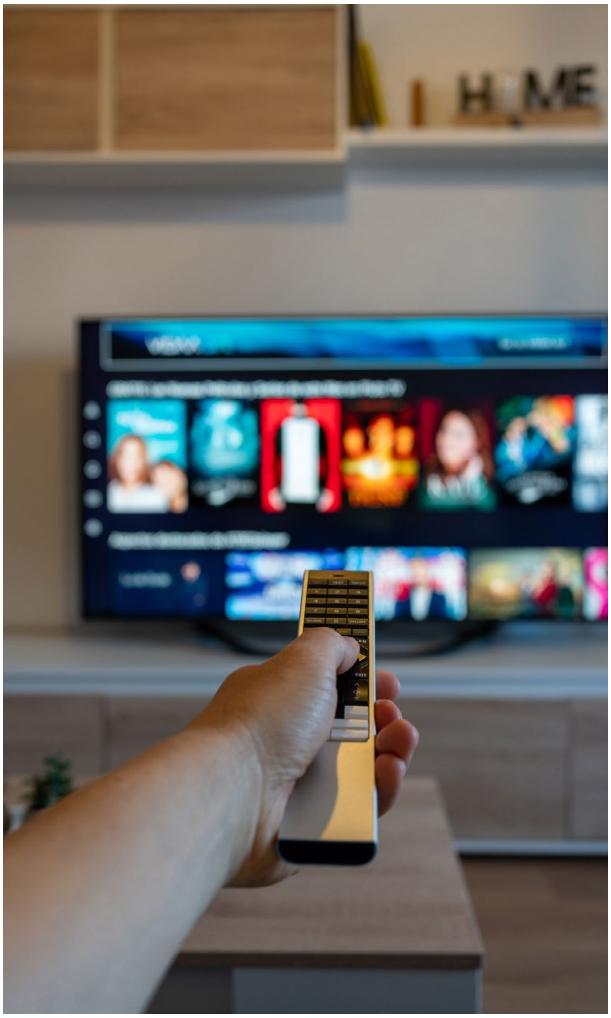
In the **UK**, newly regulated TV Selection Services (i.e. connected TV platforms) should be considering how they will comply with **new rules relevant to the inclusion, prominence and accessibility of required public service content**. This should include identification of any technical considerations which may impact the platform's ability to give due prominence to public service content. Consideration should also be given to commercial and economic questions regarding how terms of trade will be negotiated with Public Service Broadcasters, and how advertising revenues and data be shared going forward. This is especially relevant given Ofcom's new dispute resolution function.

In the **EU**, as with Public Service Broadcasters, in-scope services should consider how **new EU rules for providers of TV Selection Services to ensure prominence of public service/general interest content** might play out in practice. At the same time, newly regulated entities (such as manufacturers and developers of connected TV platforms) should be preparing for introduction of the **new customisation right** by May 2027 (introduced under the EU **Media Freedom Act**), which of course is without prejudice to any national measures introduced to ensure prominence under national law.

Large Digital Platforms

Consideration in the **UK** and **EU** will be given to a **potential expansion of prominence measures by large digital platforms** in relation to public service content, to ensure this content is adequately visible and discoverable by viewers. This will increasingly be driven by concerns about disinformation and the importance of ensuring access to 'trusted' sources of information in the modern digital environment.

In the **EU**, **child protection measures** and potential **changes in relation to regulation of influencer content** should also be on the digital platform agenda. In relation to child protection measures, the Commission is expected to assess whether existing child protection rules in the AVMSD are still fit for purpose, as well as ensuring coherence between the and AVMSD and the DSA in this respect. Therefore, large digital platforms currently within scope of both the AVMSD and the DSA should consider their response to this in the round. In relation to influencers, the Commission's review will also assess how the AVMSD should contribute to the competitiveness and fairness of the media ecosystem, and the adequate protection of viewers when they access audiovisual content, including that created or made available by influencers. The Commission has indicated that one outcome from their review could be additional compliance responsibilities for influencers that may derive from new or enhanced obligations in this area. Therefore, it will be necessary for platforms to clearly demarcate responsibility for any new obligations that may result.



4. Consumer Fairness

The rubber hits the road in the UK

EXECUTIVE SUMMARY

The Competition and Markets Authority ***(CMA)*** *has recently begun to exercise its powers across multiple sectors of the economy under the UK's landmark new consumer protection regime, something that is expected to continue during 2026. This means that a wide range of companies selling online are now effectively on notice, particularly in relation to ensuring compliant online pricing practices and consumer reviews (with further detail on the exact requirements relevant to subscription contracts expected later in the year). In the EU, the long-awaited* ***Digital Fairness Act*** *legislative proposal will be released. This is expected to address specific concerns relevant to addictive design, something that should already be on the company agenda given the related provisions of the* ***DSA*** *and previous Member State led enforcement activity. In both the UK and EU, companies should be reviewing their online sales and marketing operations, and putting in place any necessary changes and controls, in order to prepare.*

Responding to the new consumer protection regime in the UK

Given the focus on 'big tech' compliance with new digital rules, it can be easy to overlook the fact that that many regulatory requirements also apply to how businesses across the economy interact with consumers online.

In the **UK**, much of the new consumer protection regime – under the Digital Markets, Competition and Consumers Act **(DMCCA)** – is now in effect. This means that all business-to-consumer **(B2C)** firms with an online presence should be taking active steps to be fully compliant with its applicable provisions.

The new regime includes some significant new updates to the **UK's digital consumer enforcement regime**. To recap, this includes new rules relevant to online pricing practices, consumer reviews and subscription contracts, as follows:

- **Online pricing practices:** a new prohibition on 'drip pricing' by requiring mandatory disclosure of full prices from the outset, including fees, taxes and charges. If the exact price cannot be calculated in advance, clear information for an estimate must be provided.
- **Consumer reviews:** a prohibition of fake reviews and undisclosed incentivised reviews. The ban applies to both businesses' own websites and intermediaries who publish reviews, imposing an obligation on firms to actively prevent and remove such content online.
- **Subscription contracts:** new requirements concerning pre-contractual information, reminder notices and cancellation rights. Unlike the abovementioned measures, these provisions are not yet in force, as they still require secondary legislation. They are expected to take effect in autumn 2026.

Importantly, the new regime also contains procedural changes enabling the CMA to now **directly enforce a range of consumer law**, without needing to litigate through the courts. In the case of non-compliant behaviour, the CMA can impose remedial measures and fines of up to £300,000 or 10% of worldwide turnover (whichever is higher).

How business can respond to the new regime

After the new regime went live in April 2025, the CMA initially adopted a policy of issuing guidance and engaging in outreach to help businesses comply. However, that period has now elapsed, with the CMA launching **its first wave of enforcement action** and related activity under the new regime in November 2025. Sectors within scope of this activity include **live events**, **homeware**, **retail**, **parking**, **holidays**, **cinemas**, **food delivery**, **gyms**, **driving schools** and **bus**, **coach** and **rail travel**.

While the CMA still sees advice and guidance as an effective route to compliance, it has also clearly stated in its 2026-2029 strategy that it intends to act decisively and take enforcement action on conduct which harms consumers and disadvantages fair-dealing businesses.

Therefore, companies should be actively reviewing their online sales and marketing activity against the new requirements. This includes identifying any commercial activities that may be deemed unfair and, importantly, being able to demonstrate clear, actionable steps towards resolving these issues (something we have written about in more detail here).

These considerations also apply to future products and offerings that companies may be planning to release in the **UK** market, where compliance should already be embedded in the design phase.

Online pricing practices

Concerns about **online pricing** triggered the first use of the CMA's powers under the new regime at the end of 2025. These concerns become even more relevant in contexts where vulnerable customers may be affected or where consumers may feel under pressure to make a snap decision (e.g. due to false or misleading scarcity claims).

Consistent with the scope of this ongoing enforcement activity, companies should be reviewing their use of undisclosed mandatory fees, automatic opt-in to purchasing additional services and inaccurate time-limited sales in particular.

Previous enforcement action by the CMA has also highlighted that undisclosed 'double-tier selling' (i.e. selling the same product at different price 'tiers' without warning consumers that prices will increase once the ones in the most affordable tier are sold out, relevant to the sale of concert tickets for example) is not acceptable. Companies should therefore ensure that consumers have access to clear and sufficient information about possible price changes.

> *"Companies should be actively reviewing their online sales and marketing activity against the new requirements."*

Consumer reviews

Another area that the CMA has prioritised under the new regime has been compliance with its **new guidance on fake reviews** (i.e. a consumer review that purports to be, but is not, based on a person's genuine experience). This is not just limited to individual reviews, but also includes aggregated ratings and star rating systems, which the CMA expects to be based solely on genuine data.

After an initial period of review which involved sending **letters to companies** whose practices the CMA has concerns about, the CMA is expected to **formally investigate suspected non-compliance** over the course of 2026. In this increasingly enforcement-focused environment, businesses should note that the CMA considers proactive steps towards rectifying non-compliant behaviour as a mitigating factor in any enforcement proceeding.

In *Figure 6* below we set out a summary of the requirements relevant to addressing fake reviews (based on our review of CMA guidance), along with actions that companies can take in response.

Figure 6 – requirements and actions relevant to addressing online fake reviews

AREA	REQUIREMENTS*	ACTIONS COMPANIES CAN TAKE**
Policy	Have a publicly accessible policy that prohibits fake reviews and describes the approach taken to incentivised reviews and the handling of review information.	• Develop the policy, ensuring internal dissemination. • Focus on accessibility and visibility of the policy on the website (e.g. ensuring it is easy to find and easily understandable to consumers).
Risk assessment	Conduct risk assessments on a regular basis to assess the risks that consumers may encounter banned and fake reviews and identify appropriate measures to address such risks effectively.	• Run an initial risk assessment, then set a cadence for review as well as triggers for ad hoc assessments (e.g. in case of significant changes to business model and/or platform layout). • Document how the assessment is used to guide governance & controls or design changes.
Prevention	Take appropriate steps to minimise the risk of prohibited reviews appearing on the website/platform.	• Implement pre-publication controls, allowing automatic flagging of suspicious reviews requiring further screening. • Ensure users provide sufficient evidence (e.g. allowing only verified users to post reviews, requiring reviews about specific transactions to include order ID/date).
Detection & removal	Establish a process to detect, investigate and remove prohibited reviews.	• Implement adequate monitoring tools (e.g. a mix of internal review, automatic flagging and user reporting). • Set up a procedure to investigate suspicious reviews (e.g. ensuring traceability of users). • Have clear rules on removal and penalties for fake reviews (e.g. suspension of account). • Ensure all of the above are included in the public policy.

**non-exhaustive, please refer to original document for a comprehensive overview*
***for indicative purposes only*

AREA	REQUIREMENTS*	ACTIONS COMPANIES CAN TAKE**
Third parties	Even if relying on services and/or products provided by a third-party (e.g. for collating aggregated reviews or data), companies remain responsible for what they publish on their platform.	• Include review moderation in pre-contractual due diligence checks, in order to gather sufficient assurance on third-party moderation and user verification policies. • Ensure third-party contracts include terms detailing compliance with CMA expectations and emphasise willingness to collaborate on moderating reviews.

Subscription contracts

Incoming DMCCA requirements will mean companies must offer a straightforward way out of subscriptions without the consumer having to take steps that are not 'reasonably necessary'. This does not necessarily prohibit companies from making alternative offers or requesting feedback, but these should not unduly extend the exit process (e.g. by being mandatory or by having too many steps).

This means that services will likely need to **review the design of their user journey**, with a clear rationale to justify choices such as the number of steps required to exit contracts and the number of offers presented to users before termination of the contract.

To address these priorities, companies should embed robust processes and controls to ensure fairness in online environments right from the early stages of product design. To achieve this, identifying, bringing together, and, where necessary, training all relevant internal teams – including legal, design, risk, marketing, compliance and technology – will be a crucial step.

Preparing for the upcoming Digital Fairness Act in the EU

In the **EU**, the main legislative priority to look out for will be the publication of the European Commission's legal proposal for a new Digital Fairness Act expected in Q4 2026. This proposal aims to address issues identified during the Commission's **2024 Digital Fitness Check of existing EU consumer law**. That review highlighted the need for regulations better adapted to the harmful practices and challenges consumers encounter online.

A **call for evidence**, published in July 2025, provided greater clarity on the specific issues the proposal aims to address, with a particular emphasis on concerns relevant to addictive design. This includes the deliberate structuring of online services and platforms likely to foster addictive behaviour, particularly in relation to minors. In the case of video games for instance, such features can range from gambling-like elements, to penalties for disengagement and incentives to 'play by appointment' at certain moments during the day.

Minors have long been at the centre of the debate on addictive design. A **2023 report from the European Parliament**, which informed the subsequent Fitness Check, already called on the Commission to prohibit harmful addictive techniques not covered by existing legislation. New rules may therefore introduce outright bans on features such as infinite scrolling, autoplay, streaks and loot boxes.

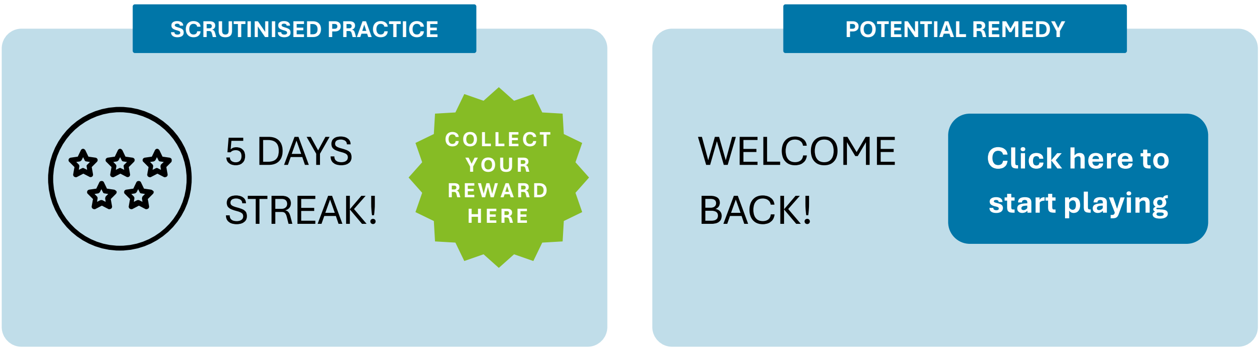
Case Study: addressing regulatory concerns relevant to addictive design

During 2025, the EU's Consumer Protection Cooperation Network (led by the Netherlands Authority for Consumers and Markets and the Norwegian Consumer Authority, coordinated by the European Commission) adopted **key principles to promote transparency and fairness in video games**. Although broader than just addictive design, this activity already highlights how regulatory bodies are responding to these concerns in a gaming context. An example of this is shown in *Figure 7* below, which provides a simplified example of how such concerns can be addressed.

In addition, the **DSA's guidelines on the protection of minors** (applicable to all online companies in scope of the DSA regardless of their size), already take a firm stance against addictive design. For instance, platforms are required to block children's access to any features that resemble gambling, such as 'loot boxes'. This aligns closely with the objectives of the forthcoming Digital Fairness Act, which could further regulate these practices.

By adopting DSA compliance measures – such as implementing tiered service models that limit minors' access to these features – businesses can already lay a solid foundation to meet some of the expected requirements of the Digital Fairness Act.

Figure 7 – responding to regulatory concern about addictive video game design



5. Competition

A fluid EU environment, with the first UK requirements expected

EXECUTIVE SUMMARY

*With Digital Markets Act **(DMA)** obligations in the EU approaching their two-year anniversary, despite some notable developments, the situation remains in something of a state of flux. In the year ahead, companies can expect further clarity arising out of existing investigative activity and the Commission's DMA review. In the UK, the CMA continues to implement its regime, with the first set of UK requirements (in relation to search and mobile ecosystems) set to be finalised. In-scope companies will likely be able to leverage some of their existing measures already introduced in the EU, but a 'lift and shift' will certainly not suffice. For both regimes, tangible steps can still be taken, such as developing a gap analysis on the interplay with the General Data Protection Regulation **(GDPR)** in the EU or preparing for new bespoke compliance reporting requirements in the UK.*

In the Competition chapter of last year's Digital Regulatory Outlook, we observed in relation to the **EU** regime that *"The coming year will be an early indicator of whether the intended shift from an 'ex post' approach (characterised by lengthy investigations after the event), to an 'ex ante' approach (characterised by ongoing dialogue and compliance), is materialising."* One year on, it's fair to say that the intended shift to an ex-ante approach has not materialised as of yet. In launching the first **review of the DMA's effectiveness** during the summer of 2025, the Commission noted that it has observed a positive impact so far, whilst also recognising that it has only been applicable for a relatively short period of time. Published responses to the Commission's consultation indicate the jury is still out on whether Gatekeepers and third parties alike believe it is currently having the desired effect.

Tracking outcomes relevant to existing DMA investigations

Looking back on the previous year, 2025 was characterised by **intensive DMA investigative activity** on a range of topics, culminating in a variety of outcomes including no further action, legally binding specification decisions, fines and preliminary findings of breaches. This remains a fluid environment, with affected Gatekeepers actively responding to preliminary findings where required, while simultaneously appealing various elements of the final decisions in court. The outcome of all this activity in 2026 will provide further clarity on key DMA obligations for affected stakeholders, including:

- For Gatekeepers that **process personal data**, what in practice constitutes a 'less personalised but equivalent' service, and what degree of personalisation is acceptable, given the need to offer such a service if a user refuses consent to such data processing. Incoming guidelines on GDPR-DMA interplay, considered later in this Chapter, will also be relevant here.
- For Gatekeepers who operate **app stores**, what contractual and business terms can be imposed on third party app developers whilst still complying with obligations to enable app developers to freely 'steer' users beyond the Gatekeeper's app store, and to allow apps to be distributed through other routes such as third-party app stores.

- For Gatekeepers who provide **search services**, how their own services can be integrated within search results without violating self-preferencing rules. This includes whether such services can be treated differently in any way, for example through dedicated spaces, different visual formats or direct interactivity within the search interface.

The outcomes of these various activities in 2026 are expected to provide clarity on the practical interpretation and enforcement of the DMA. Consequently, all Gatekeepers, including those not currently subject to specific investigations, should monitor these developments and proactively consider design and operational changes where relevant.

Preparing for new DMA priorities following the initial review

In parallel, the Commission will conclude its first **statutory DMA review**, with a report expected by May 2026. The review will retrospectively assess the DMA's effectiveness in ensuring contestable and fair markets, and its impact on business users (especially SMEs) and end-users.

The review is expected to influence future policy direction and enforcement priorities. In particular, the Commission will consider the need for rule and scope changes. We expect the Commission to prioritise several areas as part of this review, set out in *Figure 8* below.

Figure 8 – DMA review priorities

AREA	DESCRIPTION OF ACTIVITY	IMPLICATION
AI Integration	Examining how existing rules apply to AI integrated into regulated services (e.g. search) and how the DMA can meet any emerging AI competition challenges, such as AI agent integration and the potential for Gatekeeper actions to hinder third-party AI agents or favour their own.	Ultimately, this could inform rule changes to respond to the integration of AI or the deployment of new AI services such as AI agents, or future enforcement priorities.
Expansion of Core Platform Services (CPS):	Considering whether the existing list of CPS needs to be amended, with the potential for new categories such as standalone AI services. A key test remains whether a service acts as a gateway between consumers and business users.	Given the 'gateway' requirement, AI services enabling user-business interaction may be potentially in-scope (e.g. AI agents facilitating this interaction and chatbots enabling direct purchases or directing users to businesses), whereas chatbots solely providing information may not.

AREA	DESCRIPTION OF ACTIVITY	IMPLICATION
Interoperability	Considering the extension of interoperability obligations to designated social media services. Interoperability obligations currently apply to in-scope messaging services, requiring them to facilitate third-party interoperability upon request, with the depth of interoperability required expanding over time (for example, requiring full group chat interoperability).	The Commission is expected to weigh up the expected demand and benefit of expanded interoperability against the challenges it could raise for regulated firms. Were the Commission to proceed, requirements would likely be implemented in phases, as done for messaging services. Technology teams would need to draw up appropriate technical documentation, whilst product teams would need to consider how interoperability might impact the broader service.

Developing an initial gap analysis based on interactions with GDPR

In 2026, the EDPB is expected to publish long-awaited **guidelines on the interplay between the DMA and GDPR**. Draft guidelines, released in late 2025, clarify how firms can ensure compliance with DMA requirements, including around data processing, data portability and interoperability. For instance, the DMA prohibits certain types of data processing without valid end-user consent. The draft guidelines set out that valid consent requires separate opt-ins for each purpose (e.g. content and advertising personalisation), unambiguous requests, a clear refusal option presented equally to acceptance and no pre-ticked consent boxes.

Whilst not finalised, firms can use this draft guidance to begin a gap analysis, confirming whether existing controls and features, such as user-consent requests, align with the guidelines or if targeted changes are required. Alongside this, firms should also consider proposed changes to data protection regulations, including to the definition of personal data, set out in the **Digital Omnibus** (see *Chapter* 6). Alignment with the final guidelines should be prioritised upon their expected publication later this year.

A maturing UK digital markets competition regime

Whilst the Commission reviews its regime, requirements under the **UK** regime are still being established. In autumn 2025, the CMA confirmed Strategic Market Status **(SMS) designations** for one firm in **general search and search advertising** and two firms in **mobile platforms**. These firms now face enhanced merger control requirements and an 'SMS levy' covering regulatory costs. Further obligations, such as conduct requirements **(CRs)** or **pro-competition interventions**, must be specifically developed for each SMS firm and require prior consultation.

At the time of writing, the CMA is expected to consult shortly on its first set of CRs in relation to search and mobile platforms. Early actions expected to be prioritised were set out in **Roadmaps published in summer 2025**. These are subject to change, meaning firms should monitor carefully for the CRs ultimately proposed. The CMA is expected to publish updated Roadmaps in the first half of the year, clarifying medium-term priorities.

Beyond search and mobile, the CMA may also launch **further SMS designation investigations** in 2026. As discussed in *Chapter 7*, **Cloud** is a likely focus area. It is important to remember that only the largest digital firms, meeting a turnover threshold of £25bn worldwide or of £1bn in the **UK**, can be designated. Ultimately, any SMS designation would lead to bespoke CRs, as previously discussed. However, since an SMS designation investigation must precede any CR consultation, any new requirements are unlikely to be in force before 2027.

> *“simply applying EU-adopted measures will not guarantee UK compliance, meaning firms must carefully consider their approach based on the final CRs."*

Expect some consistency between UK and EU requirements, with a targeted UK response still required

In developing its proposals, the CMA has considered DMA requirements, not least because the **UK Government’s Strategic Steer to the CMA** highlights the importance of considering international regulation. Firms may therefore be able to leverage DMA compliance to a certain degree. For instance, potential CRs relating to data portability and choice screens are also DMA requirements, and recent Commission enforcement on app developer steering aligns with potential UK requirements.

However, even with broad alignment, CMA CRs will likely necessitate targeted changes. CRs can be more prescriptive than high-level DMA requirements, such as potential firm-specific 'fair ranking' principles for search. For app developer steering, the CMA has indicated it will consider international developments but will not 'lift and shift', instead developing a **UK-specific approach**. Therefore, simply applying **EU-adopted measures** will not guarantee UK compliance, meaning firms must carefully consider their approach based on the final CRs. Now that the regime is properly up and running, firms will also need to prepare to comply with a range of supervisory requirements, set out in *Figure 9*.

The evolution of merger policy

Beyond specific digital market regimes, broader merger policy will continue to be relevant for digital firms. In the **EU**, as part of the **Merger Guidelines review**, the Commission is considering the unique characteristics of digital markets, such as network effects and the strategic importance of ecosystems. While final guidelines are due in 2027, draft guidelines are expected this year. The current direction of travel suggests digital platforms should anticipate continued scrutiny of acquisitions, potentially involving **extended forward-looking assessments** given the fast-moving nature of digital markets, alongside greater consideration of the impact on data accumulation or reduced consumer choice related to privacy.

In the **UK**, whilst SMS firms are subject to specific obligations including merger reporting, the **broader merger control regime** remains relevant. After consulting in late 2025, the CMA’s revised guidance on merger remedies is now in effect, designed to embed the CMA’s ‘4ps’ – pace, predictability, proportionality, and process. The CMA previously indicated changes were expected to introduce a wider scope for behavioural remedies and process changes designed to enable greater transparency and early engagement with businesses, potentially allowing more deals to be cleared with remedies, and at an earlier stage. Subsequently, in January 2026, the CMA launched a **call for evidence** designed to inform a review of its approach to merger efficiencies, with changes expected to be implemented by the summer.

Figure 9 – DMCCA supervisory requirements

Nominated officers

SMS firms will need to assign a nominated officer with responsibility for each CR. The nominated officer will be required to **monitor compliance** and **ensure cooperation with the CMA**. Nominated officers will also be responsible for **ensuring compliance with new reporting requirements** discussed below. Companies should ensure they have a plan in place to appoint such officers for future CRs and consider **training** or **upskilling** to ensure they can effectively fulfil their role.

Reporting requirements

Details of reporting requirements for each CR will be set out in '**compliance reporting notices**'. The requirements may differ from information required under the DMA. Capturing and submitting UK-specific data may therefore impose new **data collection**, **validation**, **reporting**, and **governance** requirements on the relevant internal teams.

Skilled person reports

As the regime matures, the CMA may begin to exercise its power to require the appointment of a skilled person to develop a report. This may occur, for example, where **specific expertise on a technical matter,** or an **independent assessment of a particular issue** is required, for example as part of a compliance review or breach investigation. As such, the scope of the topics that may be covered in a skilled person report can be very broad, depending on the nature of the investigation and associated CR.

6. AI

Focus on the known knowns whilst preparing for further change

EXECUTIVE SUMMARY

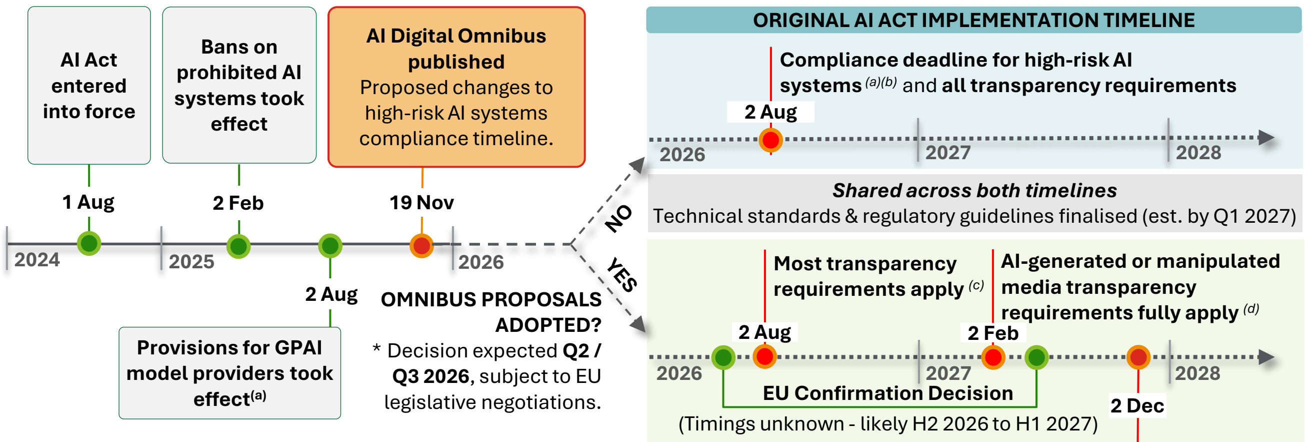
*2026 is poised to be another dynamic year for AI regulation. Some elements have now become clearer, including many of the specifics of **AI Act** rules applying to providers of General Purpose AI **(GPAI)** models, meaning firms should have settled compliance strategies in place. However, some details, particularly timelines for transparency and high-risk requirements, are expected to shift based on **Digital Omnibus** proposals. This adjustment aims to provide sufficient time for the development of relevant standards and guidelines before requirements take effect, though the final position will only be confirmed once the EU institutional decision-making process has concluded. The interplay between AI and other relevant regulation (such as copyright, data protection, telecoms, media, online safety and competition), should also be factored into the company response. All of this means agility will be required.*

The AI Act and the Digital Omnibus

The AI Act remains the key regulation to focus on for affected companies active in the **EU**, albeit now with an additional focus on the implications of the recent Digital Omnibus, which proposes to simplify certain elements of this framework. The Digital Omnibus has created something of a dilemma for in-scope companies. Many AI Act requirements are already in force, including prohibitions on unacceptable AI practices and requirements for GPAI models.

Looking ahead however, the Omnibus has proposed **delays to timelines for incoming transparency and high-risk AI system requirements**. For these proposed delays to take effect before requirements kick in, the **EU** legislative process to adopt the Omnibus proposals must conclude by August 2026, creating a tight schedule for lawmakers. If the process is not completed in time, companies could find themselves still legally subject to existing timelines, as set out in *Figure 10*.

Figure 10 – AI Act timeline


AI Act entered into force
Bans on prohibited AI systems took effect
AI Digital Omnibus published
Proposed changes to high-risk AI systems compliance timeline.
1 Aug
2 Feb
19 Nov
2024
2025
2026
2 Aug
Provisions for GPAI model providers took effect(a)
OMNIBUS PROPOSALS ADOPTED?
* Decision expected Q2 / Q3 2026, subject to EU legislative negotiations.
NO
YES
ORIGINAL AI ACT IMPLEMENTATION TIMELINE
Compliance deadline for high-risk AI systems (a)(b) and all transparency requirements
2 Aug
2026
2027
2028
Shared across both timelines
Technical standards & regulatory guidelines finalised (est. by Q1 2027)
Most transparency requirements apply (c)
AI-generated or manipulated media transparency requirements fully apply (d)
2 Aug
2 Feb
2026
2027
2028
EU Confirmation Decision
(Timings unknown - likely H2 2026 to H1 2027)
Commission confirms technical standards / guidance ready.
High-risk AI compliance due 6 months post-decision.
2 Dec
Backstop deadline (a)(b)
If no decision is issued
PROPOSED NEW AI ACT IMPLEMENTATION TIMELINE

(a) *Different compliance timelines apply to GPAI and high-risk AI systems placed on the market or put into service before the compliance deadlines with the EU AI Act.*

(b) *Different compliance timelines apply to high-risk systems listed in Annex I of EU AI Act.*

(c) *Except AI-generated or manipulated media requirements for systems already on the market prior to 2 August 2026*

(d) *For systems on the market before 2 August 2026*

Focus on the known knowns

As firms respond to these developments, it is critical to ensure that robust foundations are in place.

This begins with comprehensive visibility of company AI deployment, typically via an AI inventory, alongside an AI policy that establishes a clear governance framework. An effective framework can evaluate AI use cases against regulatory requirements and organisational risks, enabling appropriate controls and mitigations, combined with clear ownership and accountability.

Whilst the Digital Omnibus proposes removing formal AI literacy obligations on firms, ensuring the relevant personnel sufficiently understand AI will still be essential to discharge governance, risk and compliance responsibilities. Firms may also consider making use of specific AI guidance and standards, such as the **NIST AI Risk Management Framework** and **ISO/IEC 42001**, which can offer practical guidance for AI governance and risk management. Finally, effective horizon scanning is crucial to identify emerging requirements that may impact AI strategy.

Getting these elements right will stand firms in good stead to respond to specific regulatory requirements and adapt as rules evolve. More detail on the steps that companies can take in relation to these requirements are set out in this Chapter.

AI Act - GPAI requirements

Firms training and developing foundational GPAI models, i.e. those that underpin the development and deployment of downstream AI system and services, will need to prioritise ongoing compliance with the AI Act in this respect.

AI Act obligations already apply to GPAI models placed on the EU market since August 2025, meaning providers of such models are required to comply with a range of requirements relating to transparency and copyright, with additional safety and security requirements for GPAI models with systemic risk. Models placed on the market before 2 August 2025 benefit from an extended compliance timeline, with a deadline of August 2027.

To support firms in compliance, the **GPAI Code of Practice** was published last summer. Whilst this is voluntary, the Commission has confirmed that full alignment with the Code can demonstrate compliance with AI Act obligations. Code signatories should ensure they can demonstrate full compliance with the Code, including by proactively documenting and evidencing measures adopted. Non-signatories should consider whether there are elements of the Code they may be able to adopt. Where this is not feasible, they will need to ensure they have alternative measures in place and be able to justify how these meet the Act's requirements; not least as full enforcement powers take effect from August 2026.

> *"As firms respond to these developments, it is critical to ensure that robust foundations are in place... Getting these elements right will stand firms in good stead to respond to specific regulatory requirements and adapt as rules evolve."*

AI Act – transparency and high-risk requirements

Beyond rules affecting the underlying AI models, the AI Act imposes **requirements on** a range of AI systems relevant to the need for **transparency and the inherent risk associated with specific use-cases**.

Further information on a number of these requirements, along with a brief overview of key implications for affected companies, is set out in *Figure 11*.

Figure 11 – Key AI Act requirements relevant to transparency & high-risk AI

ISSUE	DESCRIPTION	IMPLICATION
Transparency: Interaction with users	AI systems directly interacting with individuals (e.g. **chatbots**) are required to clearly inform users that they are engaging with AI, unless this is obvious to a reasonable user given the context.	Firms should carefully consider how this disclosure can be integrated into the user journey ahead of requirements coming into force in August 2026.
Transparency: AI-generated or manipulated media	**AI-generated or manipulated media** (images, audio, video) are required to be clearly marked as such. Providers of AI systems enabling this functionality need to ensure outputs are labelled in a machine-readable, detectable format. To support compliance and clarify expectations for consistent watermarking, labelling and disclosure, the Commission is developing a voluntary **Code of Practice**. Following a first draft published in December 2025, a final version is expected by mid-2026.	Firms should prioritise implementation and documentation of transparency measures as soon as feasible, drawing on the draft Code as a guide, whilst monitoring for updated drafts and the final version. Even with a proposed six-month compliance extension for systems already on the market before August 2026, implementation timelines are likely to still be tight following the Code's finalisation.
High-risk AI requirements	High-risk AI rules apply to specific **use cases that can pose serious risks to health, safety, or fundamental rights** (e.g. AI used in critical digital infrastructure or recruitment decisions) with different requirements applying to AI providers and deployers. Over a dozen guidance documents and technical standards for high-risk systems are expected throughout 2026 and early 2027.	If the Digital Omnibus is finalised as currently drafted, firms will have longer to comply, with requirements commencing six months after formal **EU** confirmation of ready technical standards and guidance, or by December 2027 at the latest. If negotiations extend beyond August 2026, high-risk AI requirements would technically come into force, meaning firms that have not taken the necessary steps are at risk of being in breach. Given this uncertainty, organisations should assess the implications of operating within the high-risk category, developing a corresponding deployment strategy as required.

Interplay with copyright

Beyond the AI Act, copyright rules are particularly relevant for firms developing foundational GPAI models. The **EU's voluntary GPAI Code** offers clear guidance, requiring signatories to limit web-crawling to lawfully accessible content, respect rights reservations and mitigate the risk of copyright infringement. Additionally, the EU has published a mandatory template for providers to disclose training data summaries, to help them comply with their AI Act obligation to make this information publicly available.

Looking forward, following a consultation launched in December 2025, the Commission will develop a **list of generally agreed machine-readable opt-out solutions**, to provide greater clarity on how firms can practically respect rights reservations. Ongoing legal debate at Member State level is also relevant, such as a recent **German court decision** that found an AI model and its outputs breached copyright by reproducing recognisable protected lyrics although they did not store copies.

The **UK** situation is more fluid, though further clarity is expected in 2026. First, the Government is **reviewing copyright rules, with an impact assessment and report** due by 18 March 2026. Any changes, particularly regarding the specifics of whether and how rights-holders can opt-out, will influence technical barriers to UK model training. For example, firms may need to implement technical safeguards to ensure such opt-outs are respected.

Second, legal debate and challenges may clarify how **existing copyright law** applies. For example**, a late 2025 ruling** indicated that imported AI models trained outside the **UK** which never store or reproduce copyright-protected works are not 'infringing copies', that infringement may depend on how AI models are made available and that developers cannot shift liability to users via their terms and conditions. However, uncertainty remains where models are trained in the UK, meaning firms should monitor future cases and appeals, which may provide further clarity on areas such as the legal status of UK-based AI training.

Interplay with data protection

Given the frequent use of personal data in training and testing AI, **proposed changes to data protection rules under the Digital Omnibus** are relevant. Proposals include a clarified, potentially narrower, definition of personal data, alongside widening the legal grounds for processing such data for AI training and testing.

If these (and other) proposed changes are ultimately adopted, this could offer firms a clearer runway for AI development and deployment, widening the scope for digital firms to use data gathered as part of their operations to train and test AI models. However, firms would still need to maintain robust governance and checks and balances, clear legitimate interest assessments, and proportionate measures to uphold individual rights and data protection principles, particularly for special categories of data.

Interplay with sectoral regulation

In the **UK**, the Government has previously indicated that any future rules would likely target the largest, most powerful AI models, suggesting a potentially more limited scope than the EU AI Act. However, more recent statements suggest **no overarching AI Bill** is forthcoming, with a focus instead on action in specific areas like copyright.

In the absence of centralised regulation, sectoral regulators are expected to continue to provide clarity on how existing frameworks apply in their areas. This will be an evolving area as both firms and regulators understand how AI is likely to be used within the ecosystem, and related risks and opportunities. For example, in the **telecoms sector**, providers deploying AI for network and traffic management should implement safeguards to ensure adherence to existing resilience and security requirements, safeguarding network reliability. In the **media sector**, audiovisual media services may consider deploying AI to meet some of their regulatory obligations, for example to generate subtitling and audio descriptions to comply with accessibility obligations. In this case, the onus would be on the regulated service to implement safeguards that ensure the accuracy of these AI-generated outputs.

Interplay with online safety and competition regulation

Existing online safety and competition regulation is also relevant to AI provision, deployment and use, with a number of developments expected in the year ahead, as shown in *Figure 12*, below.

Figure 12 – Interplay with online safety and competition regulation

REGULATION	DESCRIPTION	IMPLICATION
DSA	Under Digital Omnibus proposals, in order to improve supervisory coherence, the **AI Office** will directly oversee AI systems that constitute, or are integrated into, a VLOP or VLOSE. While no standalone AI systems are currently designated, we may see designations in 2026 for those exceeding 45 million monthly users. If the Digital Omnibus is adopted as proposed, the initial assessment of AI systems will use **DSA-mandated risk assessment** and **audit frameworks**. However, the AI Office will have the power to subsequently enforce under the AI Act if not satisfied with compliance.	For VLOPs and VLOSEs, this reiterates the importance of conducting **fresh DSA risk assessments** and **implementing risk mitigation measures** when new AI features are deployed, considering both DSA and AI Act requirements. In relation to minors, the Commission’s recent guidelines on the protection of minors are also relevant (see *Chapter 1*), as they highlight safeguards and clear warnings for children's AI use.
OSA	Absent UK AI-specific regulations, the OSA will be a key framework for digital services, relevant to **AI features involving user-generated content** (e.g. user-created chatbots), search, or pornography. However, unlike the AI Act, this regime does not impose specific requirements on wider AI systems, nor does it regulate the underlying models.	In-scope services will need to **conduct risk assessments** and **develop mitigations**, guided by Ofcom's Codes. Larger services could face additional obligations in due course, including transparency reporting, enhanced risk assessments and fraud prevention (see *Chapter 2*). The Government has indicated the potential for further legislation to capture chatbots more widely, but this remains uncertain.
DMA and DMCCA	Regulators will also focus on competition risks arising from both standalone AI systems and **AI integration into regulated services**. For example, the High-Level Group on the DMA recently endorsed a paper highlighting the role the DMA can play in fostering an open AI value chain, in particular by opening up access to AI infrastructure and distribution and access to data.	In addition to action under the DMA and the ongoing EU DMA Review (see *Chapter 5*), the CMA’s Roadmap of possible measures in search (published before the SMS investigation concluded) is relevant. The CMA expects to prioritise ensuring **transparency**, **attribution** and **choice** for publishers whose content is used in AI-generated responses to search queries. The CMA also indicated it will consider **fair and reasonable terms** for publisher content used in this way.

7. Cloud and the Data Economy

Unlocking competition and innovation, with AI as a golden thread

EXECUTIVE SUMMARY

*The EU's cloud switching and interoperability framework under the **Data Act** is now largely finalised, requiring in-scope providers to have fit for purpose governance in place. Regulators in both the EU and UK are also assessing the application of new digital competition rules to the sector, necessitating a strategic response from the largest market players in the year ahead. From a data economy perspective, the EU's new cross-sector data sharing framework is largely settled (as enhanced by the proposed **Digital Omnibus**), with a smart data discussion picking up in the UK under the new **Data (Use and Access) Act**. Companies, in particular strategy and technology teams, should map the related opportunities and risks, taking insights from sectors (such as transport) where the data sharing discussion is more advanced. The importance of data access in realising the innovation and economic benefits of AI, driven by Agentic AI, acts as a golden thread across all this activity.*

Cloud

Promoting competition and user choice in cloud is expected to remain a key regulatory priority in the year ahead. Given the majority of **cloud switching obligations under the EU Data Act** came into force in September 2025, in-scope cloud service providers should already have taken steps to address the necessary technical, legal, commercial and operational considerations that are required in response (something we have previously written about here).

This is not, however, a one-shot game, given the likely need for **further regulatory specification** as market experience evolves. For example, the new requirement that cloud providers *"shall not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles relevant to different elements of the switching process"* could well be interpreted differently by cloud providers on the one hand, and corporate customers on the other. In addition, although a mandatory switching period of 30 days has been introduced, it can be extended to seven months in the event that the 30-day period is not *"technically feasible"* – again, a concept that is open to interpretation.

As a result, it will be important that affected cloud providers have the necessary governance processes in place in case they are asked to explain their approach during a commercial disagreement or even potential regulatory dispute. **National regulators now have an important enforcement role to play** here, something that is expected to become more visible as market experience evolves. On the flip side, SME and mid-cap cloud providers should take steps to differentiate between contracts signed before and after the application of the Data Act (i.e. 12 September 2025), given the Digital Omnibus proposal to exempt such providers from cloud switching obligations before this date (which the Commission expects to result in around €1.5 billion in one-off savings for eligible cloud providers given they would avoid costly and complex contract re-negotiations).

Affected cloud providers should also ensure they are well placed to respond to the **interoperability provisions of the Data Act**, given the accepted challenges associated with differing levels of interoperability across the cloud stack. This should be high on the agenda of technology teams, with the anticipated **new common EU repository on the interoperability of cloud services** still eagerly awaited.

Beyond the Data Act, the potential for the two largest cloud service providers to be regulated under the **DMA** remains a possibility, given the Commission's **recently announced investigation**, set to conclude by 18 November 2026, which is examining whether these providers meet the tests to be designated as gatekeepers for cloud computing services.

In what remains a fluid regulatory environment, the following activities necessitate a strategic response from the largest market players in the year ahead:

- The **interplay between** the scope of any new cloud services designation under the **DMA** and the cloud switching and interoperability obligations already in place under the **EU Data Act**.
- The **output from** the accompanying **Commission cloud services market investigation**, which is focusing on how the DMA may address practices that may limit competitiveness and fairness in the cloud sector (set to conclude by 18 May 2027).
- **Next steps in the UK**, given previous UK investigations (by both Ofcom and the CMA) have examined these markets in some detail, **outlining concerns relevant to market concentration, lock in and licensing practices**. The CMA has stated that it anticipates that options for SMS designation investigations under the new UK competition regime will be considered by the CMA Board in early 2026.

More broadly, cloud compute capacity also has a central role to play in the innovation and growth agenda. This factor was highlighted in the **Draghi report**, which identified the importance of increasing computational capacity in the EU as a critical component of a mature data economy which underpins many established and emerging digital use cases, particularly for AI development. This is a topic that we cover (in relation to the forthcoming **EU Cloud and AI Development Act**) in *Chapter 8*.

> *"Promoting the Data Economy is a key driver of the EU's competitiveness agenda, with the new Data Union Strategy including a focus on scaling up access to quality data for AI and innovation."*

Data Economy

Promoting the Data Economy is a key driver of the EU's competitiveness agenda, with the new **Data Union Strategy** including a focus on scaling up access to quality data for AI and innovation. This emphasises the importance of further developing **EU data spaces** across various sectors of the economy, including health, manufacturing and agriculture.

The EU Data Act is also central to the EU's data economy vision. First, to require that users of a connected product or related service can access, in a timely manner, the data generated by the use of that connected product or related service **(B2C sharing)**. Second, to ensure those users can use the data, including by enabling data sharing across the commercial data ecosystem **(B2B sharing)**.

In our 2025 Outlook, we wrote that *"it seems to us that there is a lot of work still to be done to fully realise this regime"*. In so doing, we noted that at that time of writing only 12 **data intermediation services**, who have an integral role to play in enabling data sharing, had been formally notified under the EU's existing mandatory registration framework. Fast forward 12 months, and that number has risen to 30, showing signs of progress.

The EU's Digital Omnibus proposes introducing measures to reduce compliance costs specifically for data intermediary services, for example by making registration a voluntary process. The Commission will no doubt hope that this leads to a significant increase in their number, along with new measures announced in the Data Union Strategy, such as a new Data Act legal helpdesk on how to apply the new rules.

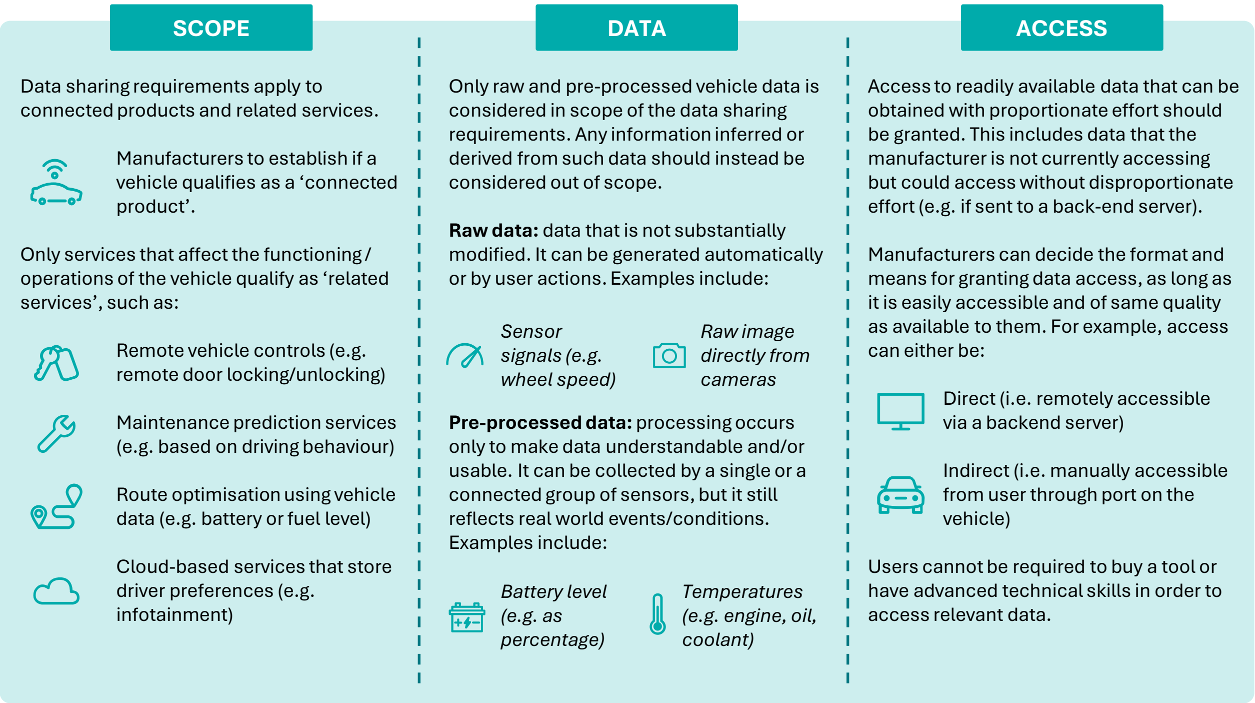
The majority of the **Data Act's data sharing provisions** came into force in September 2025, with in-scope companies required to provide users with indirect data access from a connected product or service (e.g. by the use of a third-party storage device) from that date. One important exception to this is the requirement to provide **direct data access from a connected product or service** (e.g. online), where relevant and technologically feasible, which will become fully applicable in September 2026. Other topics expected on the Commission's data economy roadmap during the year ahead include:

- Guidance on **reasonable compensation for data sharing** (something we have previously written about here).
- Guidance on the **read-across between data and trade secrets** (noting that the Digital Omnibus proposes strengthening protection of trade secrets in this respect).
- **Model contractual terms** on B2B data sharing.
- Further work on **data quality standards** (emphasising the need to define transparency, precision, accuracy, and timeliness of data for specific use cases).
- Development of **data capture standards** (such as data from sensors and cameras, easing use in AI model training, again highlighting the data/AI interdependency).

Case study – automotive data sharing under the EU Data Act

The Commission's recent **guidance on automotive data sharing** provides additional clarification on how the obligations in the Data Act should be interpreted in an automotive context, as illustrated in *Figure 13*.

Figure 13 – overview of the application of the EU Data Act in the automotive sector



SCOPE

Data sharing requirements apply to connected products and related services.

Manufacturers to establish if a vehicle qualifies as a 'connected product'.

Only services that affect the functioning / operations of the vehicle qualify as 'related services', such as:

Remote vehicle controls (e.g. remote door locking/unlocking)

Maintenance prediction services (e.g. based on driving behaviour)

Route optimisation using vehicle data (e.g. battery or fuel level)

Cloud-based services that store driver preferences (e.g. infotainment)

DATA

Only raw and pre-processed vehicle data is considered in scope of the data sharing requirements. Any information inferred or derived from such data should instead be considered out of scope.

Raw data: data that is not substantially modified. It can be generated automatically or by user actions. Examples include:

Sensor signals (e.g. wheel speed)

Raw image directly from cameras

Pre-processed data: processing occurs only to make data understandable and/or usable. It can be collected by a single or a connected group of sensors, but it still reflects real world events/conditions. Examples include:

Battery level (e.g. as percentage)

Temperatures (e.g. engine, oil, coolant)

ACCESS

Access to readily available data that can be obtained with proportionate effort should be granted. This includes data that the manufacturer is not currently accessing but could access without disproportionate effort (e.g. if sent to a back-end server).

Manufacturers can decide the format and means for granting data access, as long as it is easily accessible and of same quality as available to them. For example, access can either be:

Direct (i.e. remotely accessible via a backend server)

Indirect (i.e. manually accessible from user through port on the vehicle)

Users cannot be required to buy a tool or have advanced technical skills in order to access relevant data.

This guidance has a number of important implications for the operational, technical and governance processes that in-scope automotive manufacturers should have in place, for example:

- **Reviewing affected vehicle models** against the definition of a Connected Product (if not already done so) and taking a view on the basis on which data access should be granted, where applicable (including whether access is granted on a direct and/or an indirect basis).
- **Differentiating between in-scope data** (i.e. raw & pre-processed data) **and out of scope data** (i.e. inferred data), identifying where and how the data is generated.
- **Mapping all in-scope data** potentially accessible to the manufacturer and assessing the technical feasibility of accessing it.
- **Being able to demonstrate and justify the rationale** behind the format and means chosen for data sharing, for instance by gathering sufficient evidence through consumer preferences surveys or vehicle road testing.

In the **UK**, now that the enabling framework of the Data (Use and Access) Act is in place, the stage is set for the Government to introduce secondary legislation on the rules that will govern how smart data schemes will be rolled out in priority sectors. There has already been a flurry of Government and regulatory activity immediately following Royal Assent of the Act. This demonstrates that data sharing is seen as a central element of industrial growth, with the **UK Government industrial strategy** confirming that it will progress proposals for schemes in energy and financial services and explore the potential for schemes in other sectors, including transport, digital markets and property. It also reinforces the important role that data intermediaries have to play in realising this strategy, as well as the need for a joined-up regulatory approach, with the DRCF due to conduct work on how it can contribute to regulators' preparations for the **implementation of Smart Data**.

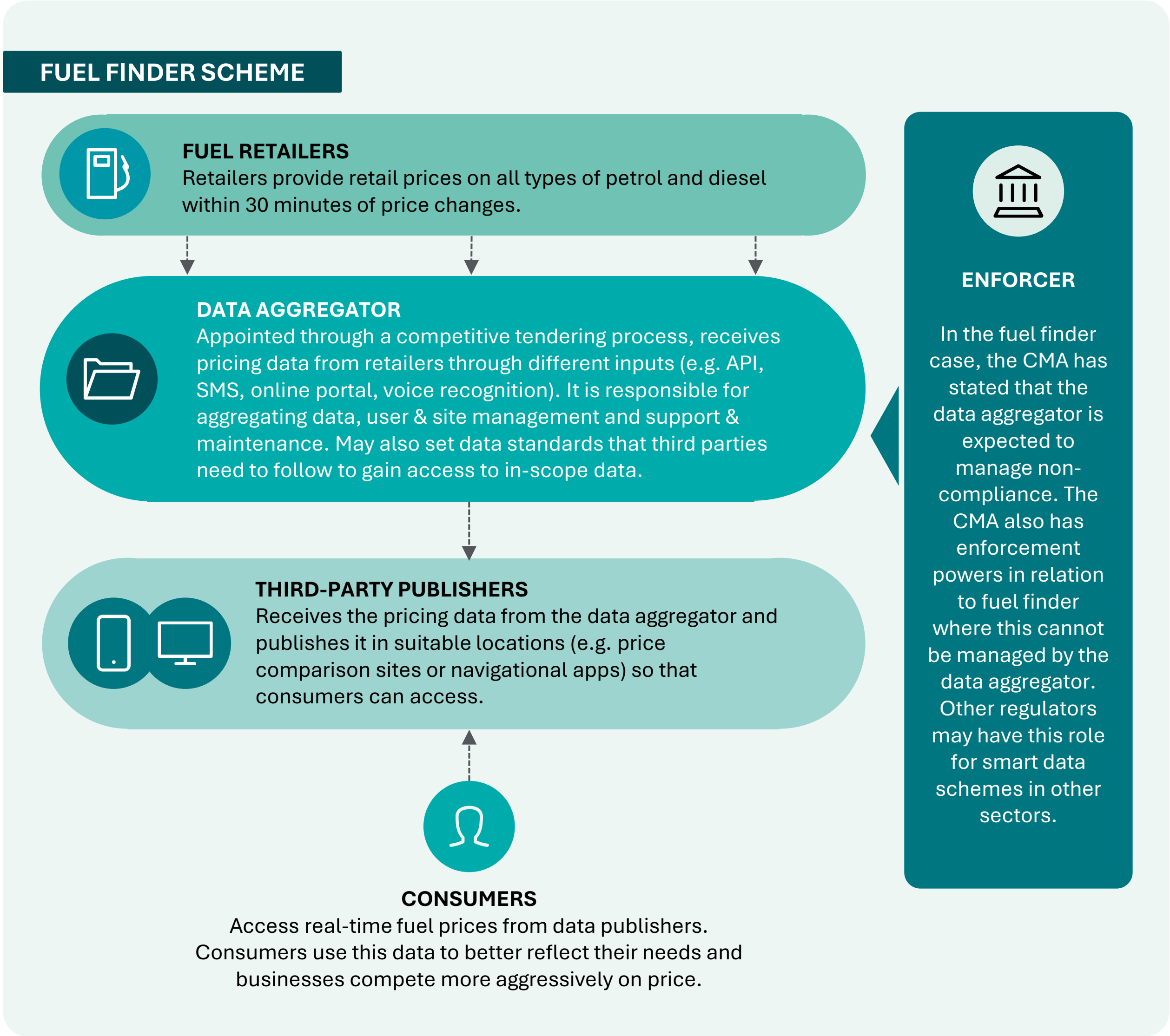
What might a UK smart data scheme look like? The Fuel Finder example

For an insight into a (relatively speaking) mature UK example, a good place to start is the **CMA's work on Smart Data pricing transparency**. This work has explored how price transparency schemes, enabled by new smart data legislation, can enhance consumer confidence in markets – particularly those where it can be difficult to search and compare options. The **UK's Fuel Finder scheme**, under which fuel retailers must start reporting price changes from 2 February 2026, was identified as being relevant in this context. *Figure 14* sets out a simplified overview of the scheme.

The interplay between smart data transparency and use of Agentic AI

This example also provides a simple illustration of how Agentic AI capability could help users automatically select the best deals. Generating, aggregating and sharing business data, such as pricing and product data, can help consumers (or their AI agents) make better-informed decisions and strengthen price competition in certain markets. In the year ahead, we expect there to be more **policy discussion on the interaction between Agentic AI and the availability of data sets in priority markets**, driven by smart data implementation. In digital markets for example, there is likely to be renewed interest in how Agentic AI can facilitate enhanced switching (building on previous work from Ofcom in this area, for example in relation to broadband switching). This is something that strategy teams at affected companies can start preparing for now.

Figure 14 – a simplified overview of the UK's Fuel Finder scheme



FUEL FINDER SCHEME

FUEL RETAILERS
Retailers provide retail prices on all types of petrol and diesel within 30 minutes of price changes.

DATA AGGREGATOR
Appointed through a competitive tendering process, receives pricing data from retailers through different inputs (e.g. API, SMS, online portal, voice recognition). It is responsible for aggregating data, user & site management and support & maintenance. May also set data standards that third parties need to follow to gain access to in-scope data.

THIRD-PARTY PUBLISHERS
Receives the pricing data from the data aggregator and publishes it in suitable locations (e.g. price comparison sites or navigational apps) so that consumers can access.

CONSUMERS
Access real-time fuel prices from data publishers. Consumers use this data to better reflect their needs and businesses compete more aggressively on price.

ENFORCER
In the fuel finder case, the CMA has stated that the data aggregator is expected to manage non-compliance. The CMA also has enforcement powers in relation to fuel finder where this cannot be managed by the data aggregator. Other regulators may have this role for smart data schemes in other sectors.

8. Digital Networks and Sovereignty

Business roadmap required

EXECUTIVE SUMMARY

There cannot be an effective digital ecosystem without the networks that convey the vast array of digital services on which we all rely. Reflecting this, the deployment and operation of digital networks is now bound up in a variety of tactical and strategic considerations central to broader geopolitical debate, such as competitiveness and sovereignty. Responding to the sovereignty agenda highlights the need for the development of a company-specific business roadmap, requiring alignment across affected internal teams (in particular External Affairs, Strategy, Commercial and Governance).

Further to the **Draghi** and **Letta reports**, the Development of a new **Digital Networks Act** to help boost high-speed broadband, support competitiveness and ensure affordable quality services for consumers in the **EU** is one of the Commission's strategic priorities for its current mandate. The wide-ranging regulatory debate is a dynamic one, setting positions on issues that could have a profound impact on the future development and deployment of fixed and mobile network infrastructure in the EU.

At the time of writing, the publication of the legislative proposal for a Digital Networks Act is imminent, delayed from Q4 2025. The initiative is expected to place a particular emphasis on the following:

- **Simplification** – such as the reduction of reporting obligations and simplified regulatory authorisations.
- **Mobile spectrum** – considering options such as greater harmonisation and longer licences.
- **Network access regulation** – assessing potential roll back of ex-ante regulation as well as measures to accelerate copper switch off.
- '**Level Playing Field**' – relevant to interactions between different players in the value chain and the application of net neutrality.
- **Regulatory governance** – options to enhance EU governance to reinforce the Single Market.

This initiative also incorporates a review and evaluation of the European Electronic Communications Code **(EECC)**, essentially the **EU's rulebook for companies operating and providing in-scope networks and services** in the EU.

This activity raises different issues relevant to the competition, innovation and growth agenda and has already been accompanied by an animated regulatory debate. We see four clear ways in which companies can respond to this ongoing initiative:

- **Evidence activities relevant to the potential new obligations** – to determine whether they are captured or otherwise relevant to the objectives of the legislative proposal.
- **Analyse existing regulatory obligations relevant to the simplification agenda** – working with governance teams in relation to existing requirements (e.g. reporting obligations), identifying any areas of potential disproportionality or duplication.
- **Review competitive positions relevant to in-scope regulation** – in order to identify any concerns/instances where the rollback of

existing ex-ante regulation would be likely to have a material adverse effect on the position of the company in the market.

- **Identify regulatory fragmentation** – where a fragmented regulatory approach across different EU countries may be unduly impeding or otherwise acting as a barrier to a harmonised deployment of services, consistent with the single market objective.

On a related theme, sovereignty is currently central to the **EU digital policy agenda**, driven by concerns about reliance on 'non-EU' providers in an era of persistent geopolitical headwinds. The concept itself, whilst not new, has also continued to evolve. Sovereignty is no longer just a question of where data is stored or whether companies from certain non-EU countries are involved in the digital network supply chain. It now brings in a variety of operational considerations related to the underlying software and broader network infrastructure (including third-party dependencies), as well as legal considerations such as company formation, decision making and control.

This trend is illustrated by the **European Commission's Cloud Sovereignty Framework**, published in October 2025, which applies to companies aiming to provide certain types of cloud services in the EU. The requirements reflect that the document was drafted in the context of a tender for sovereign cloud services to EU institutions, bodies, offices and agencies (i.e. requirements are tailored to meet the needs of an EU public authority). At the same time, it offers an articulation of how the Commission is approaching the concept of sovereign cloud, outlining principles that provide insight into the direction of policy on this topic. In the Commission's own words: *"The Cloud Sovereignty Framework is envisioned as a reference point for cloud providers and a catalyst for the growth of the EU cloud market, especially in the public sector"*.

In *Figure 15* below we set out the **EU** sovereignty objectives and related considerations that have been outlined as part of this new framework, summarising related actions that affected companies can consider to evidence sovereignty in response.

Figure 15 – EU Cloud sovereignty indicators and how companies can respond

SOVEREIGNTY OBJECTIVE	HIGH LEVEL DESCRIPTION RELEVANT TO COMPANY PROVIDING SERVICES*	STEPS THAT COMPANIES CAN CONSIDER TO EVIDENCE SOVEREIGNTY**
Strategic Sovereignty	Ownership stability, governance influence, alignment with EU strategic priorities.	• Ensure that bodies having decisive authority over company services are located within an EU jurisdiction. • Demonstrate investment, jobs and value creation within the EU.
Legal & Jurisdictional Sovereignty	Legal environment, exposure to foreign authority, enforceability of rights.	• Address any exposure to non-EU laws with cross-border reach. • Manage legal, contractual or technical channels by which non-EU authorities could compel access to data or systems.

**non-exhaustive, please refer to original document for a comprehensive overview*
***for indicative purposes only*

SOVEREIGNTY OBJECTIVE	HIGH LEVEL DESCRIPTION RELEVANT TO COMPANY PROVIDING SERVICES*	STEPS THAT COMPANIES CAN CONSIDER TO EVIDENCE SOVEREIGNTY**
Data & AI Sovereignty	Protection, control and independence of data assets and AI services.	• Ensure confinement of storage and processing to European jurisdictions. • Determine extent to which AI models and data pipelines are developed, trained, hosted and governed under EU control.
Operational Sovereignty	Practical ability to run, support and evolve a technology independently of foreign control.	• Ensure ease of migrating workloads or integrating with alternative EU-controlled solutions. • Assure that operational support is delivered from within the EU and subject exclusively to EU legal frameworks.
Supply Chain Sovereignty	Geographic origin, transparency and resilience of the technology supply chain.	• Manage degree of reliance on non-EU vendors, facilities, or proprietary technologies. • Ensure visibility into the entire supplier and sub-supplier chain, including audit rights.
Technology Sovereignty	Degree of openness, transparency and independence in the underlying technological stack.	• Demonstrate ability to integrate with other technologies via documented and non-proprietary APIs or protocols. • Ensure visibility of design and functioning of the service (e.g. architecture, data flows & dependencies).
Security & Compliance Sovereignty	Extent to which security operations, compliance obligations and resilience measures are controlled within the EU.	• Attain EU and internationally recognized certifications (e.g. ISO, ENISA schemes). • Ensure transparent, timely and EU-compliant reporting of breaches or vulnerabilities.
Environmental Sustainability	Autonomy and resilience of cloud services over the long term in relation to energy usage, dependency and raw material scarcity.	• Adopt energy-efficient infrastructure and measurable improvement targets. • Put in place transparent measurement and disclosure on sustainability indicators such as carbon emissions and water usage.

Sovereignty is also set to remain a live topic in the **UK** during 2026, with the Department for Science, Innovation and Technology **(DSIT)** expected to provide details of how it intends to approach digital sovereignty for use across the UK and for the UK public sector.

Linking Cloud and AI, an important **EU** policy driver is the objective of ensuring sufficient computational capacity, including sovereign computational capacity, for AI. **The Commission's AI Continent Action Plan** already made it clear that for highly critical use cases, including AI applications, sovereignty and operational autonomy require highly secure EU-based cloud capacity. The **Cloud and AI Development Act**, one of the headline initiatives of the European Commission's **Competitiveness Agenda**, is relevant to how this goal will play out in regulation. At the time of writing, a legislative proposal is expected by the end of March 2026.

It will be important for in-scope companies to review 'sovereign' use cases under the Cloud and AI Development Act and reconcile them against current service provision and strategic priorities. Some would likely be public sector (such as defence). However, the Commission has also been clear that the 'problem statement' extends into other economic sectors which exhibit highly critical use cases with high security needs. This could bring in energy and healthcare, for example.

Beyond cloud, AI and the Commission's **review of the EU Cybersecurity Act**, regulatory developments affecting other electronic communications networks and services, in particular **satellite** and **submarine cables**, are relevant to how the sovereignty debate plays out in the year ahead.

- The draft **EU Space Act** proposes new rules to apply to both EU and non-EU satellite operators, designed to ensure the safety (e.g. around disposal of satellites at end of life), resilience (focused on risk assessments to address potential vulnerabilities) and sustainability (e.g. around the use of environmental impact assessments) of relevant EU space activities. It is also influenced by an intention to address potential regulatory fragmentation for satellite licensing (given emerging approaches at Member State level).
- In addition, **further regulatory and policy developments relevant to submarine cables** are expected to include actions to improve coordination across the **EU**. This activity includes measures to strengthen governance structures and enhance security and resilience. It also provides for new investment to fund digital infrastructure projects, including smart subsea cables, prioritising strategic 'Cable Projects of European Interest'.

> *"It will be important for in-scope companies to review 'sovereign' use cases under the Cloud and AI Development Act and reconcile them against current service provision and strategic priorities."*

Developing a sovereignty roadmap

Sovereignty trends will be relevant to both companies operating strategic network technologies and corporate customers seeking to ensure their technology investment is suitably ‘future proof’.

We see four main ways in which companies can respond to the evolving sovereignty landscape, which will require effective alignment across affected teams (in particular External Affairs, Strategy, Commercial, Technology and Governance):

- **Map sovereignty risks and/or opportunities** – developing a company-specific sovereignty response should start with a review which maps relevant internal (e.g. commercial, strategic) and external (e.g. political and regulatory) factors. Although the Commission’s Cloud Sovereignty Framework will not be rolled out ‘like for like’ to other technologies, it provides a valuable insight into how the Commission is currently approaching this area, which could form part of an internal review.
- **Prioritise the greatest risks and/or opportunities** – there will be different levels of risks, and/or opportunities, depending on the nature of the company (e.g. the place of incorporation, the scope of business activities) and the application of the relevant factors. Prioritising the most material findings will provide a firm basis on which to proceed.
- **Develop a target-state activity/service view mapping** – to ensure that the company has an optimal sovereignty strategy that is complementary to its business strategy.
- **Develop a business roadmap to be reviewed on an ongoing basis** – this is a fast-moving area with dependencies changing in light of the evolving external political landscape. Ensuring that a business roadmap is in place, with check-in points enabling review on an ongoing basis, will therefore be essential. This will help guide future investment, legal entity and governance structures and activity/ service offering decisions.

Authors

Suchitra Nair

Partner
Head of EMEA Centre for Regulatory Strategy
snair@deloitte.co.uk

Robert MacDougall

Director
EMEA Centre for Regulatory Strategy
rmacdougall@deloitte.co.uk

Nick Evans

Senior Manager
EMEA Centre for Regulatory Strategy
nickaevans@deloitte.co.uk

Matteo Orta

Manager
EMEA Centre for Regulatory Strategy
morta@deloitte.co.uk

Giulia De Bernardi

Senior Analyst
EMEA Centre for Regulatory Strategy
giuliadebernardi@deloitte.co.uk

About Deloitte’s EMEA Centre for Regulatory Strategy

This document was written by Deloitte’s EMEA Centre for Regulatory Strategy (ECRS). The ECRS is a source of critical insight and advice, designed to assist clients to anticipate change and respond with confidence to the strategic and aggregate impact of regulation.

Acknowledgements

The authors would like to thank Nicola Sergeant and Jennifer McMillan for their input on the Global Introduction and Nick Seeber, Laurie Gilchrist, James Smith, Radha Gohil, Marcus White, Sian Bundred, Omar Rashid, Amber Andrade, Roger Smith, Susan Biddle, Valeria Gallo and Ben Thornhill for their contributions to the rest of the document.

Deloitte.

CENTRE *for*
REGULATORY
STRATEGY
EMEA

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.Deloitte.com/about to learn more about our global network of member firms.

MAKING AN
IMPACT THAT
MATTERS
since 1845