Digital Risk Outlook 2024

For what comes next
tlt.com

Introduction

If your business works in digital markets, you'll be affected by a raft of UK legislation this year.

Once you're aware, you can prepare – so our Digital Risk Outlook report helps you get to grips with:

- **Legislating for new technology as AI accelerates.**
- **The UK's new digital markets regulatory regime under the DMCC Bill.**
- **Marketing and regulation in cryptoassets.**
- **Upcoming changes in digital consumer protection and enforcement.**
- **New data protection and cybersecurity regulations.**
- **Regulating digital platforms and marketplaces.**
- **The CMA's focus on competition in relation to AI Foundation Models.**
- **Payment orchestration and the use of AI in the payments sector.**

All these changes arrive alongside opportunities. For example, the CMA's pro-competition powers under the DMCC Bill have the potential to open up digital markets and level the playing field for businesses that depend on the largest tech firms. But there's also significant risk if you don't manage these regulatory developments well.

Our specialist lawyers in payments, data protection, technology, competition and regulatory compliance have provided their expert insights and advice for this report. Each topic offers a look ahead to approaching changes, clarifies the most important points to be aware of, and highlights where you need to take action.

We've laid out the report this way so you can understand exactly how, where, when and why your business will be affected, helping you to prioritise your next moves.

Please let us know if you have any questions – **our team** is here for what comes next in digital.

What's coming in 2024

- **3 January 2024** – CMA's invitation to comment on the partnership between Microsoft and OpenAI closes. CMA will then decide whether to launch a Phase 1 investigation.
- **15 January 2024** – Closing date for ISU's consultation on the refinement of the UK's national security screening regime.
- **29 January 2024** – Competition Appeal Tribunal (CAT) trial in the 'opt out' class action case of Justin Le Patourel v BT
- **23 February 2024** – Closing date for Ofcom's consultation on protecting people from illegal harms online
- **Early 2024** – The Data Protection and Digital Information Bill to progress through the House of Lords with the intention that it will receive royal asset some time in 2024
- **Early 2024** – Government due to publish outcome of Smarter Regulation consultation on drip/hidden pricing, consumer law obligations for digital platforms and product safety for online marketplaces
- **Spring – Autumn 2024** – DMCC Bill expected to come into force
- **September – December 2024** – CMA's provisional decision target date and response hearings on interim decision for investigation into Cloud Services market
- **Late 2024** – CMA expected to launch consultation on first Strategic Market Status designations under DMCC Bill
- **February – April 2025** – CMA's target conclusion date of investigation into Cloud Services market (statutory deadline on 4 April 2025)

Use the icons below to navigate quickly to the most relevant section or use the whole report as a comprehensive guide.


AI


Crypto


Competition & digital markets


Digital platforms & online marketplaces


Consumer


Data protection & cybersecurity


Payments

Contents

AI – can the law keep up?

A look ahead

One of the main challenges of trying to legislate for emerging technologies is simply keeping up. Given the pace of developments in the past year alone, this might be the case with the EU Artificial Intelligence Act (the **Act**), which was drafted in 2021. The risk-based Act has three main categories:

- **Low Risk:** where the AI application needs to fulfil certain transparency obligations regarding its use.
- **Prohibited AI:** the effective banning of subliminal AI applications; AI used for social credit scoring or attributing values to citizens based on their behaviours.
- **High-risk:** any use of AI applications for the public sector or deemed to be high risk by the European Commission must satisfy strict security and accuracy criteria before being deployed. This requirement includes oversight by humans to ensure the AI technology high risk applications are trustworthy from a very human perspective.

This is a valid approach to regulating AI, but deciding which applications fall under the "high risk" category is difficult. "High-risk" is widely defined and includes everything from critical infrastructure vital for citizens' health and life, to educational or vocational training that may determine access to education. It can also encompass safety, components of products, employment management, workers, and essential private and public services.

> The Act may also be closing the legislative stable door after the horse has bolted…

The Act may also be closing the legislative stable door after the horse has bolted because it was drafted before Chat GPT heralded the arrival of Generative AI technologies. Indeed, its own terms may already be outdated as Generative AI technologies are now built in as standard to many office applications already being used across every economic sector in a way that the Act deems high risk. Whereas the Act is aimed at regulating these applications as if they were ad hoc, distinct, and separable.

What makes the UK's approach to regulating AI different from the EU?

The UK government released its AI white paper on 29 March 2023. It outlines a principles-based approach to put the UK at the forefront of the AI race. Emphasising business accountability while encouraging innovation and a measure of calculated risk, the paper details five fundamental principles:

- **safety, security and robustness**
- **appropriate transparency and explainability**
- **fairness**
- **accountability and governance**
- **contestability and redress.**

This is a non-statutory framework so existing regulators, such as the ICO, the FCA and the CMA, are expected to interpret and apply the principles within their existing regulatory remits. At the end of an initial implementation period, the government intends to introduce a statutory duty on regulators to have "due regard" to the principles. However, the white paper also allows the government to keep the framework non-statutory if it's working well. Either way, the white paper does not envisage any additional legal duties on those operating within the AI ecosystem.

The UK has hosted the global AI safety summit since the white paper was published. This has resulted in the Bletchley Declaration being adopted by countries including the UK, the USA and China – the three largest AI economies globally. The key theme throughout the declaration is the need to legislate on a global basis to address the safety concerns and fears that have been expressed to date:

"AI should be designed, developed, deployed, and used, in a manner that is safe, in such a way as to be human-centric, trustworthy and responsible… …We resolve to work together in an inclusive manner to ensure human-centric, trustworthy and responsible AI that is safe, and supports the good of all through existing international fora and other relevant initiatives, to promote cooperation to address the broad range of risks posed by AI"

It remains to be seen what future legislative instruments will emerge internationally affecting the Bletchley Declaration. In the meantime, the White Paper will govern whatever legislative approaches maybe adopted so it's important for you to ask your relevant regulator/s how they will practically implement the principles set out in the white paper.

"The key theme throughout the declaration is the need to legislate on a global basis to address the safety concerns and fears that have been expressed to date…

Competition in AI: CMA's guiding principles for AI Foundation Models

Be aware

The UK is keen to cement its reputation as a global leader in AI tech. Part of this strategy entails ensuring tech firms have fair and equal access to the technology needed to develop AI Foundation Models (**FMs**), which are the deep learning neural networks that underpin generative AI software.

Image and text-based FMs feed on massive datasets and need several key inputs to develop. These include access to data, immense computing power, technical expertise and capital. Consequently, the CMA has launched a review of the FM market to ensure tech firms have fair and equal access to these inputs. It is particularly keen to mitigate potential AI competition concerns given that regulators were slow to act on other digital market competition issues in the past decade.

The CMA has shifted its approach in recent years to proactively tackling structural competition barriers (e.g., the emergence of market 'gatekeepers') before they arise. This approach is hard-wired in the DMCC Bill (see below) and later in this report we'll unpack how the CMA may use its powers to impose conduct requirements on tech firms with 'Strategic Market Status' to **regulate FM markets**.

Here are the 7 guiding principles which the CMA believes should govern the FM market (from its **Initial Report** published in September 2023):

1. **Accountability** – FM developers and deployers are accountable for outputs provided to consumers.
2. **Access** – ongoing ready access to key inputs, without unnecessary restrictions.
3. **Diversity** – sustained diversity of business models, including both open and closed.
4. **Choice** – sufficient choice for businesses so they can decide how to use FMs.
5. **Flexibility** – having the flexibility to switch and/or use multiple FMs according to need.
6. **Fair dealing** – no anti-competitive conduct including anti-competitive self-preferencing, tying or bundling.
7. **Transparency** – consumers and businesses are given information about the risks and limitations of FM-generated content so they can make informed choices

The CMA has also been monitoring the impact of deals that could potentially weaken competition in the development or use of FMs. In December 2023 it announced that it was investigating Microsoft's partnership with OpenAI (the developer of ChatGPT). The partnership includes a multi-year, multi-billion dollar investment, collaboration in technology development, and exclusive provision of cloud services by Microsoft to OpenAI. The CMA **stated** that the partnership "represents a close, multi-faceted relationship between two firms with significant activities in FMs and related markets". It will gather comments from interested parties before deciding whether to launch a phase 1 investigation.

> The CMA has shifted its approach in recent years to proactively tackling structural competition barriers before they arise.

Take action

If your business uses or is involved in generative AI, you should monitor the developments in this space closely. The CMA's work is ongoing, with the final report expected later in 2024. While the CMA's Digital Markets Unit may use its powers under the DMCC Bill to impose conduct requirements on the largest tech firms, this may create opportunities for others who would benefit from more open access to FM technologies.

CMA's guiding principles for AI foundation models

Model development Use of models in other markets Use of models by consumers	Accountability FM developers and deployers are accountable for outputs provided to consumers.	**Access** Ongoing ready access to key outputs.	• Access to date, compute, expertise and capital without undue restrictions. • Continuing effective challenge to early movers from new entrants. • Successful FM developers do not gain an entrenched and disproportionate advantage by being the first to develop a FM, having economies of scale or benefiting from feedback loops. • Powerful partnerships and integrated firms do not reduce others' ability to compete.
		Diversity Sustained diversity of business models, including both open and closed.	• Both open and closed source models push the frontier of new capabilities. • Open-source models help reduce barriers to entry and expansion.
		Choice Sufficient choice for businesses so they can decide how to use FMs.	• A range of deployment options, including in-house FM development, partnerships, APIs or plug-ins.
		Flexibility Flexibility to switch or use multiple FMs according to need.	• Interoperability to support firms mixing and matching or deploying multiple FMs. • Consumer can switch and/or use multiple services easily and are not locked into one provider or ecosystem.
		Fair Dealing No anti-competitive conduct, including anti-competitive self-preferencing, tying or bundling.	• Confidence that the best products and services will win out. • No anti-competitive conduct, including anti-competitive self-preferencing, tying or bundling, especially from vertical integration. • Competition can counteract any data feedback or first mover effects.
		Transparency Consumers and businesses are given information about the risks and limitations of FM-generated content so they can make informed choices.	• People and businesses are informed of FMs' use and limitations. • Developers give deployers the information to allow them to manage their responsibilities to consumers.

Integrating AI into B2C products: consumer protection risks

Be aware

AI offers huge potential to optimise experiences and drive efficiencies for consumers. While the Competition and Markets Authority (**CMA**) recognises these benefits, it's also alert to AI's potential to cause consumers economic harm.

This is reflected in the 'fair dealing' and 'transparency' principles in the CMA's 7 guiding principles of AI Foundation Models (**see previous article**).

The CMA has highlighted the following risks:

- **Chatbot errors:** Foundation models can get things wrong, and developers have not been able to reduce the chatbot error rate to zero. This issue is potentially exacerbated by the fact chatbots can sound very convincing and consumers may, therefore, be more inclined to trust the responses they receive. This could present a problem if a chatbot provides a consumer with false or misleading information about products or their consumer rights.
- **Harmful search algorithms:** Search algorithms can help direct consumers to the products and services they need. But there's a risk they could be distorted by factors that harm their economic interests, for example by diverting consumers to products which earn sellers the highest level of commission. The CMA already focuses on online architecture because of this theory of harm. But it's concerned that more sophisticated AI tools could exacerbate the problem.
- **Targeting vulnerable consumers:** Using ad tech to target ads more effectively brings consumer benefits. But the CMA is concerned that AI could also be used to exploit consumers when they are vulnerable, for example at times when their judgement is impaired, and they may make impulsive buying decisions.
- **Fake product reviews:** The DMCC Bill sets out new rules to combat fake product reviews (see below). While the CMA has been using AI to help identify fake reviews it's also concerned AI could create sophisticated fake reviews that are much harder to detect.

Take action

The Consumer Protection from Unfair Trading Regulations 2008 (**CPRs**) will be recast in Part 4 of the DMCC Bill. They already provide the CMA with significant powers to take enforcement action in relation to unfair commercial practices and it is anticipated that these will be sufficient to deal with the kind of harm highlighted above. Any business that interfaces with consumers should consider the consumer law risks associated with integrating AI into B2C products.

> Any business that interfaces with consumers should consider the consumer law risks associated with integrating AI into B2C products.

10 key points: the FCA's Rules for marketing cryptoassets

A look ahead

From 8 October 2023, the marketing of qualifying cryptoassets was brought within the scope of the UK financial promotion regime, regulated by the Financial Conduct Authority (the **FCA**). Continuing issues with the crypto sector have highlighted the need for tighter regulation, but cryptoassets are still high risk and largely unregulated even after these changes.

The regulation and oversight of cryptoassets has been a hot topic for many years and there have been growing concerns about protecting consumers. Here's how we got to the latest changes:

- **2018:** The Cryptoassets Taskforce (HM Treasury, the Bank of England and the FCA) found that misleading advertising and a lack of suitable information was a key consumer protection issue in the cryptoasset market.
- **July 2020:** The Government published a consultation on a proposal to bring certain cryptoassets into the scope of the Financial Services and Markets Act 2000 (Financial Promotions Order) 2005.
- **January 2022:** the Government published the **response** to the consultation. There was significant support from the findings for new regulation to ensure that cryptoasset promotions are fair, clear and not mis-leading. The proposed legislative approach was updated in a **policy statement** published on 1 February 2023.
- **January 2022:** The FCA consulted on financial promotion rules for high-risk investments including cryptoassets (**CP22/2**). The final rules for other high-risk investments were published in August 2022 and it was noted that rules for cryptoassets would be provided once the relevant legislation has been made.

On 7 June 2023, the Government published the final version of the Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023 (the **FPAO**). The following day the FCA published Policy Statement – Financial promotion rules for cryptoassets (**PS23/6**) (the **Policy Statement**). This sets out the rules for the marketing of qualifying cryptoassets. Alongside the Policy Statement, the FCA published a **Guidance Consultation** to help firms understand the expectations. The **Final Guidance** was published on **2 November 2023**.

The new rules are designed to protect the interests of consumers by advancing the FCA's objectives of consumer protection, market integrity and effective competition.

10 key points of the rules:

1. **When were the rules in force?** 8 October 2023.
2. **What do the rules apply to?** 'Qualifying crypto assets', broadly defined in the FCA's Final Guidance as *"any cryptographically secured digital representation of value or contractual rights that are transferable and fungible"*. However, the rules do not apply to *"cryptoassets which meet the definition of electronic money or an existing controlled investment"*.
3. **Where do the rules apply?** The UK financial promotion regime applies to any communication that is "capable of having an effect in the UK". Therefore, the new rules apply to all firms marketing qualifying cryptoassets to UK consumers, regardless of where the firm is based.
4. **The risk warning:** A financial promotion of a qualifying cryptoasset must contain a warning which states: "Don't invest unless you're prepared to lose all the money you invest. This is a high-risk investment, and you are unlikely to be protected if something goes wrong".
5. **Banning investment incentives:** Firms must not offer monetary or non-monetary incentives to UK consumers to invest in qualifying cryptoassets. Incentives which are no longer permitted include (a) bonuses for first-time investors, (b) bonuses for referring another person to invest, (c) cashback, (d) discounts when investing a particular amount, (e) free gifts, and (f) additional free or discounted investments.
6. **Direct Offer Financial Promotions (DOFP):** There are a number of requirements that a firm must carry out before offering a DOFP to a UK consumer, including (a) the first time a particular UK consumer requests to receive the DOFP, there must be a minimum 24-hour cooling-off period. After this period, the consumer must re-confirm that they wish to receive the DOFP before they are able to receive it and (b) the firm must display a personalised risk warning stating: *"[Client name], this is a high-risk investment. How would you feel if you lost the money you're about to invest? Take 2 mins to learn more"*.
7. **Record keeping:** Firms must maintain an adequate record of the various information including (a) the categorisation of each consumer, and the evidence obtained in support of that categorisation, and (b) the total number of appropriateness assessments undertaken, the number resulting in a determination that the investment was appropriate and the number resulting in a determination that the investment was not appropriate.
8. **Legal routes to making a financial promotion relating to a qualifying cryptoasset:** All financial promotions of qualifying cryptoassets must be fair, clear and not misleading. In accordance with the new rules, there are now four ways in which firms can legally make a financial promotion relating to a qualifying cryptoasset.
9. **Consequences of breach:** The FCA has stated that they will take robust action against firms breaching the new rules, including: (a) requesting that websites in breach are taken down, (b) placing firms on the FCA's warning list, (c) placing restrictions on firms to prevent harmful promotions, and (d) enforcement action, which may include applying to a court for injunctions, seeking payment of compensation or, in the most serious cases, criminal prosecution.
10. **Application of the Consumer Duty:** The Consumer Duty came into force on 31 July 2023 and the FCA has stated that, in addition to building on the core requirement that communications are fair, clear and not misleading, it will strengthen the FCA's expectations of firms communicating or approving financial promotions of qualifying cryptoassets. The Consumer Duty doesn't require firms to ensure consumers always receive a good investment, but firms must ensure consumers are provided with adequate information which they can be reasonably expected to understand, and from which they are able to make properly informed decisions. The FCA also state in their Final Guidance that if, for example, all consumers were losing money on a particular investment, firms would be expected to consider whether the continued promotion of the qualifying cryptoasset was consistent with the outcomes of the Consumer Duty.

> The FCA has stated that they will take robust action against firms breaching the new rules...

What does this mean for regulation of cryptoassets?

The new rules are much stricter in terms of what's allowed in the financial promotion of a qualifying cryptoasset. But even with the new rules in place, the FCA makes it clear that cryptoassets are still high risk and largely unregulated. The Policy Statement states that consumers "should only invest in cryptoassets if they understand the risks involved and are prepared to lose all their money". With their growing popularity you should expect cryptoassets to remain a prominent focus for regulators for some time. There is clearly a lot more regulation to come, so watch this space.

New regulatory regime for 'big tech' under DMCC Bill

A look ahead

The Digital Markets, Competition and Consumers (**DMCC**) Bill represents a sea change in how the CMA regulates competition concerns in digital markets. Global competition regulators have long been criticised for being slow to act in addressing structural competition concerns in digital markets. When penalties are imposed, it is often followed by many years of appeals and litigation, meaning that the market has already moved on by the time things are settled.

As a result, the CMA is moving to an ex-ante regulatory regime that enables it to act quickly to impose market remedies without needing to demonstrate that a tech firm has abused a dominant position in the market. It will do this by designating the most influential tech firms with Strategic Market Status (**SMS**). Once a firm has SMS, the CMA's Digital Markets Unit (**DMU**) can:

- Impose bespoke 'conduct requirements' tailored to the tech firm in question's digital activities.
- Impose 'pro-competitive interventions' enabling the CMA to react quickly to address structural competition concerns as and when they arise.

The new regime is designed to give the DMU maximum flexibility so that it can intervene quickly where necessary to address competition issues in digital markets.

Which tech firms will the Codes of Conduct apply to?

Codes of Conduct can't be imposed out of the blue on any tech firm. They can only be imposed on a company which has been designated as SMS (following a formal investigation process).

The CMA published an overview of its proposed approach for implementing the new digital markets regime on 11 January 2024. It confirmed that it expects to initiate 3–4 investigations in the first year of the Bill. The CMA also confirmed this will mainly focus on the markets and activities it has already been investigating. This includes platforms funded by digital advertising (including search and social media) and mobile ecosystems. It is therefore expected that Google, Meta and Apple will be the first firms to receive SMS designations.

For more information on the CMA five-part criteria designating a firm as SMS, take a look at our recent article "**DMCC Bill in focus: part 4**", which focusses specifically on what the 'big tech' Codes of Conduct mean in practice.

Will each SMS firm have their own Code of Conduct?

Yes, the Bill gives the CMA the power to impose tailored Codes of Conduct on SMS firms in relation to the digital activities for which they are designated. This means the conduct requirements will likely look very different for each SMS firm to reflect the particular concerns the CMA has in relation to their activities.

The CMA has to consult publicly before imposing (or indeed varying or revoking) a conduct requirement on an SMS firm but retains broad discretion. Once in force, the CMA must publish guidance about how the conduct requirements will operate in practice and keep requirements under review to assess their effectiveness and determine whether they should be varied or revoked.

What kind of behaviour will Codes of Conduct cover?

Strictly speaking, the CMA can only impose certain "permitted types" of conduct requirement. However, in practice these afford the CMA very wide discretion to introduce requirements that promote **fair trading, open choices, trust and transparency**. This has proved controversial with some arguing that they afford the CMA too much power to direct the affairs of SMS firms. For example, the CMA can require SMS firms to trade on "reasonable and fair terms", which could affect businesses trading with SMS firms, including by stopping SMS firms from imposing unfair payment terms on users.

In general terms, the CMA conduct requirements for an SMS firm are divided into two categories: obligations and restrictions. Please read our article "**DMCC Bill in focus: part 4**" for a deeper dive on the topic.

What are the consequences of breaching a Code of Conduct requirement?

The CMA may investigate where, on the basis of available evidence, it has reasonable grounds to suspect an SMS-designated firm has breached a conduct requirement.

The CMA has confirmed that it expects to initiate 3-4 SMS investigations in the first year of the Bill. It is expected that Google, Meta and Apple will be the first to receive SMS designations.

While the CMA will have flexibility in how it chooses to enforce a breach of conduct requirement **an infringement finding could result in financial penalties of up to 10% of global (group) turnover.**

While the scope of direct private enforcement under the Bill has yet to be finalised, it is also likely that companies will be able to take direct action against SMS firms in the court if they have suffered loss as a result of a breach of conduct requirement.

Regulatory divergence: DMCC Bill v EU Digital Markets Act

The UK DMCC Bill marks a clear departure from the EU's approach for regulating the market power of big tech in the Digital Markets Act (**DMA**).

In the UK, the CMA is afforded immense levels of discretion and flexibility to pick and choose the tech firms it regulates, and how. Each SMS firm will have their own codes of conduct and the CMA also has wide discretion to intervene on an ad-hoc basis under its Pro-competitive Intervention powers.

In contrast, the EU Digital Markets Act takes a broader brush approach for regulating 'gatekeepers' that satisfy certain thresholds. Firms are categorised according to the different types of 'core platform services' they provide (e.g., browsers, operating systems, intermediation etc.). Each classification triggers different general conduct requirements.

While the DMA is still in its infancy, it is (unlike the DMCC Bill) already in force and in September 2023 the European Commission designated 6 tech firms as 'gatekeepers' covering 22 different core platform services: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. Those firms will be subject to their new obligations from **6 March 2024**.

Note that Apple, Meta and ByteDance (TikTok) have all filed appeals contesting various aspects of their gatekeeper designations with the EU courts. The outcome of those appeals are expected to be provide further guidance on the scope of the EU's nascent digital markets regime.

CMA market investigation into cloud storage

Be aware

On **5 October 2023**, Ofcom referred the public cloud infrastructure services market to the CMA for an independent market investigation. The purpose was to further examine the market, decide whether there are competition concerns and, if so, what interventions can improve the supply of these vital services for UK customers.

Cloud services are being rapidly adopted by most businesses and have become an essential part of how many digital services are delivered to consumers. Ofcom has estimated that the UK market was worth up to £7.5 billion in 2022.

In its **market study**, Ofcom identified the following cloud services supply features making it more difficult for customers to switch and use multiple cloud suppliers:

- **Egress fees:** charges cloud customers must pay to move their data out of the cloud.
- **Discounts:** which may incentivise customers to use only one cloud provider.
- **Technical barriers to switching:** which may prevent customers from switching between different clouds or using more than one provider.

Ofcom's report also outlines concerns about the software licensing practices of some cloud providers, particularly Microsoft.

Take action

The CMA's market investigation powers are wide. For example, it can implement new legislation imposing sector-specific regulation on the market under investigation. Given the exposure all companies have to cloud storage fees, we recommend monitoring the CMA market investigation closely to track what structural remedies, if any, they may impose.

> Cloud services are being rapidly adopted by most businesses and have become an essential part of how many digital services are delivered to consumers.

Opt-out collective proceedings in CAT relating to digital markets

Be aware

A number of important digital consumer 'opt-out' collective proceedings continue to make their way through the Competition Appeal Tribunal (**CAT**). Collective proceedings are damage claims arising out of alleged breaches of competition law where the level of damages awarded is determined by the aggregated harm caused to consumers, who are automatically included in the claim unless they expressly opt-out.

In the UK (unlike the US) large-scale collective proceedings of this nature cannot be brought on the basis of consumer protection law breaches – the cause of action must relate to a breach of competition law. As a result, in the past year we've seen an increasing number of applications for Collective Proceedings Orders (**CPOs**) being framed as abuse of dominance claims under Chapter II of the Competition Act, but where the alleged harm in question related to the unfair treatment of customers.

Given the huge sums claimed on behalf of consumers in these cases, and the significant costs and time spent defending a claim, there are significant litigation risks for firms that are at risk of being 'dominant' in narrowly defined markets. It's notable that some of these cases adopt flexible market definitions to categorise firms as being 'dominant' in their own customer ecosystems. It is also important to note that most of these cases are brought on a 'standalone' basis, in other words they're brought independently of any regulatory enforcement action by the CMA. However regulatory decisions are still important. Justin Le Patourel has brought a case against BT following an Ofcom regulatory decision and adopts that decision as a key feature of his claim. The importance of regulatory decisions, especially market investigations, should not be underestimated in opening the door to Chapter II damages claims.

The collective proceedings regime is still in its infancy. No case has yet gone to trial although the first trial is due to begin in late January 2024. In the past few years since the EU's **Damages Directive** changes have been in force the number of collective proceedings claims has jumped. Only nine CPOs were issued before 2021, but 40 have been issued since. Of those only one CPO case has settled and been approved by the CAT (**McLaren**).

Take action

If you're a large firm active in digital markets, watching these cases closely will help you assess your own competition lawrisk exposure. It is also important to note that there are increasing calls to extend the right to bring opt-out class action cases, specifically to enable claims to be brought on consumer protection law grounds. This could include unfair commercial practices such as misleading pricing. Amendments to this effect have been discussed in both the House of Commons and the House of Lords as the DMCC Bill is debated in Parliament. While it seems unlikely these will be taken forward in the final version of the Bill it remains to be seen whether calls for greater class action powers will continue once the Bill is in force. Watch this space

> It is also important to note that that there are increasing calls to extend the right to bring opt-out class action cases…

Class action claim	What is the consumer harm?	Current position
Justin Le Patourel v BT	A claim against BT alleging BT abused its dominance in two markets for standalone landline telephone services, by charging unfair prices to customers supplied with certain residential landline services. As summarised by the CAT the Claim alleges that "BT abused its dominant position in the market for voice only telephony by charging customers supra-competitive prices" which are alleged to be unfair, excessive and contrary to section 18 of the Competition Act 1998, which prohibits the abuse of a dominant position.	This is the first collective proceedings claim to proceed to trial, which is listed for an estimated eight weeks starting 29 January 2024.
Justin Gutmann v Vodafone, EE, O2 and Three	Claim for over £3 billion (including interest) against major network providers Vodafone, EE, Three and O2 for alleged abuse of market dominance charging 'loyalty penalties'. It's alleged that the network providers charged existing customers more than new customers for the same services by not reducing payments on their monthly contracts to airtime services only (or 'SIM only') once the handset had been fully paid. The term 'loyalty penalties' was coined by the fact existing customers were essentially being penalised for their loyalty.	Justin Gutmann, as the potential PCR, has lodged four separate CPO applications (one for each of the four network providers) to the CAT.
Liza Gormsen v Meta	Claims Meta should pay consumers for the use of their personal data as Facebook was able to monetise that data. If liability is established the court will have to rule on how the personal data used should be valued.	After the CAT granted a stay of proceedings, the Proposed Class Representative (**PCR**)) filed additional evidence to supplement its original CPO application. A hearing for the revised CPO application took place in early January 2024, but, at the time of publication, the judgment had not been issued..
Justin Gutmann v Apple	Claim that Apple used iOS upgrades to conceal a new 'performance management' feature that 'throttled' device processor (to address battery defects) without consumers' knowledge 26.1 million iPhone users allegedly affected; losses estimated at £853 million.	Following a hearing in September 2023, the CAT held that the PCR had met the requirements of the CPO application on the basis that it was it was "just and reasonable" for Gutmann to act as the class representative. Apple's application for strike out was dismissed. However, Apple has **lodged an application** to appeal the CAT's certification of the CPO application. If it proceeds to trial, it will be done in two-stages to address (1) whether Apple has been abusive and (2) the issue of dominance and the amount of damages payable

Class action claim	What is the consumer harm?	Current position
Elizabeth Coll v Google	Claim in region of £263 - £752 million on behalf of consumers who it's alleged suffered loss as a result of Google's alleged abusive conduct in relation to the Play Store. The claim alleged that Google (i) bundled the Play Store with other apps; (ii) imposed a contractual and technical restrictions which restrict the ability of Android app developers to distribute Android apps via distribution channels other than the Play Store; (iii) required that payments for Android app purchases be made exclusively through Google's Play Store payment processing system; and (iv) charged an excessive and unfair commission in respect of all Android app purchases.	The Claim is currently at disclosure stage of proceedings with trial anticipated for late 2025. A series of case management conferences have taken place. Google has been ordered to provide further disclosure of financial data and witness evidence, which will be subject to forensic accounting experts reviewing and agreeing the data and information that's required from Google for the purposes of their forensic accounting reports and the form in which such reports should be provided.
Alex Neill v Sony (PlayStation)	Claim for up to £5 billion (plus interest) against Sony for alleged abuse of dominant position in the following markets: • PlayStation system software; • distribution of digital PlayStation games; and • distribution of add-on content for PlayStation games. The claim alleges Sony abused its monopoly in those markets by imposing restrictive terms and conditions on developers and publishers by compelling game developers and publishers to sell via PlayStation's online store. This allegedly gave PlayStation users no alternative to purchase digital games and add-on content to games elsewhere. Consequently, it's alleged that Sony charged excessive and unfair prices for digital games and add-on content.	The CAT has granted the application for a Collective Proceedings Order (as well as dismissing Sony's application for Strike Out) in November 2023. This is approval from the Tribunal that the Claim can proceed. However, the Tribunal has granted permission for Sony to appeal the Tribunal's November 2023 decision. Although the Tribunal's view is there is no real prospect of success, they accept there is a compelling reason to grant permission for the appeal. Principally, the need for a 'conclusive decision' on the lawfulness of funding arrangements in light of a Supreme Court ruling in the case *PACCAR*.

Changes to merger control thresholds for SMS firms

A look ahead

The draft Digital Markets, Competition and Consumers (**DMCC**) Bill subjects tech firms with SMS to a much more stringent merger control regime. This is designed to give the CMA greater visibility of transactions involving the largest tech firms. The CMA's recent decision to examine whether it has jurisdiction to scrutinise Microsoft's high-value partnership with OpenAI underlines the potential limitations with the current merger control regime.

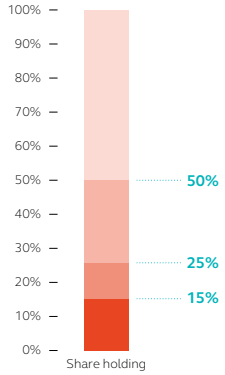
The DMCC Bill will therefore introduce a mandatory notification obligation for SMS-designated firms where a deal meets certain control and value thresholds. Unlike normal merger control rules, this includes cases where an SMS firm simply increases its shareholding without acquiring control of the target. This will give the CMA's Digital Markets Unit much greater scope to scrutinise the merger activity of the largest tech firms.

The general voluntary UK merger control regime will continue to apply for mergers not meeting the relevant requirements. But under the new proposed rules SMS firms must report mergers (prior to completion) worth £25million or more which result in the relevant SMS corporate group **increasing the percentage of shares and/or voting rights** it holds in a UK-connected body corporate to or beyond any of the following "qualifying status" thresholds:

- from less than 15% to 15% or more
- from less than 25% to 25% or more; or
- from 50% or less to more than 50%

Please read **Part 5 of our DMCC Bill in Focus** series for more information on the mandatory notification criteria (including those for joint ventures).

Strategic Market Status – mandatory reporting requirement



SMS firms must notify the CMA if:

1. the SMS firm's shareholding in the target surpasses certain **thresholds**;
2. it involves a firm that is active in the UK; AND
3. it is for a consideration, or contribution to joint venture, exceeds **£25m**.

Unlike voluntary merger reporting for non-SMS firms, reporting is mandatory.

The CMA has five working days to accept the report after the SMS firm has notified of the proposed merger. The deal cannot complete during this period and the CMA will decide whether to refer the merger for a formal investigation. A failure to comply with the obligation can lead to a fine of up to 10% of the SMS firm's global turnover.

General (non-SMS) turnover threshold changes

Old thresholds

4. Enterprises cease to be distinct; AND
5. Either:
   A. the target's UK turnover exceeds £70m; OR
   B. the parties' combined market share will be 25% or more.

New thresholds

3. Enterprises cease to be distinct; AND
4. Either:
   E. the target's UK turnover exceeds **£100m**; OR
   F. the parties' combined market share in the UK will be 25% or more; **OR**
   G. **either party has a market share in the UK of 33% or more and UK turnover exceeding £350m.**

New Safe Harbour: both parties each have a UK turnover of £10m or less.

In addition, the merger reporting thresholds will also change for more general mergers (not involving firms with SMS). You can read more about the changes in Part 5 of our DMCC Bill in Focus article, but the threshold changes for non-SMS firms are summarised above.

M&A in the tech sector: changes to the UK's national security screening regime

A look ahead

On **4 January 2022**, the **National Security and Investment Act 2021 (NSIA)** introduced a new investment screening regime for corporate transactions which might raise national security concerns for the UK. This has the potential to capture a number of deals in the technology sector (see below).

The purpose of NSIA is to protect the UK from risks posed to its national security by hostile parties acquiring control (or influence) over UK entities or assets. However, its practical remit is far broader than many similar foreign direct investment screening regimes as:

- It currently catches domestic parties and transactions with **no foreign acquirer** involved.
- The **"trigger events"** go beyond a simple change of control of a relevant business – minority investments, internal reorganisations and transfers of land, tangible moveable property (such as equipment and machinery) and ideas, information and techniques (i.e., intellectual property) are also captured.
- The regime doesn't define "national security". Instead, it lists **17 "sensitive" sectors** considered strategic enough to require a mandatory notification to the UK government's Investment Security Unit (**ISU**) where a "trigger event" involving a business operating in any of those sectors is proposed.
- It includes a **voluntary notification regime** for transactions that may otherwise be of interest from a national security perspective and gives the Secretary of State the power to **"call in"** such transactions if not notified.
- It has **retrospective effect** so a relevant transaction can be called in for review if it took place after 11 November 2020.
  - Sanctions for failing to make a mandatory notification when required to do so and going ahead with a transaction are serious; they include the transaction being legally void, a fine of up to 5% of worldwide turnover or £10 million (whichever is greater) being imposed on the acquirer; and/or
  - imprisonment up to 5 years of the acquirer's officers in certain circumstances.

Technology-focused sensitive sectors

Many of the "sensitive sectors" are relevant to technology businesses. These include: Advanced Materials, Advanced Robotics, Artificial Intelligence, Communications, Computing Hardware, Cryptographic Authentication, Data Infrastructure, Quantum Technologies, Satellite and Space Technologies.

The UK Government has produced **guidance** setting out whether the activities of an entity may fall within the sensitive sectors. You can read this alongside the very detailed **National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021**.

Between 1 April 2022 and 31 March 2023, the ISU received 866 notifications (671 of these were mandatory notifications). Of these 671 notifications, 47% related to the Defence sector but the Artificial Intelligence, Data Infrastructure, Advanced Materials and Communications sectors all also gave rise to significant numbers of notifications.

For more detail on this regime, please see our **Frequently Asked Questions** and **analysis of the Cabinet Office's Annual Report** on the regime's first full year.

Watch this space

Oliver Dowden MP, the Secretary of State overseeing the regime has launched a **consultation** asking for views on how the regime can be refined and burdens placed on businesses and investors may be reduced.
Key considerations include whether:

- there should be exemptions for certain internal reorganisations;
- the scope of some of the 17 sensitive sectors should be changed, specifically whether:
  - the definitions of Advanced Materials, Critical Suppliers to Government, Defence, Suppliers to Emergency Services and Synthetic Biology should be clarified and/or simplified;
  - the definition of AI should be narrowed so it focuses on businesses that concentrate solely on AI or incorporate or develop AI as part of a wider approach to their sector or business and whether "generative AI" should be brought within scope; and
  - the definitions of Communications, Data Infrastructure, Energy or Suppliers to the Emergency Services should be updated;
- new mandatory notification sectors for Semiconductors (currently included in Advanced Materials) and Critical Minerals should be added; and
- there should be changes to the notification forms requesting additional information to reduce the number of subsequent information and attendance notices.

The consultation's call for feedback closes on **15 January 2024** and timing of the outcome and any resulting changes to the rules aren't yet known.

DBT consultation on platform duty to consumers

Be aware

The application of consumer protection law to digital platforms and online marketplaces hasn't always been clear, in part because they typically (although not always) act as an intermediary and don't enter into direct contracts with consumers.

Digital platforms are subject to the "professional diligence" requirement under existing consumer protection laws, which will be recast in the DMCC Bill once it's in force. However, the complex statutory formulation of this test is derived from the EU Unfair Commercial Practices Directive and isn't always easy to apply in practice. Specifically, the rules on unfair commercial practices require traders to act "*…with reasonable skill and care, commensurate with honest market practice and the general principle of good faith in their field of activity".*

The Department for Business and Trade (DBT) launched a **smarter regulation consultation** in October 2023 that considered whether there should be further guidance to clarify how this test would work in practice.

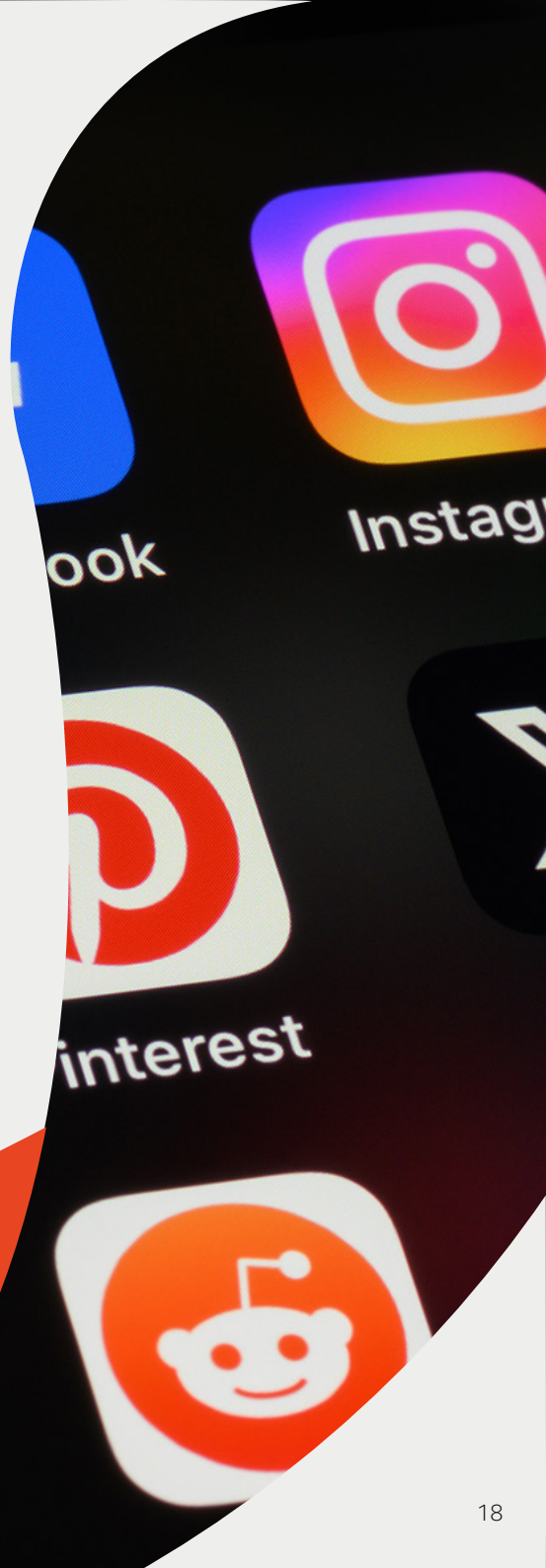
The CMA's response to the consultation made a number of proposals:

- Implementing **appropriate automated and manual moderation systems** to prevent economically harmful content appearing on the platform.
- Introducing reporting **and flagging mechanisms** to make it easy for consumers and other parties to report potentially harmful content. On becoming aware of the presence of such content (through whatever means) the platform operator should investigate promptly and tackle any economically harmful illegal content.
- Applying appropriate and effective **sanctions** to deter this content/activity in future - such as banning repeat offenders – and keeping records of sanctions.

Take action

If you operate a digital platform or online marketplace, you should consider your policies for moderating the activities of traders who use the platform and ensure they comply with any further guidance in relation to the 'professional diligence' test under the CPRs and forthcoming DMCC Bill.

At the time of publication, DBT had not published its findings from its smarter regulation consultation. It would be prudent to keep an eye out for the outcome to stay informed and consider the potential implications it may have on your business.



Amazon and Facebook decision: CMA hints at approach for regulating 'big tech'

A look ahead

On 3 November 2023 the CMA announced it had accepted commitments from **Amazon** and **Meta** in relation to its long-running competition investigations into both tech firms.

The commitments are designed to ensure fairer conditions of competition for third party sellers on both firms' marketplaces. They cover a range of issues, including alleged self-preferential algorithms and unfair use of third-party data.

The CMA avoided the need to go through the lengthy and contentious process of evidencing that Amazon or Meta breached competition laws by securing the pro-competitive outcomes it wanted to achieve via voluntary commitments. This approach might become the CMA's modus operandi for tackling competition concerns in digital markets when it gains new powers for regulating big tech under the Digital Markets, Competition and Consumers (**DMCC**) Bill. Expect to see a shift in its approach after the event interventions, to more proactive ex-ante regulation of digital markets, at least as far as "big tech" is concerned.

Amazon and Meta are both likely to be designated with Strategic Market Status (**SMS**) under the DMCC Bill, which will enable the CMA to impose bespoke **conduct requirements** similar to these commitments without needing to pinpoint any abuse of dominance by either firm. Indeed, the CMA has said that the commitments may be superseded by conduct requirements for Amazon and Meta when the DMCC Bill comes into force (although it seems likely that the CMA will initiate an SMS investigation into Meta before Amazon).

There are a number of similarities between the Meta and Amazon cases. First, both were premised on the CMA's assumption (albeit not proven) that Amazon and Meta are both dominant in their respective digital markets in the UK: Amazon for supply of e-commerce marketplace services and Meta for the supply of digital display advertising. Both cases also concerned, to varying extents, the ability of Amazon and Meta to exploit data obtained from competitors who use their platforms to benefit their own products and services.

But aside from these points the facts of the cases were different. The Amazon case focused exclusively on the Amazon Marketplace, where Amazon sell its own products alongside those of third-party sellers. Among other things, the commitments addressed specific concerns that Amazon's algorithms for determining which products featured in the highly desirable 'Buy Box' were self-preferential. In other words, they favoured their own products and/or third-party sellers who used Amazon's own fulfilment services.

> "Expect to see a shift in its approach after the event interventions, to more proactive ex-ante regulation of digital markets, at least as far as "big tech" is concerned.

The Meta case was more complex in that it involved Meta (allegedly) leveraging its dominance in the supply of digital display advertising via Facebook into a different market – namely Facebook Marketplace. Facebook Marketplace is a peer-to-peer selling platform primarily used by private sellers or small businesses. The CMA did not allege that Meta was dominant in this secondary, adjacent market (which it defined as the market for 'online classified advertising' services). However, it did claim that Meta was giving its marketplace an unfair advantage over other online classified advertising services (such as Gumtree, Etsy and eBay) who advertise on Facebook. When those competitors purchase digital display advertising on Facebook, Meta obtains certain information about the advertisers' products and customers which, in the CMA's view, was exploited by Meta to develop Facebook Marketplace in a way that wouldn't have been possible in normal market conditions. The CMA also believed there was a risk Meta could use this advertising data to develop or improve other competing products.

For more information about the commitments Amazon and Meta provided, please read our **insight**.

Increased product safety liability for online marketplaces

Be aware

The Department for Business and Trade and Office for Product Safety and Standards (**OPSS**) published a consultation in August 2023 setting out its proposals to reform and update the UK's product safety regime.

One of the key recommendations is the creation of **duty of care** requirements on online marketplaces for the identification and removal of unsafe product listings. This would require online marketplaces to assess if they're meeting due care requirements by identifying any specific risks, developing systems and processes proportionate to their business and risk level, and publicly and/or privately reporting on their performance.

> If you're an online market operator you should closely monitor these developments.

In addition, OPSS wants to ensure that online listings have clear **consumer-facing information** to make it safer for consumers to shop online by including:

- warnings to consumers;
- a clear, prominent indication of whether the product has been listed by a third-party seller (alongside the name and contact address of the seller);
- details of what checks (if any) have been carried out on the product or seller;
- key product safety information, which is already on the product, its packaging or accompanying documents.

Finally, OPSS proposes introducing enhanced **co-operation duties**, which would apply to online marketplaces when managing product safety issues and/or recalls – including engagement with enforcement bodies and third parties.

Take action

If you're an online market operator you should closely monitor these developments. In particular assess whether the product safety policies and procedures you have in place for products produced and/or sold by third party suppliers comply with the principles outlined in the OPSS consultation.

Far reaching obligations under the Online Safety Act 2023

Be aware

The Online Safety Act 2023 (**OSA**) was enacted in October 2023. It's a significant piece of legislation, imposing extensive regulatory requirements on a diverse range of online services.

Broadly, the OSA aims to make in-scope online services safer by imposing "duties of care" on companies that provide such services to have processes in place to address user safety. The OSA also appointed Ofcom as the online safety regulator and established enforcement powers to include fines of up to £18 million or 10% of global turnover, whichever's higher, for non-compliance.

Many of the OSA provisions are not yet in force but will implemented by regulations made over the coming months. Ofcom will issue codes of practice and guidance to clarify the obligations under the OSA and will supervise compliance.

Much of the media focus on the impact of the OSA has been on social media giants, but Ofcom estimates that the number of online services subject to regulation in its scope could exceed 100,000. These include three categories of internet services: user-to-user services (U2U); search services and services involving provider pornographic content.

- **U2U services** are those enabling users to generate, share or upload content other users of the service may encounter. Examples include social media services and video-sharing services but also online marketplaces, review services, gaming services and file sharing services.
- **Search services** enable a person to search some or all websites or databases so will include vertical search services that enable searching for specific products or services offered by third parties, such as insurance, flights or financial products.

U2U and search services are regulated by the OSA where they have links with the UK and are not exempt. And there's a vast range of services with obligations under the OSA.

Which of the duties of care apply depends on the size and nature of the online service. But a key duty is preventing the proliferation of illegal content and online activity. This duty requires companies providing in-scope services to establish systems and processes to improve user safety.

The OSA focuses on ensuring in-scope services are safe in the way they are designed and operated. It doesn't specify how this should be achieved but requires steps that are proportionate to the size and activities of the platform. We expect further clarity on the practical measures required under Ofcom codes of practice and guidance.

In-scope services are also required to assess whether children are likely to access their services. If so, there are additional duties under the OSA regarding the removal of content that is legal but harmful to children.

There are also duties to protect against fraudulent advertising.

Take action

All the provisions of the OSA are not yet in force. But sanctions will potentially be significant, so if you're an online service provider it's important to assess whether you're in-scope and how the OSA will impact you. You should audit your current systems and processes to map the changes required to ensure compliance, and how this will sit alongside other existing legal and regulatory obligations.

Ofcom has recently opened its consultation on **protecting people from illegal harms online** and in-scope services may also want to respond with feedback on the measures that they may be required to put in place. The consultation closes 23rd February 2024.

You should expect changes in this area of regulation to continue rapidly as jurisdictions across the world regulate, therefore the best time to take action is now.

Regulatory divergence: Online Safety Act v EU Digital Services Act

While the UK's OSA is focused primarily on safety and illegal content, the DSA has a much wider remit including rules on content moderation, online targeted advertising, the settings of online interfaces, recommender systems, and online marketplaces.

The rules under the DSA are more prescriptive as there is no general "duty of care" for in-scope firms. The relevant requirements are determined by the size of the digital platform and the services they provide.

In April 2023 the European Commission designated 17 Very Large Online Platforms and 2 Very Large Online Search Engines, which are subject to the strictest rules.

In December 2023 the European Commission opened its first formal proceedings under the DSA to assess whether X may have breached the rules in areas linked to risk management, content moderation, dark patterns, advertising transparency and data access for researchers.

CMA to be handed ‘game changing’ consumer enforcement powers

Be aware

Under the Digital Markets, Competition and Consumers (**DMCC**) Bill the Competition and Markets Authority (**CMA**) will gain new powers to impose penalties of up to 10% of global turnover on companies that breach consumer protection law.

At the moment the CMA generally tries to work with businesses to change their behaviour via undertakings when it identifies consumer protection concerns. But this approach will change when the DMCC Bill comes into force towards the end of 2024.

The changes will bring the CMA’s consumer enforcement powers in line with its existing competition/ antitrust toolkit (where multi-million-pound fines are the norm). The changes are widely viewed as ‘game changing’ for consumer law enforcement.

It is important to note that the CMA may use its power to impose penalties in relation to a wide range of unfair commercial practices in the digital space, such as:

- unfair or misleading use of AI or online choice architecture to distort consumers’ economic behaviour;
- including unfair terms in consumer contracts;
- unfair pricing practices (including ‘drip pricing’);
- false or misleading product reviews;
- misleading forms of pressure selling – see for example the CMA’s current investigations into **Wowcher** and **Emma Sleep**.

Take action

The CMA now has a laser focus on digital markets. If your business is active in this space, you should take these changes into account to minimise risk when targeting consumers online. We recommend conducting risk assessments as early as possible, throughout new product development, and before making website or app design changes, or updating terms and conditions.

For more information about the CMA’s new consumer enforcement powers, **read our focused insight**.

> The CMA will gain new powers to impose penalties of up to 10% of global turnover on companies that breach consumer protection law… this could apply to a wide range of unfair commercial practices.

New rules for subscription contracts

Be aware

The consumer protection rules for subscription contracts will change when the DMCC Bill comes into force.

The government intends to introduce a new, more stringent set of rules for auto-renewing contracts, so consumers don't find themselves trapped in subscriptions they either don't want, or don't realise they're still paying for.

The proposed rules mean traders will have to:

- Provide consumers with **key information** about the subscription before they enter the contract, including how it will operate, how much it will cost after any free or discounted trial period, the frequency of payments and how to exit the contract.
- Send consumers **reminder notices** before renewal payments are due. These must specify when and how much they will be charged and how they can cancel before they're liable to pay. These need to be sent at six-month intervals and, for contracts with free or discounted trial periods, before a consumer's first full payment is due. An extra notice will also need to be sent in advance of renewals of 12+month contracts. Recent amendments to the Bill allow the Secretary of State to disapply these rules for certain types of trader / contract.
- Introduce a **14-day renewal cooling-off period** following the expiry of a free or discounted trial period when the consumer starts paying the full price of the contract, and again on renewal of a 12 month+ subscription contract.
- Inform consumers of their 14-day cooling-off rights and how to exercise them by sending them a **cooling-off notice** when their free / discounted trial is about to expire or their 12 months+ contract is about to renew.
- Make sure consumers can **exit their subscription easily**, in one single communication with no unnecessary steps, as well as sending them a **cancellation notice** to confirm this.

Contracts for utilities, financial services and childcare are expressly excluded. However, the definition of a subscription contract under the DMCC Bill is very wide so it is reasonable to expect that most auto-renewing contracts will be captured.

> The government intends to introduce a new, more stringent set of rules for auto-renewing contracts, so consumers don't find themselves trapped in subscriptions...

Consumers will be able to cancel their contracts without penalty and with immediate effect if traders fail to meet a number of these requirements, including if they're not sent a reminder notice or given the ability to exit the contract easily. Any terms that contravene the rules will also be unenforceable.

This chapter of the Bill is also within scope of the **CMA's new enforcement powers**, so failure to comply could result in penalties of up to 10% of global turnover.

Take action

It's important to be aware that the finer detail of the new rules for B2C subscription contracts is still being debated in the House of Lords and, in any event, is likely to be supplemented by secondary legislation.

Nevertheless, as compliance with these new rules will require changes to subscription terms and conditions, as well as front- and back-end processes, traders may want to consider getting the ball rolling with implementing these changes ahead of the commencement of the Bill, currently expected in Autumn 2024.

Read more about the new subscription contracts rules in Part 2 of our **DMCC Bill in Focus** series.

Further regulation of drip pricing and hidden fees

Be aware

On 24 January 2024, the Government announced that it would legislate to crack down on the practice of 'drip pricing' and hidden fees, as part of the DMCC Bill.

Drip pricing happens when consumers are presented with a first price for a product or service (known as the base price) at the beginning of the sales journey, with additional fees being introduced (or 'dripped') as they move towards checkout.

The Department for Business for Trade (**DBT**) is concerned this can result in consumers being 'baited' into choosing a product because of its lower base price, then ultimately ending up paying more once further fees or products are added.

There are instances when genuinely optional new prices might be presented towards the end of the checkout process – for example, a charge for gift wrapping. These should be distinguished from fixed mandatory charges consumers can't avoid (like booking fees for cinema and train tickets). The CMA explored this issue in its **online car hire intermediaries** investigation and found that the headline price for a car rental must include all compulsory additional charges.

In its announcement, the Government was clear that the ban **will only apply to mandatory hidden fees**, not optional ones. It gives the example of airline seat upgrades for flights as a kind of optional extra that would not be caught by the new rules.

For now, it remains unclear how the new rules will be implemented and, as always, the devil will be in the detail. In particular, the legal position is less clear in cases where charges are mandatory but **variable** in nature (i.e., they cannot reasonably be calculated in advance) or when it isn't clear if additional charges can genuinely be described as 'optional'. In its October 2023 consultation, DBT provided these examples of dripped charges that may be **inaccurately described as optional**:

- traders selling phones and adding charging cables as an optional fee;
- toys being sold without the required batteries, which are charged as an optional fee to consumers;
- long-haul flight tickets being sold to consumers without luggage, which is then charged as an optional fee later in the purchasing process.

> The DBT is concerned this can result in consumers being 'baited' into choosing a product because of its lower base price, then ultimately ending up paying more once further fees or products are added.

The **CMA's responses to the DBT consultation** recommended that the ban should extend to other charges which are 'optional' but which it is reasonably foreseeable that most consumers would pay. The CMA also wants a requirement that mandatory variable and 'optional' charges are included in the stated headline price, to prevent some traders keeping their headline price low by simply making all such charges variable or 'optional'.

As we await further detail and guidance on the new rules it's not yet clear how far the government will go in addressing the CMA's concerns via legislation.

Thankfully, the DBT consultation in 2023 did recognise that a 'one size fits all' approach to regulation may be counterproductive since pricing practices can vary significantly across different industries. This is particularly relevant in digital markets as customer sales journeys often vary hugely depending on the products or services being sold. For example, an online food delivery order process will look very different to the checkout process for purchasing cinema tickets or buying goods on an online marketplace.

Take action

If you promote more complex products with various layers of pricing, you should continue to monitor developments in this space closely. It is likely that there will be further stakeholder consultations and we recommend that you engage with these to ensure any subsequent guidance or regulation accurately reflects the nuances of your business practices.

New regulations for online product reviews

Be aware

There are currently no specific UK laws targeting fake product reviews. Knowingly buying or selling fake reviews is likely to breach existing consumer protection laws (which are flexible and principle-based) but there's a long-held belief that the consumer protection laws should specifically cover this kind of behaviour.

The DMCC Bill will change that by giving the Secretary of State the power to use secondary legislation to add to the current list of banned unfair commercial practices at Schedule 18 of the DMCC Bill [1].

The Department of Business and Trade's (**DBT**) recent consultation clarifies this extension of banned unfair commercial practices and will likely cover:

- Submitting a fake review, or commissioning or incentivising any person to write and/or submit a fake review of products or traders.
- Offering or advertising to submit, commission or facilitate a fake review.
- Misrepresenting reviews, or publishing or providing access to reviews of products and/or traders without:
  - taking reasonable and proportionate steps to remove and prevent consumers from encountering fake reviews; and/or
  - taking reasonable and proportionate steps to prevent any other information presented on the platform that is determined or influenced by reviews from being false or in any way capable of misleading consumers.

Take action

The DBT consultation is clear that online retailers and marketplaces must take **reasonable and proportionate steps to remove and prevent consumers from encountering fake reviews** when the new amendments are adopted.

The CMA is expected to publish formal guidance setting out what it expects traders to do to comply with this obligation. But this new requirement will likely involve having policies and processes in place for regularly and proactively assessing risk, detecting suspicious reviews, removing fake reviews, and sanctioning those who facilitate or post them.

If the government does ultimately press ahead with the proposals outlined in the DBT consultation, online retailers and marketplaces will need to reflect carefully on the policies and procedures that underpin their product reviews – including content moderation. This is particularly important if AI tools are used to screen and filter reviews that don't comply with the site's terms of use.

For more information on the use of AI to manage consumer reviews, read our earlier article on "**Integrating AI into B2C products: assessing the consumer protection risks**".

> … online retailers and marketplaces will need to reflect carefully on the policies and procedures that underpin their product reviews – including content moderation.

1 Note that the DMCC Bill revokes the CPRs and moves the operative provisions to Part 4 of the DMCC Bill largely unchanged, save for a few subtle amendments.

UK cyber resilience framework to be strengthened

Be aware

In early 2023, the government announced its intention to reform the Network and Information Systems Regulations 2018 (**Regulations**) to strengthen the security of digital services in the UK.

The Regulations require "operators of essential services" within key sectors and "digital service providers" (**DSPs**) like online marketplaces and cloud service providers to implement appropriate and proportionate security measures and to report incidents. And there are penalties of up to £17 million for non-compliance

The government also proposes to update the Regulations to bring "managed service providers" (**MSPs**) within the definition of DSPs. MSPs will be subject to the Regulations if they provide services on a B2B basis, relating to the provision of IT services, which rely on the use of network and information systems, and involving regular and ongoing management support, active administration and/or monitoring of IT systems, infrastructure or networks. The government has provided a non-exhaustive list of example services that will be within scope, which include: IT outsourcing, private WAN/LAN managed services, application management, managed security operations centre services, security monitoring and incident response.

Other proposed reforms include:

- a risk-based, two-tier supervisory regime for DSPs;
- expanding incident reporting obligations;
- future-proofing the Regulations by providing ministers with delegated powers to update the Regulations, expand their scope and designate critical suppliers.

> "...there are penalties of up to £17 million for non-compliance.

Take action

If these reforms go ahead, businesses that are not currently subject to the NIS Regulations will be brought within scope. You should consider whether you, or your suppliers, will be covered by the expanded scope. And if so, ensure you comply with the requirements to take appropriate and proportionate security measures, and have processes in place to report cybersecurity incidents.

International data transfers: where are we now?

Be aware

With the recent focus on transfers of personal data from the EU and UK to the US, the international data transfers landscape is continuing to evolve.

First, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework (**DPF**) in July 2023, following a period of legal uncertainty for organisations transferring the personal data of EU individuals to the US. It concludes that the US ensures an adequate level of protection for the transfer of personal data of EU individuals to companies in the US participating in the DPF.

The UK closely followed, with the Data Protection (Adequacy (United States of America) Regulations 2023) implementing the UK-US data bridge (**Data Bridge**). The Data Bridge came into effect on 12 October 2023 and determines that the US provides an adequate level of protection for personal data transfers of UK individuals to organisations located in the US, provided that the US organisation is certified to the DPF and is participating in the UK extension to the DPF.

This is good news in practice. It means organisations can send personal data freely from the EU and UK to US companies participating in the DPF and the UK extension to the DPF, without the need to undertake a transfer impact assessment (**TIA**) or implement any additional safeguards (such as supplementary measures). This will likely accelerate internal processes for organisations looking to contract with US companies, and potentially reduce associated costs too.

However, some notable reservations remain over both the DPF and the Data Bridge:

- Whilst the ICO indicated in a recent **Opinion** that the Data Bridge provides an adequate level of data protection, the ICO also flagged four areas of concern that could pose risks to UK individuals if the protections identified are not properly applied.
- An application by a French MP to annul the DPF was recently dismissed by the European Union General Court. However, the DPF is still susceptible to further challenge.

Take action

If you're an EU/UK organisation intending to rely on the DPF and the UK extension to the DPF, you'd be well-advised to incorporate the standard contractual clauses (**SCCs**) into your contracts with US companies. The SCCs could apply contractually as a "fallback" position to permit the continued flow of personal data to the US, in the event the DPF and/or the UK extension to the DPF is withdrawn, invalidated and/or the US company fails to remain certified.

As a result of the above (and the significant risk of legal challenge to the DPF), we expect many organisations will continue to rely on the SCCs as their primary transfer mechanism of choice. Although organisations relying on the SCCs for transfers to the US should still undertake a TIA, due to the legally binding safeguards introduced under Biden's Executive Order 14086 (which formed the basis for the respective adequacy decisions adopted by the EU and UK), this process should be significantly streamlined. It's also more likely that organisations may decide that supplementary measures aren't required.

Finally, it's important to be alert to further changes to the UK's approach to international data transfers. The Data Protection and Digital Information Bill (**Bill**) introduces a new "data protection test" when undertaking personal data transfers to third countries. Because it's intended to further streamline the regulatory burden on businesses in this area, it's worth watching progress closely.

> "… the ICO also flagged four areas of concern that could pose risks to UK individuals if the protections identified are not properly applied.

Data Protection and Digital Information Bill intended to become law in 2024

Be aware

The Data Protection and Digital Information Bill (**Bill**) was introduced in the House of Commons on 8 March 2023, replacing a first bill that had been paused in June 2022.

It's designed to make the UK's data protection regime more practicable and less burdensome for businesses than the current regime under the UK's version of the General Data Protection Regulation (**UK GDPR**).

The Bill introduces reforms including:

- Replacing the traditional role of "data protection officer" with an obligation to appoint a "senior responsible individual", required for public bodies or organisations carrying out high-risk processing.
- Amending the obligation to keep records of processing activities, so that these only apply to organisations carrying out high-risk processing.
- A non-exhaustive list of examples of processing activities that may be necessary for the purposes of legitimate interests, including direct marketing, intra-group data sharing for administrative purposes and ensuring IT security.
- A list of "recognised legitimate interests", which can be relied on without having to carry out the balancing test typically required to rely on legitimate interests as a lawful basis.
- Hanging the threshold of "manifestly unfounded or excessive" for refusing to respond to data subject rights requests, to a right to refuse requests that are "vexatious or excessive".
- Amending the obligations relating to automated decision-making to make these more permissive than the current regime.
- Amending the Privacy and Electronic Communications Regulations 2003 (**PECR**) to add new exemptions to the consent requirements for setting cookies, with the effect that cookies presenting a low risk to people's privacy will not require consent.
- Ringing the regulator's enforcement powers for breaches of the PECR in line with the UK GDPR. An organisation can currently be fined up to £17million or 4% of turnover for UK GDPR breaches, but fines for breaches of PECR are capped at £500,000.

Take action

The Bill is still in draft form and is making its way through UK legislation. However, you should keep a close eye on its progress and any further amendments to the obligations we've mentioned above. The proposals don't represent a wholesale change to data protection laws; rather, they're minor amendments aimed at reducing some of the burden on businesses in low-risk processing situations. Many businesses will choose to retain their existing UK GDPR standards of compliance, particularly those organisations that operate on a global level and are likely subject to both UK and EU data protection law.

> The Bill is still in draft form and is making its way through UK legislation. However, you should keep a close eye on its progress and any further amendments to the obligations we've mentioned above.

Rise of payment orchestration and related legal considerations

A look ahead

Digital businesses want greater global reach as they expand into different geographies and to be able to offer the latest payment options, quickly and seamlessly. But payment service providers can't offer all payment methods and currencies in all geographies. So, to plug this gap and enable the payment processing capability of businesses to align with their strategic roadmaps, a new payments model is emerging with a 'many to many' technical mindset: payment orchestration platforms (**POPs**).

POPs can have significant benefits for digital businesses. However, because they're complex, it's important businesses considering implementing them fully understand their risks, and benefits.

What is payment orchestration?

POPs integrate and manage different payment service providers, acquirers, payment gateways, banks and other value add services (such as fraud technology) on a single, unified software layer. This enables businesses to integrate with several different payment processors via a single API. As well as reducing implementation complexity, POPs are able to centralise the reconciliation and processing of customer data from these various payment services providers, giving businesses more holistic oversight of their payments data and related trends.

"POPs can have significant benefits for digital businesses. However, because they're complex, it's important businesses considering implementing them fully understand their risks, and benefits.

Benefits of POPs for businesses include:

- access to a variety of payment methods and payment processors across the world;
- integration of value-add fraud and compliance services;
- reduced likelihood of false declines;
- greater ability to route transactions to specific payment processors;
- potential for lower processing fees;
- valuable data insights.

Risks to address

While payment orchestration may be a 'one stop shop' for businesses from a technical integration perspective, the laws and rules that regulate payments are still complex and the use of POPs doesn't reduce the risks associated with the payments cycle for either the procuring merchant business or its downstream payment services providers. So, in addition to having a contract with their POPs providers, businesses will almost certainly need to enter into direct contracts with payment services providers. This will be necessary to cover off key areas such as card scheme and regulatory requirements (e.g., anti-money laundering), settlement of funds, the processing of data and other elements of the payments cycle those POPs providers are unable to sub-contract. Depending on the extent and nature of a merchant's payment stack, this network of related contracts could be extensive and span a number of territories. Merchant businesses will want to ensure these contracts are properly dovetailed with each other to ensure clarity and alignment on important matters such as liability and termination.

The POPs provide the technical 'middleware' that orchestrates which payment options are offered and how they work together. For certain elements relating to the API / technical integration, data encryption, data analytics and those elements it is able to sub-contract, the POPs provider acts as prime contractor and effectively subcontracts certain elements of the payment cycle to third party providers that it integrates with. This could be items such as point-of-sale terminal equipment hire, fraud screening solutions or other ancillary services. As the merchant business is therefore one step removed (contractually) from the third parties actually providing certain elements of the services in this scenario, it has no privity of contract with them and relies upon the POPs provider to negotiate (and stand in front of) important operational aspects of the relationship, such as service warranties and service levels for those elements. The warranties, service levels and other payment service-related terms offered by third party providers to POPs to onward offer to their merchant business customers are likely to be minimal (if offered at all), and only the largest merchant businesses may be in a position to force the POPs providers to procure better ones.

Although POPs can harness greater economies of scale in their pricing, they may be operating with several different subcontractors across several regions and so are very unlikely to offer fixed processing costs for a specific, fixed term. Any price increases (whether pass-through or otherwise) are likely to be passed on to merchant business customers immediately (or on short notice), making cost forecasting difficult. Additionally, merchant businesses shouldn't overlook the total end-to-end processing costs. For example, factoring-in all added costs under the separate, direct contracts it has with payment services providers involved in their funds flow and payments cycles.

With the addition of another party and layer of integration in a merchant's payment stack, the personal data mapping and analysis for each payment service becomes a little more complex and (consequently) carries a little more risk. As all payments operate from one layer of technology, a POPs provider represents a single point of failure in the event of an outage (or indeed insolvency) and so merchant businesses will be keen to ensure robust business continuity plans are in place, together with strong service levels on availability.

The breadth of connectivity into acquirers and payment methods also defines the robustness of a POPs provider's service, which can become outdated quickly if it doesn't keep pace. Merchant businesses should ensure contracts include continuous improvement obligations on the POPs provider, and larger businesses may be able to take it a step further by dictating which payment services are integrated. POPs providers (conversely) will want to remain truly agnostic and in full control of their strategic roadmaps, and so they're likely to resist such provisions.

> "…merchant businesses will be keen to ensure robust business continuity plans are in place, together with strong service levels on availability.

Balancing AI opportunities and risks in payments

A look ahead

The Payments sector is increasingly harnessing the benefits of AI technology. Tangible use of AI within Payments is evidenced by the acceleration of online banking, digital wallets, and the more recent use of payment authorisation via facial recognition. And voice shopping and actionable audio adverts are also becoming more common. In addition to being instrumental at the point of sale, AI can streamline backend processes, help to detect and minimise fraud, analyse transactional data trends, personalise e-commerce experiences and automate onboarding. Without doubt, AI is already a key player in the Payments ecosystem, and its significance to this sector looks only set to increase. We touch on some of the key benefits and risks for the Payments sector below.

Automation

For both merchants and payment services providers, AI can be useful in automating tasks, reducing margin for error, and improving efficiency. For example, real-time fraud detection can be accentuated through AI tools, given their capability to review significant quantities of data at speed, extract potential fraud incidents, flag associated risks and ultimately serve as valuable fraud mitigation assets.

Invoice payment processing can also be facilitated by AI, removing the need for manual data entry and reconciliation. Onboarding processes can benefit similarly, via AI complementing automated document authentication and identity verification. For transactions meanwhile, the ability to store and automatically populate payment details via AI can speed up the payments process and allow payers to quickly access multiple payment methods via their preferred devices. These automation efficiencies can improve the speed, efficiency and safety of onboarding and transaction processing, in turn bolstering productivity and consumer confidence for payment service providers and their merchants.

Data analysis

AI data analytics can allow both payment service providers and merchants to access and analyse data more granularly than ever before to improve their market and customer insights and promotional activities. Transaction patterns, browsing habits and information on demographics can be collated and analysed by AI tools alongside wider data sets to maximise understanding and anticipation. By doing so, AI tools can help to predict future payments, not only in terms of which products and services consumers and businesses are inclined to spend money on, but also on the methods they are most likely to use when doing so.

The ability of AI to monitor trends and improve data analytics can be leveraged by payment service providers and merchants to inform their marketing, opportunities, investment, and strategy. Those players confidently moving beyond their exploratory phase of AI and capitalising on the advantages in these areas will no doubt reap the benefits.

> Legally, the use of AI and related data and outputs gives rise to several complex legal considerations.

Risk

However, AI in Payments is not without risk, both practically and legally. While the technology can be used successfully by payment service providers and merchants, it can also be used by fraudsters to maliciously to exploit data, improve impersonation, and facilitate convincing and elaborate scams.

Legally, the use of AI and related data and outputs gives rise to several complex legal considerations. These include data protection law compliance (where personal data is involved), regulatory compliance (particularly where tools are used to support regulated processes, such as onboarding) intellectual property licensing and ownership and the allocation of risk across those involved in the AI supply and procurement arrangements.

Provided the risks are appropriately navigated and mitigated, the further integration of AI across the Payments sector is a welcome development. As the Payments sector use evolves, those taking advantage of AI technology should ensure they are doing so compliantly and in a way that maximises their ability to lawfully commercialise outputs.

TLT contacts

Daniel Lloyd
Partner – AI, Consumer, Platforms and online marketplaces

m +44 (0)7715 766 602
e daniel.lloyd@tlt.com

Emma Erskine-Fox
Managing Associate – AI, Data protection and cybersecurity

m +44 (0)7811 805 133
e emma.erskine-fox@tlt.com

Richard Collie
Managing Associate - AI, Consumer, Competition and digital markets

m +44 (0)7788 336 803
e richard.collie@tlt.com

David Gardner
Partner – Crypto, Payments

m +44 (0)7833 483 362
e david.gardner@tlt.com

Clare Stothard
Partner – Crypto

m +44 (0)7816 370 156
e clare.stothard@tlt.com

Adam Kuan
Partner – AI

m +44 (0)7929 723 719
e adam.kuan@tlt.com

Alanna Tregear
Partner – Crypto

m +44 (0)7976 890 052
e alanna.tregear@tlt.com

Gareth Oldale
Partner – AI, Data protection and cybersecurity

m +44 (0)7584 706 566
e gareth.oldale@tlt.com

Duncan Reed
Partner – AI and Consumer

m +44 (0)7825 922 908
e duncan.reed@tlt.com

Stuart Murray
Partner – Competition and digital markets

m +44 (0)7976 939 249
e stuart.murray@tlt.com

Alex Williamson
Partner – Payments

m +44 (0)7500 033 818
e alex.williamson@tlt.com

Grace Roddie
Managing Associate – Data protection and cybersecurity

m +44 (0)7890 596 192
e grace.roddie@tlt.com

Molly Efford
Associate – AI, Consumer, Competition and digital markets

m +44 (0)7813 998 122
e molly.efford@tlt.com

Emily Rhodes
Associate – Consumer, Platforms and online marketplaces

m +44 (0)7790 360 106
e emily.rhodes@tlt.com

Liz Smillie
Associate – AI, Consumer, Competition and digital markets

m +44 (0)7970 496427
e elizabeth.smillie@tlt.com

About TLT

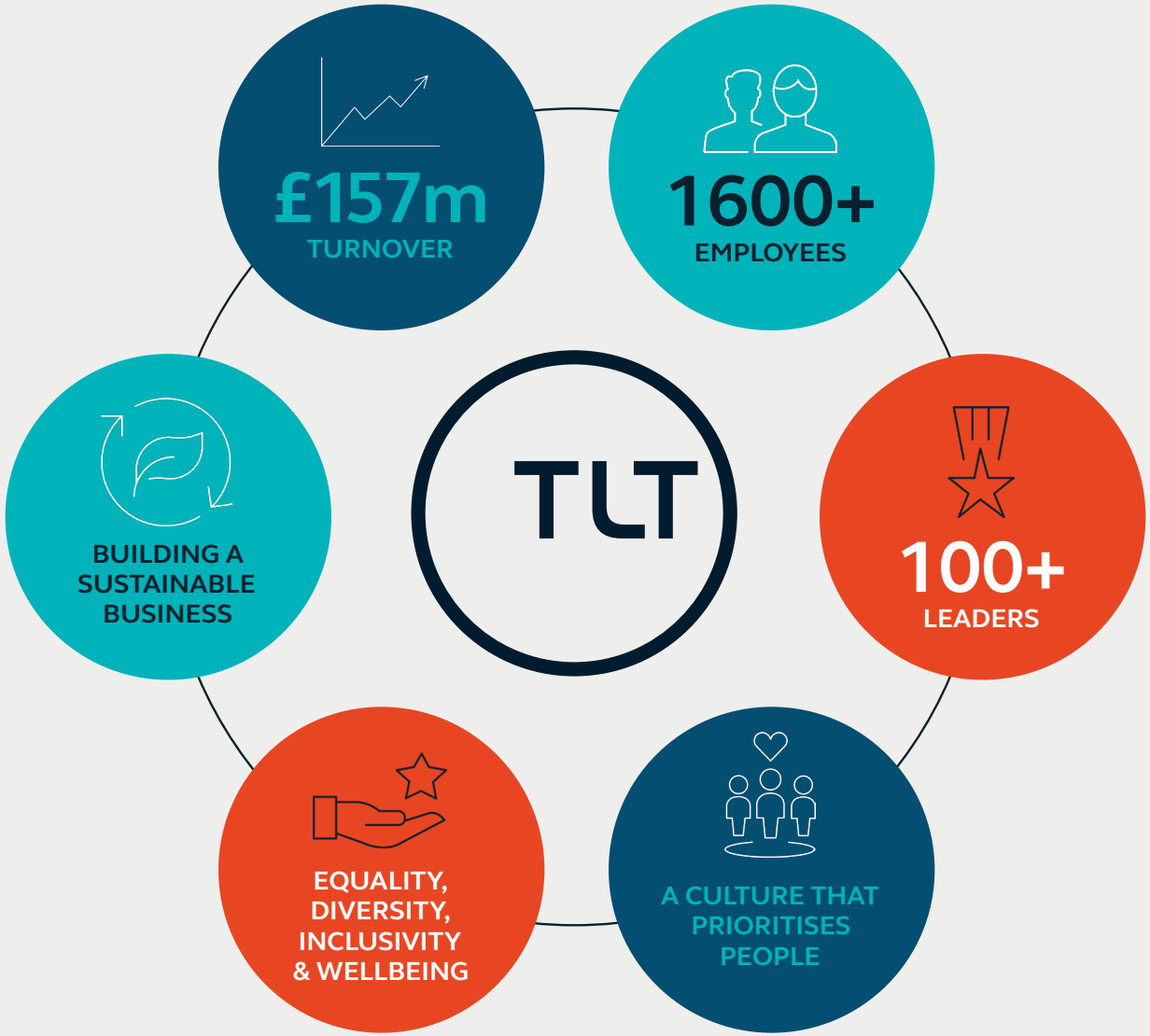
For what comes next

We're your business advisers as well as your lawyers, working in step with you to protect your interests today and progress your ambitions for tomorrow.

With local, national and international reach, we draw on our diverse expertise to find solutions and look ahead to create new opportunities. In an unpredictable world, your business adapts and evolves to succeed, and so do we. Bringing together our expertise with efficient processes and integrated technology, we'll anticipate change to keep you ahead of your challenges.

Whether it's building relationships or the sustainability of our actions, we think long term – working with you to put people, communities and the environment at the forefront. Your success is our responsibility. No half measures, part of your team and with you every step of the way.

tlt.com



tlt.com/contact

Belfast | Birmingham | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus