

# Digital Regulatory Outlook 2025

What to expect in UK and EU digital  
regulation in the year ahead

January 2025

# Contents



## **Introduction**



## **1. Online safety:**

sustained and evolving regulatory supervision



## **2. Researcher access to data:**

responding to the new EU framework



## **3. Competition in digital markets:**

further change expected



## **4. AI:**

adopting a multifaceted approach



## **5. Transparency, accountability & independent review:**

adapting to the new regulatory equilibrium



## **6. Data economy:**

achieving the data sharing vision



## **7. Cloud:**

crossing the regulatory Rubicon



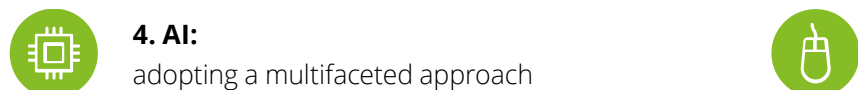
## **8. Media:**

responding to continued convergence



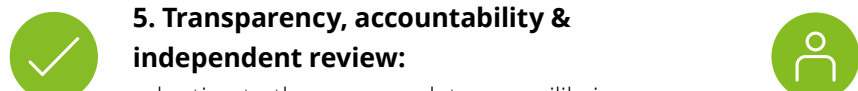
## **9. Consumer fairness:**

walking the end-to-end digital journey



## **10. Online choice architecture:**

ensuring fit for purpose processes and testing



## **Authors**

## Introduction

The **Digital Regulatory Outlook 2025** sets out our view of digital regulation which we expect to be particularly important in the year ahead, with a focus on the competition and consumer protection issues which companies across the internet ecosystem should be preparing for.

Approached from UK and EU perspectives, it is primarily written for Boards and Senior Executives of large digital and technology companies. As regulators increasingly prioritise action to ensure a fair consumer digital journey, it is also relevant to many business-to-consumer companies across the economy who may not have been 'born online', but for whom the internet is an important route to market.

Given digital is so central to how we live, work, transact and communicate, recent years have seen the finalisation of an unprecedented amount of digital regulation. As an overriding theme, 2025 is set to be a pivotal year in terms of the implementation of much of this regulation. In this document we set out key issues that affected companies should have on their radar, including on the following:

- **Online safety** and **competition** obligations, where we will see both the relative maturing of the EU regimes and the corresponding UK regimes coming into effect.
- A continuing regulatory focus on **AI**, coalescing around the key themes of risk, growth, competitiveness, and accountability.
- Important requirements in **cloud** and **data** markets, where there is a sustained regulatory emphasis on unlocking socioeconomic benefits in the interests of the market and end-users alike.
- An **increasing regulatory convergence**, for example between **media** and **online safety**, and **competition** and **AI**.
- How regulators are exercising **new supervisory regulatory tools** in order to promote **transparency, accountability** and **independent review** in digital markets and services.
- The new powers of the UK Competition and Markets Authority to **enforce a wide range of consumer law direct**, which should also be high on the Board and Executive agenda of consumer facing companies across the economy that have a significant online presence.

However, it is not just about implementation. At the start of the new European Commission mandate, and with a new UK Government in place, there is an emphasis on whether, and if so how, additional digital regulation should be introduced in certain areas. In the EU, this is relevant to topics such as addictive design

and the future regulation of digital networks, areas on which EU legislative proposals are expected in the year ahead. In the UK, additions to the online safety regime continue to be debated in Parliament, as does a new Data Bill.

More generally, political priorities such as **sovereignty, growth** and **competitiveness** are paramount. Digital regulation brings these factors into sharp relief, as well as broader considerations around **misinformation** and **disinformation**, topics that remain very high on the agenda at the start of the year. Many digital companies will be asking regulators for an emphasis on implementation of existing regulation, rather than the introduction of new regulation, in 2025. Given the evolving landscape, we do not see pressure from new digital regulation easing up any time soon. Either way, **the role that digital regulation has to play in today's society will continue to be central to the public, political and regulatory debate in the year ahead.**



*"We need to ensure a level playing field, security and a safe online space for our citizens. Everybody who wishes to do business in Europe has to follow European rules."*

**- Henna Virkkunen, Executive Vice-President of the European Commission for Tech Sovereignty, Security and Democracy, November 2024**

*"The safety spotlight is now firmly on tech firms and it's time for them to act. We'll be watching the industry closely to ensure firms match up to the strict safety standards set for them under our first codes and guidance, with further requirements to follow swiftly in the first half of next year."*

**- Melanie Dawes, Chief Executive, Ofcom, December 2024**



## Chapter 1

# Online safety: sustained and evolving regulatory supervision

### SUMMARY

*Sustained activity is expected under the Digital Services Act (DSA) in the EU in the year ahead which will further impact the governance, processes, and controls that in-scope companies will need to adopt. This includes priority areas such as protection of children, the supervision of marketplaces and the provision of data to researchers. Companies should also remain agile as the EU regulatory discussion evolves into new areas such as addictive design. In the UK, the Online Safety Act (OSA) compliance timeframes will start to bite, with affected online services being required to complete risk assessments, starting from March 2025.*

During 2024, the European Commission embraced its new regulatory responsibilities under the DSA with gusto, initiating a range of investigations and requests for information to the online services now subject to the new regime. We see three key themes arising out of this activity which we expect to continue in the year ahead:

- First, a continued priority will be the **protection of minors** online, with the Commission due to publish its guidelines on how platforms can mitigate risks related to the protection of minors and ensure a high level of privacy and security for children. Expected to be adopted in summer 2025, they will form a key part of the supervisory approach under the DSA. There are a number of important issues at play here, such as age verification, which have significant implications in terms of the processes that platforms should adopt. The Commission's position on such issues is expected to crystallise as part of its new guidance.
- Second, **marketplaces** will remain high on the supervisory and regulatory agenda, with a focus on areas such as notice and action mechanisms, traceability of traders and complaint handling systems. Member States are expected to keep up the pressure here, amplifying the call during 2024 for stronger EU market surveillance and enforcement in relation to the availability of online products which do not comply with applicable regulation (e.g. product safety). Providers of marketplaces in the EU should prepare for further detailed oversight.
- Third, **researcher access** – enabling vetted researchers to request access to Very Large Online Platform (**VLOP**) or Very Large Online Search Engine (**VLOSE**) data to study systemic risks – is likely to remain a key regulatory priority, in light of the long-awaited Delegated Act coming into force. This is something that we cover in more detail in Chapter 2.

More broadly, efforts to convert both the **EU Code on Illegal Hate Speech Online** and the **EU Code of Practice on Disinformation** into a DSA Code of Conduct will continue, with the European Board of Digital Services expected to make progress in this respect. It will be important for companies to be ready to demonstrate compliance with their commitments under these Codes as part of the audit obligations under the DSA. Another key update to look out for will be the European Commission's first report on **systemic risks** and their mitigation, to be published in

February 2025 at the latest. This will be another critical element in respect of the ongoing maturity of the regime. Other active areas in the year ahead will likely include a continued focus on the **transparency of recommender systems, adequacy of content moderation processes** as well as **deepfakes** and **AI**.

In terms of new legislative priorities at EU level, there is a clear read-across between the DSA and a number of the Commission's new priorities. For example:

- Concerns around **addictive design** already underpinned the Commission's DSA enforcement activity in 2024, and additional rules are expected in this area. The observation of the prevailing European Parliament report on this topic that “*despite a strongly evolving EU legal framework in the digital field, including the DSA or the AI Act, the issue of addictive design is not sufficiently covered in existing EU legislation*” is a strong signal of what is to come.
- **The use of dark patterns and online choice architecture (OCA)** has remained high on the regulatory agenda, relevant to a number of files including the DSA, and is also expected to be a central part of a potential new **Digital Fairness Act** (See Chapter 9 where we provide additional information on what this new Act might involve).
- Further targeted regulation to address concerns about **unlawful advertising**, already a feature of the DSA, is also possible under the new Commission's mandate.

Finally, the institutional side of the DSA remains an area where further progress is expected during 2025. The Commission has already initiated enforcement action against those Member States that have not fully implemented the regime (e.g. not fully equipping its Digital Services Coordinator (**DSC**)), which has left consumer complaints about national online services unanswered in a number of countries. The Coimisiún na Meán, the Irish DSC, has already been active in this area, requesting information to ensure platforms deal effectively with reports of illegal content online as well as finalising its Online Safety Code which sets binding rules for video-sharing platforms who have their EU headquarters in Ireland. We have [previously highlighted](#) how a range of companies within the scope of the DSA can prepare for such oversight. We would expect DSCs in other Member States to become active during 2025. In-scope online services at Member State level – e.g. online platforms not sizable enough to be designated as

VLOPs – should prepare for DSC muscle flexing.

In the UK, a key requirement for the 100,000+ online services that Ofcom envisages are within the scope of the new Online Safety Act is to carry out **regulatory risk assessments**. Details of the anticipated timeframes for completion of the required risk assessments for all online services within the scope of the OSA are set out in Figure 1 below. All affected companies can prepare for these requirements by taking a scalable approach, maintaining an end-to-end process, having an internal engagement strategy, putting in place effective governance & knowledge management and implementing an appropriate data strategy. This is something we have previously written about [here](#).

Like the Commission, Ofcom is also focused on the **protection of children**. Additionally, during the next year Ofcom will also be focusing on content that disproportionately affects women and girls by publishing draft guidance on assessing and reducing the risks to women and girls. Such guidance is expected to be published for consultation in February 2025.

**“In the UK, a key requirement for the 100,000+ online services that Ofcom envisages are within the scope of the new Online Safety Act is to carry out regulatory risk assessments”**

The **categorised service provider regime**, setting out the additional duties that will apply to some of the most widely used online sites and apps in the UK, will also be largely complete by the end of the year (in advance of coming into force during 2026). Ofcom has reinforced the importance of affected companies maintaining a dialogue with it as part of this process, whilst also highlighting it is ready to take strong action where required.

We also expect the **debate on the scope of the Online Safety**

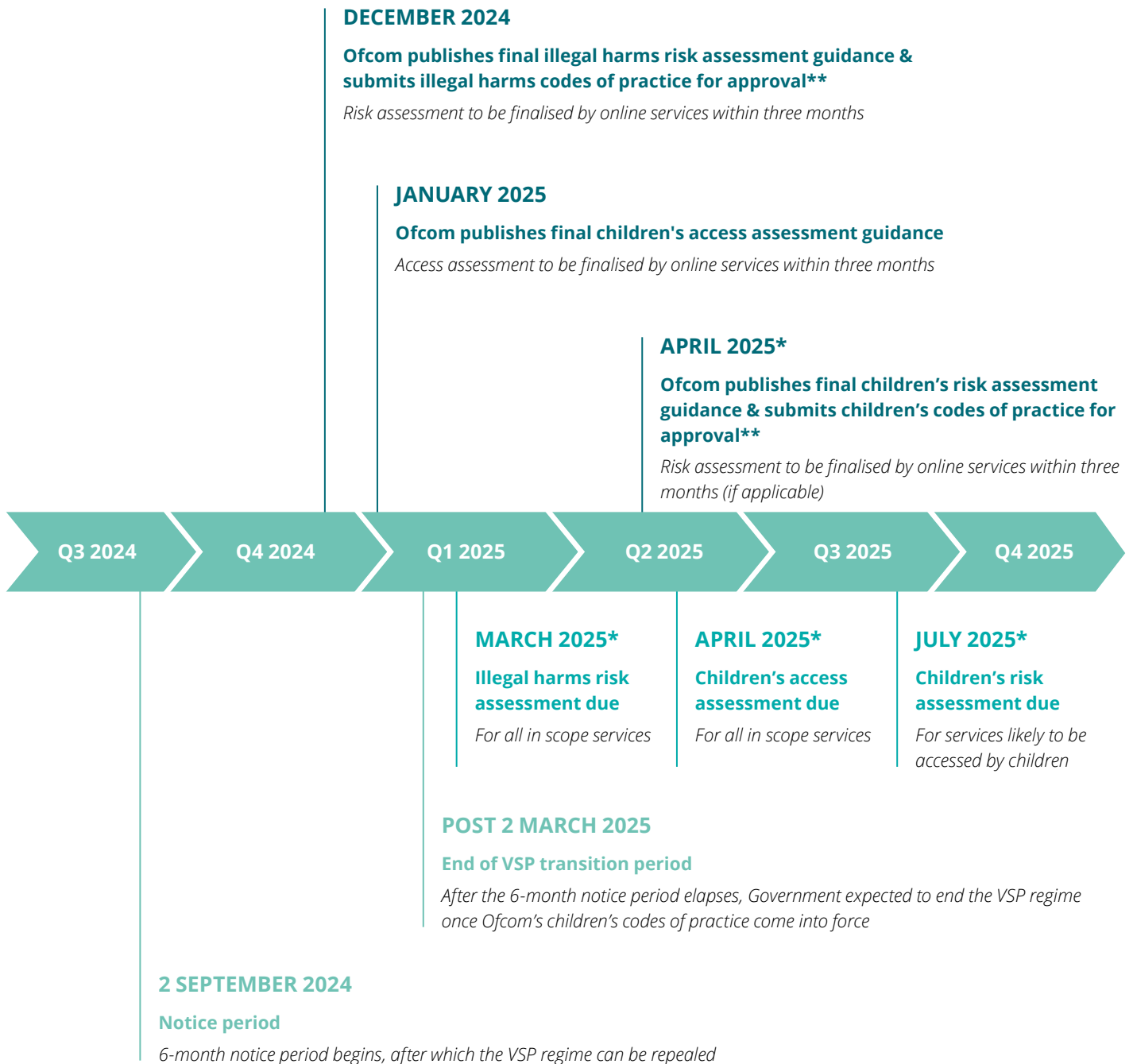
**Act** to continue, which may ebb and flow depending on external events (as we saw in the UK with the civil unrest in some areas during the summer). Relevant topics in this context are liability in relation to the onward sharing of abusive content and also ‘legal but harmful’ content. It remains to be seen whether there will be further debate around Ofcom’s approach to ‘small but risky’ platforms, given Ofcom’s previous response to the Government which set out how it intends to combat risks associated with such services under the OSA. It is clear the OSA may evolve over time given market developments and changing political priorities. Parliament has already been discussing regulation to update the priority offences to more comprehensively tackle image abuse. The **Online Safety Act 2023 (Priority Offences) (Amendment) Regulations 2024** broadens providers’ duties for intimate image abuse content. As the Minister for Data Protection and Telecoms said during Parliamentary debate, this regulation would require *“service providers to take proactive steps to search for, remove and limit people’s exposure to intimate image abuse content, including where it has been manufactured or manipulated and is in effect a deepfake”*.

Online services should also monitor the progress of both the **Product Safety and Metrology Bill** and the **Crime and Policing Bill**. The former Bill endeavours to ‘ensure a level playing field’ between the high street and online marketplaces, by clarifying responsibilities of online marketplaces in relation to the safety of goods placed on the UK market. This chimes with the abovementioned EU priorities in relation to marketplaces and product safety. The latter Bill is expected to include provisions relevant to online safety, such as sanctions on senior executives of online companies in order to tackle knife crime. This example also highlights a continuing trend of placing liability on individual company officers for non-compliance, following on from the Senior Manager liability provisions of the OSA (see Chapter 5 where we provide examples of such requirements, and others, in a digital regulatory context).





**Figure 1:** Timeline for completion of OSA risk assessments



#### Key

- Actions for service providers
- VSP regime - OSA transition
- Ofcom implementation of Online Safety Act

\* Please note this is a best-effort estimate, expected dates may be subject to change according to OSA implementation timeline

\*\* Ofcom will first submit the codes of practice to the Secretary of State. Subject to approval, they will then be laid in Parliament for 40 days. After passing through Parliament, the codes will come into force after a 21-day implementation period.

## Chapter 2

# Researcher access to data: responding to the new EU framework

### SUMMARY

*The provision of data by large internet companies to researchers is widely acknowledged as an important way of promoting a greater understanding of vital societal issues, such as the protection of children or the fight against disinformation. Now that the European Commission has published a Delegated Act on how the new EU regulatory framework will function, companies can prepare in earnest to address the prescriptive regime. Doing so will likely have a number of process, people, technology and governance implications. With the UK Government also proposing new requirements in this area, the topic will be a key one for in-scope companies in the year ahead.*

In the EU, the DSA requires that VLOPs and VLOSEs provide vetted researchers access to data with two broad aims in mind. First, to **study systemic risks** relevant to the online services provided. Second, to **assess the effectiveness of the risk mitigation measures** that have been put in place to reduce those risks. There is a wide variety of data that could be potentially requested by researchers under this regime, including content moderation data, advertising data and data relevant to the testing of new platform features prior to deployment.

Despite the DSA having become fully effective in February 2024, it has taken longer than expected for detail to be provided on how the researcher access regime will actually work, with the Commission's **draft Delegated Act** only being published for consultation in October 2024. That said, this text provides important clarity on how this new – and potentially complex and contentious – regime is intended to function. It covers areas such as the responsibilities that companies, researchers and regulators alike have to play in the process, as well as technical detail on how data should be transmitted to the researcher (along with the appropriate safeguards that might be required). With the Delegated Act expected to come into force in 2025, affected companies should be preparing for it now.

**“Researcher access has been an enforcement priority for the European Commission, within the scope of compliance investigations that have continued during 2024. We expect, therefore, that there will be significant attention on how the new regime is implemented in practice.”**

Before outlining how the new EU regime is intended to operate, it's worth taking a step back to provide policy and geopolitical context on the topic. It's an area that provokes a strong response amongst academic/research institutions, EU citizens and non-governmental associations, with these groups representing – by some distance – the main contributors to the Commission's earlier call for evidence on the subject. A subsequent technical report produced to support an EU-US Trade and Technology Council highlighted concern, noting that “a changing landscape of platforms' data access

*mechanisms and policies has created uncertainty and difficulty for critical research projects.”* Researcher access has been an enforcement priority for the European Commission, within the scope of compliance investigations that have continued during 2024. We expect, therefore, that there will be significant attention on how the new regime is implemented in practice.

The cornerstone of the regime as set out in the draft Delegated Act will be the creation of a new **DSA data access portal** to facilitate the management of the overall researcher data access process. The European Commission is responsible for establishing and hosting this portal. VLOPs & VLOSEs will need to ensure, amongst other things, that they:

- **Register** in this portal and **link to it** in their online interfaces.
- Make a **data inventory** of their services available online, as well as the data that is available and (where possible) proposed ways of accessing them.
- Ensure the **navigation** and **usability** of the accessed data, with companies required to provide researchers with the relevant metadata and documentation describing the data that is made available, such as codebooks, changelogs and architectural documentation.
- **Identify a mediator** and be **responsible for costs of the mediation**, in the event of a **dispute** arising relevant to the data being requested.

Another notable aspect of the new framework is the central role that each Member State DSC has to play (see Chapter 1 for more detail on the DSC framework). The DSC will oversee the transmission of data from the VLOP or VLOSE to the researcher established within their jurisdiction. This includes publishing an overview of the researcher request in the DSA data access portal and verifying whether the data access request meets the requirements of confidentiality, security and protection of personal data. The DSC will also consider any required mitigations relevant to the request (e.g. data access agreements or non-disclosure agreements) and ultimately determine how, from a technical perspective, the data should be shared with the researcher in question. Finally, the DSC will also participate in any dispute resolution relevant to the request for data.

**Researchers** obviously have an important role to play in this process too, ensuring that their request is consistent with

obligations outlined by the DSC, for example that they fulfil the requirements of data security, data confidentiality and protection of personal data.

Beyond the prescribed responsibilities that will be formalised in the finalised Delegated Act, the new regime will likely have a variety of different organisational implications for VLOPs and VLOSEs:

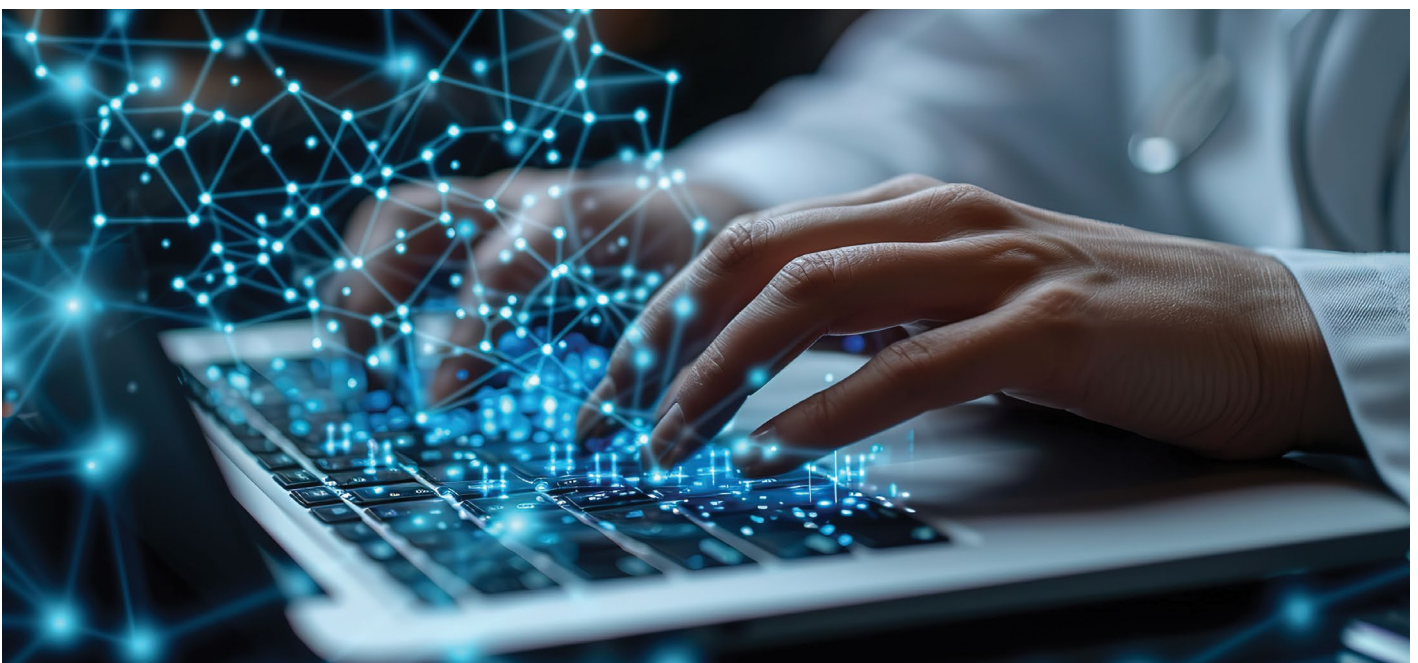
- **Effective governance** will obviously be a key consideration. It will be necessary to ensure that **data access requests are processed in line with the DSA** (e.g. that data is provided without 'undue delay'), the **Delegated Act** and **other applicable regulation** (e.g. the General Data Protection Regulation (**GDPR**)). In the event that the company does not agree with the request for researcher access issued by the DSC, appropriate governance will also be required relevant to the **submission of a possible amendment request**, and, potentially, to the **initiation and management of a subsequent dispute**.
- A **new dedicated process** may also be required to respond to data access requests, with internal guidelines on eligibility and supporting documentation (consistent with the requirements set out by the DSC). As the regime matures, it could also be helpful to establish a process that categorises the various data access requests based on their nature (e.g. standard and non-standard).
- From a **people perspective**, it will be necessary to identify the operational team who will handle the data access requests, and also interact with the DSC, if different. The other internal teams to be involved in the end-to-end data sharing process – e.g. privacy, security, legal – should also be

identified.

- Finally, **technology considerations** will be paramount, in terms of confirming the underlying tools and technology that will be used to transmit the data relevant to the request, as well as related topics such as content tagging and data modelling. A technology roadmap may need to be developed in order to provide access to relevant data sets.

Compared to the EU, the UK researcher access regime is currently very different in nature. The OSA does not currently create additional obligations for regulated services in this area. Instead, it requires that Ofcom produce a report setting out (broadly speaking) how, and to what extent, researcher access is currently provided by regulated services, along with ways in which greater access might be provided. This report must be submitted to the Government and published. That said, affected companies should closely track the progress of the new **UK Data (Use and Access) Bill**, introduced to Parliament in October 2024. This Bill proposes to amend the parts of the OSA relevant to how the UK researcher access regime would function, introducing the potential for the Government to introduce new, and more specific, requirements in this area.

In summary, there will be plenty for affected companies to assess and respond to in the year ahead. Some of this will be within their control, such as complying with the finalised Delegated Act, or considering the merits of the EU framework vis-à-vis the UK's proposed new approach. However, some of it will not (e.g. not all elements of the overall DSA regime are in place yet, with DSCs still not confirmed in all Member States). The challenge will be to start putting the jigsaw puzzle together in the knowledge that there are still some missing pieces.





## Chapter 3

# Competition in digital markets: further change expected

### SUMMARY

*The first year of gatekeeper compliance under the Digital Markets Act (DMA) in the EU has been something of an iterative compliance process, accompanied by initial market changes such as the emergence of some new third-party app stores. Affected companies should prepare for further change during 2025, with the extent of that change heavily influenced by the outcome of the first wave of gatekeeper investigations. In the UK, affected companies should expect the Competition & Markets Authority (CMA) to swiftly move through the gears to implement the new Digital Markets, Competition and Consumers (DMCC) Act which went live in January. The CMA is expected to launch two Strategic Market Status (SMS) designation investigation in January, with a third investigation expected to commence later in the year.*

During 2024 we have already seen some important emerging examples of how the interaction between the EU and UK digital competition regimes will play out in practice. In terms of consistency between the two regimes, we saw examples of changes in the UK being introduced by designated gatekeepers as a voluntary 'by product' of changes now required in the EU (e.g. in relation to the availability to UK consumers of a Data Portability API). We also saw the CMA reflecting on changes arising out of the DMA as part of its remedies thinking in an ongoing market investigation (choice screens relevant to mobile browsers). In terms of fragmentation between the two regimes, there has been at least one example of the DMA being cited by a gatekeeper as a reason for not rolling out AI functionality in the EU at the same time as the UK (due to concerns about the privacy and security impact of the interoperability requirements). As it stands, we would expect such fragmentation to be the exception rather than the rule, however much will of course depend on how the new UK rules are implemented. This is clearly an area to monitor in the year ahead.

**"With affected third parties such as app developers calling for greater visibility of testing and design data gathered by gatekeepers, testing and controls processes are expected to remain under the spotlight for the foreseeable future."**

The initial wave of Commission investigations, combined with the announcement of two new specification proceedings in September 2024 "to assist" a gatekeeper in complying with its interoperability obligations under the DMA, was a strong indication that the Commission is certainly not taking a 'hands-off' approach. 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 in the EU.

Clearly, the outcomes of the various investigations that the Commission launched during 2024 into the compliance of five

gatekeepers – following submission of the first gatekeeper compliance reports in March 2024 – will be important developments to look out for during 2025. The investigations themselves raise a variety of complex issues, and of course the gatekeepers under investigation have a right of appeal. The Commission has challenging investigative timescales on these cases, with all but one set to conclude by March 2025. We see four key themes to look out for arising out of these investigations, which are expected to impact market dynamics and the user experience going forward:

- First, **gatekeeper relationships with third party app developers** are clearly a key area of focus, with the relevant investigations expected to shape a number of operational, technical, commercial and contractual parameters relevant to these relationships going forward. This includes the extent to which app developers can provide pricing information within the app and conclude contracts through the distribution channel of their choice (e.g. within the app as opposed to via an external website). Other key areas relate to fees charged to third party app developers, the processes by which users download and install alternative app stores, and eligibility requirements for app developers. This topic is also of particular relevance to the business models of third-party payment providers.
- Second, as expected, the need for **appropriate online choice architecture (OCA)** underpins a number of the investigations. First, it is obviously a key factor in considering whether users are able to properly exercise their choice of web-browser. Second, it is material in the context of concerns about self-preferencing in vertical search (e.g. the display of search results in specific market segments, such as flights or hotels). Third, it has a bearing on processes by which users download and install alternative app stores. With affected third parties such as app developers calling for greater visibility of testing and design data gathered by gatekeepers, testing and controls processes are expected to remain under the spotlight for the foreseeable future.
- Third, the **interplay between the DMA and the GDPR** is also expected to remain a key consideration. It is notable that in September 2024 the Commission announced that the team in charge of DMA enforcement and the European Data

Protection Board had agreed to work together to clarify and give guidance on the interplay between the DMA and the GDPR. This guidance (as well as an updated joint statement from the UK's CMA and Information Commissioner's Office (ICO) on competition and data protection), should be on the radar of interested companies in the year ahead.

- Finally, the topic of **interoperability** is clearly a priority area. As already outlined, in September 2024 the Commission opened proceedings to specify a gatekeeper's obligations in this respect under the DMA. This case has two dimensions; the first to specify how the gatekeeper should provide effective interoperability relevant to notifications, device pairing and connectivity; the second in relation to the gatekeeper's process for addressing interoperability requests to ensure they are suitably transparent, timely, and fair. Specifying interoperability requirements is a non-trivial and highly technical exercise, therefore the outcome of this investigation will be an early indicator of the 'effectiveness' of the DMA in this respect.

The Commission may also take further action in respect of existing DMA designations, or even new DMA designations, as required. In relation to existing designations, the Commission will be expected to actively monitor how **AI capability** is being integrated into online search engines. Steps to either explicitly clarify that AI functionality is within the scope of an existing designation, or to expand an existing designation to include AI functionality, cannot be ruled out. In relation to new designations, the topic of **cloud computing services** could emerge again (along with voice assistants, one of only two Core Platform Services that has not yet been triggered under the DMA). Resourcing is likely to be a very practical consideration for the Commission regarding the number of new DMA related activities it pursues, given the range of resource-intensive compliance activity it has

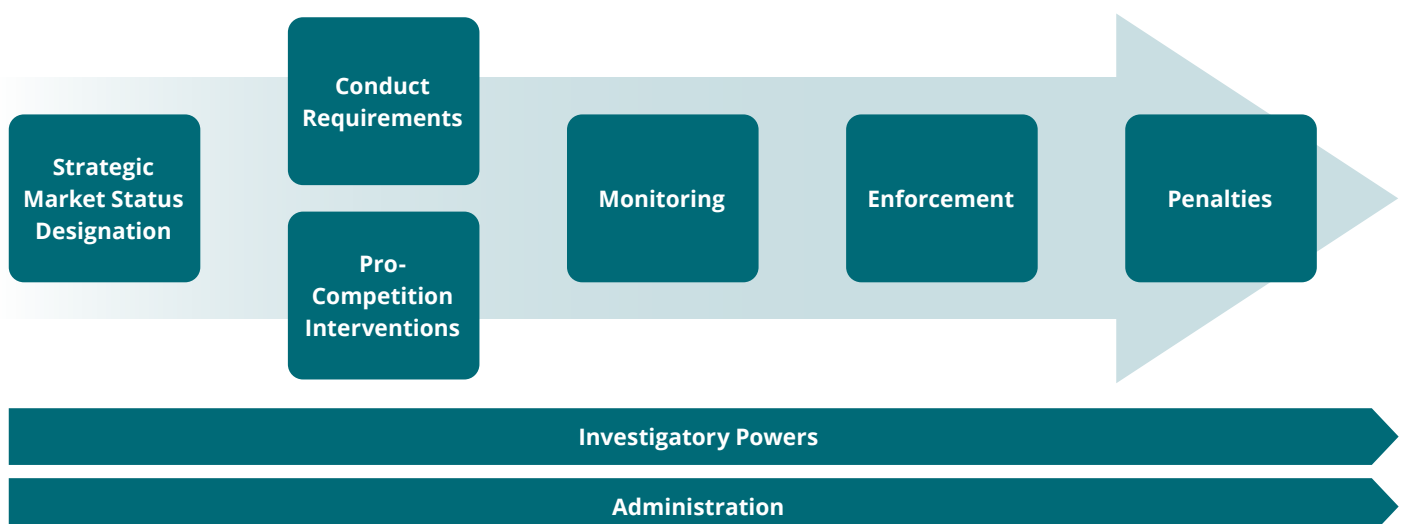
launched in the last year.

In relation to the **new UK competition regime, which is of course now live as of January 2025**, the CMA has already considered, or is considering, a number of different competition issues in digital markets, many of which are potentially relevant to its new powers under the Act. Consistent with the provisions of the Act, the CMA breaks down this regime into eight distinct areas, which we set out in Figure 2 below (note: this overview does not contain merger control requirements on SMS firms). We've already written about the [topics likely to be high on the radar of the CMA's Digital Markets Unit](#) as it implements the new regime. The CMA is certainly not starting from scratch; by leveraging this experience, and being cognisant of developments in the EU, affected companies should expect it to hit the ground running.

At the time of writing, the CMA was poised to commence **two SMS designation investigations** in relation to specific areas of digital activity, which may ultimately be regulated under the new regime. Each investigation will take up to 9 months, and the CMA has indicated it will consult on an initial set of proposed conduct requirements in parallel with these investigations. A third SMS designation investigation is expected to commence later this year. We have also previously written about the [actions that affected companies can take to prepare](#) for this. This includes the analytical tests that need to be met for designation with SMS, potential rules that could be applied to guide conduct, and also responsibilities relevant to any CMA investigations, monitoring and enforcement. The desire of the European Commission to incorporate the views of third parties and users has already been a feature of DMA implementation, as shown by the examples above. Given the CMA's stated objective to make the UK regime participative, there are benefits to affected companies pursuing a pro-active approach.



**Figure 2:** UK Digital Markets competition regime overview



## Chapter 4

### AI: adopting a multifaceted approach

#### SUMMARY

*More than any other digital topic, the transcendent nature of AI illustrates the potential risks, as well as the opportunities, presented by technological advancement. In the EU, a key area of focus will clearly be on implementation of the **EU AI Act**. However, there are a number of important areas for companies to focus on relevant to AI in the year ahead, centred around the themes of risk, competition, growth and accountability. Regulatory and policy developments in these areas will not just impact on companies in the technology sector, but companies across all sectors of the economy who integrate AI into their operations.*

It goes without saying that AI will be central to regulatory and policy priorities in 2025. This will manifest itself most obviously in regulatory activity specifically focused on AI (e.g. implementation of the AI Act, or the prioritisation of AI innovation opportunities). However, it will also be apparent in the context of the application of adjacent digital regulation relevant to AI (e.g. online safety or competition regulation). Of course, for some topics, there is likely to be ongoing debate (e.g. around accountability for AI related risks, or copyright protection), prompting consideration of whether further targeted regulatory intervention is required. We set out how companies can prepare for these issues, and more, by reference to the themes of **risk, competition, growth** and **accountability**, below.

#### Risk

Clearly, the implementation of the **EU AI Act** will need to be at the centre of company operational and governance priorities for those firms that place on the market or deploy AI systems in the EU. Firms should already be assessing which of their current and planned AI systems and models fall within the scope of this regulation and conducting a gap analysis against key requirements. There are two key deadlines below that firms should be aware of in the year ahead, along with further regulatory detail that is expected on each:

- The first area is the **ban on prohibited AI systems** (e.g. systems which infer emotions in areas of the workplace, except for medical or safety reasons), which will apply from February 2025. By this point firms should have completed their assessment of which of their current and planned AI systems are falling within this prohibition and developed a plan for remediation or decommissioning such systems.
- The second area are the **requirements for General Purpose AI (GPAI) systems and models** which will apply from August 2025. All GPAI models (such as large language models) are subject to transparency requirements to ensure fair allocation of responsibilities along the AI value chain. High-impact GPAI models deemed as posing systemic risks face additional stricter obligations, such as conducting model evaluations or adversarial testing. Again, firms should have reviewed their operations relevant to the development or deployment of GPAI systems and models by this date, responding accordingly. The publication of the first Code of

Practice setting out rules for GPAI model providers should also be on the radar of firms in this respect, as well as expected supplemental regulation on whether a GPAI model is systemic or not.

Responding to these requirements demands operational and cultural shifts to create effective collaboration across risk, legal, compliance, technology, and business teams. This should be underpinned by robust AI training programmes, not least to meet the AI Act's general requirement for **AI literacy** from February 2025.

As would be expected with what many view as the world's first comprehensive and legally binding cross-sector framework for AI, there is a significant amount of AI Act implementation activity to be expected in the year ahead. This is something we have [previously written about](#). One important area to look out for relates to the **technical standards** that will give firms a presumption of conformity with the AI Act. At the time of writing, standards bodies have been asked to complete this work by April 2025, although this deadline appears challenging. In addition, more detail on the **authorities that will oversee and enforce** the AI Act is expected, where not already confirmed. As an example, in October 2024, Ireland designated the nine different national public bodies that will uphold fundamental rights in high-risk AI systems, including the Media Regulator, the Data Protection Commission and the Financial Services & Pensions Ombudsman.

**“As would be expected with what many view as the world’s first comprehensive and legally binding cross-sector framework for AI, there is a significant amount of AI Act implementation activity to be expected in the year ahead.”**

In the UK, the new Government is expected to publish a consultation on **targeted new AI regulation** imminently, focusing on providers of the most powerful foundation models (such as LLM powering leading Gen AI systems). It is also expected to establish the formal legal basis of the AI Safety Institute. Beyond that, companies should remain alert to the possibility of UK regulators opening ‘test cases’ under UK regulation relevant to AI

deployment and use. Indeed, one such example is the open letter that Ofcom has already written to online service providers operating in the UK about how the OSA will apply to Generative AI and chatbots, with Ofcom stating that if companies fail to meet these requirements, it is prepared to take enforcement action, which may include issuing fines. We note that there have already been examples of AI enforcement in the US, including against firms that sell AI technology that can be used in deceptive and unfair ways, as part of the Federal Trade Commission's ongoing Operation AI comply.

## Competition

In the year ahead, regulators will remain live to potential competition risks posed by the development or deployment of AI, either through application of adjacent regulation, or ongoing targeted review.

As we noted in Chapter 3 potential competition concerns relevant to AI also arise in the context of the regulation of large digital platforms under competition regulation in the EU and the UK. This includes, for example, **integration of AI capability into search, or remuneration of the creative industries relevant to the use of AI**. Companies across the value chain should expect regulatory authorities to remain live to concerns relevant to competition and AI in the context of this new regulation. We cover copyright and AI in more detail in Chapter 8.

In terms of ongoing regulatory review, towards the end of 2024, the European Commission noted that it would remain vigilant to a number of concerns that may arise in relation to the development of GPAI models, including **access to data, AI accelerator chips, computing infrastructure, cloud capacity and technical expertise**. This should also be on the radar of companies across the value chain for whom AI is a key input.

In the UK, the CMA's ongoing review of AI foundation models (launched in May 2023) is clearly central to regulatory activity relevant to competition related considerations associated with AI. In May 2024 the CMA outlined three key overarching risks it had identified relevant to fair, open and effective competition in this area, expressing potential concerns about the **control of critical inputs**, the **distortion of consumer or business choice** and also **anti-competitive partnerships**. At the time of writing, an update from the CMA on this review is expected shortly.

## Growth

Given the desire of policymakers to unlock the economic benefits associated with AI, companies should identify opportunities associated with pro-innovation activities. This could have profound implications for firms either in, or providing services to, certain priority sectors (e.g. healthcare). In the EU, it is notable that growth featured as one of the areas to be prioritised in the first 100 days of the tenure of the new European Commission Executive Vice-President for Tech Sovereignty, Security and Democracy. This includes providing access to tailored supercomputing capacity for AI start-ups and industry through the **AI Factories** initiative, and

an **Apply AI strategy** to boost new industrial use-cases of AI. With potential pro-growth regulation emerging as a result, this should also be on the radar of affected companies, such as those who are seeking to incorporate innovative AI use-cases into their product or service development.

In the UK, the Government has signalled its commitment to AI as a pillar of its industrial strategy with the recent publication of its **AI Opportunities Action Plan**. The plan, commissioned in late 2024, outlines 50 recommendations, which the Government has now said it will take forwards (two of which with caveats). Key regulatory policy proposals include strengthening the AI Safety Institute, enhancing regulators' AI capabilities, and mandating annual reports on their support for AI-driven innovation. The plan also calls for copyright and intellectual property reforms to support AI innovation, which are currently under consultation (see Chapter 8 for more detail). AI is also a key priority of the newly established **Regulatory Innovation Office (RIO)**, set up to provide regulatory certainty and reduce unnecessary delays in order to drive economic growth. Initially focusing on engineering biology, space, digital healthcare and connected and autonomous technology, this creates an opportunity for companies to approach the RIO with examples which they consider relevant to their ongoing policy making in this area. This also creates an opportunity for lessons learned in these industries to be transferred more widely across the economy.

## Accountability

In the context of accountability, as policymakers maintain a close eye on emerging issues, firms should be reviewing their own operations to identify any issues relevant to **AI liability** across the supply chain and also looking at the contracts that they have in place with third party suppliers and partners. In late 2024 the European Parliament's research service issued a report with recommendations to reinvigorate the Commission's earlier AI Liability Directive proposal and turn it into a regulation for software liability more generally. With consumer associations also arguing this topic should be pursued, and the Hungarian Presidency of the Council of the EU having proposed further activity in this area during 2024, ongoing consideration of the topic is to be expected.

In the UK, it's worth recalling that DSIT's February 2024 statement on '**A pro-innovation approach to AI regulation**' confirmed that "*just under a third of respondents felt that the government should clarify AI-related liability*". The statement noted that DSIT would continue to consider potential obligations relevant to GPAI developers - such as pre-market permits, model licensing, accountability and governance frameworks. It also stated it would continue to consider introducing measures to effectively allocate accountability and fairly distribute legal responsibility to those in the life cycle best able to mitigate AI-related risks. Firms across the value chain should document and if appropriate share any issues relevant to their own experience in this area, given DSIT is still reflecting on its approach.





## Chapter 5

# Transparency, accountability & independent review: adapting to the new regulatory equilibrium

### SUMMARY

*Digital markets and services evolve quickly. The authorities that have now taken on responsibility for regulating these markets and services need to be similarly agile, using the new supervisory tools they have at their disposal. Given the information asymmetries at play, there are increasing regulatory demands for companies to ensure they can quickly and effectively respond to regulatory supervision, ensuring company officer accountability, and leveraging independent review, in a transparent way. Given the extent to which the use of digital services is ingrained in our everyday lives, regulatory priorities are also influenced by changes in the external landscape. There are actions that in-scope companies can take now to adapt to the new 'regulatory equilibrium' going forward.*

Regulation, and how it is implemented, can take many different forms. Compare the regulation of electronic communications (telecoms), financial services and digital services in the UK. Over many years, operators of telecoms networks and providers of telecoms services have seen their regulatory framework evolve. This has been characterised by distinct phases of policy development, complemented by various forms of regulatory intervention (and enforcement) to promote competition and protect consumers, such as access regulation and price caps. Telecoms companies, unlike financial services companies, would not have considered themselves subject to a 'supervisory' regulatory model. However, it is this supervisory model that has now become a key component of digital regulation, with Ofcom recently establishing a new supervision team to help implement its new Online Safety Act responsibilities. Supervision is described by Ofcom in this context as "a set of activities to manage Ofcom's relationships with services to understand and mitigate future risks and secure improvements in Ofcom's focus areas of Governance, Design and Operations, Choice and Trust".







**The swathe of new digital regulation requires firms to be able to demonstrate to the appropriate authorities that they are complying with their obligations in a responsive way,** leveraging company officer accountability, independent review and transparent systems and controls in the process. We have already seen some initial examples of this new supervisory approach during 2024 (e.g. publication of the first independent audit reports under the DSA, described by the European Commission as a "step-change in transparency and accountability"). There are expected to be a number of further developments in relation to the application of this new supervisory model to digital markets and services in the year ahead (e.g. in relation to the role of AI assurance, accountability of senior managers or use of skilled person reports). As digital regulatory regimes mature, these developments provide affected firms with important indicators on how regulators are approaching these new responsibilities, along with associated learnings that can be derived.

We set out a number of examples in Figure 3 below that we think highlight how an increased emphasis on accountability, independent review and transparency is playing out in this new digital regulatory domain, along with some initial strategic

implications arising. We then draw out three concluding observations on how companies can respond to the new 'regulatory equilibrium' going forward, focusing on **preparation, culture and responsiveness**.



**Figure 3:** Emerging examples of digital regulatory obligations relevant to transparency, accountability & independent review

AREA	SUMMARY OF REQUIREMENT	INITIAL STRATEGIC IMPLICATIONS
 EU DMA – consumer profiling audit	Gatekeepers are required to provide independently audited reports on consumer profiling techniques which provide information on techniques used for profiling of consumers relevant to the core platform services that they provide. This is a requirement that is rooted in transparency.	There does not yet appear to be a consistent approach on the information to be included in these reports, with differences in the level of detail across the different gatekeepers in question. The DMA envisages that the Commission may adopt an implementing act to develop the methodology and procedure of this audit going forward.
 EU DSA – compliance audit	VLOPs and VLOSEs are subject to an annual audit, carried out by an independent auditor (not to be confused with statutory accounting audits), to assess their compliance with their DSA obligations and with any commitments undertaken pursuant to codes of conduct and crisis protocols adopted.	Clearly this is the first step in an ongoing process. Comparable services should be able to leverage experience as experience evolves, both in terms of measuring controls (e.g. processing a complaint in a specific number of days), and approaches to risk mitigation (e.g. how to approach the safety of minors).
 UK AI policy – assurance policy	DSIT has recently highlighted that independent AI Assurance is a “a crucial component of wider organisational risk management frameworks for developing, procuring, and deploying AI systems, as well as demonstrating compliance with existing - and any relevant future – regulation”. The Digital Regulation Cooperation Forum’s ( <b>DRCF</b> ) recent review of AI Assurance highlighted stakeholder feedback on importance of well-defined, universally accepted standards in this context.	Ongoing Government policy in this area (e.g. the development of a roadmap to trusted third-party AI assurance) and further regulatory review (e.g. the DRCF’s ongoing work) should be on the radar of firms who use or provide AI systems. Companies should consider the interplay between regulatory requirements on one hand, and independent assurance best practices on the other, in the round.
 UK OSA – Senior Manager accountability	Key priorities for Ofcom will be to ensure that firms have strong safety governance and that they design and operate services with safety in mind. Where Ofcom decides to exercise its supervision powers in respect of achieving these objectives, it may issue an information notice as a first step. This must name a Senior Manager with responsibility for ensuring compliance with Ofcom’s requests.	There are many leading practices that in-scope companies can take in relation to Senior Manager accountability, something we have previously written about <a href="#">here</a> (e.g. affected Senior Managers should have a Statement of Responsibilities clearly stating what they are accountable for). Firms can already begin to consider the new obligations that may be expected in relation to Senior Manager responsibilities in this respect.
 UK DMCCA – nominated officer accountability	A company designated with SMS must have in place a nominated officer responsible for each competition requirement to which it is subject. The nominated officer must monitor the SMS company’s compliance with applicable obligations, cooperating with the CMA to secure compliance and compliance reporting.	Companies can plan for potential identification of nominated officer(s) who may need to demonstrate compliance with these requirements. Given the potentially substantive nature of the obligations across different business units, individuals could require upskilling.
 UK OSA & DMCCA – skilled person reports	Both Ofcom and the CMA can require the appointment of a ‘skilled person’ to (broadly speaking) assist in identifying and assessing a compliance failure, or a possible compliance failure, along with possible risk mitigation. Either the company, or the authority, may appoint an appropriate skilled person, who is usually an independent third party. This technique has long been used in UK financial services regulation, to support the FCA’s supervision and enforcement functions.	According to the FCA’s 2024 Annual Report, it used its skilled person powers in 83 cases during 2023/24 (with the firm being required to appoint the skilled person in the majority of cases). The reviews addressed areas such as controls and risk management frameworks, corporate governance arrangements and culture. It’s still early days for Ofcom and the CMA as far as the use of skilled person reports is concerned. However, if the FCA’s experience is anything to go by, firms should prepare for its increasing use over time, as well as an onus on the firm to nominate the independent skilled person, which will then be subject to regulatory approval.

## Conclusion

In light of these (non-exhaustive) examples, there are a number of steps that companies can already take to respond to the new 'regulatory equilibrium' going forward.

In terms of **preparation**, companies can already begin to map out how regulators may use these new supervisory tools relevant to their activities. Some (e.g. audits) are recurring. Others (e.g. use of skilled persons reports) will be more ad-hoc. Organisational processes and governance relevant to current, and potential obligations, should be considered in the round.

In addition, an understanding and appreciation of how these supervisory tools may be used should be embedded into a company's **culture**. On a practical level, compliance can be built into people management policies and practices, including performance management, training, role descriptions, pay and bonuses.

Finally, a **responsive** approach is key. Authorities have already sought to increase transparency and accountability on priority topics that have been influenced by external events. One example is the focus on an independent review of company adherence to the EU Code of Practice on Disinformation, which was influenced by concerns around election interference. Companies should have in place early warning indicators around how consumers are engaging with their services and any emerging risks in the context of broader social, economic or political developments. Companies should in turn consider how these may trigger use of these new supervisory regulatory tools.

**"Companies should have in place early warning indicators around how consumers are engaging with their services and any emerging risks in the context of broader social, economic or political developments. Companies should in turn consider how these may trigger use of these new supervisory regulatory tools."**



## Chapter 6

# Data economy: achieving the data sharing vision

### SUMMARY

*Realising the opportunities associated with data remains high on the political and regulatory agenda. In the EU, focus is on the implementation of new data sharing regulation, as well as steps to create an 'EU Data Union' under the new Commission mandate. The **EU Data Act** in particular has a variety of strategic implications relevant to data sharing for companies across the economy, with further steps likely to be taken by the relevant authorities in order to ensure it is on the corporate agenda. In the UK, companies should track progress of the **Data (Use and Access) Bill**, a priority for the new Government, in particular the Smart Data provisions which are also designed to unlock economic growth via increased data sharing.*

Data policy remains a key part of the new European Commission mandate, with the incoming responsible EU Commissioner having a mission to "present a European Data Union strategy, drawing on existing data rules to ensure a simplified, clear and coherent legal framework for businesses and administrations to share data seamlessly and at scale, while respecting high privacy and security standards". With the **EU Data Act** becoming applicable in September 2025, building on the framework that already applies under the earlier **EU Data Governance Act**, the following year is set to be an integral one in terms of the implementation of new data rules. Much of this activity is aimed at achieving the socioeconomic benefits associated with sharing non-personal data across the economy.

As it stands, it seems to us that there is a lot of work still to be done to fully realise this regime, with two observations on the Data Governance Act appearing relevant in this respect. First, the Data Governance Act envisages a key role for a new wave of data intermediation services that will emerge to play a key role in the data economy (e.g. the 'neutral third party' that will facilitate this commercial data sharing, such as data marketplaces). At the time of writing, Member States have notified only 12 data intermediation services in the EU, indicating there is scope for further progress in this area. Second, in May 2024 the European Commission initiated infringement proceedings against 18 Member States for failure to comply with the Data Governance Act (e.g. designation of responsible authorities at national level). In sum, some key elements of the regime still need to be put in place.

Therefore, **we think it is likely that not all the companies that are affected by this new suite of data regulation have the required awareness of it** (contrasting with the level of company awareness regarding GDPR compliance, for example). As a result, we expect that the Commission, in collaboration with the bodies tasked with responsibilities under the Data Act at national level, will continue to generate awareness of these new rules. And that in due course, designated competent authorities at Member State level (working closely with the European Commission) will seek to take enforcement cases to demonstrate their application.

With this in mind, compliance with the **Data Act raises significant questions for company business models where data plays a central role**. For example:

- From a **Business-to-Consumer** (B2C) perspective, how

should a manufacturer of a smart home device provide the user with data generated by that device?

- From a **Business-to-Business** (B2B) perspective, how should an automotive manufacturer comply with the Data Act when sharing data with a financial services firm/insurance company seeking to develop new or optimise existing business models?
- From a **Business-to-Government** (B2G) perspective, how should a company respond to a data request from public sector bodies such as the European Commission or the European Central Bank in the event of an exceptional need?

These data sharing scenarios raise a variety of technical, legal, commercial, operational and governance questions for companies across the economy, something [we have recently written about](#) in the context of the interpretation of the requirement for data holders to share B2B data with data recipients in a 'fair, reasonable and non-discriminatory' manner. Overall, we think companies should respond in three key ways in order to prepare:

- First, **establish the current state and readiness** of the business for the Data Act. This should include stakeholder interviews and documentation review, a gap analysis against a reputable framework that includes key changes and collation of findings and recommendations.
- Second, **business ambitions and risk appetite should be defined** with senior stakeholders. This should include consideration of the firm's strategy around data sharing more broadly, including those relevant to strategic opportunities (in terms of sharing data and/or seeking access to data) and also pricing considerations.
- Finally, a **plan should be developed to close gaps to meet business ambitions**, for example by exploring opportunities or updating processes as required.

Firms should also monitor any updates relevant to the obligations. On this point, there are a number of important Commission-led implementation activities that companies should have on their radar. This includes the following:

- From a technical perspective, this includes a European Commission standardisation request on a trusted data interoperability framework relevant to EU Data Spaces (further to Article 33 of the Data Act). This request is currently under



consultation with relevant stakeholders, including European standards organisations, with the formal adoption of this request expected shortly.

- From a legal and contracting perspective, a Commission recommendation is expected before 12 September 2025 on **model contractual terms** on data access and use, including terms on reasonable compensation and the protection of trade secrets to assist parties in drafting and negotiating contracts with fair, reasonable and non-discriminatory contractual rights and obligations.
- From a commercial perspective, **Commission guidance on reasonable compensation** is expected after the Data Act becomes fully applicable in September 2025, given the need to consult the newly formed European Data Innovation Board first.

More broadly, there is a read-across between the objectives underlying this recent data regulation and other EU digital regulation. The topic of **synthetic data** (data which mimics 'real world' data) brings this interdependency to light. Synthetic data has the potential to help businesses determine how best to extract value from with the data they generate, mindful of GDPR considerations in B2C scenarios. It is also expected to play an increasingly important role in AI model training (such as the development of autonomous driving systems), raising considerations around the application of the AI Act and applicable sector specific regulation. Companies should take an end-to-end approach when developing required compliance strategies.

In the UK, the primary focus will be on the passage of the new **Data (Use and Access) Bill**, introduced to Parliament in October 2024. From a data economy perspective, the **smart data schemes**, which aim to secure sharing of a customer's data upon

their request with authorised third-party providers, are of particular relevance. The UK Government confirmed in its recent **Industrial Strategy Green Paper** that once this legislative framework is in place, consumers can be empowered to share their data with a range of industry sectors, **encouraging the economic growth seen under Open Banking**. Indeed, in September 2024 the CMA confirmed that the nine banks mandated under the Retail Banking Market Investigation Order have now completed the final Roadmap for Open Banking. **With an open banking ecosystem now valued at over £4 billion**, this helps to explain the continued policymaker ambition to realise these benefits across other sectors of the economy.

The earlier **Data Protection and Digital Information Bill** (which did not make it through the final Parliamentary wash-up of the previous Government) also contained smart data proposals similar are those set out in the new Data (Use and Access) Bill. On the assumption the sectors previously identified by DSIT in this area remain a priority from a Government policy perspective, companies in the **energy, banking, finance, retail, transport, homebuying and telecoms** sectors should continue to track the evolution of the Bill, building on the prior policy work carried out by DSIT and others.



**“These data sharing scenarios raise a variety of technical, legal, commercial, operational and governance questions for companies across the economy.”**



## Chapter 7

# Cloud: crossing the regulatory Rubicon

### SUMMARY

*Cloud service provision underpins many different activities in multiple sectors of the economy. Given its vitally important role across commercial and digital ecosystems, regulatory scrutiny is intensifying. 2025 promises to be a landmark year for European cloud policy and regulation on themes relevant to competition, AI, operational resilience, sustainability and sovereignty. A continued, intensifying regulatory dialogue is expected on all of these topics. In the short term, the activation of new regulatory obligations that have been implemented with multi-cloud policy objectives in mind (e.g. switching and operational resilience) will affect cloud service providers and customers alike.*

In the EU, the obligations in the Data Act which give customers a **new right to switch between cloud computing services** will come into effect in September 2025. The required changes, which aim to foster a multi-cloud approach, have implications for technology, commercial, strategy and legal teams across providers and customers. There are two specific European Commission-led implementation activities to look out for in the year ahead:

- On the technology side, the launch of the **common EU repository on interoperability of cloud services** will aim to drive a harmonised, transparency approach in this area. As a result, cloud providers will be required to ensure that the interfaces they make available to customers are compatible with the standards/specifications referenced in this repository.
- On the legal side, a **Commission Recommendation on standard contractual clauses for cloud computing** is expected. These clauses cover topics relevant to switching, security, business continuity and liability and can be adapted by providers and customers according to their contractual needs.

In relation to pricing, certain cloud service providers have already signalled the removal of a number of **data egress charges**, further to the obligations in the EU Data Act regarding their ultimate removal (by January 2027). However, due to the multifaceted nature of these charges, we don't expect the regulatory dialogue to end there. In its 2024 working paper on egress charges the UK CMA noted that the terminology and definition of these fees are not consistently used by cloud providers, and that changes made to date related to switching only and not multi-cloud use. The Data Act already provides for a potential additional regulation in this area, in the form of a Delegated Act to introduce a mechanism for the Commission to monitor switching charges, consistent with their reduction and ultimate withdrawal. Further Commission oversight in this area would not be surprising, something that will also likely become clearer by the end of 2025.

In the UK, clearly the final outcome of the CMA's cloud services market investigation (covering topics such as switching,

interoperability, egress charges and software licensing practices) is of central relevance to competition in the UK cloud services market. The conclusion of this investigation is expected by August 2025.

In summary, this activity evidences the shift to ex-ante regulation of the market (even aside of the ongoing debate around **'cloudification'** of telecoms markets and **implications for future EU regulation**, something the European Commission already consulted on during 2024). This trend is also illustrated by the fact that many national regulatory authorities for electronic communications are expected to be tasked with overseeing these obligations under the Data Act (leveraging their experience of regulating these topics in telecoms markets). Indeed, the draft 2025 work plan of the Body of European Regulators for Electronic Communications (**BEREC**) envisages that BEREC will contribute expertise on switching between service providers, the monitoring of switching charges, interoperability and complaints handling. These are complex markets, so change will be iterative. Nevertheless, cloud service providers and end-users alike should prepare for further discussion of whether new regulatory oversight is required, something that is of course already evident in the context of the Data Act.

### Competition

Potential **competition** concerns relevant to access to cloud computing capability also underpin ongoing regulatory scrutiny of **AI**, although these considerations are at a much less advanced stage. EU, UK and US authorities have already highlighted the key role that cloud has to play in training AI models, highlighting the criticality of access to compute. The CMA's work on **foundation models** has included a forward-looking assessment on the potential impact of foundation models on how competition works in the provision of cloud services. Activity to increase the **availability of compute** is also high on the political agenda. In the coming year, the Commission is expected to take forward proposals for a new **EU Cloud & AI Development Act**, to increase computational capacity and create an EU-wide framework for providing 'computational capital' to SMEs. More detail on what that will include is expected in the coming year. The funding of additional compute capacity has also been a live political discussion in the UK during 2024, set to continue into 2025.

## Sovereignty

Sovereignty will remain a key policy priority in the year ahead. The influential Draghi report, published in 2024, clearly stated that *“it is important that EU companies maintain a foothold in areas where technological sovereignty is required, such as security and encryption (“sovereign cloud” solutions)”*. The subsequent inclusion of the term ‘sovereignty’ in the job title of the new EU Digital Commissioner further highlights the Commission’s emphasis on this area. To achieve this goal, the Draghi report recommended *“adopting EU-wide data security policies for collaboration between EU and non-EU cloud providers, allowing access to US hyperscalers’ latest cloud technologies while preserving encryption, security and ring-fenced services for trusted EU providers.”* Of course, there has been a challenging discussion for some years now regarding the inclusion of so-called ‘sovereignty’ requirements as part of the development of an EU Cloud Certification Scheme by the EU Agency for Cybersecurity (ENISA). This scheme is required under the existing EU Cybersecurity Act. At the time of writing, this scheme has still not been finalised, with different views still apparent on the sovereignty provisions at Member State level. Given the increased focus on sovereignty as part of the new European Commission mandate, providers should expect this discussion to intensify and deepen in the year to come.

**“Given the increased focus on sovereignty as part of the new European Commission mandate, providers should expect this discussion to intensify and deepen in the year to come.”**

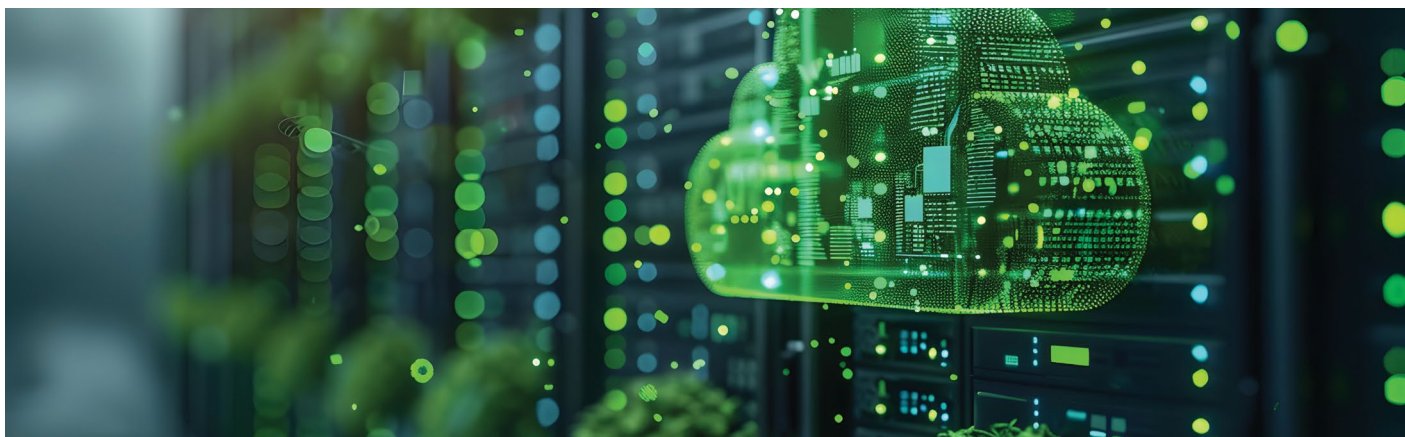
Mixing the themes of sovereignty and competition, the Commission is also expected to prioritise the development of a single EU wide cloud policy for public administrations and public procurement, in light of the Draghi report’s goal to *“level the playing field for EU companies against larger non-EU players”*. Cloud service providers with significant public sector activity or aspirations should also have this development on their radar.

## Sustainability

**Data Centre sustainability** will also remain high on the regulatory agenda. 2024 saw an increasingly high-profile debate in a number of countries (e.g. Ireland) in relation to climate goals and data centre use. Developments in other countries in the year ahead, such as provisions of the **German Efficiency Act** coming into force which require operators of data centres to set up compliant energy and environment management systems by July 2025, clearly necessitate operational and strategic review. 2025 will also see the second year of reporting required under the EU’s recent Delegated Regulation under the **Energy Efficiency Directive** on the energy performance and sustainability of data centres. The reported data is to be used to assess in 2025 whether targets on sustainability metrics (currently self-regulatory in the Climate Neutral Data Centre Pact) should be legislated. In summary, internal processes and controls relevant to data centre sustainability governance and reporting is an area that is only expected to receive more policymaker attention going forward, given that achieving net zero for data centres will be a long-term goal in the EU.

## Operational Resilience

Finally, 2025 also looks set to be a landmark year for cloud service provision and **operational resilience** obligations relevant to the provision of services to financial services companies. The EU’s Digital Operational Resilience Act (DORA) became fully applicable on 17 January 2025, allowing financial services regulators to directly supervise key third-party providers designated as ‘critical’. The UK’s first designations under a comparable regime are also expected in the first half of 2025. We wrote about the [finalisation of the UK Critical Third Party regime](#) in late 2024. Cloud service providers are likely to be in scope of both these regimes from the outset, something we have [also previously written about](#). Both regimes involve a new supervisory approach, with the UK regime (as an example) including remedies such as the ultimate prevention of a non-compliant provider from serving a regulated financial services firm. Providers should therefore ensure they put in place the required systems, processes, people and third parties relevant to the delivery of services to financial services clients.





## Chapter 8

# Media: responding to continued convergence

### SUMMARY

*The introduction of new media regulatory frameworks in both the UK and the EU raises strategic, operational, commercial and technological considerations for the companies concerned. A key driver for this new regulation has been technological change, which is transforming how people listen to, and watch, media content. This highlights both the increased pace of convergence between the content and online services segment and also an increasing regulatory interdependency between media regulation and digital platform regulation. The relationship between media owners and AI developers (e.g. in the context of copyright and AI) and digital platforms more generally (e.g. via new digital markets competition regulation) also remains highly relevant.*

In the UK, Ofcom's focus will be on implementation of the new **Media Act**, which represents the first major update to UK media legislation in over 20 years. The Media Act has a number of different elements, relevant to regulation of topics such as public service television, listed events, availability and prominence, video on demand and regulation of radio services.

This includes new rules to ensure online **Public Service Broadcasting services** are both available on popular TV platforms and capable of being easily found and discovered by audiences. **Availability & Prominence of media content** across digital platforms is also a key consideration, with new duties for different voice-activated platforms. There will be new duties for **video-on-demand (VOD)** services with the introduction of many new requirements designed to ensure these services are subject to a similar set of rules to broadcast television. This includes obligations in relation to the compliance of content and also accessibility provisions (such as the provision of subtitling, audio description and signing). Finally, in relation to listed events (such as the Olympic Games), instead of being restricted to traditional broadcast channels, it will now include any services which can be used to show live coverage of **listed events** to audiences in the UK, including the PSBs' on-demand players, global media platforms and other internet-based streaming services.

The new UK media regulatory framework will have a number of implications for affected companies, platforms and services:

- It will be necessary to **update technical and operational processes** to ensure that the new requirements are met, for example those around availability, prominence and accessibility quotas.
- **Appropriate governance** will also need to be put in place regarding new dispute resolution provisions.
- Companies will need to put in place the **necessary control frameworks** to prepare for Ofcom notification and compliance with resulting Codes (e.g. for providers of devices like smart speakers and in-car entertainment systems that enable consumers to select radio services).
- Finally, **strategic decision making** will need to take into account this new regulatory landscape, for example rights acquisition strategies for listed events. With many elements of

the new regime expected to be finalised by the end of the year (e.g. Ofcom's new VOD code, notification process for internet radio services that wish to notify as radio selection services), it will be important for affected companies to track the various implementation activities underway.

Alongside implementation of the Media Act, Ofcom is conducting its Public Service Media (**PSM**) Review – it is required to conduct such a review at least every five years. Ofcom has already published a statement focusing on how Public Service Broadcasters (**PSBs**), such as the BBC, ITV and Channel 4, have delivered for UK audiences over the last five years, and setting out some of the challenges to future provision. Ofcom is expected to publish a further statement in summer 2025 setting out opportunities to support the sustainability of PSM and the availability of high quality and accurate news in the future. Whilst this publication is unlikely to result in immediate changes, it may set out areas where Ofcom plans to consult on changing its rules and it could prompt further Government intervention based on its recommendations. As a result, the outcome of this review will be revealing for the future direction of media regulation in the UK.

Beyond the PSM Review and the implementation of the Media Act, changes to the UK regime on advertising of **Less Healthy Products** (previously referred to as products high in fat, salt or sugar) on TV and online will come into force in October 2025. Broadly speaking, this introduces a 9pm watershed for less healthy food and drink advertising on TV (including all on demand programme services regulated by Ofcom) and a restriction on paid-for less healthy food and drink advertising online at all times (including non-Ofcom regulated on demand services). There will be new enforcement responsibilities for both Ofcom and the Advertising Standards Authority going forward. This again shows an increasing regulatory convergence, both across different forms of content delivery (i.e. broadcast and online), and also different sectors (i.e. broadcast and on-demand).

In the EU, the new **Media Freedom Act**, designed to protect media freedom and pluralism, will apply in full from August 2025. The Media Freedom Act is a **clear example of the increasing interdependency between media and digital regulation**, which has implications for the companies concerned. In particular, it incorporates new requirements that VLOPs designated under the DSA need to follow when assessing whether a media service



provider on their platform should be removed. This includes giving the media service provider the opportunity to confirm they comply with obligations under the Media Freedom Act, for example that they have the required editorial independence and that they do not provide content generated by AI systems without subjecting it to human review or editorial control. Implementation of these new rules will therefore be a regulatory priority for the European Commission in the year ahead. During 2025 the Commission is expected to issue guidelines to assist VLOPs in establishing the functionality to enable declaration of media service providers on their platforms.

**“The new UK media regulatory framework will have a number of implications for affected companies, platforms and services. It will be necessary to update technical and operational processes to ensure that the new requirements are met, for example those around availability, prominence and accessibility quotas.”**

VLOPs should also prepare for new **reporting requirements** in the Media Freedom Act which require them to make public, on an annual basis, detailed information on the number of times they have imposed any restriction or suspension on a media service provider on their platforms, and the grounds for imposing such restrictions or suspensions. The Media Freedom Act also introduces a right for users to **change the configuration** of any

media device/user interface consistent with their interests, as well as provisions which aim to **increase transparency in audience measurement** for media service providers and advertisers. Affected companies should be reviewing their technical and operational processes with such impending requirements in mind.

**Further regulatory debate on copyright and AI (relevant to the position of the creative industries) is also expected in the year ahead.** In the UK, the consultation on the UK Government’s proposals in this area is set to close on 25 February. With a high-profile public discussion on this contentious topic already well underway, it remains to be seen whether targeted regulation can navigate a path through the various interests at play. In the meantime, the implementation of the DMCC Act is also relevant, for both the internet companies designated as having SMS (e.g. large internet platforms), and companies who may provide digital content to these platforms. Indeed, in October 2024 the UK Prime Minister himself stated that *“this landmark legislation will help rebalance the relationship between platforms and those, such as publishers, who rely on them”*. This is in part due to the so-called ‘final offer’ provisions which are potentially relevant to the commercial relationship between content owners and designated digital platforms (albeit that the effects of such provisions would likely not be felt for some time yet, certainly not before 2026). In the EU, the EU AI Act does not address the issue of remuneration of content head-on, although as a general rule compliance with copyright law is a prerequisite for compliance with the EU AI Act. Discussion of further specific rulemaking in the EU relevant to the remuneration of creators whose works are being used to train AI models, particularly given the strong views of some Member States on this issue, can’t be ruled out in the year ahead.



## Chapter 9

# Consumer fairness: walking the end-to-end digital journey

### SUMMARY

*As digitisation becomes increasingly pervasive across the business-to-consumer (B2C) landscape, companies should be prepared to demonstrate to authorities why their online processes are fair. There is a variety of consumer law and regulation designed to ensure consumers are treated fairly. This regulation can be enforced against many different consumer facing businesses that transact over the internet, in sectors such as supermarkets and travel. In the UK, the coming year will see the activation of the CMA's landmark new powers to enforce consumer law direct, along with the new remedies it now has at its disposal. Preparing for this should be a priority for Boards and Executives of B2C businesses across the country.*

The **UK consumer protection regime is expected to undergo significant change in 2025**. For the first time it is expected that the **CMA will be able to decide whether important consumer laws have been broken**, rather than taking a case to court. If the CMA finds a breach, the CMA will be able to impose remedies, which may include requiring firms to offer compensation or other redress for consumers. It will also be able to **impose new financial penalties for breaches** (£300,000 or, if higher, 10% of a company's world-wide turnover). This represents a major evolution of the UK's consumer enforcement regime, and companies across the economy should be prepared for the CMA to test these new powers.

A key question will clearly be the investigations that the CMA intends to pursue under the new regime. At a UK event recently hosted by the CMA to discuss these landmark new consumer enforcement powers, the message from the senior CMA official to business leaders was clear; that they should "*walk the end-to-end journey of dealing with your firm*". Companies should expect regulatory priorities for 2025 to reflect the fact that **a significant amount of B2C journeys now take place on the internet**.

**"The UK consumer protection regime is expected to undergo significant change in 2025. For the first time it is expected that the CMA will be able to decide whether important consumer laws have been broken, rather than taking a case to court."**

A likely CMA enforcement priority that companies should be aware of going forward relates to OCA. OCA is a neutral term and (generally speaking) refers to the design of online environments that affect a consumer's decision making and action. OCA can be good and bad. Common examples of 'Bad' OCA include difficulty in cancelling a subscription, the default selection of an option that may not be the most beneficial to the customer, and 'drip pricing' where consumers are shown an initial price for a good or service while additional fees are revealed later in the checkout process. The public debate on the use of so-called '**dynamic pricing**' for concert tickets in 2024, still under investigation by the CMA at the

time of writing, is a recent example of an investigation into whether consumers are being given clear and timely information to explain that prices could change depending on demand and how this would operate. It also shows that authorities are particularly sensitive to consumers potentially being put under undue pressure to make purchasing decisions within a short period of time (another form of 'Bad' OCA). We set out examples of what companies should look out for in this area, along with the best practices they can adopt to ensure 'Good' OCA, in Chapter 10.

The changes to the UK regime will begin in April 2025, when the Government expects to commence the new consumer enforcement regime. Secondary legislation will set out rules for the CMA's new direct enforcement powers, alongside guidance on these new powers. The regime applies to commercial practices relevant to the activities of a trader which has a 'UK Connection' (e.g. they are directed at consumers in the UK). It does not matter whether the activities are carried on in the United Kingdom or elsewhere. This development should therefore be on the radar of online companies who are targeting UK consumers, even if they do not have a physical presence there. B2C companies operating in more than one country should expect to see authorities cooperate in their enforcement against unfair online practices. This can be achieved through existing frameworks that they have in place (such as the Consumer Protection Cooperation Network in the EU and the International Consumer Protection and Enforcement Network).

In the EU, digital also features prominently in the Mission Letter of the new EU Commissioner for Democracy, Justice and the Rule of Law, in terms of the preparation of a new **Digital Fairness Act** in particular and an emphasis on e-commerce in general. The EU Digital Fairness Act is expected to address concerns about unethical techniques and commercial practices related to dark patterns/unfair OCA, marketing by social media influencers and addictive design of digital products. The broader emphasis on e-commerce will likely focus on e-commerce platforms, by taking steps to protect consumers and ensure a level playing field (again chiming with the focus on marketplaces under the DSA, and Member State calls for enhanced surveillance and enforcement in this area, something we covered in Chapter 1). This activity also dovetails with the European Commission's ongoing '**fitness check**' of existing Consumer Law on Digital Fairness. Specific



areas of concern that have been called out by the Commission so far include practices relevant to dark patterns and **OCA, addictive design, influencer marketing, subscription contracts and cancellations, AI chatbots and ticket sales.**

In summary, companies should be prepared to **demonstrate to authorities that their customers are being treated fairly when making online purchasing decisions** (e.g. that there is sufficient transparency around pricing, that purchasing options are displayed in a 'fair' way or that it is sufficiently straightforward to cancel a contract). B2C companies for whom online transactions are an important part of their business model should review, and where required update, their operations and processes to ensure they are **consistent with positive customer outcomes.**

**“The EU Digital Fairness Act is expected to address concerns about unethical techniques and commercial practices related to dark patterns/unfair online choice architecture, marketing by social media influencers and addictive design of digital products.”**



## Chapter 10

# Online choice architecture: ensuring fit for purpose processes and testing

### SUMMARY

*As we have set out elsewhere in this document, OCA refers to the design of online environments – such as an online customer journey to book a holiday – that affect a consumer's decision making and action. Companies should be prepared to demonstrate to appropriate authorities how their OCA is fair. Previous investigations relevant to OCA can help companies identify regulatory concerns and inform their practices to ensure compliance. This includes testing to evidence the use of 'Good' OCA, something that regulators have highlighted the need for.*

OCA is a **key priority for authorities** in the UK and EU, relevant to both consumer protection objectives (e.g. ensuring that an option for a consumer to cancel a contract is sufficiently prominent) and competition policy objectives (e.g. ensuring that the results of an online search for hotels does not distort competition between hotel booking sites).

Given this scope, there is also a range of law and regulation relevant to OCA. For example:

- On the **digital consumer side**, this includes the EU's Digital Services Act (see Chapter 1), as well as various other pieces of consumer protection legislation. It is also expected to be a key priority for the CMA under the UK's new consumer protection regime, as well as underpinning upcoming regulatory initiatives such as the EU's Digital Fairness Act (as we covered in Chapter 9).
- On the **digital competition side**, this includes the EU's Digital Markets Act, and the UK's Digital Markets, Competition and Consumers Act (as we covered in Chapter 3).

There is no specific regulation in the UK or EU that sets out prescriptive steps to design 'Good' OCA. As our case studies below highlight, the requirements fall out of the expectations from a number of discrete pieces of regulation that are use-case specific.

To help inform the practical steps that companies can take to ensure 'Good' OCA, in this section we first **highlight three recent regulatory investigations in both the UK and the EU** which demonstrate concerns that regulators have in this area. We then highlight **best practices that companies can adopt** in order to help ensure a fair online digital journey going forward.

### Case Study 1 – Unfair OCA Practices highlighted by the EU Consumer Protection Cooperation (CPC) Network

The EU CPC Network (a network of EU competent public enforcers established to tackle consumer protection issues in a coordinated manner) recently notified an online marketplace of a number of practices on its platform that it considered infringed EU consumer law. The CPC Network's action, announced at the end of 2024, was led by the competent national authorities of Belgium, Germany and Ireland, under the coordination of the European Commission.

The CPC Network identified six OCA practices, including those relevant to **pricing, pressure selling, missing and misleading information**, which it considered may mislead consumers or unduly influence their purchasing decisions. These were considered to be in breach of obligations under a number of different EU consumer laws, including the DSA, the Unfair Commercial Practices Directive and the Consumer Rights Directive. These are set out in more detail in Figure 4, below.



**Figure 4:** Examples of unfair OCA highlighted by the EU CPC Network

**1 FAKE DISCOUNTS**  
Giving the false impression that products are offered with a discount where there is none.

**2 PRESSURE SELLING**  
Putting consumers under pressure to complete purchases using tactics like false claims about limited supplies.

**3 FORCED GAMIFICATION**  
Forcing consumers to play a 'spin the fortune wheel' game while hiding essential information about the conditions of use linked to the rewards of the game.

**4 MISSING AND MISLEADING INFORMATION**  
Failing to inform consumers in advance that their order needs to reach a certain minimum value before they can complete their purchase.

**5 FAKE REVIEWS**  
Giving inadequate information about the authenticity of reviews published on the website, some of which are suspected to be unauthentic.

**6 HIDDEN CONTACT DETAILS**  
Consumers cannot easily contact for questions or complaints due to missing link to contact details.

**4** You have 0 item(s) in your basket

**1** **SMARTPHONE COVER** **£7.50 NOW ONLY £5.99**

**5** See what others think

Hurry up! Only few remaining! **2**

**6** **ANY PROBLEMS?**  
Contact us or send this item back for free!  
Check out our zero-stress free return policy!

**3** **SPIN OUR WHEEL OF FORTUNE AND WIN EXCLUSIVE DISCOUNTS**

**CHECKOUT**  
(Blocked - spin the wheel to proceed)

★★★★★ Amazing! Great value for price

★★★★★ BEST COVER EVER!!!

★★★★★ Nice product, quick delivery

★★★★★ BEST COVER EVER!!!

### Case Study 2 – Unfair OCA Practices highlighted by the UK CMA

In the UK, during 2024, the CMA completed an investigation into **urgency** and **scarcity** claims used by a website, resulting in commitments from the company under investigation. This investigation had been opened by the CMA following the publication of an open letter to UK businesses detailing 'online red lines' on misleading urgency and price reduction claims. In this letter the CMA outlined practical illustrations of where common online tactics may be misleading consumers or applying unfair pressure.

In concluding the investigation, the CMA obtained a number of commitments from the company in question in relation to its online selling practices. These included that it would not use timers that mislead consumers or give a false impression that they have to act quickly to avoid missing out on a deal, that it would make sure all scarcity and popularity marketing claims are clear and accurate, and that it would refund customers who were signed up to a membership scheme via a pre-ticked box. Examples of the CMA's concerns are highlighted in Figure 5 below.

**Figure 5:** Examples of unfair OCA highlighted by the UK CMA

**1** 04:56  
REMAINING TO  
COMPLETE THE  
PURCHASE

**YOU HAVE 1 ITEM  
IN YOUR CART**

**YOUR ORDER:**  
Cinema ticket for movie A

**2** **DEAL OF THE DAY**  
Price: £10.99  
Ends tonight!

**QUANTITY:**  
— 1 —

**3** **HIGH DEMAND**  
150 sold in 24 hours\*

**BUY NOW**

**4** [Be quick! 10 people are viewing this now!](#)

**1** **UNTRUE CHECKOUT TIMER**  
The timer starts again when the webpage is refreshed or when the time runs out. This is misleading as there is no effective time limit to complete the purchase and therefore putting unfair pressure on the consumer to complete the transaction.

**2** **MISLEADING CLAIM**  
The promotion ends that day, but new promotions offer substantially the same deal as the movie is screened daily. This deceives consumers into thinking they need to act quickly to secure the price advantage, when in fact there is no real need.

**3** **DECEPTIVE SALES RATES**  
The claim is not factually false but refers to tickets sold for all movies screened in that cinema theatre. Additionally, the 24 hours timeframe did not necessarily happen within the past 24 hours. This is unfair even if there is an explanation elsewhere on the webpage as the headline claim is still likely to deceive consumers.

**4** **WRONG VIEWS TIMEFRAME**  
The claim is triggered when 20 people have viewed the product in the past hour. This is misleading because where algorithms are used to trigger a claim, the underlying data should match the claim precisely (e.g. '20 people viewed this in the past hour').

The key piece of consumer protection legislation relevant to the CMA's investigation was the Consumer Protection from Unfair Trading Regulations 2008 (**CPRs**). The CPRs contain a general prohibition against unfair commercial practices and specific prohibitions against misleading actions and misleading omissions. As we set out in Chapter 9, under the new UK consumer protection regime set to go live in 2025, the CMA will be able to determine itself that the law has been broken, including new powers to fine companies up to 10% of global annual turnover for infringements of certain consumer protection legislation, including the CPRs.

### Case study 3 – Unfair OCA Practices highlighted by the Spanish Ministry for Social Rights, Consumers and the 2030 Agenda

In Spain, the responsible Ministry has recently taken action against

certain airlines in respect of so-called '**drip pricing**' techniques (i.e. when consumers are shown an initial price for a good or service while additional fees are revealed (or "dripped") later in the checkout process). The Ministry considered that this conduct infringed the Spanish General Law for the Defence of Consumers and Users.

In this case, the OCA had both a consumer protection and a competition dimension. From a consumer protection perspective, the authority was concerned that it resulted in consumers paying more than originally envisaged. From a competition perspective, the Ministry considered that it enabled the companies in question to highlight the initial prices in their advertising, and also affected ranking and search engine optimisation. Examples of the Ministry's concerns are set out in Figure 6 below.

**Figure 6:** examples of unfair OCA highlighted by the responsible Spanish Ministry


**MAD – LGW Flights**

**FROM**  
MADRID

**TO**  
LONDON

**DATE** Thursday 17 October

**AIRLINE A**  
09.30 → 11.00

**AIRLINE B**  
18.10 → 11.45

**£76.50**  
BOOK NOW  
Add a luggage for £35

**£95.00**  
BOOK NOW  
Free luggage included

#### DRIP PRICING (CONSUMER PROTECTION CONCERN)

1

Advertising a headline price only to add additional charges later can lead to worse consumer outcomes, especially where these are hardly avoidable. For example, bringing luggage on board a means of transportation (e.g. train, airplane, etc.) can be regarded as hardly avoidable.

#### UNFAIR RANKING (COMPETITION CONCERN)

2

Drip pricing can unfairly favour a company against competitors, as a lower headline price results in better search engine optimisation against alternatives that cost the same or less but advertise the full price. In this case, Airline B is the most convenient option when taking luggage price into account. However, Airline A is still ranked first as it offers a lower headline price.

### What companies can do to prepare

There is much that online companies can do to ensure that their online selling practice, in particular their use of OCA, is fair. We highlight the following examples of best practice:

- As a starting point, **online selling practices should be reviewed across all the firm's consumer-facing online activities**. This can include advertisements (e.g. marketing emails, display, search results), webpages, apps and pop-ups (e.g. home page, search results, product details, basket, payment).
- An important consideration is also to ensure that **relevant personnel** (e.g. those responsible for the design, approval or use of online content design, marketing, website or app development) **are aware of and understand the relevant legal and regulatory requirements applying to the design of online choices**.
- In addition, companies should check that they have **appropriate safeguards** and **standard processes in place** so that they do not present unfair and/or misleading claims to consumers online. For example, price promotions should be verified as compliant before they are published online, search engine ads should continue to accurately reflect current offers, and special offer prices should not continue beyond the promotion's end date.

- It is also important to be able to **evidence that design choices were made with fairness and neutrality in mind**. For instance, ensuring adequate levels of record-keeping (e.g. to demonstrate that a given discount is real and not just the headline price framed more compellingly) and clear internal standards/principles for how information can be used (e.g. for how long it is acceptable to show a discounted price on a website compared to the headline price).

Finally, the use of testing is an important means of supporting company decision making, something that regulators are also highlighting the need for:

- One such example is **A/B testing**, which allows online companies to measure the effectiveness of design changes to their websites. It usually involves a randomised experiment based on two variations of the same page, i.e. 'Variation A' (the initial website design) and 'Variation B' (a different design of the website that includes relevant changes). The company then lets random samples of users interact with the two variants while keeping track of their respective behaviour. This provides data to the company on the effectiveness of changes implemented in variation B compared to the original website (variation A). A/B testing is generally used to assess factors like page revenue, click rates, and number of purchases.

- Another example relates to the use of **customer surveys**. Customer surveys allow firms to gather direct feedback from users. Surveys can adopt different approaches, for example focusing on gathering qualitative data (leaving more room for users to express their subjective opinions, experiences, and satisfaction levels) or quantitative data (focusing on gathering more quantifiable and statistically relevant measurements). This form of testing can potentially provide less targeted insight compared to other methods. However, surveys leave more room for bottom-up feedback that can potentially lead to unexpected results and provide an outlook into the broader OCA landscape.

In summary, with authorities expected to prioritise efforts to ensure the use of 'Good' OCA in the year ahead, it is a topic that should be high on the agenda for all companies as they review and design their consumer facing online processes going forward.



**“It is important to be able to evidence that design choices were made with fairness and neutrality in mind.”**





## Authors



### **Suchitra Nair**

Partner  
Head of EMEA Centre for Regulatory Strategy  
snair@deloitte.co.uk  
+44 2073037963



### **Robert MacDougall**

Director, Digital Markets  
EMEA Centre for Regulatory Strategy  
rmacdougall@deloitte.co.uk  
+44 2070070148



### **Matteo Orta**

Senior Consultant  
EMEA Centre for Regulatory Strategy  
morta@deloitte.co.uk  
+44 2080397554

### **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 Nick Seeber, Laurie Gilchrist, Brij Sharma, Sian Bundred, Valeria Gallo, Scott Bailey, Anais Bauduin, Ahmed Hamdy, Lukas Kruger, Curtis Barnes and Roger Smith for their contributions to this digital regulatory outlook.



#### **About this publication**

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](http://www.Deloitte.com/about) to learn more about our global network of member firms.

Deloitte LLP is authorised and regulated by the Solicitors Regulation Authority (SRA) to provide certain legal services (licence number: 646135). Deloitte Legal means the legal practices of Deloitte Touche Tohmatsu Limited member firms or their affiliates that provide legal services. In the UK, Deloitte Legal covers both legal advisory (authorised and regulated by the SRA) and non-SRA regulated legal consulting services. For legal, regulatory and other reasons not all member firms provide legal services.

© 2025 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM1965133