RPC

Snapshots for Meta

Key UK and EU developments for Meta's commercial lawyers

The UK's new Data (Use and Access) Bill

ICO statement on AI generative model training

New Safer Phones Bill aims at "making social media less addictive" for young people

Ofcom rolls out implementation phases for compliance with the Online Safety Act

WINTER 2024

RPC Snapshots app

Google Play

Apple Store

Welcome to the winter 2024 edition of Snapshots for Meta

We aim to cover everything Meta's lawyers need to know in the UK and EU from the previous quarter (well, almost!). We hope it hits the spot, as we aim to address most of the key changes affecting Meta, including data, digital, consumer and advertising developments as well as the latest UK commercial case law. Please do let us know if you have any feedback or queries.

Best wishes
Olly

Olly Bray
Senior partner
oliver.bray@rpclegal.com

WITH THANKS TO OUR FANTASTIC CONTRIBUTORS

- Amy Blackburn
- Helen Yost
- Hettie Homewood
- Praveeta Thayalan
- Gowri Chandrashekar
- Sami Thompson
- Jessica Kingsbury
- Ela Broderick-Basar
- Kiran Dhoot
- Lewis Manning
- Abbey Smith
- Rory Graham
- Mia Pullara
- Carla Skelton-Garcia
- Ed Warren
- Aiswarya Nadesan
- Maddie Wakeman
- Joey Tran
- Brendan Marrinan
- Oluchi Nnadi
- Abigail Gim
- Andy Hodgson
- Kristin Smith
- Joe Towse
- Charlie Osborne
- Dom Barnes
- Megan Latham
- Filippo Marchiori
- Briana Cumberbatch
- Elizabeth Terry
- Oliver Clarke

EDITORIAL

Sub-editors Olly Bray, Eleanor Harley, Joshy Thomas, Praveeta Thayalan, Abigail Gim

Design Rebecca Harbour

Contents

The UK's new Data (Use and Access) Bill

The question

What does the UK's new Data (Use and Access) Bill (the **Data Bill**) mean for businesses?

The key takeaway

The Data Bill, whilst not as ambitious as the previous Data Protection and Digital Information Bill (the **DPDI Bill**), introduces several new business-friendly changes to the UK data protection regime.

The background

The previous Government had introduced the DPDI Bill as a progressive, business-friendly framework that would cut down on costs and paperwork. The DPDI Bill then went through several iterations and was described as a 'Christmas-tree' bill for the number of different provisions it sought to include. On the whole, however, the new regime would still have been very similar to the EU GDPR on the basis that too great a departure would threaten the UK's EU adequacy (which is also a concern with the new Data Bill).

Ultimately, the DPDI Bill did not pass through Parliament before its dissolution on 24 May 2024 ahead of the general election on 4 July 2024 and it failed to become law. Eyes were on the new Government as to whether it would resurrect the DPDI Bill and in what form.

The development

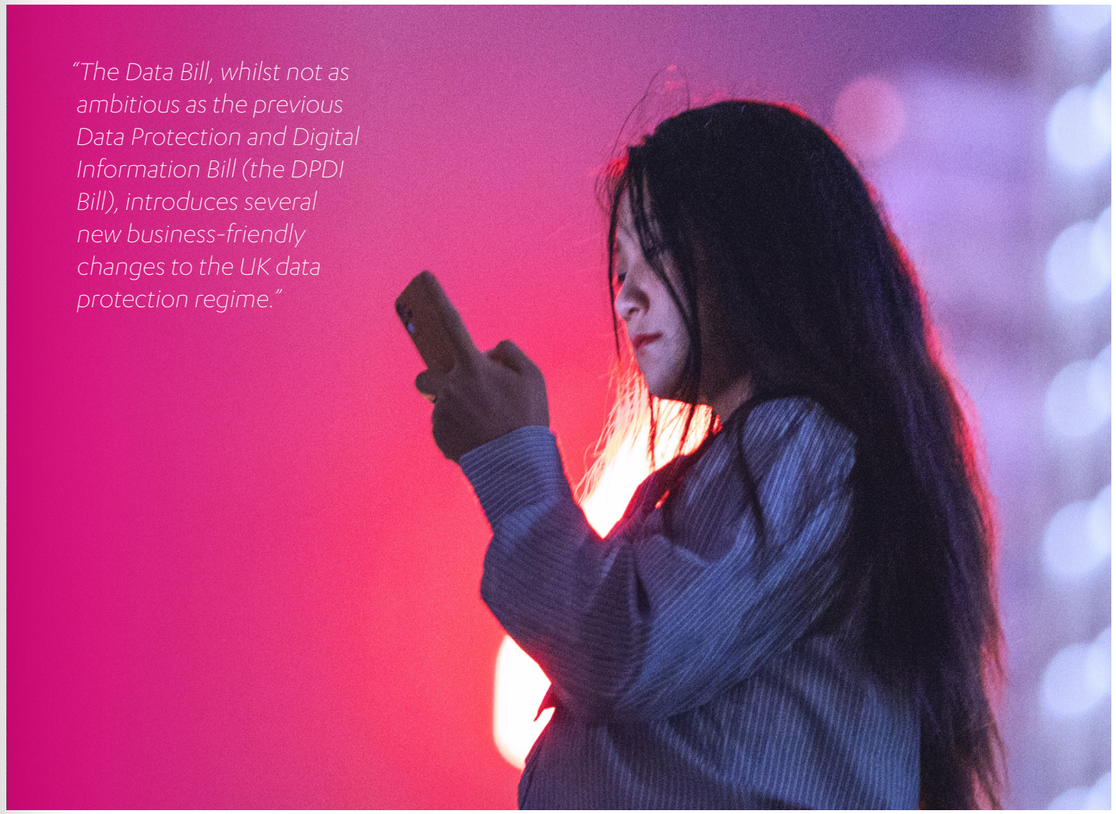
On 23 October 2024, the Government introduced the Data Bill to Parliament. Like the DPDI Bill, the Data Bill serves multiple purposes. In addition to making GDPR-specific changes, the Data Bill introduces a new Smart Data scheme (that allows for the sharing and access of customer and business data), new digital verification services, and changes to the structure of the ICO.

The Data Bill introduces the following amendments to the UK data protection regime:

- **legitimate interests**: the Data Bill includes certain "recognised legitimate interests" which do not require that a balancing test is performed to be relied on as a lawful basis of processing. Additions to this list can be made by the Secretary of State but must be in the public interest. Otherwise, businesses can rely on the existing legitimate interest lawful basis subject to performing the balancing test. The Data Bill includes certain types of processing that might fall within this category eg processing for direct marketing, intra-group transmission for admin purposes and to ensure security of IT systems (these examples were already in the recitals of the UK GDPR but for clarity have been moved into the substantive provisions)
- **automated decision-making**: the Data Bill permits automated decision-making in many cases. However, there are safeguards to protect the rights and interests of the data subject for 'significant decisions' based solely on automated processing. These include providing information about the automated decision-making and allowing the affected individual to make representations, obtain meaningful human intervention and contest decisions
- **research and statistics**: the Data Bill clarifies the meaning of scientific research purposes and statistical purposes in the UK GDPR. For example, it makes clear that data processing in the context of privately-funded commercial activity or technology development can still benefit from the provisions related to scientific research as long as the activities can reasonably be described as scientific
- **data protection test**: the Data Bill provides for a new "data protection test" instead of the adequacy test under the EU GDPR to be carried out prior to any international transfer. Organisations will be required to consider whether the standard of data protection in a third country is "not materially lower" than that under the UK GDPR
- **special category data**: the Data Bill allows the Secretary of State to amend the Article 9 prohibition on processing special category data to add new special categories of data (eg neuro data), state that certain processing does not fall within the prohibition and amend how an exception to the prohibition should apply
- **DSARs**: the Data Bill codifies case law by providing that organisations only have to carry out reasonable and proportionate searches when responding to a DSAR but must do so "without delay" and in any case within a month of receiving the request, subject to exceptions where an extension is available
- **processing purposes**: the Data Bill clarifies when processing may be carried out for a new purpose which is compatible with the original purpose of processing
- **PECR**: the Data Bill aligns the fine for PECR breaches and the time limit for reporting PECR breaches to the GDPR standard in both cases. It also introduces an exception to the requirement for consent for certain non-intrusive cookies or similar technologies (eg to measure website use in order to improve the site), provided that users are given clear and comprehensive information about the cookies and an opportunity to object.

DATA

"The Data Bill, whilst not as ambitious as the previous Data Protection and Digital Information Bill (the DPDI Bill), introduces several new business-friendly changes to the UK data protection regime."



On the other hand, the Data Bill does not include the following amendments that were proposed in the DPDI Bill:

- **accountability**: the DPDI Bill sought to simplify the accountability regime for organisations by introducing the concept of a Senior Responsible Individual (to replace a DPO), limiting the obligation to produce records of processing activity only to high risk processing, replacing data protection impact assessments with assessments of high risk processing, and removing the requirement for overseas organisations to have a UK representative. These changes have not been carried through
- **definition of personal data**: the DPDI Bill intended to restrict the definition of "personal data" to where the information is identifiable by the controller or a third party by reasonable means. This has not been carried into the Data Bill
- **vexatious/excessive requests**: under the DPDI Bill, organisations had the right to refuse a data subject request where it was vexatious or excessive. This light has been removed.

Why is this important?

The Data Bill is the Labour government's attempt at recalibrating the UK's approach to data protection, after the previous Government failed to push the DPDI Bill through. The narrower scope of the Data Bill will disappoint businesses expecting a less burdensome regime, but this may be a tactical decision to ensure that the UK does not lose its EU adequacy. However, with the more ambitious DPDI Bill, organisations that operate across the UK and EU would have needed to decide how to manage both sets of requirements – either adopt a dual-track system for the UK and EU or require that the entire business complies with the stricter EU regime. With the more limited changes proposed by the Data Bill, such organisations will not need to make such strategic decisions, but they may be able to take advantage of minor tweaks to their UK processing.

Any practical tips?

The Data Bill is currently making its way through the House of Lords before continuing through the House of Commons. It's still very early days and the text may go through several rounds of amendments. However, much of the Data Bill had cross-party support when it appeared in the DPDI Bill and some of the more controversial reforms to the data protection regime have been removed, so the Government's target of achieving Royal Assent by Spring 2025 with commencement later in the year does not seem overly ambitious. Clearly it is worth keeping track of the draft through the Parliamentary process and to begin assessing how these changes may affect data processes within specific business areas.

New standard contractual clauses for data importers outside the EAA but subject to the GDPR

The question

Are the EU's Standard Contractual Clauses (**SCCs**) needed if a data importer is located outside the European Economic Area (**EEA**) and already directly subject to the EU General Data Protection Regulation (**EU GDPR**)? In other words, where third party controllers and processors are based outside the EAA but subject to the GDPR, do you still need the SCCs to enable a lawful international transfer to them?

The key takeaway

Organisations engaged in the transfer of personal data to jurisdictions that are not considered to offer an adequate level of protection under the EU GDPR for that data should be aware that new SCCs are being developed for the scenario where the data importer is themselves subject to the GDPR.

The background

The EU's revised and modernised SCCs, which were published by the European Commission on 27 June 2021 (**Current SCCs**) are a template set of terms and conditions that can be incorporated into contractual arrangements to facilitate compliance with international data transfer requirements under EU law. This is one way in which organisations that are subject to the EU GDPR can ensure that certain standards of data protection are adhered to when transferring personal data internationally to a "third country" outside of the EEA (meaning one that is not considered to offer an equivalent level of protection for personal data to that in the EU itself).

The Current SCCs consist of four modules, which should be incorporated into contracts between a data importer and a data exporter depending on the processing relationship in question. For example, Module 1 relates to controller-to-controller data transfers while Module 2 is applicable to controller-to-processor data transfers. The Current SCCs have also been used by the UK Government as the basis for UK-specific SCCs through the introduction of an Addendum to the Current SCCs. This means they can be adapted for use, in a UK law context, to comply with the restricted transfer requirements under UK data protection law.

The development

On 12 September 2024, the European Commission announced its intention to launch a public consultation on a proposed new module of the Current SCCs, which will cover international data transfers where both the data exporter and the data importer are subject to the EU GDPR (**New SCCs**). This scenario is not currently covered by the Current SCCs, and the European Commission has faced calls to address this gap.

These calls for a revised, specific set of SCCs that deal with this scenario were heightened following the decision by the Dutch DPA (**DPA**) to fine Uber €290 million for its failure to adequately protect the personal data of its drivers when transferring this data to its servers in the US (see Snapshots Autumn 2024 for further information on this decision). Significantly, the DPA rejected Uber's argument that SCCs were not required even though Uber's US entity was already subject to the EU GDPR as a joint controller of personal data that came within the scope of the legislation. This case exposed a clear gap in the Current SCCs, which the Commission has sought to address with the announcement of a public consultation over this proposal for New SCCs.

Drafts of the New SCCs have not yet been released; however, their publication is expected in advance of the launch of the public consultation. The public consultation is planned for the fourth quarter of 2024, and it is anticipated that the New SCCs will be adopted by the Commission in the second quarter of 2025.

Why is this important?

As drafts of the New SCCs have not yet been published, it remains to be seen what obligations they will impose on data exporters and importers. Similarly, any initial drafts published will be subject to change depending on the outcome of the consultation. However, the consultation does provide an opportunity for individuals and organisations with experience in this area to input into and shape the New SCCs.

Any practical tips?

In anticipation of the publication of the New SCCs, it would be prudent for organisations to review their international data transfer frameworks to identify which data importers are located outside the EAA and are directly subject to the GDPR. It is these relationships into which the New SCCs may need to be incorporated. This is a necessary step for determining which SCCs can be used, as the Current SCCs will remain applicable where the data importer is not subject to the GDPR.

ICO statement on generative AI model training

The question

What position does the Information Commissioner's Office (**ICO**) continue to take on Generative AI Model training?

The key takeaway

The ICO has issued a statement outlining the steps businesses need to take to remain compliant with data regulation when training generative AI models. These include: clear and comprehensible information to data subjects about the training; providing data subjects with real choice on whether their personal data will be used to train generative AI models; and ensuring that there is a robust and comprehensive Data Protection Impact Assessment (**DPIA**) justifying the approach taken.

The background

On 13 September 2024, the ICO published a statement setting out its position to businesses collecting user data to train generative AI models. This guidance also covers DPIAs which controllers are required to complete before conducting data processing which could pose a high risk to the rights and freedoms of data subjects under UK GDPR.

The ICO is becoming increasingly active in its regulation of how generative AI models are trained. On 20 September, the ICO commented on LinkedIn suspending its training of generative AI models using UK users' data pending 'further engagement' with the company. A lack of a clear opt-out function for users who did not want their user generated data used to train LinkedIn's generative AI models was a key concern for the ICO. Ongoing engagement with the ICO will continue before LinkedIn is likely to reboot its model training in the UK in a potentially altered form.

This sits against the backdrop of an increasingly collaborative regulatory approach between data protection authorities globally. For example, the Irish Data Protection Commission (**DPC**) has started a cross-border enquiry with its peer regulators on the continent into the production of a DPIA concerning a large tech company's generative AI model training programme.

The development

The ICO made a statement highlighting the following key considerations for companies aiming to utilise user data to train AI models, including:

- making it simpler for users to object to data processing and ensuring that any opt-outs are clearly provided
- increasing transparency about the usage of individuals' data in the model training process by using plain language to provide meaningful information about the training
- conducting a thorough and robust DPIA which fully highlights the risks posed to data subjects and the mitigations taken to lower this risk to an acceptable level, and where the risks cannot be reduced to an acceptable level, consulting with the ICO or relevant supervisory authority.

The ICO further emphasised the importance of businesses independently continuing to meet high regulatory standards. It highlights the ongoing and evolving nature of the regulatory process, against a broader regulatory backdrop that is growing worldwide towards collaborative investigation of generative AI model training.

Why is this important?

Businesses must take note of the ICO's comments and the broader regulatory backdrop. Supervisory authorities have been clear that organisations must comply with data processing laws and regulations prior to processing personal data necessary for the training; a failure to do so could potentially result in a halt to the project for a regulatory review.

The ICO's engagement with LinkedIn is a pertinent example of the need for proactive compliance with data processing laws; failure can mean a pause to AI model training, incurring cost and delay from an operational perspective. Furthermore, the external risk of regulatory enforcement action (including fines and investigations) remains, alongside the risk of reputational harm in an increasingly privacy-conscious public.

Businesses should keep up to date on guidance from the ICO and other regulatory bodies to demonstrate continual compliance with applicable laws. Companies should continue to be transparent about their data processing and give clear privacy-friendly exits for data subjects.

Compliance should be proactive and clearly evidenced, with co-operation with relevant regulatory bodies such as the ICO where appropriate. Proactive steps which businesses can take include: (i) conducting a DPIA and engaging with the ICO or relevant supervisory authority at an early stage in order to validate the model and implement any necessary safeguards; (ii) reviewing online user journeys to ensure that clear and easy to use opt-outs are available for users; and (iii) updating privacy notices to ensure that meaningful information about the training process is provided to users.

ICO reprimands Sky Betting and Gaming for using non-essential cookies without users' consent

The question

What proactive steps should website operators take to ensure that their use of cookies complies with UK data protection law? Put another way, are you sure personal data is not being collected by your website's advertising cookies before users have consented to their deployment?

The key takeaway

The UK's Information Commissioner's Office (**ICO**) is stepping up enforcement in the area of cookie use. The action against Sky Betting and Gaming (**Sky Betting**) reminds organisations of the need for care over the use of cookies on their websites, including those used for advertising purposes. Website visitors must always be given information about cookies, and the option to accept or decline non-essential cookies, before the cookies are placed or any personal data derived from them is processed or shared with third parties.

The background

Following a report by the campaign charity Clean Up Gambling, an investigation was conducted by the ICO into the use of consumers' personal information by Sky Betting. Although a pop-up cookie banner appeared when users first visited Sky Betting's SkyBet website and which allowed them to "accept All Cookies", the ICO found that some advertising cookies were actually placed (and personal data transferred to third parties) as soon as website visitors accessed the site and before they could choose to consent to the use of these cookies.

The development

In September 2024, the ICO issued a reprimand to Sky Betting for unlawfully processing consumers' data in a seven-week period from January to March 2023. The placement of advertising cookies enabled website visitors' personal information to be processed by third party adtech providers without the individuals' consent. Although the ICO concluded that this was not deliberate, processing personal data in this way was not lawful or fair under the UK GDPR and it issued the reprimand on the basis of infringements of Article 5(1)(a) (lawful, fair and transparent processing), Article 6(1)(a) (consent) and Article 7(1) (controller to demonstrate consent). Notably, the ICO enforcement notice solely focuses on the UK GDPR, rather than also referring to the cookie consent provisions in PECR.

As part of its decision to issue the reprimand, the ICO examined the potentially harmful impacts resulting from Sky Betting's infringements, such as loss of freedom of choice and privacy intrusion, which the ICO viewed as heightened in respect of gambling websites. In processing personal data before giving users the opportunity to consent, the ICO alluded to concerns over facilitating gambling addictions through targeted ads to vulnerable data subjects. The ICO also took into account Sky Betting's existing processes, such as account set-up checks for underage and self-excluded gamblers and removal of certain individuals (such as those near or at their spending limit) from marketing lists, as well as the contractual terms of Sky Betting's agreement with the relevant demand side platform, which contained restrictions on the use of personal data and information conveyed about data subjects.

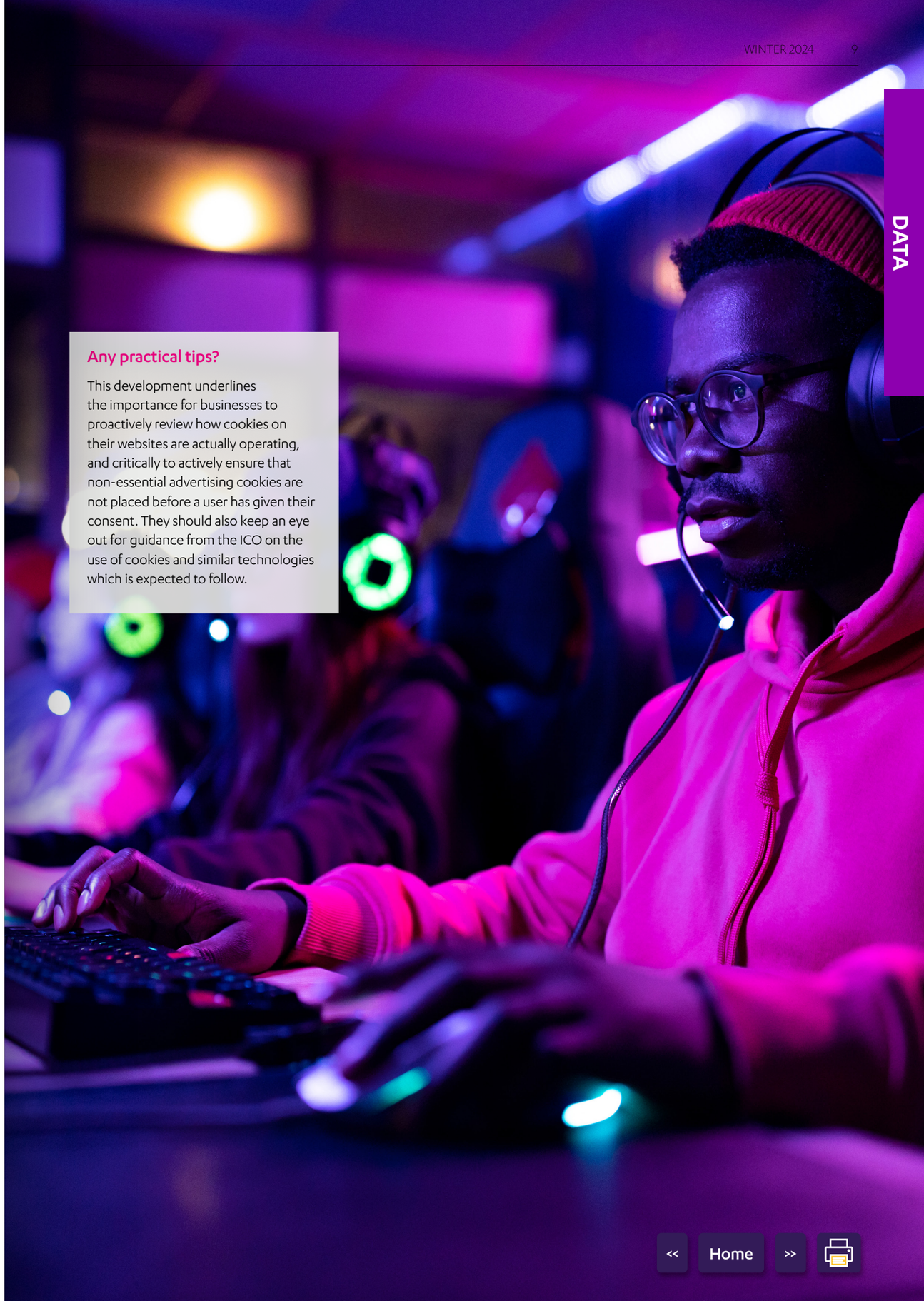
The ICO recommended that Sky Betting reviews its processes to ensure compliance with the UK GDPR and obtains valid consent from users before placing non-essential cookies. Any failure by Sky Betting to comply with the law as set out in the ICO's reprimand may also be taken into account as an aggravating factor should the ICO conduct future investigations against Sky Betting for data protection infringements.

Why is this important?

The ICO is increasing its monitoring of the use of cookies and other tracking technologies. This issue has also been a focus of EU regulators, for example in Belgium (against Mediahuis) and in France (against Yahoo). In a press release, the ICO Deputy Commissioner Stephen Bonner indicated that enforcement action against Sky Betting is a warning for organisations who breach the law and deny consumers the choice of whether to enable targeted advertising.

As part of its strategy to improve compliance, the ICO recently reviewed how the top 100 websites in the UK were using advertising cookies. It wrote to 53 of these websites to warn them of enforcement action if they did not change how users' data is processed. 52 of these websites either fixed the infringing issue or took steps to resolve it. The ICO has said it is planning to review the next 100 websites ("and the 100 after that") on the same basis.

By issuing its reprimand against Sky Betting, the ICO has exposed the consequences of the unlawful use of non-essential cookies, even where an organisation has not deliberately misused website users' personal data. Organisations using advertising cookies and similar technologies on their websites and apps should be aware of the ICO's willingness to scrutinise non-compliance, which may occur in the absence of a specific individual complaint.



Any practical tips?

This development underlines the importance for businesses to proactively review how cookies on their websites are actually operating, and critically to actively ensure that non-essential advertising cookies are not placed before a user has given their consent. They should also keep an eye out for guidance from the ICO on the use of cookies and similar technologies which is expected to follow.

Irish DPC fines LinkedIn €310m for behavioural analysis and targeted advertising breaches

The question

How certain do data controllers need to be of their lawful basis for processing personal data when engaging in behavioural analysis and targeted advertising, and how clearly must this be reflected in a privacy policy?

The key takeaway

LinkedIn failed to demonstrate a clear lawful basis for undertaking behavioural analysis and targeted advertising when using personal data of its members which it had collected itself directly and from its third party partners. The Irish Data Protection Commission's (**DPC**) decision is a reminder of the key data protection principles required for these activities, including transparency and fairness and the need to communicate the lawful basis clearly to users in a privacy policy.

The background

A complaint about the lawfulness of LinkedIn's personal data processing was initially made in May 2018 to the French data protection authority. The complainant, a French non-profit organisation named La Quadrature Du Net, also filed four other complaints of a similar nature against Google, Apple, Facebook and Amazon. An inquiry was subsequently launched by the DPC as LinkedIn's lead supervisory authority in the EU. The DPC examined LinkedIn's use of personal data for behavioural analysis of, and targeted advertising to, users with LinkedIn profiles, ultimately finding several issues from an EU GDPR perspective. The DPC published a draft enforcement decision in July 2024, which did not face any objections. This was followed by the DPC's final decision on 22 October 2024.

The development

The DPC's decision noted three infringements of the EU GDPR, specifically finding breaches of the following provisions:

- **lawful basis for processing (Article 6 EU GDPR)**: LinkedIn was not able to successfully establish any of the six ways that data processing can be considered lawful under the EU GDPR. In particular, the DPC found that LinkedIn did not obtain "sufficiently informed" consent to use this as the lawful basis to process users' third-party data for the purpose of behavioural analysis and targeted advertising. The DPC found that it was also not possible for LinkedIn to rely on the lawful bases related to contractual necessity and legitimate interests
- **transparency (Articles 13 and 14 EU GDPR)**: LinkedIn did not give the necessary information about the personal data collected, and not collected, to data subjects, in relation to the details of the lawful basis for processing that were set out in its privacy notices
- **fair processing (Article 5(1)(a) EU GDPR)**: by failing to establish a lawful basis and to set that basis out in its privacy notice, the DPC found that LinkedIn breached the principle of fairness in relation to its data subjects. This prohibits the processing of data in a way that is detrimental, discriminatory, unexpected or misleading to the individual.

As a result of these findings, LinkedIn received a €310m fine, a reprimand from the DPC and an order to bring its processing into compliance with the EU GDPR within three months. The full decision is still to be published by the DPC, and in response LinkedIn has said that it would 'consider its options to appeal'.

Why is this important?

The decision is a reminder of the approach taken by European data protection regulators to processing for online advertising purposes, including their appetite for fining levels where there has been a breach. The action also reflects how one breach of the EU GDPR (in this case lawful basis) can have a knock-on effect for compliance in other areas (transparency and fairness). The sanctions imposed and the DPC's reasoning are particularly relevant to technology and other companies with their EU bases in Ireland, as the DPC is likely to be the lead supervisory authority for any such organisation.

Any practical tips?

When processing users' data, businesses should ensure that they comply with applicable data protection laws including the EU GDPR. When processing individuals' personal data for targeted advertising purposes, it is important that those users receive sufficiently clear information about what their data will be used for. Any targeted advertising programme should also be designed with privacy in mind and with a clear lawful basis for processing, that can be set out in the relevant privacy notice.

DATA

EDPB's new publications on the ePrivacy Directive, processors and legitimate interests

The question

What are the key takeaways for organisations processing personal data set out in the recent Guidelines and Opinions adopted by the European Data Protection Board (**EDPB**)?

The key takeaway

One of the EDPB's priorities is to ensure that regulatory frameworks keep pace with the latest technological developments. While certain exceptions apply, both the Guidelines and the Opinion reinforce that when processing or controlling personal data, businesses (a) must comply with applicable data protection laws including the EU General Data Protection Legislation (**EU GDPR**), and (b) have a responsibility to ensure that data protection standards are maintained even when personal data is transferred to third parties.

The background

The EDPB is an independent organisation that aims to ensure that EU data protection laws are applied consistently across relevant jurisdictions. It publishes guidance, adopts recommendations and encourages closer co-operation between national data protection authorities that enforce the EU GDPR. While its recommendations and guidance are no longer directly applicable in the UK, due to the similarities between the two pieces of legislation they are often relevant to organisations following UK data protection laws.

The EDPB has recently issued several guidelines and opinions that are relevant to organisations that process personal data subject to the EU GDPR. These include guidelines on the scope of the EU's ePrivacy Directive (the **ePD**) and on the application of the legitimate interests lawful basis for processing personal data, and an opinion on the use of processors and sub-processors by a data controller.

The development

The key takeaways from each EDPB publication are as follows:

Guidelines on the Technical Scope of Article 5(3) of the ePrivacy Directive

- Following consultations, the EDPB adopted the final version of the guidelines on the technical scope of the ePD on 7 October 2024. While there have been no significant amendments to the draft dated 14 November 2023, these guidelines remain crucial for explaining the applicability of the ePD to emerging tracking tools. See our Snapshots Winter 2023 article for our previous discussion on this topic
- These guidelines emphasise that new tracking tools such as pixel tracking and tracking based on IP are not exempt from the regulations. The emergence of these tools in the market has caught the attention of regulators and more targeted rules are likely to follow.

Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

- In this opinion, adopted on 7 October 2024, the EDPB provides advice on the extent of checks a controller must implement to verify whether processors and sub-processors provide "sufficient guarantees" to ensure the implementation of appropriate technical and organisational measures under Article 28 EU GDPR. In particular, controllers should be able to identify processors and sub-processors and have this information readily available at all times.

Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

- Legitimate interest is one of the six lawful bases under which data controllers can process personal data in compliance with the EU GDPR. These guidelines outline the requirements a controller must meet before relying on this lawful basis. The draft guidelines were adopted on 8 October 2024 and were subject to public consultation until 20 November 2024.
- When relying on legitimate interests as the lawful basis for direct marketing, controllers must meet three conditions: (i) a legitimate interest must be pursued; (ii) data processing must be necessary for that interest; and (iii) a balancing test must confirm that the interest does not override individuals' rights.
- The EDPB clarifies in the draft guidance that extensive data processing, such as tracking individuals across multiple platforms, is less likely to pass the balancing test. Less intrusive activities, like sending commercial communications to existing customers who have purchased similar products, are easier to justify as a valid legitimate interest for processing personal data.

Why is this important?

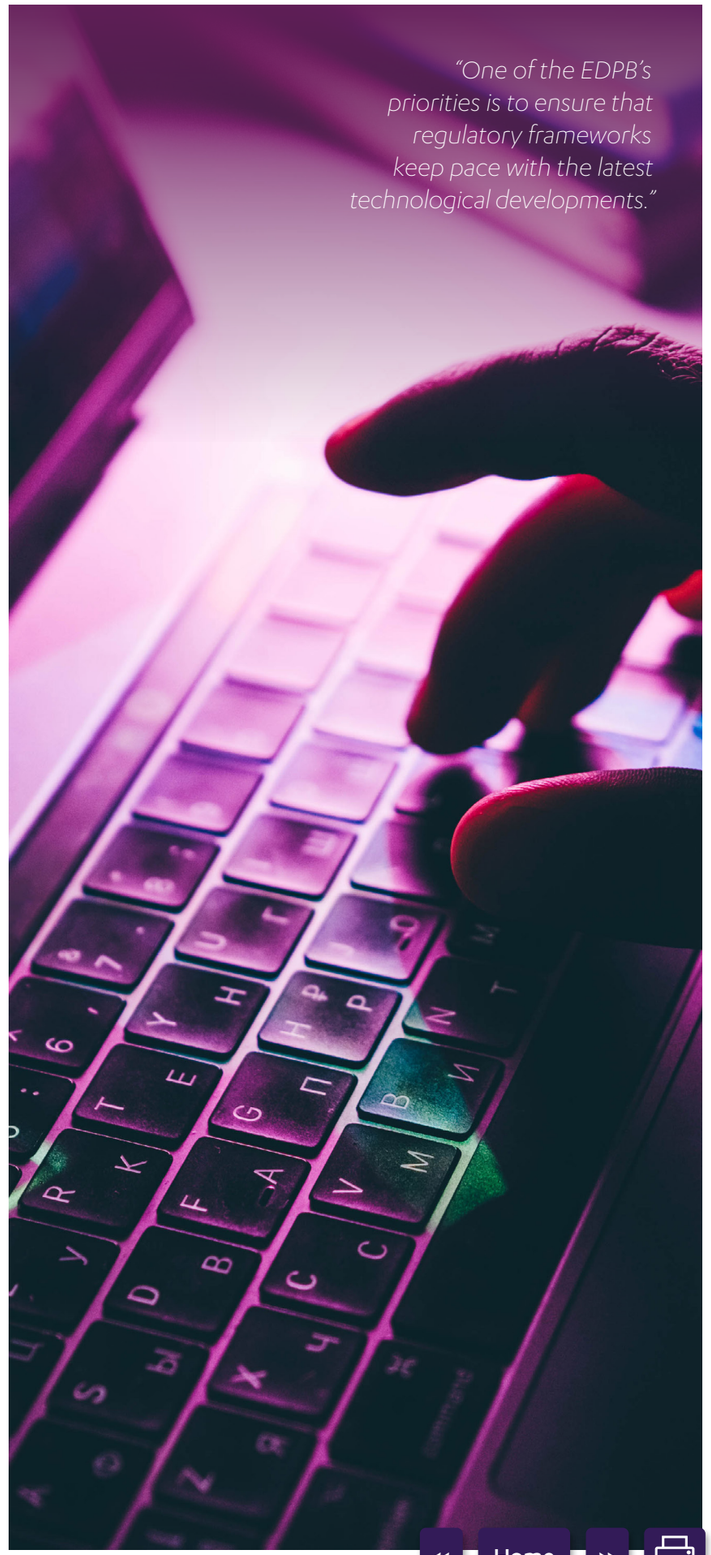
In the UK, the Privacy and Electronic Communications Regulations (**PECR**) implement the ePD, with Article 5(3) of the ePD being reflected in Section 6 of the PECR. PECR complements the general data protection regime in the UK under the Data Protection Act 2018 and the EU GDPR as it forms part of retained EU law in the UK (the **UK GDPR**). Whilst the new guidelines on the ePD are not directly applicable to PECR (ie given that the UK has left the EU), they may offer further guidance into newly emerging tracking tools.

The guidelines on legitimate interests and on the reliance on processors also show the direction of legislative travel for these areas and provide useful guardrails for organisations that are subject to the UK GDPR as well as the EU GDPR.

Any practical tips?

New tracking tools that can optimise consumer data may offer businesses attractive opportunities. However, when adopting these technologies, businesses should consider the EDPB's guidance, as regulators are likely to expect them to have considered this when implementing them.

Similarly, when outsourcing data processing to third parties, businesses must be cautious and bear the EDPB's recommendations in mind. It is critical to ensure the third-party processor provides the same level of protection for that data as the controller. Practically, organisations should aim to achieve this by performing due diligence on processors, and ensuring that the contracts with processors include all the appropriate protections.



Ofcom rolls out implementation phases for compliance with the Online Safety Act

The question

What is Ofcom's timeframe for implementation of the Online Safety Act (**OSA**) and what actions will in-scope services need to take to ensure compliance?

The key takeaway

From December 2024, in-scope services must take action to ensure compliance with their duties under the Online Safety Act 2023 (**OSA**). Ofcom's timeline for implementation provides a phased approach, and online service providers must be alive to the short compliance windows following publication of Ofcom's final codes and guidance. It is anticipated that services must comply with their illegal content safety duties from March 2025, and with their child protection safety duties from July 2025. From the moment the OSA duties come into force, failure to comply could lead to enforcement action including: fines; access restrictions to payment providers and advertisers; and a total ban of the service in the UK in the most serious cases.

The background

Under the OSA, online user-to-user and search services have several new duties to protect users from illegal content and to protect children from online harms. All in-scope services with a significant number of UK users, or targeting the UK, must ensure compliance. Since the legislation was passed, Ofcom have consulted on its various codes and guidance for illegal harms, age assurance for pornography services and children's safety. They have also advised the Government on the thresholds for categorised services, which are subject to additional, more stringent duties aimed at enhanced levels of safety, transparency, and accountability. The regulator has now published its expected timeline for publication of the codes and guidance and corresponding compliance by in-scope services. Businesses must ensure they remain vigilant and are prepared to meet the deadlines for compliance over the coming year to avoid regulatory penalties.

The development

Ofcom's proposed timeline (which could be subject to change) is summarised below:

Phase 1: Illegal harms

- In December 2024, Ofcom will publish its illegal harms codes of practice and accompanying illegal content risk assessment guidance.
- Services will then be required to complete their illegal harms risk assessments by mid-March 2025, at which point the illegal harms safety duties will become enforceable.

Phase 2: Child safety, pornography and the protection of women and girls

- In January 2025, Ofcom's final age assurance guidance for publishers of pornography content will be issued. Around the same time, the duties relevant to providers of pornographic content will become enforceable and Ofcom will begin monitoring compliance.
- Also in January 2025, the final children's access assessment guidance will be published, and services will have until April 2025 to assess whether their service is likely to be accessed by children.
- In April 2025, Ofcom will publish its children's risk assessment guidance, and services which are likely to be accessed by children must complete their children's risk assessment by July 2025, at which point the child protection safety duties will become enforceable.
- Ofcom will open a consultation on best practice guidance relating to the protection of women and girls online in February 2025.

Phase 3: Categorisation and additional duties for categorised services

- Ofcom expects the Government to confirm the thresholds for categorisation in secondary legislation by the end of 2024. As such, Ofcom aims to publish its register of categorised services in Summer 2025 and issue draft transparency notices within a few weeks of the register's publication, with final transparency notices to follow soon after (more information on these notices can be found here).
- The draft proposals regarding the additional duties on categorised services are expected in early 2026.

Why is this important?

The implementation of the OSA represents a shift towards more stringent regulation of online services, with an eagle-eye on user safety, transparency, and accountability. The stakes are high as non-compliance could result in substantial financial penalties, service blocks in the UK and reputational damage. Even with their current powers pre-dating the OSA's enforcement, Ofcom frequently issue large fines for regulatory breaches, often in the millions, providing an indication of the level of fines that could be issued under the OSA, particularly for large and well-resourced companies. Prompt and adequate compliance with Ofcom's codes and guidance will not only protect businesses against regulatory sanctions but also bolster consumer trust in an era where online safety is increasingly under scrutiny.

Any practical tips?

To stay ahead, services should carefully consider Ofcom's draft codes and guidance to identify any proactive steps to ensure compliance before the final guidance is issued and their duties become enforceable. Some practical considerations could include:

- pre-emptively conducting an internal audit to identify risks associated with illegal content and harm to children
- reviewing algorithmic and content monitoring processes, including the use of human versus automated moderation and considering where further investment could be beneficial
- analysing the effectiveness of age verification and assurance systems; and importantly
- reviewing and updating terms of services, privacy policies, and user agreements to align with Ofcom's draft codes and guidance.

Services should also capitalise on the opportunity to respond to Ofcom's various consultations which will be published over the next year, including the most recent consultation on the proposed new fees and penalties regime, which closes on 9 January 2025.

New Safer Phones Bill aims at "making social media less addictive" for young people

The question

How does the Safer Phones Bill intend to protect young people online?

The key takeaway

The Protection of Children (Digital Safety and Data Protection) Bill (the **Safer Phones Bill**) proposes to impose additional obligations on social media companies with the intention of further protecting teenagers and young adults who use social media applications. This could include an obligation requiring platforms to exclude young people from algorithms.

The background

Labour sponsor and MP for Whitehaven and Workington, Josh MacAlister introduced the Safer Phones Bill on Wednesday 16 October 2024 to the House of Commons. MacAlister said "The evidence is mounting that children doomscrolling for hours a day is causing widespread harm. We need the equivalent of the 'seatbelt' legislation for social media use for children". The Safer Phones Bill has had backing from the Labour and Conservative parties which, as a Private Members Bill, increases its chances of succeeding in its passage through Parliament.

The Online Safety Act 2023 (the **OSA**) introduced extensive measures on in-scope services (including many social media platforms), with measures aimed at protecting children from content deemed "harmful" under the OSA such as content which promotes self-injury, pornographic content, "bullying content" and content depicting serious violence or injury. The OSA was passed last year and obligations on in-scope services are due to come into effect from mid-December 2024.

The Bill, rather than focusing on the type of content, aims to reduce the amount of time young people spend on their phones by limiting access to content generated by algorithms. Various measures are proposed in the Bill to seek to achieve this, including by increasing the age of "internet adulthood", meaning the age at which children no longer require parental consent to increase the data allowance on their mobile phones, from 13 to 16. This would make it harder for teenagers under 16 to increase the data allowance on their mobile phones, with the intention of ultimately limiting under 16s use of social media. The Bill also proposes to give Ofcom further powers to prevent children from accessing allegedly addictive content and review how phones are advertised to younger audiences to ensure their wellbeing is taken into consideration.

The Bill also seeks to leg ally ban mobiles phones in schools entirely. However, a Government spokesperson said they were not intending to back that part of the Bill, adding that "the Online Safety Act will introduce strong safeguards for children, preventing them from accessing harmful and age-inappropriate content...The vast majority of schools already handle the use of mobile phones effectively, including with bans. Legislating for an outright ban would simply remove the autonomy from school leaders who know their pupils and their communities best."

The development

The Private Members' Bill was presented to Parliament on Wednesday 16 October 2024 through the ballot procedure and the second reading is due to take place on Friday 7 March 2025.

Why is this important?

This is the latest piece of legislation which aims to regulate tech platforms. Those within scope of the Safer Phones Bill will want to keep an eye on its progression and think about how the proposed additional obligations can be complied with alongside and in combination with their existing duties in the ever-changing regulatory landscape.

Any practical tips?

Nothing immediate in respect of the Bill: the second reading is not until 7 March 2025. That said, it's clear which way the general political wind is blowing in terms of children and social media, not least given the introduction in Australia of an outright ban on social media for children under 16 on 28 November 2024. France introduced legislation to block social media access for children under 15 without parental consent and Norway has pledged to follow the Australian ban. Meanwhile, the UK's technology secretary, Peter Kyle, has said that a ban on social media for under 16s in the UK is "on the table".

With everything pointing towards stricter controls for children on social media, it makes sense to start thinking carefully about the impact on businesses and how they might respond. Not forgetting of course that services which are in-scope of the OSA need to be aware that some obligations under that Act kick in from mid-December 2024. See our separate article in this Snapshot edition on Ofcom's useful guidance on relevant OSA dates.

EU's publishes draft code for general-purpose AI models

The question

What measures are proposed by the EU AI Office to regulate general-purpose AI (**GPAI**) models?

The key takeaway

A draft code of practice for general-purpose AI (the **Code**) has been published. Providers of GPAI models will have until the implementation date of 2 May 2025 to ensure that their practices are compliant with the Code and therefore the EU AI Act (the **AI Act**).

The background

The AI Act, which came into force on 1 August 2024, sets out a risk-based framework that places requirements on AI technology depending on the risk posed to society. In addition to this general regime, "providers" of GPAI models have separate and more onerous obligations under the AI Act. "Providers" is defined as any party that develops a GPAI model or has a GPAI model developed and places it on the market or put the AI system into service under its own name or trademark. A "GPAI model" is one that has been trained on large amounts of data and can be used to perform a wide range of general tasks. Consequently, large model providers such as OpenAI (developers of GPT models used for ChatGPT), Google (developers of Gemini GPAIs), and Meta (developers of Llama) will most likely fall within the definition of a GPAI provider. In addition, GPAI models that present 'systemic risk' (based on a technical definition of computational power) are subject to additional requirements. For our previous discussion on the AI Act, see our Snapshots Summer 2024 article.

The Code was required to be drawn up under the AI Act to facilitate the implementation of these obligations. To do this, the AI Office put together four specialist working groups, led by Chairs and Vice-Chairs with expertise and experience in computer science, AI governance and law. In line with the AI Act's encouragement of relevant stakeholder participation in the process (ie from civil society organisations, industry, and academia), a multi-stakeholder consultation opened in August 2024 which received almost 430 submissions.

The development

On 14 November 2024, the first draft of the Code was published. The working groups had six key principles in mind when drafting:

- alignment with EU principles and values
- alignment with the AI Act and international approaches
- proportionality to risks
- future proofing
- proportionality to the size of the GPAI model provider
- support and growth of the AI safety ecosystem.

Guidance for providers of GPAI models

Transparency: transparency is the key requirement for GPAI models under the Code. Providers must keep up to date technical documentation for both the AI Office and downstream providers. This documentation should include information such as details of the GPAI model and provider, intended and restricted or prohibited tasks, the type of AI systems in which the model can be integrated into, the acceptable use policy, design specification, and training process (including the data used).

Copyright: measures to be taken include implementing a copyright policy, carrying out reasonable copyright due diligence before contracting with third parties, implementing reasonable downstream copyright measures to mitigate any risk, and lawful engagement in text and data mining. To satisfy the transparency requirement, providers must provide information on the measures they adopted to comply with EU law on copyright.

GPAI models that pose "systemic risks"

The Code provides further guidance on what will be considered a systemic risk; types of risks identified are cyber risks, chemical, biological, radiological and nuclear risks, loss of control, unpredicted developments as a result of using automated models for AI development, large-scale persuasion and manipulation including disinformation/misinformation risks to democratic values, and large-scale discrimination of individuals, communities or societies. This is a non-exhaustive list and further risks may be identified if, for example, they cause large-scale negative effects on public health, safety, public and economic security etc.

Whether or not a GPAI model would be put in this category will depend on its attributes such as whether it has dangerous model capabilities (ie weapon acquisition, self-replication, persuasion, manipulation, and deception) and dangerous model propensities (ie misalignment with human intent/values, bias, lack of reliability, and security). Further, specific inputs, configurations and contextual elements may increase risk such as any potential to remove guardrails, human oversight, number of business users and end-users. For these GPAI models, the Code proposes a Safety and Security Framework (SSF) detailing the risk analysis and management steps taken by providers, which should be "proportional to the severity of expected systemic risks":

- **risk assessment**: identification of systemic risks stemming from the model by continuous and thorough analysis of risks identified, mapping pathways to risks, developing triggers for any risk indicators, and collect evidence on the specific risks. Risk assessment must be carried out continuously during the full lifecycle of the development and deployment of the GPAI model (ie before and during training, during deployment and post deployment)
- **technical risk mitigation**: systemic risks must be kept below an "intolerable level" by putting in place safety mitigation measures (ie behavioural modifications to a model, safeguards for deployment in a system, and other safety tools) and security mitigation measures, as well as identifying limitation to these mitigations. Safety Security Reports (**SSR**) must be created for each model at appropriate steps in the lifecycle, detailing the risk and mitigation assessments which can form the basis of any development and deployment decisions
- **governance risk mitigation**: providers must ensure the ownership regarding systemic risks at each level of the organisation, including at executive and board levels, regularly assess the provider's adherence to the SSF and engage independent experts to carry out systemic risk and mitigation assessments. Providers should have in place processes for reporting serious incidents to the AI Office as well as whistleblowing protections. SSFs and SSRs should be published to increase public transparency.

Why is this important?

The final version of the Code is expected to be published in Spring next year. Businesses that comply with the Code will be presumed to comply with the GPAI-related provisions under the AI Act. The Code, therefore, is a very helpful practical standard for businesses to follow. This will be important given the potentially significant fines under the AI Act (ie up to €35m or 7% of a company's annual turnover), but also to align with the EU's objective to increase transparency in the development and use of GPAI models. This will in turn increase public confidence in technology companies that demonstrate lawful and safe development of AI models.

Any practical tips?

The current version of the Code is very much a draft and contains open questions to stakeholders. Businesses should review the draft Code and consider to what extent they fall, first, within the definition of GPAI provider and, second, whether their model presents any "systemic risks". These determinations will then drive the assessment of how the measures outlined may be implemented in practice and to what extent current practices must be updated to be in line with the principles set out in the Code, particularly in relation to the overarching theme of "transparency". Relevant teams should monitor the progress of the Code, particularly the fact that, as noted by the AI Office, the current assumption is that there will only be a small number of GPAI models with systemic risks. The AI Office proposes that, if incorrect, future drafts will require a tiered system of measures focusing on models providing the largest systemic risks.

Two years on from the Digital Services Act

The question

How has the European Commission (**Commission**) enforced the Digital Services Act (**DSA**) since its inception?

The key takeaway

In its first two years of application, the Commission has taken an active role in monitoring and enforcing the provisions of the DSA, with at least 22 online platforms receiving requests for information, and some of these platforms (see below) being the target of more significant action.

The background

The DSA came into force on 16 November 2022, with most of its operative provisions taking effect across all EU Member States on 17 February 2024 (for further context of the parliamentary process of the DSA, see our Snapshots Spring 2023 article). The main aim of the DSA is to implement a new framework of obligations applying to all digital services to keep users safe from illegal goods, content or services, and to protect their fundamental rights online. The rules apply to providers of online intermediary services (eg online platforms, online marketplaces, and hosting providers) to consumers and business in the EU.

The DSA operates on a tiered system whereby different obligations apply to entities depending on their size and the services they provide. The two groups of companies that receive the highest level of scrutiny under the DSA are "very large online platforms" (**VLOPs**) and "very large online search engines" (**VLOSEs**). A company is given this designation by the Commission if it has more than 45 million users per month in the EU. Receiving this designation means the VLOP or VLOSE must comply with a number of additional obligations set out in the DSA, for example, auditing, monitoring and data sharing with authorities to reduce systemic risk in the EU.

The development

The DSA broadly gives the Commission both investigative and sanctioning powers, and almost two years to the day in which the DSA came into force, the Commission has exercised its powers under the DSA with increased regularity.

As at writing, the Commission has sent requests for information or started formal proceedings against 22 online platforms in relation to a variety of issues including illegal products, dark practices, misinformation, risk to minors, and advertising practices.

The first formal proceedings under the DSA were initiated against the platform X (formerly known as Twitter) in December 2023. The investigative stage has focused on infringements relating to illegal content, the controls X has in place to combat misinformation and transparency and the suspected deceptive design of the 'blue checks' on the platform. As of July 2024, the Commission has informed X of its preliminary findings, highlighting that its current practices are: (i) not compliant with the transparency rules on advertising; (ii) deceiving for users as the blue checks denotes a form of verification has taken place (which it has not); and (iii) that X has prohibited "eligible researchers from independently accessing its public data". X now has the chance to raise a defence against the preliminary findings, however failure to raise a successful defence would lead to the Commission adopting a non-compliance decision finding that X is in breach of Articles 25, 39 and 40(12) entailing potential fines of up to 6% of total worldwide annual turnover.

Under a similar process, the Commission opened two formal proceedings against Meta in April and May 2024 concerning the Facebook and Instagram platforms. The April proceedings centred on four DSA compliance issues: handling of deceptive ads and disinformation, transparency in political content demotion, lack of real-time election monitoring tools due to the deprecation of "CrowdTangle" and inadequate user-friendly mechanisms for flagging illegal content and handling complaints. The Commission's May investigations relate to the use of the platforms by minors, including the potential for the services to reinforce addictive behaviours, the adequacy of measures used to maintain privacy, safety and security and the controls surrounding minors' access to inappropriate content. The Commission will now conduct further investigation, gathering evidence through requests for information, interviews, and inspections. The formal proceedings allow the Commission to take enforcement actions, including interim measures or non-compliance decisions, and to accept any commitments Meta may offer to resolve the issues.

In the retail sphere, Temu and Shein were both issued with requests for information in June 2024, with the latter only receiving its designation as a VLOP in April 2024. The Commission gave both platforms around a month to detail their measures for complying with DSA obligations on the "Notice and Action" mechanism for reporting illegal products, user-friendly interfaces free from deceptive "dark patterns," protection of minors, transparency of recommendation systems, trader traceability, and compliance by design. On 31 October 2024, the Commission opened formal proceedings to evaluate whether Temu may have violated the DSA in relation to the sale of illegal products, the service's potentially addictive design, its purchase recommendation systems, and researcher data access. The Commission will continue to gather evidence in its consideration of whether to bring further enforcement action against Temu, however it may also consider Temu's efforts to remedy these practices.

Why is this important?

Since the DSA's provisions took effect in February this year, the Commission has been on a war path to exercise their powers against any online platforms it considered problematic under the DSA. As Thierry Breton, Commissioner for Internal Market, said about the proceedings against X, "[the formal proceedings] makes it clear that, with the DSA, the time of big online platforms behaving like they are "too big to care" has come to an end." The preliminary findings against X suggest that the Commission is preparing to impose potentially significant fines against it (noting again the maximum limit being 6% of total worldwide annual turnover).

Any practical tips?

The proceedings against the platforms discussed above have detailed specific areas of concern relating to the user experience on their respective sites and other VLOPs should ensure they stay abreast with Commission proceedings to ensure that they do not fall foul of similar DSA infringements. In particular, the proceedings against X mark the first time in which the Commission has taken an action against a VLOP to the second stage which is likely to have ramifications for other platforms facing similar proceedings. The result of this second stage will be an important gauge as to how VLOPs can manage this process and how cooperation with the findings of a Commission investigation may help in avoiding or reducing the potential financial penalties.

European consumer body challenges in-game premium currencies

The question

When does the use of in-app and in-game premium currencies pose consumer regulatory issues? Does this consumer complaint herald a tightening by the EU on revenue streams for game and app developers and platforms?

The key takeaway

A complaint by European Consumer Organisation (**BEUC**) on in-app and in-game currencies has underlined the need for games and app developers and platforms to consider how they use and interact with consumers on in-game and in-app transactions, especially where they involve premium currencies or consumers under the age of 18. The focus of the complaint is around transparency to consumers in the video game and platform sectors.

The background

The European Commission (**EC**) is conducting a 'Digital Fairness Fitness Check' of EU consumer protection legislation including the Unfair Commercial Practices Directive (**UCPD**), the Consumer Rights Directive (**CRD**) and the Unfair Contract Terms Directive (**UCTD**).

The BEUC (full name the Bureau Europeen des Unions de Consommateurs) has responded to the EC's call for evidence with a complaint regarding business practices around in-app and in-game sales involving premium currencies (ie in-game currencies that can be purchased with 'real-world money' eg pounds sterling), particularly in relation to sales to children.

In-game purchases are a now well-known revenue stream to game developers and platforms. Consumers can use real-world money to buy items or advantages within a game, or to buy premium currencies which can then be used to make in-game purchases. Examples of premium currencies include Robux (from Roblox), V-bucks (from Fortnite), and MineCoins (from Minecraft), which currencies can be bought using real currency or earned via playing the game. The BEUC notes that in-game purchases are now a major revenue stream, generating more than $15 billion in 2020, and that in-app and social media spending is also growing.

The BEUC contends that the existing legislation requires app and game developers to be transparent about in-app and in-game purchases, but that they are failing to meet their obligations, particularly where the transaction involves premium currencies. The BEUC calls for further policy, regulation and enforcement of in-app and in-game transactions involving premium currencies in the video game and platform sectors.

The development

The BEUC has made a number of recommendations as to how the EC could better regulate these premium currencies, which include:

- banning the use of in-app and in-game premium currencies entirely (or, at a minimum, for consumers under 18) and mandating purchases to be denominated in real-world currency
- strengthening the transparency requirements in the Consumer Rights Directive and the Unfair Commercial Practices Directive in relation to in-app and in-game purchases involving premium currencies, eg by requiring the real money price next to the virtual currency 'price'
- imposing stricter requirements around (i) activation of in-app payment mechanisms (to require consumers to activate these mechanisms before they can make purchases); and (ii) payment authorisation, to prevent unwanted purchases
- amending or clarifying consumer legislation to ensure that consumers' rights in respect of digital monetary transactions extend to in-app and in-game purchases, and to transactions involving premium currencies. For example, the BEUC suggests that currently consumers generally:
  - license the right to play games and therefore do not own the in-game and in-app premium currencies obtained in the game
  - are not entitled to rights of withdrawal as they would be with other digital monetary transactions
  - are not entitled to exchange premium currencies back into national currencies
- allowing consumers to choose the amount of premium currency they wish to buy without being forced to choose from bundles created by the developer
- enforcing regulatory requirements against game and app developers as a priority, including conducting sweeps to identify widespread or recurrent unfair practices in relation to premium currencies.

Why is this important?

The bans proposed by the BEUC – either the general ban or the prohibition for under-18s – would require a drastic revamp of a crucial revenue stream for game and app developers and platforms. In particular, it would affect developers whose monetisation strategy depends on the one-way conversion of real-world currency into their premium currency.

The BEUC's other recommendations, if adopted by the EC, could also significantly impact developers' monetisation and consumer engagement models, and

have further implications for the design and delivery of apps and games and transactions within them. For example, the BEUC's suggestion that all games with in-game purchases can only be installed once a password has been inputted would likely impact all storefronts or channels through which games can be purchased in Europe.

More generally, the BEUC's complaint suggests there is significant consumer dissatisfaction around the use of premium currencies, including around the lack of transparency of the real-world value of the premium currency. Given the values of in-game and in-app transactions, game and app developers can expect to be the target of class actions which seek to give consumers greater visibility and control over their spend within a game or app.

Any practical tips?

Although the EC is yet to complete its Digital Fairness Fitness Check, we expect scrutiny of in-app monetisation models and use of premium currencies will increase, particularly where there is a risk of sales to under-18s. It would be prudent for game and app developers and platforms to start considering how the BEUC's recommendations would impact their businesses, including:

- to what extent does the monetisation and consumer engagement model depend on the use of in-app or in-game purchases or transactions involving premium currencies?
- how easy is it for consumers to determine the real-world monetary value of any item displayed on screen?
- does your contractual documentation (such as developer agreements, end-user license agreements, and associated terms and conditions) cover in-app payments and transactions involving premium currencies?
- do your contracts treat in-app payments and transactions involving premium currencies differently to other digital transactions?
- are consumers able to seek returns and refunds for items purchased in-app/in-game, including where the transaction involves premium currencies? How easy or difficult is it for the consumer to successfully carry out a return or refund?
- are controls in place to protect children from making unwanted payments? Do these controls reflect current practices or are they future-proofed?

"Dynamic pricing does not automatically breach consumer protection legislation."

CMA investigates Ticketmaster for dynamic pricing of Oasis tickets

The question

Can dynamic pricing breach consumer protection rules?

The key takeaway

Dynamic pricing does not automatically breach consumer protection legislation. However, if the pricing system materially distorts the economic behaviour of the average consumer, then it may constitute an unfair consumer practice in breach of UK consumer regulation (ie under the soon-to-be-in-force Digital Markets, Competition and Consumers Act 2024 (the **DMCCA**), which replaces the Consumer Protection from Unfair Trading Regulations 2008). The stakes are higher with the Competition and Markets Authority (**CMA**) about to take up new powers under the DMCCA to directly fine companies which undertake unfair consumer practices (up to £300,000 or 10% of their global turnover, if higher).

The background

In August 2024, Oasis announced that they would be returning for their first tour in 15 years. There were 17 dates announced. Tickets for the shows were sold on Ticketmaster and they all sold out within 10 hours. The face value of tickets increased from £150 to £350 within hours due to dynamic pricing. The CMA is now investigating Ticketmaster for its conduct in relation to these ticket sales.

The development

The CMA is investigating whether Ticketmaster engaged in unfair commercial practices which are prohibited under the CPRs, including offences relating to whether:

- there was clear and timely information explaining dynamic pricing to consumers
- people were put under pressure to buy tickets within a short amount of time.

Fans have been asked to provide evidence of their experiences in relation to purchasing or attempting to purchase Oasis tickets. The CMA is now engaging with Ticketmaster to consider whether it believes that there has been a breach of consumer protection law.

Why is this important?

It is not just other ticket agencies that will be interested in the outcome of this investigation; other industries where dynamic pricing is commonplace (such as flight and hotel booking retailers) will also want to see where the CMA land on this topic. The stakes are higher because of the CMA's new enforcement and fining powers under the forthcoming DMCCA.

This is particularly pertinent as, although separate to the Oasis investigation, on 13 November 2024 the CMA launched a new project to evaluate how dynamic pricing is used in various sectors of the economy. The project demonstrates the CMA's increased interest in dynamic pricing. Companies which use dynamic pricing need to be aware of the increased regulatory interest in this area and ensure that consumers are provided with the requisite information about these types of pricing models.

Any practical tips?

Clear and timely information should be provided to consumers prior to offering products or services for sale using a dynamic pricing system. Customers should not be put under pressure to buy tickets in a short amount of time without the relevant information available. Companies should carefully follow the CMA's dynamic pricing monitoring project for sector specific updates.

CMA publishes guidance for fashion retailers on environmental claims

The question

How best can fashion retailers protect themselves from regulatory action when making green claims?

The key takeaway

The CMA has published further guidance on how fashion retailers can comply with the Green Claims Code; the key set of rules determining whether claims about the environmental impact of products or brands (aka green claims) infringe consumer protection regulations in the UK. Much of this guidance broadly restates existing guidance (see our previous Snapshots article for example), but with some useful fashion-focused features to help retailers understand exactly what does and doesn't go in the industry. It also heavily features practical examples of certain practices the CMA deems non-compliant.

The background

Green claims have been a hot topic with both the ASA and the CMA for years now, and the CMA in particular has focused in on the fashion sector. Its investigation into fashion concluded with undertakings from ASOS, Boohoo and George at Asda. But that investigation did not mark the end of the CMA's interest in fashion green claims, noting the ongoing focus of the impact of fast fashion on the environment. This guidance should therefore be seen in the context of anticipated continued scrutiny by the CMA over claims made in this sector.

The development

The CMA has published guidance for all businesses making claims about clothing, footwear, fashion accessories and related services (including packaging and delivery). The CMA's actions are clearly focused on retailers, but the guidance is intended to be relevant all the way up the supply chain, including manufacturers and suppliers, and wholesalers and distributors. If you are active in the fashion sector, and you are making (or even passing along) green claims, this guidance will be pertinent for you.

The specific recommendations are as follows:

- **(predictably) all green claims should be clear and accurate**: this applies to all claims, whether made on-product, on apps, websites, and social media (the retailer's or any other's)
- don't hide important information: the CMA is alive to retailers hiding information behind dropdown boxes, website links and QR codes. All of the important information about the claim should be immediately available at the point of purchase
- **avoid using unclear terms**: "green", "sustainable" and "eco-friendly" are high-risk terms on the basis they are wide-meaning and therefore incredibly difficult to substantiate. The more specific your green claim is, the more likely you will be able to substantiate it, and the more likely it will be compliant
- **do not mislead using imagery and icons**: consider the overall impression of each ad that contains a green claim, and how a consumer would interpret it. Note in particular recent ASA guidance, which referenced a consumer "cascade of assumptions" about green imagery which meant certain claims (eg that a product is carbon neutral) could be implied even if those words are never used in the ad
- **ensure comparisons are clear**: set out a prominent summary of the basis for a comparison when making one. Comparisons should be like for like, consumers should understand what is being compared and the comparison should be fair and clear
- **explain clearly any action the consumer needs to take**: if a claim is based on the consumer taking a certain action post-purchase, that action needs to be made obvious to the consumer. The example given is a children's jacket, the hems of which could be unpicked to increase the arm length (making it last longer as the child grows). The details of the unpicking and the knock-on impact on the environment should be made clear
- **be clear when using filters and other website navigational tools**: the CMA has cottoned on to the use of search result filters such as "sustainable" for products on websites. When such generic tags are applied, they will have to be substantiable for every product on the website with that tag. Where possible, be more specific about the filters eg "50%+ recycled"
- **recognise that product ranges are higher risk**: certain retailers have a range of products marketed as being more environmentally friendly. Such ranges are more likely to attract CMA attention, and you will want to ensure:
  - the criteria for a product's inclusion is clear and available to consumers
  - the name of the range is not misleading in itself, and
  - that any marketing of the range is also not misleading
- **describe fabrics clearly and precisely**: descriptions should be specific and objective eg "recycled polyester" is preferable to "responsible polyester" because the meaning of "responsible" is less clear. Do not imply that an entire product is made of one fabric (excluding buttons, zippers and threads) if it isn't. Consider fabric claims by reference to what percentage of the product is made of the subject matter fabric, and include that percentage information in the claim
- **ensure you are deploying affiliations and accreditations properly**: the CMA is happy for you to share your accreditations at a general level, but when making specific claims based on accreditations, ensure the claims made to consumers align precisely with the details of the actual accreditation you have been given by the third-party accreditor. Consider in particular:
  - is the claim misleading about the product as a whole?
  - have the benefits of the scheme been summarised?
  - have you made your connection to the scheme clear?
  - have you provided a link to the scheme's website?
  - have you made further details available to consumers?
- **put in place processes to ensure claims are correct**: appropriate policies should be put in place, necessary training should be provided to key staff and systems should operate to check the factual basis for claims being made.

Why is this important?

The CMA is paying a lot of attention to this space and, through their previous investigations, they have clearly wised up to certain fashion retailer trends/behaviours. This applies especially to vague claims such as "sustainable" or when marketing on a clear pro-environment platform (eg in respect of a specific range), making regulatory interest much more likely.

Aside from the risk of dealing with a burdensome regulatory investigation, note the CMA's new powers under the Digital Markets, Competition and Consumers Act 2024 (DMCCA) will be coming into force shortly (likely April 2025). After that, the CMA will have the power to issue fines for up to £300,000 (or 10% of your global turnover if higher) for breach of consumer protection laws.

Decisions as to whether such a breach has occurred in this context will be determined by reference to the CMA's Green Claims Code, and in turn this guidance.

Any practical tips?

Green claims should already be on businesses' radars and so this guidance is mainly of practical relevance, in that it assists fashion retailers to understand how the rules apply to this specific sector. The basics continue to apply: don't use vague terms; ensure you can substantiate everything you say; and put yourself in the shoes of consumers when considering how a claim will be interpreted. Where possible, get marketing teams to work forwards and not backwards. That is, start by looking at what you can substantiate, and create your green claim out of that; it's far riskier to create a claim and then try to reverse engineer any substantiation.

CJEU rules on pricing display strategies of Aldi Süd

The question

How do you correctly advertise pricing discounts given the "prior price" rule in the Pricing Information Directive (in particular where the retailer has sold the product at a lower price within the 30 days preceding the price reduction)?

The key takeaway

Businesses selling goods in the EU should review their pricing display strategies following the CJEU ruling which confirms that labels claiming a percentage price reduction must do so relative to the lowest price in the last 30 days.

The background

Aldi Süd, the German retailer, had sold fruit within the previous 30 days at three different prices: the lowest price (which was no longer offered), the current 'sale' price (the middle price), and a higher price. The labelling then calculated an advertised discount rate as a percentage difference between the middle price and the higher price, as well as also displaying the lowest price the product had been on sale for in the last 30 days in small print at the bottom of the display.

The development

The Court of Justice ruled that the Aldi strategy was inconsistent with the goal of the Pricing Information Directive (as updated by the Omnibus Directive) to 'improve consumer information'. Indications of price reductions in the EU need to be calculated based on the "prior price", which is generally the lowest price at which the retailer had sold that product within the 30 days preceding the price reduction.

Why is this important?

Whilst this decision does not change the law as stated by the updated Pricing Indication Directive, it is important in clarifying and confirming its strict application. Whilst there are many ways that businesses may wish to present pricing advantages, including was/now pricing, percentage-based discounts and presentations that adopt both, the landscape has become trickier to navigate. This case makes it clear that even if the lowest price in the prior 30 days has been set out somewhere on the pricing label, this does not mean that the percentage discount could then be calculated by reference to a different price (ie the usual selling price). Clearly this has the potential to leave businesses in an unsavoury position where a discounted current price is better than the usual selling price but not as good as a sale price that has been available in the prior 30 days.

Any practical tips?

Businesses selling to consumers in the EU will want to be extra vigilant when making any kind of price reduction announcements in relation to products that have been on promotion within the prior 30 days. This is of particular concern at this time of year, when Black Friday promotions are often closely followed by Christmas holiday promotions.

UK pricing practices in the spotlight

The question

What should businesses take note of recent amendments to the UK's Price Marking Order and the CMA's newly published report on loyalty pricing?

The key takeaway

Consumer-facing businesses should carefully consider the compliance of their pricing display strategies following amendments to the UK Price Marking Order by the new Government and the CMA's recent publication of its report on loyalty pricing in the grocery sector.

The background

The Price Marking (Amendment) Order 2024 (**PMO**) came into effect on 1 October 2025, amending the Price Marking Order 2004 (**2004 Order**). It aims to help consumers identify and compare selling and unit prices both offline and online. The amendments follow the Competition and Markets Authority (CMA) investigation into loyalty and unit pricing, previously reported on in RPC Bites #60.

The development

The PMO

The amendments in the updated PMO implements:

- consistency of units for unit pricing: Article 14 of the 2004 Order is revoked so that, if products are sold by "unit price", businesses are required to display prices per product in metric units (kilogram, litre, metre, square, or cubic metre), depending on how the product is sold
- more stringent legibility requirements: price indications, which includes selling price, unit price, commission, conversion rate or VAT changes, must be displayed in a clear and reasonably sized font
- exclusion of deposits: from the "selling price" and "unit price" of goods
- display of the reduced selling price and reduced unit price for general reductions.

The PMO provides further rules in relation to where a product is offered at multiple selling prices dependent on whether a consumer meets a defined criterion (ie standard v loyalty scheme). In this case, each selling/unit price and the relevant conditions must be clearly displayed nearby.

Loyalty pricing

The coming into force of the updated PMO has been swiftly followed with the CMA publishing its findings from its investigation into around 50,000 grocery products on loyalty price promotions. Perhaps somewhat surprisingly, given the current trend of regulatory activity in pursuit of the protection of consumers, the findings were positive for retailers. The CMA found "very little evidence" of supermarkets inflating the prices of groceries to make their loyalty promotions appear misleadingly attractive. It concluded that 92% of the products reviewed offered genuine savings on the usual price. In any event, the CMA has written to UK supermarkets using loyalty promotions to advise them to review their practices to ensure compliance with consumer law and the CMA's advice, particularly when alternating these promotions with others ie was/now promotions. An additional question has also been put to supermarkets for consideration – whether they should do more to ensure more groups of consumers can join and use the loyalty schemes ie those without smartphones.

Why is this important?

This reaffirms the CMA's increased interest in specific pricing rules in the UK to ensure that consumers can make their purchasing decisions as rationally as possible and comes off the back of consumer research the CMA undertook in 2023 and published in early 2024.

Businesses should ensure compliance with the updated PMO and the CMA's loyalty pricing advice (which points businesses towards the CTSI Guidance for Traders on Pricing Practices), particularly given that the CMA will have strengthened enforcement powers from spring next year, under the Digital Markets, Competition and Consumers act 2024.

Any practical tips?

Real estate on price labels (and shelf edge labels in physical shops) is the main victim of these new PMO rules – with potentially multiple unit prices needing to be displayed in some circumstances. For example, where a product is offered for sale with a promotional 3 for 2 deal, the price label will need to show both the unit price for when a product is bought by itself, and the unit price for when the product is purchased on the multibuy promotion.

Businesses should ensure that those responsible for pricing strategies and their display and design have updated training in order to ensure that all the necessary pricing information (including loyalty pricing) is both displayed and is completely clear and understandable for consumers.

News flash: timeline for the Digital Markets, Competition and Consumers Act

On 24 May 2024, the UK's Digital Markets, Competition and Consumers Act (**DMCCA**) received Royal Assent.

The Act introduces a range of reforms to the competition and consumer protection landscape, including empowering the Competition and Markets Authority (**CMA**) to independently determine and remedy breaches of competition law without requiring a case to be heard before a court.

While the DMCCA has passed into law itself, a wave of secondary legislation and guidance is required before the DMCCA's key reforms come into full effect. On 9 September 2024, the Government issued a statement setting out a timeline for implementation:

- **December 2024/January 2025**: the Government aims to commence Part 1 (digital markets regime), Part 2 (wider reforms to the competition regime) and Part 5 (miscellaneous measures such as arrangements to provide investigative assistance to overseas regulators) of the DMCCA.
- **April 2025**: the Government expects to commence Part 3 and Part 4, Chapter 1 (new consumer laws and enforcement regime) of the DMCCA.
- **Spring 2026**: reforms to subscription contract rules are anticipated to begin. Work has begun on this area already with the Government publishing a consultation on the implementation of the new subscription contracts regime on 18 November 2024. The consultation closes on 10 February 2025.

Though the timeline is subject to change, the Government has emphasised that it plans to bring the DMCCA into play as quickly as possible, albeit at a pace that allows regulators and businesses the time necessary to prepare accordingly.

For a more detailed explanation of the DMCCA and its requirements, see our Summer 2024 Snapshots, and for our take on the CMA's new draft guidance in response to the legislation, see our Autumn 2024 Snapshots.

Harmful online choice architecture: ASA criticises Nike and Sky for "dark pattern" tactics

The question

What must businesses do to ensure that their ads do not fall foul of the ASA and CMA's ongoing investigations into harmful choice architecture and dark pattern tactics?

The key takeaway

It is vital that businesses ensure that their ads conform to the CAP Code and the Digital Markets, Competition and Consumers Act 2024 (**DMCCA**) to avoid scrutiny by the Advertising Standards Authority (**ASA**) and Competition and Market Authority (**CMA**). This includes clear communication of pricing, product limitations and subscription terms, avoiding misleading design practices that exploit consumer trust.

The background

On 25 September 2024, the ASA issued rulings against Sky UK Ltd (**NOW TV**), and Nike Retail BV (**Nike**) for employing "dark pattern" tactics in their online ad campaigns.

- NOW TV: the ads failed to make clear that additional free trials bundled with memberships would auto-renew unless cancelled, with terms displayed in less prominent fonts and colours.
- Nike: ads commissioned by The Sole Supplier promoted discounted children's trainers as though the offer applied to adult sizes, misleading consumers about the product's value.

See our previous Snapshots Autumn 2024 article on online choice architecture rulings.

The development

The ASA's rulings highlighted the following key principles:

Now TV

- Ads must specify whether a paid subscription will begin automatically after a free trial and display renewal costs prominently.
- Information about auto-renewal should be immediately visible and follow the most prominent reference to the free trial. Poor placement, such as smaller fonts in subdued colours, can result in a breach.

Nike

- Omitting or obscuring material information, such as size restrictions or pricing conditions, is considered misleading.
- The use of language and emojis implying significant discounts without clarification about product limitations (eg available sizes) violates transparency rules.

Why is this important?

In a discussion paper published in April 2022, the CMA explored how online choice architecture can be exploited to hide information from consumers and distort consumer behaviour. Dark pattern tactics are a subset of harmful online choice architecture. The Organisation for Economic Co-Operation and Development (**OECD**) provided examples of these practices, including:

- misleading urgency (eg false countdown timers or "only 1 left!" prompts)
- drip pricing (revealing additional fees late in the transaction)
- obscured cancellation options and terms for subscriptions.

The DMCCA strengthens regulatory powers, enabling the CMA to address harmful practices in areas such as subscription transparency, hidden fees, and price manipulation. Whilst the DMCCA received Royal Assent on 24 May 2024 and is now being implemented in stages, its implications will significantly impact businesses' online marketing strategies. See our previous Snapshots Summer 2024 article on the DMCCA.

Any practical tips?

Businesses utilising online choice architecture in their ads must ensure that they are in full compliance with the CAP Code and the DMCCA and should:

- ensure transparency: (a) use clear, prominent language to communicate key terms such as pricing, size restrictions, and subscription renewals; and (b) highlight financial commitments associated with free trials, especially auto-renewal charges
- prepare for the DMCCA: monitor updates on secondary legislation and the CMA's enforcement guidance, ensuring systems are in place to adapt to new requirements, as discussed in our previous Snapshots Autumn 2024 article
- improve design standards: material information should be set out in a clear font of a reasonable size and colour and be located sufficiently close to the offer
- supervise third-party advertisers: approve all third-party ads to ensure compliance with regulations and avoid reputational damage
- conduct internal audits: regularly review marketing practices for compliance and consult legal experts to identify potential breaches.

Influencer posts and affiliate links: the whole marketing chain must know the rules

The question

Why did the Advertising Standards Authority (**ASA**) rule against Sainsbury's on the use of an affiliate link by an influencer (noting that Sainsbury's had no involvement in the creation of the post) and what steps could Sainsbury's take to help prevent the problem from happening again?

The key takeaway

The combination of influencer marketing and affiliate links is a dangerous combination from a compliance perspective, especially if there are a number of different parties (from brand to intermediaries to influencer). It's important to ensure that everyone in the chain knows the rules and that the advertising bolts are tightened as much as they can be to avoid a breach.

The background

An Instagram story posted by Kayleigh Johnson featured a box with the question "Are you going to breastfeed? If not what formula will you use?". Text underneath explained her approach to formula feeding and also included an affiliate link titled "Formula we use" which linked to a product page on Sainsbury's website for an infant formula milk powder.

The CAP Code prohibits the marketing of infant formula and the following issues were raised for the ASA to assess: (1) whether the post qualified as a marketing communication and therefore breached the CAP Code; and (2) whether the post was obviously identifiable as a marketing communication.

The affiliate marketing structure in this case involved multiple parties:

- the influencer who created the post with an affiliate link
- Stylink Social Media GmbH who managed the affiliate links
- CJ Affiliate Platform who hosted the affiliate program for Sainsbury's, and
- Sainsbury's who operated the program and issued compliance rules.

The development

On the first issue, the ASA ruled that including an affiliate link to infant formula constituted a prohibited promotion under the CAP Code. Sainsbury's acknowledged that the ad should not have appeared, not least as its affiliate terms specifically prohibit marketing infant formula. The interesting part of this decision is the depth which the ASA went into assessing each party's involvement in the affiliate chain, which helps underline the need for everyone in a chain to understand and comply fully with any brand requirements and limitations. Following the incident, Sainsbury's updated its affiliate program terms to provide clearer compliance guidelines.

On the second issue, the influencer had used a label "aff" which was intended to be an abbreviation for "affiliate". However, the ASA deemed the label insufficient for two reasons:

- "Aff" was positioned in a corner of the story and overshadowed by other text, making it unlikely to be noticed, and
- most consumers would not recognize "aff" as an abbreviation for affiliate, and the ad's short lifespan (five seconds) further reduced transparency.

The ASA held that the labelling failed to make the ad obvious to viewers.

Why is this important?

The case highlights the care that is needed by all parties in an affiliate marketing chain to ensure that there is no breach of advertising regulation. Retailers, influencers, and platforms must all collaborate to ensure compliance. The decision also reminds us that abbreviations like "aff" or "affiliate" are wholly inadequate when it comes to advertising disclosures.

Any practical tips?

When running affiliate schemes, consider:

- clear ad labelling: posts containing affiliate links must be clearly identified as ads. Use universally understood labels like "#ad" and ensure they are prominently displayed
- review affiliate program terms: businesses should frequently audit affiliate agreements to ensure compliance, explicitly outlining prohibited promotions and disclosure standards
- collaborate across the chain: platforms, influencers and brands must work together to proactively address compliance issues. Training and resources can help influencers understand their obligations under the CAP Code
- test ad visibility: conduct user testing to ensure that ad disclosures are clear and visible across different platforms and formats, especially for transient content like Instagram Stories.

Travel agent found to have misled consumers with "from" price claims

The question

How can advertisers avoid misleading consumers when using "from" price claims?

The key takeaway

When making "from" price claims, all non-optional fees and costs that will apply to all or most buyers must be included in the price quoted, even where the advertiser has no control over such fees or costs. If the availability of the product or service is limited or the prices are subject to change, this must be explicitly stated in the ad. If prices cannot be updated in real time, the ad must also explicitly state when the prices were last checked.

The background

Trav Expert Ltd t/a Travel Crew (**Travel Crew**), a retailer of flights and holidays, sold flights as an agent through its website www.travelcrew.co.uk. The website had a search function, enabling consumers to look up flights according to date and destination, the use of which would present consumers with a "from" starting price for the flight.

A complainant challenged whether the price listed at the booking stage for a flight from London to Buenos Aires was misleading, as the "from" price quoted when the consumer initially searched for the flight on the website had been lower.

In response to the complaint, Travel Crew argued that:

- the flight prices listed on its website did not update in real time
- it had used the wording "from" on the ad to indicate that the price advertised was a starting price for flights on that route but was subject to availability, which "changed rapidly" and so may not be the price available when a customer attempted to book
- its terms and conditions stated that the prices advertised were only indicative and could change before booking was complete
- the advertised price included taxes, but additional fees and surcharges might also apply depending on the airline and flight.

The development

The Advertising Standards Authority (**ASA**) upheld the complaint. While the ASA acknowledged that Travel Crew was an agent and did not provide flights directly itself, it found that because Travel Crew had not explicitly stated in the ad that availability was limited and that prices could change, "consumers would expect to have a reasonable chance of purchasing the flights at the prices advertised". It was not enough for Travel Crew to merely state in the ad that the price was a starting "from" price. Further, Travel Crew did not provide evidence to show that the prices advertised were genuine, and no information had been provided in the ad as to when the advertised prices were last checked. Therefore, consumers would have no way of judging the accuracy of the price. It was not sufficient that such statements and information about pricing and availability were provided in Travel Crew's terms and conditions, as these were located on a separate page to the ad.

In response to Travel Crew's claim regarding additional fees, the ASA emphasised the requirement under CAP Code rule 3.18 that quoted prices must include non-optional taxes, duties, fees and charges that apply to all or most buyers. Therefore, Travel Crew should have included in the advertised price all non-optional fees relevant to each airline and flight. Again, it was not sufficient for such information to be stated on a separate page. Travel Crew was therefore found to have misled consumers.

Why is this important?

The decision highlights the importance of price transparency in all ads, but particularly in the travel sector where prices regularly fluctuate. The ASA is keen to ensure that consumers receive more accurate information regarding flight prices, prior to the booking stage. In a similar vein, the Digital Markets, Competition and Consumers Act 2024 (**DMCCA**) adds hidden fees and "drip pricing" to the list of commercial practices prohibited in all circumstances. For more on this, see our previous Snapshot. For travel agents, it will often be the case that additional airline fees and costs apply to a product or service, over which the travel agent has no control. According to this decision, such businesses will be required to clearly state in their quoted prices to consumers the exact figures of any additional fees and costs for each flight that the agent offers.

Any practical tips?

All advertisers promoting goods or services with regularly fluctuating prices should consider the CAP guidelines on the use of qualifications to ensure any limitations or relevant information in relation to the price are clearly communicated to the consumer in the promotional material itself. It is not enough for advertisers to rely on their separately-located terms and conditions. Additionally, where automatic price updates are not in place, advertisers must ensure that the ad clearly displays the date on which the price was last checked.

ASA rules against telecoms companies on mid-contract price rises

The question

What steps should be taken to ensure contractual mid-term price rises don't fall foul of advertising regulations or Ofcom's existing and incoming transparency rules?

The key takeaway

The Advertising Standards Agency (**ASA**) has ruled against six major telecommunications companies in relation to mid-contract price rises. The ASA took a firm stance on the companies' failure to draw price rise information to the attention of consumers. Rules will be tightened further from January 2025 with Ofcom requiring communications companies to clearly set out any mid-term contract prices rises in pounds and pence before signing, with any inflation-linked rises being banned.

The background

Currently, many telecommunications companies often include mid-contract price rises in their agreements with consumers, with such price rises being linked to inflation. The concern from Ofcom has been that these price rises have left consumers with a lack of certainty about the contracts they are signing and the price rises that will take effect during the contract's term. From 2022, Ofcom has required communications providers to "specify price rises in contracts from the start", before consumers signed the contract. Failing to do so meant consumers would need to be given one month's notice before any rises, and the right to exit the contract fee-free.

The development

The ASA reviewed ads from BT, EE, Plusnet, TalkTalk, Telefonica, and Virgin Media and ruled that each had failed to make clear to consumers that the contracts would be subject to mid-term price increases. The regulator upheld the complaints against all six companies' ads for broadband or mobile data products for being insufficiently transparent over pricing, and updated guidance has since been published on the presentation of mid-contract price increases in ads.

Consumer protection measures will be strengthened further from 17 January 2025, when Ofcom will require that all new contracts that fall within its remit show, in pounds and pence, what price rises will be imposed mid-term. Inflation or percentage-linked mid-term price rises will be banned.

Why is this important?

With Ofcom's strengthened consumer protection measures coming into effect imminently, telecoms companies must ensure that their mid-contract price increases comply with the strengthened protections and do not include any inflation or percentage-linked mid-term price rises. Beyond the telecommunications sector, the ASA's rulings demonstrate that all organisations including mid-contract price rises in their agreements must ensure that their ads are transparent and comply with the new guidance.

Any practical tips?

Make sure that all mid-contract price rise information complies with the transparency rules. In particular:

- show clearly when prices will rise and by how much, in pounds and pence
- make sure that dates and increase amounts appear and remain on screen, even when scrolling
- avoid using colours and backgrounds that blend in with the background, and
- locate qualification information close to price claims and ensure that it is immediately distinguishable.

Round up of recent green claims

Key updates

ASA ruling against misleading Mazda ad

The ASA has ruled that a paid-for social media ad that promoted Mazda's electric-hybrid vehicles as "exciting, efficient and sustainable" was misleading and breached the CAP Code. According to the ASA, the term "sustainable" gave a misleading impression about the vehicle's environmental impact and had not been sufficiently substantiated. As a hybrid model, emissions were generated when the petrol engine was used, and also when the vehicle was manufactured and charged. This ruling follows the ASA's guidance on advertising electric vehicles published earlier this year.

ICC updates its advertising and marketing code

The International Chamber of Commerce (ICC) has published the 11th edition of its Advertising and Marketing Communications Code. The Code sets a global standard for responsible marketing and acts as a benchmark for almost 50 self-regulatory codes across the world. The updated Code includes a new section on substantiation of claims emphasising that advertisers must be able to substantiate all express or implied green claims, including "aspirational claims or claims expressing goals or commitments related to achieving certain environmental metrics" in the future. The Code also emphasises the importance of explaining any limitations to the claim (eg about the amount of recycled content in a product).

Annual greenwashing report published

In its third annual greenwashing report, the ESG research provider RepRisk has found a 12% decrease in greenwashing globally across all sectors and a 20% decrease in climate-related greenwashing. This is the first decline in such figures in six years - likely due to increased regulatory scrutiny and the prevalence of "greenhushing". Other notable findings include a 30% increase in particularly eg regious greenwashing cases (eg those that could have a large impact on consumers, or where there is intent to mislead) and also that 30% of companies found to be greenwashing in 2023 were then "repeat offenders" in 2024.

Sector-specific updates

Transport

- In one of the first greenwashing decisions against a cruise operator, the Dutch Advertising Code Committee has ruled that MSC Cruises' green claims, including its "net zero by 2050" target and "#Savethesea" slogan were misleading. The advertising board was particularly concerned about MSC's claim that the Liquefied Natural Gas used by its ships was "one of the cleanest" fuels without properly considering its broader environmental impact. The complaint was made by Fossil Free Netherlands, the group that won a civil case against KLM earlier this year.
- The environmental advocacy group, Climate Integrity, has submitted a complaint to the Australian Competition and Consumer Commission accusing Quantas of greenwashing. The complaint focuses on Quantas' advertising of its 'fly carbon neutral' product which enables consumers to offset the emissions of their flights, and also claims promoting its use of 'sustainable aviation fuels'. The ACCC has now been asked to investigate.

Energy

- Drax, the owner of the UK's largest power station, has been fined £25 million by Ofgem after an investigation showed that Drax had misreported its carbon emissions. Drax had claimed its practice of using wood pellets rather than coal to fuel the power station produced up to 80% less CO_2, however Ofgem found an "absence of adequate data governance and controls" had led to inaccurate reporting of data.
- In one of the first greenwashing claims in the country, the South African Advertising Regulatory Board (ARB) has upheld a complaint against TotalEnergies relating to claims that its partnership with SANParks (South African National Parks) demonstrated its commitment to "sustainable development". The ARB held the claim "committed to sustainable development" was misleading and breached the advertising code because TotalEnergies' core business relied on the ongoing exploitation of fossil fuel which was directly opposed to sustainable development and there was no evidence of a link between its support of SANParks and sustainable development.

Agreements to agree: Price for goods "to be fixed" by agreement results in partially enforceable contract

KSY Juice Blends UK Ltd v Citrosuco GmbH **[2024] EWHC 2098 (Comm)**

The question

Where a contract for the sale of goods did not expressly specify the price for a portion of the goods, was the contract for the sale of those goods, or an element of it, enforceable or unenforceable as a mere agreement to agree?

The key takeaway

In a contract for the sale of goods, providing for the price for a portion of the goods to be fixed by agreement between the parties may be construed as an agreement to agree resulting in that part of the contract being held to be unenforceable.

The background

KSY Juice Blends UK Limited (**KSY**) is a Greek company which supplies juice products internationally. Citrosuco GMBH (**Citrosuco**) is a Brazilian company which produces 100% natural orange juice.

KSY entered into a contract with Citrosuco in 2018 to sell orange pulp wash or 'wesos', that is produced when manufacturing various types of fruit juice which has then been subject to a water extraction process. KSY delivered 400 Metric Tonnes (**MT**) of wesos to Citrosuco in 2019 which Citrosuco paid for. Citrosuco then declined to take delivery of a further 800 MT by not giving instructions for the delivery of the product. In 2020, KSY delivered 126 MT of wesos – Citrosuco paid for 84 MT but not 42 MT. In September 2020, by letter, KSY terminated the contract alleging that Citrosuco was in repudiatory breach of contract. Citrosuco's case was that the letter from KSY constituted a repudiatory breach which it accepted on 26 October 2020.

The 2018 contract provided:

"3. Price
Invoicing price is 1.600euro/mt for 60 brix
Price adjustable according to Brix value +- 5 Brix
Free trucks will be offered from the seller according to the agreed volume & price of each year.
Calculation basis for the 1.200mt fixed is 1.350 euro/mt which corresponds to the 400mt/year 2019-2020-2021…

5. Delivery period:
1.200MT per each year
Deliveries to start January to December with the following split:
400mt fixed at 1.350euro/mt - invoicing price is 1600euro/mt
Difference of price in free trucks
800mt at open price to be fixed latest by December of the previous year
Difference of price in free trucks"

The contract terms contain two concepts key to calculating price. 'Brix' refers to the amount of dissolved solids in a liquid via its specific gravity. It is commonly used in this industry and fixes the price based on an assumption as to the Brix level with an adjustment to reflect the actual level. The concept of 'free trucks' is used to adjust the price in response to market price fluctuations by providing free product on top of the contracted volume to align the price of goods with current market conditions.

As the contract did not specify the price for wesos beyond 400 MT per year, the main issue was whether the contract for the sale of wesos beyond 400 MT per year was enforceable or rather unenforceable as a mere agreement to agree.

The decision

The court's starting point in considering whether a contract for the sale of goods fixes the price of the contract was to consider the express terms of the contract. The facts of this case where the contract left the prices to be determined at a later time provided a more difficult scenario given that agreements to agree are not enforceable. The court would, however, determine the case on its facts, having regard to the construction of the contract, and if necessary, implying relevant terms to seek to give effect to the bargain that the parties believed they have entered into.

The contract showed the parties' intention to deal in 1,200 MT of wesos per year for three-years. Use of the word 'target' was assessed as to whether it was an aim rather than an agreed figure. However, the court held that email correspondence between the parties indicated "the clearest intention" for a total of 3,600 MT to be bought and sold. In determining whether a price was agreed, the court engaged with the language of the contract alongside the parties' intentions and noted that a failure to agree would not destroy the entire contract, but only limit it. It reasoned that destroying rather than preserving only part of a bargain is better than destroying the bargain altogether.

On the question of price for the wesos beyond the 400 MT per year, the court agreed with Citrosuco, finding that the contract did not expressly support an agreed price of €1,600/MT for numerous reasons. Firstly, the only way of construing "open price" was for it to mean a price to be fixed by agreement between the parties using the contractual mechanisms, which under the contract would mean the parties agreeing the price by the latest in the December of the year preceding delivery. Secondly, the "invoicing price" did not reflect a fallback provision in the event the parties could not agree a price. If the parties had intended the "invoicing price" to be anything other than the price on the invoice, there would have been no reason to set the price at €1,600/MT when the agreed price for the first 400 MT per year was €1,350/MT. Thirdly, the free trucks mechanism was central to the price rather than an optional process to be operated by KSY. The court also reasoned that there was no basis to imply terms to give the contract business efficacy or to oblige the parties to use reasonable endeavours to agree a reasonable or market price.

The contract for the balance of 800 MT of wesos per year was therefore simply an agreement to agree on the issue of price which was not enforceable.

The case is subject to an appeal.

Why is this important?

The case highlights that where a contract expressly states the price for an initial quantity of goods but allows the price for a portion of goods to remain to be fixed by agreement between the parties, that part of the contract may be held to be an unenforceable "agreement to agree".

Any practical tips?

Ensure that essential terms such as price are set out expressly and precisely for all contract goods and services avoiding words suggesting that price is "to be fixed by agreement of the parties," unless there's a pricing mechanism elsewhere within the contract or enough information within the contract for price to be implied.

If there is a history of reliance, or a specific intention to rely on section 8 of the Sale of Goods Act 1979 in relation to contract price, ensure that there are no terms within the contract that would block reliance on the statutory provision.

COMMERCIAL

Construing material adverse effect/ material adverse change clauses

BM Brazil I Fundo De Investimento EM Participacoes Multistrateg ia v Sibanye BM Brazil (Pty) Ltd **[2024] EWHC 2566 (Comm)**

The question

How did the courts go about construing a material adverse effect definition (**MAE**) in a share purchase agreement (**SPA**) to determine whether an event constituted a MAE so as to discharge the buyers from their obligation to close the transaction?

The key takeaway

To be "material" in the context of the SPA the event must be significant or substantial, and there is no bright line test, with each case determined by its own facts (including size of the transaction, the nature of the assets, the length of the process of the sale, and the complexity of the SPA). In this case a 20% reduction in the equity value of the target would be material, a 15% might be material, but a 10% reduction, where the contract had particular characteristics, was too low to count as material for the purposes of the MAE provision.

The background

The parties had entered into two share purchase agreements (**SPA**) for the acquisition of two mines in Brazil by Sibanye. However, two weeks after the signing of the SPAs, between the signing and closing, a geotechnical event (**GE**) occurred at one of the mines. Following a blast, a portion of a slope at the mine pit displaced by up to two meters, with resulting cracks extending for a total height of approximately 84 meters. No injuries or material losses occurred.

The relevant SPA contained a Material Adverse Effect (**MAE**) clause allowing the purchaser to avoid the transaction if a material event occurred between the signing and closing of the SPAs.

"Material Adverse Effect" means any change, event or effect that individually or in the aggregate is or would reasonably be expected to be material and adverse to the business, financial condition, results of operations, the properties, assets, liabilities or operations of the Group Companies, taken as a whole, excluding any such change, event or effect arising out of, in connection with or resulting from (a) general global, national or regional economic, business, political, market, regulatory or social conditions [...] [emphasis added].

Following the GE, Sibanye purported to terminate the SPAs on the basis that the GE constituted an MAE under the relevant SPA. The sellers subsequently commenced proceedings against Sibanye for declaratory relief and damages for wrongful repudiation and/or renunciation of the SPAs.

The key issue was: was the GE a MAE?

The decision

The court found that, at the date of termination, the GE was not and would not reasonably have been expected to be material, and therefore that Sibanye was in breach of the SPAs in terminating the purchase.

In reaching this conclusion the court applied the ordinary principles of contract construction, as stated in the main authority: Wood v Capita Insurance Services Ltd [2017] UKSC 24, ascertaining the objective meaning of the language and considering the contract as a whole and the factual background.

In its judgment the court provided guidance, that is more generally applicable, on issues of construction including whether and how the MAE provisions apply to "revelatory occurrences"; the question of whether the "change, event or effect" "is or would reasonably be expected to be material and adverse..."; and the meaning of "material".

Revelatory effects

The sellers argued that even if there had been a revelatory effect of the GE in revealing wider problems, that did not qualify the GE as a MAE. The court agreed with the sellers that the terms of the MAE definition dictated that a matter was only a MAE if that 'change, event or effect' was itself material and adverse, and not just a 'change, event or effect' indicating the possibility that there may be other problems which existed at the time of the signing of the SPA.

What "would reasonably be expected"

The assessment of what "would reasonably be expected to be material and adverse" required an objective test, to be made from the perspective of a reasonable person in the position of the parties at the time when cancellation on the basis of the alleged MAE is notified. On the further question of what degree of likelihood is implied by "would reasonably be expected," the judge determined that a mere risk that a matter may turn out to be material was not enough. The assessment was whether a reasonable person would have considered it more likely than not that the matter would turn out to be material.

Materiality

On the question of materiality, the court considered that it was important to examine whether a company has suffered a MAE in its business or results of operations that is consequential to the company's earnings power over a commercially reasonable period (a period of years rather than months). 'Material' was also intended to mean 'significant or substantial. There was no bright line test for what constitutes materiality which would be applicable to all MAE clauses. The size of the transaction, the nature of the assets, the length of the process of the sale, and the complexity of the SPA were all relevant.

In considering the US authority cases, the court reasoned that 20% reduction in the equity value of the target would be material and 15% might also be material, but that a 10% reduction in the value of the company in the present case, where the contract had particular characteristics, was too low to count as material for the purposes of the MAE provisions.

Having established this, the court turned to the ultimate question: was the GE a MAE?

The court examined the qualitative and quantitative aspects of the GE (but showing scepticism about the relevance of the qualitative aspects) and found that the GE was not a MAE because materiality was not satisfied. Key factors supporting this conclusion were: GEs often happen at open pit mines, with 166 recorded at the mine in question in 2021, it was by no means large, no one was killed or injured, no equipment was lost, operations at the mine resumed on the same day, and there were no adverse regulatory consequences.

Additionally, the financial effect of the GE incident at the date of termination in terms of cost of waste actually removed by then, or planned ore not mined by that date was immaterial. The subsequent associated remediation was not considered to be material at a sum of more than US$20 million, which was well below 5% of the mine purchase price.

Why is this important?

The judgment's examination of UK and US authorities and wider guidance on construing the MAE definition will be of use to those drafting MAE/MAC clauses. The case also provides practical examples of what constitutes "materiality" (applied in a mining setting).

Any practical tips?

Consider in advance the specific types of material events or effects that would warrant the buyer terminating the transaction. Where a buyer wishes to protect itself from a specific event, this should be inserted as a separate condition rather than seeking to rely on the general MAE provision.

Given the likely difficulty in establishing materiality, a buyer may also wish to provide for alternative provisions it can rely on such as the termination clause so as not to have to rely solely on the MAE provision.

A commercial or financial impact must usually be suffered by the target for a period of years rather than months for a MAE to be found to have occurred. If the risk is more likely to arise from a more short term event or effect, ensure the MAE contains appropriate timeframes.

MAE provisions are judged in the context of the SPA as a whole, including the other risk allocation provisions such as warranties and indemnities. Ensure these are not inconsistent with the aims of the MAE.

COMMERCIAL

Reasonable notice termination not construed or implied into a contract with detailed termination provisions

***Artcrafts International SpA v MOU Ltd* [2024] EWHC 1558 (KB)**

The question

Where a contract contains comprehensive termination provisions, in what circumstances will the court avoid construing or implying an additional right to terminate on reasonable notice?

The key takeaway

Where a contract expressly sets out the circumstances in which a party could terminate and requirements to enact termination, it was "unarguable" that the contract could be construed to allow termination on reasonable notice or for such a term to be implied.

The background

MOU is an English luxury brand, well-known for its footwear. Artcrafts is an Italian company that distributes apparel on behalf of a portfolio of brands.

In 2011, MOU granted Artcrafts an exclusive licence to manufacture, distribute, sell, advertise and promote various of its products in return for substantial royalties.

In 2022, following the issuance of several notices of material breach by MOU, Artcrafts successfully brought proceedings against MOU to ensure the continuation of the licence agreement. In 2023, Artcrafts brought the present summary judgment proceedings against MOU, alleging that MOU was in breach of the licence agreement for advertising and distributing products the subject of the licence in the USA and elsewhere both itself and through a third party.

MOU denied that it was in breach of the agreement and alleged that on a "true construction" of the contract it was entitled to terminate the agreement on reasonable notice, despite no such express provision being contained in the agreement, and no such argument having been raised in the 2022 proceedings (in which MOU had sought to terminate for material breach).

The licence agreement was for a five year term, and included an automatic renewal right for Artcrafts. The agreement also contained a fairly detailed "Events of Termination" clause which set out various events that would entitle the parties to terminate the agreement, including insolvency, challenge to validity of the rights the subject of the agreement, change of control, non-payment of royalties, or generation of insufficient royalties over a two-year period. The court commented that this clause demonstrated that the parties had carefully crafted circumstances in which particular parties could terminate the agreement, even in the absence of any breach by the counterparty.

A separate clause (clause 29.3) provided that "the rights and remedies of the parties in connection with the agreement are cumulative and are not exclusive of any rights or remedies provided by law". This meant that if the relationship were to fall apart due to the actions or inactions of the other party, they would also have the common law rights to terminate for repudiatory or renunciatory breach.

The court considered two key issues:

- Did a true construction of the contract allow for termination on reasonable notice?
- In the context of the terms of contract could a termination clause be implied in the terms alleged?

The decision

The court granted summary judgment to Artcrafts.

True construction of the agreement

The court found MOU's plea on true construction of the agreement to be "unarguable". The contract contained extensive and carefully drafted provisions as to when termination was permitted, these provisions were detailed and, importantly, were not limited to circumstances in which Artcrafts breached the contract, including, for example, rights to termination for failure to generate sufficient royalties. The agreement was the product of negotiation between the parties and was professionally drafted by lawyers. Both parties had the benefit of leg al representation and advice at the time they entered into the contract.

These factors viewed collectively showed that the agreement had been drafted to "keep the licence agreement alive if at all possible", such that there was no scope for a true construction to provide for termination on reasonable notice. A clause mandating that the parties use their best efforts to preserve the contract by entering into negotiations, was also contrary to an objective common intention that, at the time the agreement was entered into, the parties intended that one party should have the right to unilaterally bring the contract to an end for any reason or no reason at all. While the inclusion of an entire agreement clause did not exclude the implication of a term in theory, it showed the approach of the parties was to record their agreement in detailed express provisions.

Implied term – termination on reasonable notice

In assessing whether a reasonable notice termination clause could be implied into the agreement, the court confirmed the approach that implication occurs after the express terms are given their proper construction. The detailed termination provisions in the agreement did not favour implication of the term.

In any event, the court considered that the implication of such a term would break the "cardinal rule" that an implied term must not contradict the express terms of a contract, given that termination on reasonable notice would fly in the face of various express terms of the agreement which provided (i) for termination on notice where specific conditions were met; (ii) for termination in the event of material breach, though even then the parties had to follow specific procedures before terminating; (iii) for circumstances in which the parties could terminate absent any breach; and (iv) Artcrafts with the right to extend the agreement in five-year terms, the benefit of which would be lost if termination was permitted on reasonable notice.

Even if the alleged implied term had not contradicted the express terms of the agreement, the court found that the express terms of the agreement were sufficiently definite, detailed and commercially sensible so that MOU could not bring itself within the circumstances that such a term could be implied into the agreement.

Why is this important?

Termination clauses are a valuable mechanism for parties to define the circumstances in which a contract can be brought to an end. While every case turns on its own facts, and on the terms of the contract under consideration, where a clause clearly specifies the circumstances in which a party may terminate a contract, a party is unlikely to be able to imply additional terms for termination, or terms to the contrary.

Any practical tips?

In light of the fact that it may be difficult to imply further such terms, carefully consider and define the circumstances in which the agreement should be terminated. Ensure the termination clause or clauses align with other contract provisions.

Where the contract duration is long, or where the counterparty is given renewal rights, consider providing some mechanism for early termination to avoid the inability to terminate.

Effect of a contractual liability cap on set-off and contractual interest

Topalsson Gmbh v Rolls-Royce Motor Cars Limited **[2024] EWCA Civ 1330**

The question

Under a contract's liability cap, should the cap be applied separately to each party's liability before any set-off or after calculating the net financial position between the parties?

Where there is a contract term stating that interest is the sole and substantial remedy for late payment, should interest for late payment be caught by a financial cap in a limitation of liability clause?

The key takeaways

A contractual cap on liability was interpreted to apply to each party's liability separately, before any set-off of sums due to each other. The interest on late payments fell outside of the liability cap where the parties had expressly agreed that interest was a "substantial" and "sole remedy" for late payment.

The background

Rolls-Royce contracted with software developer Topalsson to develop a new digital visualisation tool allowing prospective customers to see photo-realistic renderings of Rolls-Royce cars with different custom configurations, before purchasing.

After various delays and disputes, Rolls-Royce terminated the agreement. Topalsson brought a claim against Rolls-Royce in the High Court. Rolls-Royce defended the claim and counterclaimed for its losses arising out of the termination.

The High Court found that Rolls-Royce had validly terminated the agreement and was due termination damages in the amount of circa €7.9 million. This figure was reduced by the amount owed by Rolls-Royce to Topalsson on termination (around €800,000). The judge then applied the agreement's €5 million liability cap, and awarded Rolls-Royce €5 million in damages, plus contractual interest calculated by reference to the dates when the sums had fallen due.

The agreement included a right of set-off and the wording of the liability cap (clause 20) in the agreement was as follows:

"...the total liability of either Party to the other under this Agreement shall be limited in aggregate for all claims no matter how arising to the amount of €5m (five million euros)."

The decision

There were two broad issues for the Court of Appeal (CA) to consider. These were: (i) the interplay between the contractual liability cap and set-off; and (ii) the interplay between the liability cap and interest.

Issue 1: Liability cap and set-off

Topalsson's case was that the liability cap should be applied separately to both parties' liabilities to each other, before setting off the sums against each other. In this case, Topalsson's liability to Rolls-Royce would be capped to €5 million and Rolls-Royce's liability to Topalsson would be €800,000, leaving an overall sum due from Topalsson to Rolls-Royce following set-off of €4.2 million.

The CA agreed with Topalsson, finding that the judge in the first instance had been wrong to set-off the financial position between the two parties before applying the liability cap. It found that both parties' liabilities should be capped separately, and then the set-off applied, reducing the amount due from Topalsson to Rolls-Royce to €4.2 million.

The court focused on the wording in the agreement's liability clause: "the total liability of either party to the other", which suggested a totting up, not a netting off. If there had been an intention to apply the cap only after the net financial position between the two parties had been calculated, the clause should have stated that expressly.

The court also commented that the totting up approach was the only interpretation which made "commercial common" sense. If the claim for set-off was taken into account before the cap was applied, the result could be manipulated, so that the party with a right to set-off could avoid the consequences of the cap altogether. By way of example, on Rolls-Royce's construction, they could withhold the entirety of the contract sum (€9million) by way of set-off, and then also claim damages, to the tune of the cap of €5 million.

Issue 2: Liability cap and interest

Topalsson argued (in an amendment to its pleadings) that as a matter of construction, Rolls-Royce's claim for contractual interest for late payment by Topalsson fell within the cap in clause 20.

The court did not allow the amendment, but obiter did consider the point and suggested that interest on late payment fell outside the cap in clause 20.

The cap could not be considered in isolation. It needed to be looked at in the context of clauses 14.11 and 14.12:

"14.11 Each Party may charge simple interest at the rate of 4% per annum above the Bank of England base rate from time to time compounded at monthly intervals from the due date for such payment until the actual date of payment No interest shall be payable under the circumstances of late payment resulting from invoices that are not properly raised or submitted by the Supplier.

14.12 Each Party agrees that any interest that is payable under Clause [14.11][2] is a substantial remedy for late payment of any sum payable under this Agreement for the purposes of section 8(2) of the Late Payment of Commercial Debts (Interest) Act 1998 and shall be the sole remedy available to the Party entitled to interest for late payment whether in contract tort or restitution or otherwise."

These clauses made it plain that the parties were agreed that interest payable under clause 14.11 was "a substantial remedy for late payment" and that it was "the sole remedy" available. It would be contrary to the express agreement in those two clauses if interest on late payment was said to be within the cap at clause 20. It would mean that the innocent party, Rolls-Royce, was denied the "sole and substantial remedy" for late payment that the parties had expressly agreed. The interest was an incentive for Topalsson to pay on time. Making interest subject to the cap (and therefore limiting interest payments) would remove this incentive and would, therefore, not make commercial sense.

Why is this important?

The case highlights the importance of considering the wider commercial context surrounding parties' potential liabilities on termination or breach when drafting liability caps, and the impact any set-off is likely to have on that cap, where sums are likely to be due from both parties.

Any practical tips?

When drafting a limitation of liability clause, consider the sums that might be due to each party in the event of termination or breach. Based on the specific scenario, consider whether set-off should occur before or after the liability cap is applied.

Ensure the words used are clear and precise because the courts will look to the language used in the contract to interpret it as well as applying "commercial common sense".

To avoid any disagreement as to whether interest for late payment falls within a financial cap, expressly include or exclude this from the cap. The court made it clear that a provision that interest for late payment was included within the cap would require clear words, because otherwise it would be an obvious denial of Rolls-Royce's common law rights.

COMMERCIAL

rpclegal.com