RPC

Snapshots for Meta

SPRING 2023

KEY UK AND EU DEVELOPMENTS FOR META'S COMMERCIAL LAWYERS

New EU metaverse regulation in discussion

PLUS

UK Online Safety Bill increases focus on child safety

EU to legislate on political advertising

New UK Code of Practice for app developers and app stores

Marketplace liability for third party counterfeit products

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Welcome to the Spring 2023 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 and David

Olly Bray
Senior partner
+44 20 3060 6277
oliver.bray@rpc.co.uk

David Cran
Partner
+44 20 3060 6149
david.cran@rpc.co.uk

WITH THANKS TO OUR FANTASTIC CONTRIBUTORS

- Mimosa Canneti
- Megan Grew
- C. Kathirgamanathan
- Nicole Clerk
- Megan Grew
- Alice Parfitt
- Shaina Majithia
- Jack McAlone
- Sophie Hudson
- David Allinson
- Benjamin Simmonds
- Aiswarya Nadesan
- Lauren Butler
- Alisha Jackson
- Tamer Tayyareci
- Daniel Williams
- Joshua Ajose-Adeogun
- Laura Verrecchia
- Anila Rayani
- Constantine Christofi
- Daniel Williams
- Mars Yeung
- Adam Williamson
- Niamh Greene
- Beth Thorne
- Tom James
- Hettie Homewood
- Nneka Ezekude

EDITORIAL

Sub-editors Anila Rayani, Joshy Thomas, Praveeta Thayalan

Design Rebecca Harbour

Contents

UK's Data Protection and Digital Information Bill Version 2

The question

What has changed in the second version of the Data Protection and Digital Information Bill (the Bill)?

The key takeaway

Very little has changed in the second version of the Bill, aside from a few amendments designed to reduce the compliance burden on businesses. The Bill is now awaiting its second reading in Parliament.

The background

The original version of the Bill was introduced to Parliament last summer as a progressive, business-friendly framework that will cut down on costs and paperwork. See our Summer 2022 Snapshot pack for a summary of the original version.

This original version was withdrawn within a few months alongside the UK's leadership changes to allow ministers to consider the Bill further. Since then, there have been inconsistent messages from the Government regarding the extent that the new law will depart from the EU GDPR and, in the interim, businesses have been in a holding pattern.

The development

On 8 March 2023, the Government withdrew the original version of the Bill and introduced the revised version (titled the "Data Protection and Digital Information Bill Version 2"). The recent changes were described by the Government as "expected o unlock £4.7bn in savings for the UK economy over the next 10 years". However, there is, ultimately, very little that has changed from the original version of the Bill. The key substantive changes are:

- **legitimate interests:** The revised Bill includes examples of processing that may be necessary for a legitimate interest including processing for direct marketing purposes, intra-group transmission of personal data for administrative purposes, and to ensure the security of IT systems. However, controllers must still weigh its legitimate interests in processing for these purposes against the rights and freedoms of the data subjects
- **accountability:** The requirement to keep records of processing, to appoint a senior responsible individual (the replacement to data protection officers) and to carry out a data protection impact assessment will now broadly depend on whether the processing poses a high risk to rights and freedoms of individuals. The ICO will maintain a list of the types of processing which it considers to be high risk to inform these business decisions
- **research exemption:** The revised Bill clarifies that the exemption for processing for research purposes also applies to commercial, privately-funded research as long as it can be reasonably described as scientific
- **automated decision-making:** The Bill clarifies when there is meaningful human involvement in any decision (and therefore when the automated decision-making rules do not apply). The Secretary of State may also pass secondary legislation clarifying what "meaningful human involvement" means
- **data transfers:** The Bill includes transitional provisions to ensure that transfers made under old UK GDPR arrangements but after the new transfer rules in the Bill come into force are permitted subject to certain conditions.

The next stage for the Bill is the second reading in Parliament – the date of which is yet to be announced.

Why is this important?

The Bill represents the fork in the road as the UK breaks away from the EU framework and establishes a model that reflects its own drivers and concerns. However, for the most part, the new regime will still be very similar to the EU GDPR as too great a departure would threaten the UK's EU adequacy (up for review in 2025). Large businesses that operate across the EU and the UK must soon decide how they go forward: adopt a single legal framework across the business that meets the stricter EU threshold or adopt a dual-track system to take advantage of the reduced compliance burden in the UK.

Any practical tips?

Businesses should remind themselves of the key positions in the original version of the Bill and resume any work they had put on hold on understanding how the new law may affect processes and contracts. Either way, keeping track of the passage of this important Bill through Parliament is clearly a good idea.

ICO publishes new guidance on international transfers

The question

What do businesses need to know about the Information Commissioner's Office's (ICO) new guidance on international transfers?

The key takeaway

The ICO has released new guidance regarding international transfers, including how to carry out Transfer Risk Assessments (TRAs). The guidance, according to the ICO, seeks to clarify "an alternative approach to the one put forward by the European Data Protection Board" (EDPB).

The background

Under the UK GDPR, personal data cannot be transferred to non-adequate jurisdictions unless a specific exemption applies or an Article 46 transfer mechanism is established. The Schrems II judgment confirmed that before a company can rely on an Article 46 transfer mechanism to make a restricted transfer, it must conduct a risk assessment.

The development

On 17 November 2022, the ICO published an update to its guidance on international transfers which includes further explanation on:

- when the UK GDPR applies to transfers of data
- what constitutes a restricted transfer
- the countries covered by UK adequacy regulations
- the safeguards in Article 46 of the UK GDPR
- the exceptions to putting in place these safeguards, and
- carrying out TRAs.

The guidance also incorporates worked examples reflecting a wider variety of scenarios, clearly taking on board the fact that many companies have complicated transfer arrangements.

The most significant addition to the guidance is the section on TRAs. The ICO has developed an alternative, more streamlined approach compared to that of the EDPB which applies in respect of transfers under the EU GDPR.

The EDPB approach requires data exporters to compare the laws and practices of the importing country with the laws and practices of the exporting country to assess the risks to data subject rights, including considering safeguards regarding third party access. The ICO's approach, however, focuses on whether there is any increase in the risk to people's privacy and other human rights compared with the risk if the information remains in the UK. The ICO has also developed a "TRA Tool" – a template document that provides guidance on how to carry out a TRA.

The ICO recognises that many businesses are subject to both the EU and UK regimes. Therefore, they have made clear that they are happy for organisations exporting data from the UK to carry out an assessment that meets either the ICO's approach or the EDPB's approach.

The ICO is going to release guidance on how to use the transfer clauses it has previously produced (ie the International Data Transfer Agreement and the Addendum). The ICO is also considering including worked examples into the TRA guidance to show how the TRA Tool can work in practice.

Why is this important?

The new guidance shows that the ICO wishes to be pragmatic and reduce the burden of the EU's arguably complex risk assessment on businesses. The ICO's own assessment is lighter and more risk-focused. However, it recognises that where companies need to comply with both, they should follow the EDPB's stricter approach to ensure that they are covered.

Any practical tips?

Data transfers remain a hot topic for the regulators. Organisations that rely on data transfers within their business activities should consider if there are ways to restructure their transfers to minimise risk and to take advantage of the ICO's pragmatic approach where, for the most part, compliance with the EU regime is likely to be sufficient in respect of the UK regime. The worked examples provided by the ICO should be particularly useful given how complicated transfer arrangements can become and it would be worth comparing these to your existing transfer framework. Above all, perhaps, the ICO's guidance is a good reminder of the need to carry out TRAs. The ICO's new TRA Tool is helpful in this respect, as it is a user-friendly template which takes you through a series of questions and connected guidance.

DATA

UK's first adequacy decision since leaving EU permits data transfers to South Korea

The question

What is the impact of the UK-South Korean data transfer deal on businesses?

The key takeaway

The UK government has passed legislation which allows personal data transfers between the UK and the Republic of Korea (ROK) without the requirement for additional safeguards. This is the UK's first adequacy decision since leaving the EU.

The background

As a result of leaving the EU, the UK and EU data protection regimes have diverged. However, provisional arrangements following Brexit mean that the countries in the EEA and all countries covered by the EU's adequacy decisions pre-Brexit are also considered adequate for the purposes of the UK GDPR.

The EU passed an adequacy decision in respect of the ROK in December 2021 which does not apply to the UK GDPR. Therefore, for the purposes of the UK GDPR, the ROK was not an adequate country and parties intending to transfer data to the ROK would have to complete a transfer risk assessment and put in place safeguards to protect data.

The development

The UK government has now finalised the Data Protection (Adequacy) (Republic of Korea) Regulations 2022 (SI 2022/1213) (the Regulations) which specify the ROK as an adequate country for the purposes of data transfers under the UK GDPR.

The effect of this adequacy decision is that transfers to the ROK (which are subject to the Korean Personal Information Protection Act) no longer require a transfer risk assessment or that safeguards be in place, most commonly standard contractual clauses between sender and recipient or binding corporate rules. The UK government estimates that removing these requirements would cut administrative and financial burdens for UK businesses by £11m a year.

Why is this important?

This is the first adequacy decision made by the UK independently since leaving the EU and would allow for seamless data transfers to the ROK. It is also broader than the EU's adequacy arrangement with the ROK and allows for the transfer of personal data related to credit information. The UK Government has earmarked other countries for adequacy decisions in the future including Australia, India, Singapore and the USA.

Any practical tips?

Organisations currently transferring data to the ROK should assess the impact of this decision on their present arrangements. Standard contractual clauses and binding corporate rules are typically drafted to apply to "restricted transfers" only. Transfers to the ROK are no longer considered a "restricted transfer", so such arrangements are no longer necessary. It would be worth revisiting contracts involving data transfers with entities in the ROK at the relevant time to ensure these are brought up to speed with this change in approach.

DATA

ICO to publish names of organisations it investigates

The question

How effective will the Information Commissioner's Office's (ICO) new approach to transparency be in driving compliance with UK data regulation?

The key takeaway

The UK's data protection authority, the ICO has started publicising data sets and naming organisations that have been subject to reprimands, complaints and concerns. Given the growing importance of consumer trust in any organisation's use of personal data, the threat of publicity may prove to be a strong weapon in the ICO's armoury in improving levels of data compliance.

The background

Previously the ICO had ensured that its dealings with organisations were kept confidential, which helped to facilitate early and open reporting. In a shake-up to current operations, the ICO's Communicating Regulatory and Enforcement Activity Policy has stated that it will now publish any reprimands, complaints or concerns issued to an organisation if it "will help promote good practice" or "deter non-compliance". Currently similar data is not usually published by EU data protection authorities, which suggests that organisations regulated by the ICO will face additional challenges in comparison. In an attempt to increase the levels of good practice, the ICO hopes this revised approach will also reduce its workload following pending data protection reforms.

The development

The information which the ICO is now publicising covers the following:

- reprimands: Rather than imposing a fine for non-compliance with data protection law, the ICO may issue an organisation with a letter stating that it believes that the relevant organisation has exhibited non-compliant behaviour, providing a list of reasons and any suggested actions. Reprimands are used in cases in which the infringement is not serious enough to justify a fine or a specific action. The ICO will now publish all reprimands, including those issued from January 2022 onwards to encourage good practice among public and private organisations. However, the ICO reserves the right to not publish a reprimand for matters which could affect national security or other ongoing investigations
- complaints and concerns: The ICO is also now publishing data sets on complaints and concerns which includes a variety of information such as civil and cyber investigations, self-reported personal data breaches and data protection complaints raised by members of the public. The data is published in a reusable format, and although it contains considerably less detail than reprimands, it does include the names of organisations even where no infringement has been found. This is likely to be useful for the purposes of due diligence, allowing other companies to get a clearer idea of the level of dispute frequency associated with each organisation.

Why is this important?

UK organisations will no longer be afforded the levels of anonymity they had previously enjoyed. The ICO's stringent approach to transparency may become a cause for concern, particularly amongst organisations that carry large amounts of consumer data where breaches are more likely.

Any practical tips?

Negative publicity is a powerful regulatory tool. Indeed, it is the primary enforcement stick used by many regulators, such as the Advertising Standards Authority. If the ICO starts wielding this stick effectively, thereby raising public awareness of those organisations who are not fully engaging with data regulatory compliance, this will be a further item to take very seriously on the data risk list.

DATA

EU lawmakers to legislate on online political advertising

The question

What impact will the EU's new rules on political advertising have on online platforms?

The key takeaway

The European Parliament has adopted its proposal on legislation intended to tackle disinformation and promote transparency in online political advertising. There are a range of requirements on advertising publishers (which would include online platforms) and further requirements on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). The proposed law is intended to work alongside the Digital Services Act (DSA).

The background

In its 2018 Communication, "Tackling online disinformation: a European Approach", the European Commission outlined its views and objectives around raising public awareness about online disinformation. This was then followed up by a Code of Practice on disinformation and a Commission Action Plan against disinformation, both in 2018. Since then, the Commission has been working with stakeholders to encourage transparency in the context of political advertising.

On 25 November 2021, as part of the European Democracy Action Plan, the European Commission presented its proposal for specific legislation to regulate online political advertising (the Proposal).

The development

Most recently, the European Parliament has established its position on the Proposal and has entered into negotiations with the Council on the text. Key aspects of the Proposal (as currently adopted by the European Parliament) are:

- online platforms (as political advertising publishers) must include certain information regarding the advertisement in a transparency notice. This includes details of the advertising sponsor, period of advertising, amounts spent for the advertising, the relevant election, whether the advertisement has been suspended, and if individuals have been targeted for that advertisement
- online platforms must put in place processes to allow individuals to notify them if an advertisement does not meet the requirements under this proposed law
- VLOPs and VLOSEs are required to make the transparency notices available and updated in real time through the repositories required under the DSA, and
- VLOPs and VLOSEs must assess the systemic risks posed by their political advertising services in the context of their risk assessments under the DSA and establish proportionate mitigation measures to address those risks.

The Proposal also supplements the GDPR by including specific requirements when processing personal data for political advertising (the Article 12 Requirements):

- when using targeting techniques to provide political advertising services that involve processing non-special category data, the data controller (which may be the online platform) must comply with additional requirements concerning such techniques, and
- online platforms are not allowed to selectively deliver political advertising based on processing sensitive personal data.

If it suspects non-compliance with the Article 12 Requirements, the EDPB may initiate an investigation against VLOPS or VLOSEs. It may also order the VLOP or VLOSE not to provide advertising services to that particular sponsor for 15 days.

In the Proposal, fines for general non-compliance are to be determined by national authorities. However, it is worth noting that the Council's earlier proposal had set out fines of as high as 4% of the annual worldwide turnover of the provider of political advertising services in the preceding financial year, save for breach of the Article 12 Requirements where the fine shall be in line with the GDPR.

The draft legislation is expected to be approved by the European Parliament and Council and finally adopted by Q3 2023. It would then enter into force on the 20th day following publication in the Official Journal of the European Union.

Why is this important?

There is increasing pressure on online platforms to tackle fake news and outside actors interfering with political processes, most recently seen by Twitter being publicly censured for failing to report its efforts to tackle disinformation under the 2018 Code of Practice on Disinformation. The potential enforcement actions under the Proposal are also significant. For example, banning a platform from providing services to a particular sponsor for 15 days could have a significant impact at what might be a crucial time in politics.

Any practical tips?

Online platforms which are already gearing up for compliance with the DSA would do well to also consider the potential requirements under the Proposal, especially as many of the requirements are intended to supplement those of the DSA. One of the keys to compliance generally under the DSA is transparency and this is clearly echoed in the Proposal. It is also worth keeping an eye on the progress of the Proposal through the legislative process and whether the levels on the administrative fines are retained in the final version.

"There are a range of requirements on advertising publishers (which would include online platforms) and further requirements on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)."

ICO publishes guidance on compliance of game design with the Children's Code

The question

What steps can game designers take to ensure their games comply with the Children's Code?

The key takeaway

You must regularly assess whether under-18s are likely to play your games and be sufficiently certain on the range of players' ages. If children are likely to play, even if the game is not targeted to them, you should consider whether your data processing and privacy settings can sufficiently safeguard their interests.

The background

The Data Protection Act 2018 included provisions to protect and safeguard children when they use the internet. The Information Commissioner's Office (ICO), as the regulator, was tasked with producing guidance for organisations offering online services that children may be likely to access to set the standards for digital privacy and data processing.

The Children's Code (previously called the Age Appropriate Design Code) (the Code) fulfils this mandate. It establishes 15 standards of "age-appropriate design" with the aim of creating an open, transparent and safe online experience for young users. The Code entered into full force on 2 September 2021.

The Code applies to "information society services likely to be accessed by children". In practice, this means the Code extends to search engines, social media platforms, online marketplaces, online games and most other for-profit online services that are used by under-18s.

The development

The ICO conducted a focused audit of the gaming sector to assess how the Code is being applied. Following this exercise, the ICO has published the following recommendations for game designers to ensure the Code is complied with:

Understand the risks for your games

- Assess and document the potential for games that you design to appeal to under-18s. The ICO warns that even if a game is not intended for children, this does not mean they will not play it.
- Continue to conduct risk assessments after the game has been published. It should be an ongoing process to detect new risks or unexpected age groups of players once a game has launched.
- Engage with external stakeholders, including children, when conducting risk assessments. You could consult existing players and relevant children's rights groups, or launch a public consultation.
- Randomised rewards, such as loot boxes, should be a particular focus in assessments. In July 2022, the UK Government's call for evidence found "robust evidence" for a potential association between loot boxes and problem gambling behaviours.
- Once you are clear on the risks, consider if you need to tailor in-game content or data processing.

Ascertain and be assured of players' ages

- Consider how to identify under 18's and determine their age with sufficient certainty.
- Informed by your risk assessments, implement suitable age assurance tools across your full portfolio of games, stores or platforms. The ICO says this should be done as quickly as possible.
- Discourage and prevent players from lying about their age. The ICO suggests one method of allowing access to a data-free core of the game until parental consent is confirmed. Alternatively, the game could have a cooldown period to prevent players returning to provide a different birthdate in a specified time frame.

Be transparent with players' data privacy

- Communicate privacy information in ways that are appropriate for different player age ranges. The ICO suggests having age-appropriate video explanations, "mission-style" storylines or in-game messages.
- The ICO also suggests potentially displaying the information according to gaming ability (eg novice, intermediate and expert), rather than age.

Take care with data processing and profiling

- The default option for all optional uses of personal data must be turned off unless and until valid consent is obtained from the player (or their parent or guardian for players under 13). This includes personalised product recommendations and offers.
- Clearly separate the opt-in consent for marketing from accepting the Terms of Service and Privacy Policy. Otherwise players may think they have no choice but to consent to marketing, which would breach the transparency principle.
- Encourage children to ask a trusted adult for help and only accept profiling if they understand how it uses their personal data. Profiling for marketing purposes must be turned off by default.
- Ensure any third-party advertising in-game is only showing age-appropriate content. If the game has community servers, control and monitor product placement and advertisements within those servers.

DATA

Consider utilising parental controls and high privacy settings

- Consider the option for real-time alerts for parents or guardians. For example, if their child tries to access "riskier" in-game content or if they encounter something inappropriate. If such tools are used, the child should be notified in an age-appropriate way.
- Allow players to control who contacts them. Turn off voice chat functionality by default for young users. Allow them to permanently turn on "do not disturb" mode and prevent communications from all other players. Communications could also be limited to only come from other young users, combined with measures to scope out adult players posing as under-18s.
- Allow players to control what personal data is visible to others. The ICO gives the example of allowing players to hide their username so they cannot be searched for.
- When players try to alter privacy settings, have age-appropriate messaging before allowing the change to take effect. Settings could also be "gamified" to match the in-game theme to maximise young player engagement. The ICO says the messaging should be specific to each individual privacy setting and informative of the risks associated with lowering that particular setting.

Use nudges to support your compliance

- Use positive nudges to promote children's best interests. The ICO recommends defaulting and nudging towards high privacy settings, use of parental controls and taking regular breaks by including checkpoints or natural breaks in gameplay.
- The ICO strongly warns against using nudges to encourage poor decision making. There should be risk assessments for the use of time-limited offers on items which are targeted at young players. Instead, use neutral designs for "purchase" buttons so players feel able to change their minds before proceeding. Consider allowing reasonable cooling-off periods for refunds.
- Monitor player behaviours and click-throughs to spot any unintended nudging effects, especially in relation to privacy settings.
- Be careful with social media marketing and promotions which may require children to create social media accounts to unlock rewards. Be mindful of the age restrictions of such social media platforms relative to your players' ages.

Why is this important?

The ICO can take enforcement action against organisations that do not comply with the Code. It has tools such as assessment notices, warnings and orders to stop processing data. For the most serious of breaches, the ICO can impose fines of up to £17.5m or 4% of an organisation's annual worldwide turnover, whichever is greater.

The Online Safety Bill, a new legislative regime to protect children and adults online, is currently being debated in Parliament. The strength of safeguards for children accessing the internet is a hot topic and will be at the forefront of the ICO's mind.

Any practical tips?

Following the ICO's guidance, we recommend that game designers:

- clearly and comprehensively document the process and outcome of risk assessments, engagement with stakeholders and processing and privacy decisions. A data protection impact assessment should set out your assessment of whether children are likely to access the games, such players' ages and steps taken to comply with the Code
- consult the ICO's age-appropriate design resources which contains worked examples of age-appropriate messaging
- evaluate your existing age-assurance tools across all services. Consider if they can ascertain age with sufficient certainty and discourage false declarations of birthdates. If you do not already have these tools in place, they should be implemented as a priority
- consider running player research or consulting with children's rights groups to identify communication styles and tones that are most effective at communicating privacy and data protection issues to different age ranges.

Survey how many young users are engaging with your higher privacy settings. Think about "gamifying" or aligning these settings with the in-game theme to maximise their appeal.

EDPB's Cookie Banner Taskforce publishes report on bad cookie practices

The question

What pitfalls should website providers avoid when it comes to obtaining user consent for cookies?

The key takeaway

Cookies must be consented to and such consent must be freely given, informed and by affirmative action. Consent will not be valid if the cookie banner creates the impression that the user has no other choice than to accept (eg by hiding or not including reject options), or if the user was pushed into accepting them by default.

The background

The European Privacy and Electronic Communications Directive 2002/58/EC (e-Privacy Directive) has been transposed into UK law by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). PECR sits alongside the existing data protection requirements of the UK GDPR and the Data Protection Act 2018, but applies regardless of whether personal data is processed. PECR specifies certain requirements for electronic communications and user privacy, including the use of cookies.

Cookies are text files which a website provider, or similar online service, can "implant" onto the user's "terminal equipment" (eg a smartphone, tablet or laptop) when they access the website. This creates a unique ID which can be used to track web browsing patterns and identify a user's preferences. PECR provides that users must consent to the use of cookies unless they are "strictly necessary" for use of the website. Consent in this context, must be freely given, informed and by a clear statement or action.

In September 2021 the European Data Privacy Board (EDPB), an independent body responsible for the application of EU data protection rules, created the Cookie Banner Taskforce (the Taskforce) after receiving 422 complaints from non-profit organisation NOYB, alleging non-compliance with cookie banner requirements.

The development

On 18 January 2023, the EDPB adopted the Taskforce's report which condemned the following bad practices with respect to the use of cookies:

- not providing an option to reject cookies
- using pre-ticked boxes to consent to cookies
- hiding the "refuse/continue without accepting" option within a block of text so that it is not easy to identify
- placing "reject" options outside of the cookie banner
- using deceptive button colours or contrasts such that any option besides accepting cookies is unreadable to the user (eg the reject button blending into the background of the banner)
- not including the option to reject cookies at the first level of the banner, leading the user to believe their only option is to accept
- miscategorising non-essential cookies (eg the cookies used for the purpose of ad personalisation) as "essential" or "strictly necessary" for the use of the website, and
- not having an easy mechanism by which users can withdraw their consent at any time.

The Taskforce also found that where a data controller failed to obtain valid consent to collect personal data through cookies, the processing of that data would be in breach of the GDPR.

Why is this important?

The flood of complaints from NYOB shows that cookie banner non-compliance very much remains a live issue and the establishment of the Taskforce, directly because of those complaints, means that this topic remains high on the regulatory radar. It goes without saying that the time and cost of getting cookie banners right is minimal compared to the potential sanctions for non-compliance, for which the ICO can impose a fine of up to £500,000.

Any practical tips?

Given the Taskforce's guidance, it follows that the following are to be recommended:

- Making sure that any options besides "accept" are visibly clear and accessible to the user.
- Ensuring that no options are pre-ticked.
- Having a clear mechanism for users to withdraw their consent to cookies. The Taskforce was hesitant to mandate a particular withdrawal method for all websites, but it suggested the use of a small, permanent icon on each webpage to allow users to review and amend their privacy settings.
- Regularly assessing whether cookies used on websites are truly "essential" and be prepared to justify the classification. Authorities have access to tools which can list cookies placed on a website, but these tools will not categorise as "essential" or "non-essential". The Taskforce stated the evolving features of cookies makes it hard to develop a stable list of universally accepted "essential" cookies.

"Cookies must be consented to and such consent must be freely given, informed and by affirmative action."

The Digital Markets Act and the Digital Services Act: Recap and latest updates

The question

What are the latest updates to the Digital Markets Act (DMA) and Digital Services Act (DSA)? What has the journey looked like so far?

The background

On 15 December 2020, the EU Commission published draft proposals for its digital services package, made up of two regulations, the DMA and the DSA. Both pieces of legislation intend to regulate the responsibilities of digital platforms and service providers, making them safer and more open to innovation and competition.

In July 2022, the European Parliament formally adopted these regulations, and the official texts have been published in the Official Journal of the European Union (OJEU). For further details see our Autumn 2022 Snapshot here.

The Digital Markets Act

1 November 2022	DMA entered into force	Most of the provisions apply from 2 May 2023. After that, within two months and at the latest by 3 July 2023, potential gatekeepers will have to notify their core platform services to the Commission if they meet the thresholds established by the DMA. Once the Commission has received the complete notification, it will have 45 working days to make an assessment as to whether the undertaking in question meets the thresholds and to designate them as gatekeepers. For the latest possible submission, this would be by 6 September 2023. Following their designation, gatekeepers will have six months to comply with the requirements in the DMA, at the latest by 6 March 2024.
2 November 2022	Gatekeeper notification forms	Article 3 sets out the qualitative and quantitative thresholds for a digital business to be considered a gatekeeper. It specifies that gatekeepers would have an annual EU turnover above €7.5bn ($7.4bn), or an average market capitalisation of least €75bn in the past year. They would also provide a core platform service with at least 45m monthly EU end users, and at least 10,000 yearly EU business users. Big Tech companies are likely to be designated as gatekeepers under the DMA.
5 December 2022	Self-preferencing workshop	With so much to achieve in such a short period of time, the Commission has been reaching out to the Tech sector via a series of workshops. The first of those workshops, on 5 December 2022, dealt with the prohibition on self-preferencing in Article 6(5) DMA and focused on the interpretation of the provision as well as possible solutions to ensure compliance with it in practice.
9 December 2022	The Commission launches a public consultation on the implementation of the DMA	Large digital gatekeepers will have to submit detailed information to the European Commission on each of their distinct platform services that will fall under the DMA. The European Commission sought feedback by 6 January 2023 on the detailed provisions that will implement the DMA, setting out what information each gatekeeper will have to provide and in what format to trigger the obligations under the DMA.
16 January 2023	New DMA directorate in place headed by Alberto Bacchiega	According to the Commission's website, the new department, populated by 32 officials, will work together with enforcers from the commission's digital division to rein in Big Tech companies with new rules regulating self-preferencing, interoperability or data processing under the DMA. The division will also run standard antitrust investigations into the digital sector.

27 February 2023	Interoperability workshop	Messaging platforms attend European Commission workshop to discuss implementation of interoperability between messaging services.
27 October 2022	The DSA was published in the OJEU	Regulation (EU) 2022/2065 (DSA) was published in the OJEU, entered into force on 16 November 2022 and applies from 17 February 2024. Article 92 of the DSA provides that for very large online platforms (VLOPs) i.e. those with more than 45m monthly active EU users, and very large online search engines (VLOSEs) (designated as such by the European Commission), the regulations will apply from four months after they have been notified as being designated as such by the European Commission, even where this was earlier than 17 February 2024. Platforms were required to submit their user numbers by 17 February 2023. On 19 December 2022, Thierry Breton announced that the regulator will designate the VLOPs by May 2023 – four months ahead of the stated enforcement deadline of 1 September. 1 May is a holiday for commission staff, so if they follow Breton's prescription of "no later than" 1 September, the commission will most likely designate the VLOPs by 28 April 2023.
22 November 2022	The European Centre for Algorithmic Transparency	The European Commission announced the setting up the European Centre for Algorithmic Transparency (ECAT), expected to be fully operational in the first quarter of 2023, following the entry into force of the DSA. The DSA calls for increased oversight of the algorithmic systems used by very large online platforms and search engines. This includes how they moderate content and propose information to their users. The new Centre will support the Commission in assessing whether the functioning of such algorithms is in line with the risk management obligations under the DSA.
22 December 2022	European Commission call for feedback on regulation for supervisory fees under the EU DSA	The European Commission launched a call for feedback on the delegated regulation to specify the criteria to be used when calculating the supervisory fees provided for in Article 43 of the DSA. The regulation is intended to supplement the DSA with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of VLOPs and VLOSEs. The request for feedback closed on 19 January 2023.
17 February 2023	Obligation to publish information on average monthly active recipients	All "online platforms" and "online search engines" required to publish information on their average monthly active recipients by 17 February 2023. Guidance on identification and counting of active recipients was published on 1 February 2023.
17 February 2023	The European Commission published a draft of its implementing decision	The DSA gives the Commission the power to create laws called "implementing acts", which implement specific parts of the regulation. The draft decision covers the EU executive's investigatory and enforcement powers, platforms' right of reply to enforcement actions and their right to access commission files in disputes. The Commission is receiving feedback until midnight on 16 March 2023.

Why is it important?

The introduction of the DMA and DSA is indicative of the growing trend towards increased regulation of major online platforms. The implementation of these legislative initiatives will result in significant changes to online platforms, including increased costs, stricter regulatory scrutiny, and more extensive obligations. A failure to comply with the DMA and DSA can result in substantial penalties, amounting to 10% and 6% of the company's total worldwide annual turnover respectively. In cases of repeated infringements, these fines can be raised to up to 20%.

Any practical tips?

As the implementation phase of both the DMA and DSA is now underway, digital platforms and service providers operating in the EU are strongly advised to continue with their DSA and DMA compliance efforts and ensure that they have a comprehensive understanding of the stages involved leading up to the deadlines to avoid potential penalties.

"The Online Safety Bill requires digital platforms which host user-generated content to comply with requirements aimed at reducing harmful content."

Online Safety Bill: Latest amendments increase focus on children safety

The question

What is the focus of the latest round of amendments proposed to the Online Safety Bill and how will these impact online platforms?

The key takeaway

The Online Safety Bill requires digital platforms which host user-generated content to comply with requirements aimed at reducing harmful content. Sanctions for non-compliance are proposed to be fines of up to 10% of the global turnover of the company and a jail sentence of up to two years for senior managers.

The background

The Online Safety Bill was introduced in the House of Commons on 17 March 2022 and the most recent, second reading of the Bill took place in the House of Lords on 3 February 2023. The Bill proposes better regulation for search engines and firms that host user-generated content and aims to reduce the amount of online content deemed inappropriate for young users and that ministers believe causes serious harm to their safety. This includes content promoting self-harm, eating disorders, and those that depict sexual violence as well as child sexual abuse material, revenge pornography, selling illegal drugs or weapons, and terrorism.

The development

The measures, put forward by nearly 50 Conservative MPs and backed by the Labour Party, will impose a duty to ensure children's online safety by mitigating and managing the risks and impact of harm to children online.

Tech firms within scope are required to introduce and enforce strict age limits and publish risk assessments detailing threats their services may encounter regarding inappropriate content and keeping children safe. Ofcom will have the power to issue enforcement notices to senior managers of tech platforms who are found to have breached their child safety duties by allowing exposure to age-restricted or illegal content. Online providers must co-operate fully with an Ofcom investigation into whether their service has failed to comply with the requirements. Ofcom will only be able to prosecute senior managers if they fail to cooperate with an investigation. Failure to comply with their duties may result in fines of up to 10% of the company's global turnover and a maximum prison sentence of up to two years.

The Bill is still making its way through the House of Lords and is at the committee stage. It is expected to receive Royal Assent this summer.

Why is this important?

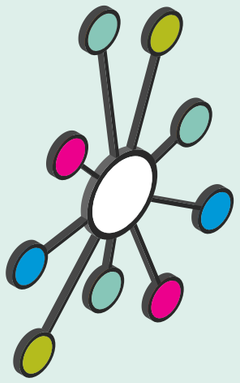
The latest amendments place the burden on tech companies to proactively assess risks of harm to their users and establish systems and processes to keep them safer online, rather than on Ofcom moderating individual pieces of content. Its scope will likely affect not only the obvious "Big Tech" social media platforms and search engines, but also thousands of smaller platforms, including messaging services, websites, platforms and online forums where information sharing, advertising and user interaction takes place.

Any practical tips?

Considering the extent of the newly proposed sanctions, organisations must fully consider whether they come within the scope of the Bill, keeping in mind that most companies that which provide online content are likely to be caught by its provisions. Beyond keeping a close eye on the passage of the Bill through Parliament, practical steps businesses should consider include:

- undertaking a risk assessment of your operations and websites, and reviewing complaints procedures and terms of service
- considering how improvements can be made to your systems for content monitoring, keeping in mind the importance of balancing freedom of expression with the need to protect users from harm
- considering setting up internal structures for identifying and reporting potential harm to children to the National Crime Agency, and
- keeping a watch on Ofcom's activities, as it consults on various aspects of the Bill and prepares to regulate on it.

DCMS publishes new Code of Practice for app developers and app store operators



The question

What do app developers and app store operators need to do to comply with the new Code of Practice published by the Department for Digital, Culture, Media and Sport (DCMS)?

The key takeaway

The DCMS has published a new Code of Practice for app store operators and app developers (the Code). The Code sets out eight voluntary principles which aim to protect the security and privacy of app users. While the Code itself is voluntary (ie there is no legal requirement for app developers and app store operators to comply with it), the DCMS anticipates that compliance with the Code may become an expectation of users in a competitive app store and app downloads market.

The background

The DCMS introduced the new Code to better protect app users from online threats given the integral role that apps now play in the work and personal lives of users. The DCMS undertook a review of the app store ecosystem between December 2020 and March 2022 and found that users could still access poorly developed and malicious apps and that some developers were not following best practice. In May 2022, the DCMS issued a public consultation seeking the views of organisations and individuals on whether a code of practice would be effective and which principles should be included in a code of practice if one were introduced. The review and subsequent activity is part of a broader programme under the UK Government's National Cyber Strategy.

The development

The Code sets out eight principles and applies to three groups:

1. App Store Operators: Individuals and organisations responsible for running app stores, with the ability to vet and add or remove apps.
2. App Developers: Individuals and organisations which create or maintain the apps distributed through an app store.
3. Platform Developers: Individuals or organisations responsible for producing the operating system and interface of a device.

Note that the "App Developers" category will include all organisations that produce apps. Organisations which produce apps, run an app store and provide an operating system on which apps can run can fall into all three categories.

The eight principles contained in the Code are summarised below:

- Principles 1 and 2: These require app stores to set out a clear security policy to developers, vet apps that are submitted to them, and remove any app within 48 hours of discovering that it is malicious. Developers are required to use industry-standard encryption within their apps, provide a means for users to delete personal data gathered by the app, and ensure that the permissions requested by an app are only those required to help the app function (and, in any case, ensure that an app still functions even if the user disables optional functionalities and permissions).
- Principle 3: This principle requires app developers to introduce a vulnerability disclosure process for their apps, and for app store operators to ensure that all apps on their platform have a vulnerability disclosure process, and that their app stores themselves have a vulnerability disclosure process.
- Principles 4 and 5: These require that apps are kept updated to protect users and that security information is provided to users in an accessible fashion. Specifically, developers are required to release updates to fix vulnerabilities in their apps and provide app stores with clear information as to the permissions (eg use of the device's camera) and personal data used by an app. App stores are required to prompt users to update apps when an update is released and display relevant security information about an app to users.
- Principles 6 and 7: These require a degree of communication and openness between app stores and developers. App store operators are required to signpost developers to the Code, publicise any changes to their developer policies and provide clear feedback to developers when they either remove an app or reject an app for publication on their store.
- Principle 8: This principle sets out obligations for app stores and developers where a personal data breach occurs. Where either party becomes aware of a personal data breach involving an app, they must notify stakeholders. In addition to existing obligations under data protection law, developers must signpost users on how to protect themselves and app stores must consider whether they should continue to distribute the app.

Why is this important?

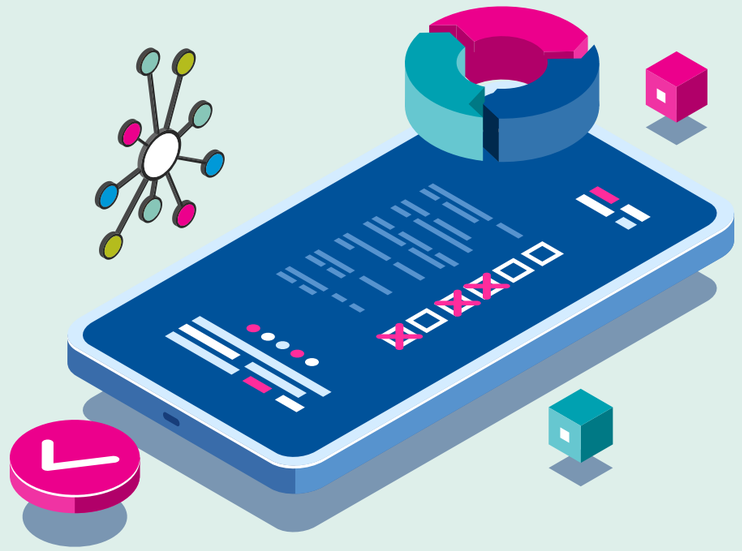
While the Code, in its current state, is voluntary, the follow-up to the public consultation states that the Code is intended to be a first step in improving security in app distribution, and that there are further steps that the Government might take forward in the future. As such, the introduction of the Code may set the tone for further regulation and/or intervention in this area.

The DCMS states that, even though the Code is not mandatory, there is likely to be public pressure on developers and app stores to comply with it, and compliance with the Code will become a differentiating factor in a competitive market. The follow-up to the consultation makes reference to the possibility of introducing a certification scheme, which would make it easy for consumers to identify which businesses are complying with the Code and would be likely to increase the pressure on businesses to comply. More generally, complying with the terms of the Code is likely to help ensure that apps and app stores are safer environments for users, and so help to avoid any reputationally-damaging security breaches.

It goes without saying that there will be some pressure from the DCMS and the Government to comply. The DCMS has already said that it will give businesses nine months to comply with the Code and will stage meetings with the major players in the industry to assess how they have begun to change their processes to comply. As the Code is not mandatory, it is not clear what, if any, enforcement measures the DCMS could take against a business refusing to comply with the Code.

Any practical tips?

Given the focus which the regulators, and the wider market, are likely to put on compliance with the Code, it makes sense for app stores, app developers and platform developers alike to get to grips with the applicable principles as quickly as possible. For example, app stores should ensure that they display all the information to users required by the Code (eg security information) and that they have means of communicating the required information to developers (eg reasons for removing an app). They should also review their internal processes to identify whether they can comply with some of the specific requirements under the Code (eg the requirement for app stores to remove any apps identified as malicious within 48 hours of discovering that they are malicious).



New metaverse regulation proposal to be discussed by EU Commission

The question

How does the European Commission (EC) intend to regulate the metaverse?

The key takeaway

As part of the EC's ongoing strategy to make Europe "fit for the digital age", the EC will address metaverse policy later this year. The form of any such metaverse initiative is as yet unknown but, in any event, changes will likely focus on data, technology, and infrastructure. The impact will be far reaching and will likely target large tech companies.

The background

EC President Ursula von der Leyen's 2022 Letter of Intent identified the metaverse as a key new initiative for 2023. Commissioner for the Internal Market Thierry Breton, in his September 2022 statement, identified the metaverse as a "pressing challenge" and that the EC intends to shape from the outset the development of a truly safe and thriving metaverse.

The development

The latest version of the EC's upcoming agenda was published on 6 February 2023 and indicated that the EC will be presenting its initiative on virtual worlds such as the metaverse in the first half of 2023. There are no further details included in this agenda. However, the EC's target areas for policy have been set out in its 2022 briefing on the metaverse:

- **Competition:** Regulators have warned about self-preferencing and dark patterns within the metaverse, or the possibility of "killer acquisitions" (large companies acquiring smaller companies to halt future competition).
- **Data protection:** The GDPR set a new benchmark on data handling, however the scale of the metaverse causes concerns about data handling, marketing and intrusive profiling.
- **Liabilities:** Metaverse content is distributed and replicated across decentralised networks, making liabilities difficult to control.
- **Financial transactions:** Non-fungible tokens (NFTs) are a key foundation of the metaverse, but there is no clear regulation on NFT ownership.
- **Cybersecurity:** Phishing, malware and hacking will remain, and the anonymity behind NFTs may make it difficult to identify perpetrators.
- **Health:** There will be a widespread impact on children, mental and physical health.
- **Accessibility and inclusiveness:** There are concerns of how accessible the metaverse will be for disabled people, or the affordability of becoming part of the metaverse.

Why is this important?

Uncertainty of what the metaverse will look like makes it difficult for regulators to decide how to govern this emerging virtual world. However, one certainty is that the EC is determined to do so. On 4 March 2023, the EC announced that it will shortly set out its policy on metaverse regulation and will begin with a public consultation. Therefore, change in some form is likely over the next few years, whether it be through new initiatives, or through existing legislation being interpreted, or indeed extended, to cover the metaverse. For example, a "Digital Euro Bill" is set to be published in May, which could mean a new central bank digital currency for the metaverse.

Any practical tips?

For businesses with a keen interest in how the metaverse develops, now is the time to influence the EC's approach to its regulation. For example, the EC has launched the Virtual and Augmented Reality Industrial Coalition, bringing together stakeholders from key metaverse technologies to help shape the future of VR and AR in Europe. Particular attention should be given to the issues highlighted in the EC's 2022 briefing, namely: competition, data protection, liabilities, financial transactions, cybersecurity, health, accessibility and inclusiveness.

UK Government sets out regulatory proposals for marketing cryptoassets

The question

What will the Government's proposed exemption to the Financial Promotion Order mean for cryptoasset businesses which are not otherwise authorised persons?

The key takeaway

New legislation creating a bespoke exemption to the restriction on financial promotions at section 21 of the Financial Services and Markets Act 2000 (FSMA) will enable businesses that are registered with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), but are not otherwise authorised persons, to make financial promotions in respect of qualifying cryptoassets.

The background

The Government has set out how it intends to support the growth of crypto businesses, whilst ensuring consumers are able to make informed decisions in the same way that they do when making other high-risk investments.

An approach initially suggested was that if crypto businesses wanted to promote cryptoassets, they would need to be authorised to do so in the same way as they would to promote other high-risk investments. However, this approach was criticised by crypto businesses and stakeholders, who said that this would amount to an effective ban on cryptoasset financial promotions, as authorised persons would not be prepared to approve cryptoasset promotions from unauthorised firms.

The development

In response to these concerns, the Government proposed bringing certain qualifying cryptoassets under the scope of the Financial Services and Markets Act (Financial Promotion) Order 2005. These proposals received broad support and on 1 February 2023, the Government published a policy statement confirming that a bespoke exemption will be introduced in section 21 FSMA for certain financial promotions of qualifying cryptoassets.

Under the exemption, all firms marketing cryptoassets to UK consumers that are FCA registered under the MLRs, but are not otherwise authorised persons, will be able to communicate their own financial promotions for qualifying cryptoassets. Unauthorised cryptoasset businesses will subsequently fall under the financial promotion rules which apply to authorised persons communicating alike promotions. Powers will be conferred on the FCA so that it can create rules which will apply to financial promotions communicated in reliance on the exemption.

Subject to the legislation receiving Parliamentary approval, the four gateways to communicating cryptoasset promotions to UK consumers will be as follows:

1. promotion by an FCA authorised person
2. promotion by an unauthorised person but approved by an FCA authorised person (further legislation creating this gateway is currently with Parliament)
3. promotion by cryptoasset businesses registered under the MLRs with the FCA, and
4. promotion which otherwise complies with the conditions of an exemption in the Financial Promotion Order.

Following the well documented recent volatility throughout crypto markets and the consequential risks faced by consumers, the Government has reduced the period of implementation from six months to four months for the changes come into effect and, once they do, the FCA will publish a final set of rules which are expected to be similar to those that apply to other high-risk investments.

The Government has also said that it is preparing to bring stablecoin under regulation, and that it will also consult on how best to approach unbacked cryptoassets.

Why is this important?

Businesses that want to make financial promotions of qualifying cryptoassets will have the freedom to do so without the need to be authorised. An added benefit of this is that cryptoasset businesses will likely be encouraged to build their businesses within the UK. Consumer protection must remain at the forefront of consideration, and by subjecting unauthorised firms that are making financial promotions via the exemption to the same rules as authorised firms, unauthorised firms will need to meet the same requirements as authorised firms to ensure the protection of consumers.

Any practical tips?

The FCA has stated that it will expect businesses to be ready, willing and organised at the point of their application to make financial promotions of cryptoassets. Once the FCA rules have been published, businesses that intend to make financial promotions of cryptoassets to UK consumers should ensure that they fully understand the rules prior to submitting their application.

CONSUMER

"The EU and UK are taking active steps to combat greenwashing. The EU is aiming to set a standardised environmental methodology through a new directive to regulate environmental claims by businesses."

The new EU Green Claims Directive and the CMA's FMCG review shows greenwashing is firmly in the sights of EU and UK regulators

The question

What do the latest steps against greenwashing by the EU and UK regulators tell us about their appetite for enforcement?

The key takeaway

The EU and UK are taking active steps to combat greenwashing. The EU is aiming to set a standardised environmental methodology through a new directive to regulate environmental claims by businesses. At the same time, the UK's Competition and Markets Authority (CMA) is expanding its investigations into green claims in the fashion industry (Summer 2022) to those in the FMCG sector. Businesses will be under increasing scrutiny to ensure that any environmental claims are accurate and capable of substantiation.

The background

Brands are increasingly looking to environmental claims to make their goods and services more appealing to consumers. This has resulted in a surge in often misleading and/or unsubstantiated green claims.

A study by the EU Commission found that, after assessing 150 claims about products' environmental credentials, 53% of environmental claims provided "vague, misleading or unfounded information". The EU is therefore making it a priority to eradicate greenwashing. In the UK, the cost of living crisis has prompted the CMA to targeting greenwashing across FMCG products (essentials such as toiletries, food, and drink), in respect of which its research shows that up to 91% of all dishwashing items and 100% of toilet products are marketed as "green".

Developments in the EU

The EU is expected to propose new rules by the end of March 2023 to regulate green claims through the Green Claims Directive. This aims to scrutinise green claims from EU businesses through an authorised methodology that meets specific requirements. These claims will be reviewed by an independent verifier against the methodology to ensure they are substantiated. Furthermore, the Directive will require businesses to review and update their claims alongside findings that may impact the validity of the claim. Member States' authorities will regularly check green claims to ensure compliance and are encouraged to impose sanctions on any business that does not take satisfactory remedial action.

Developments in the UK

The CMA is set to review green claims across the FMCG to scrutinise potential breaches of the Green Claims Code and the Consumer Protection from Unfair Trading Regulations 2008. The CMA could use its formal powers against businesses that are found to be greenwashing, including investigations and enforcement action where appropriate against specific companies.

Why is this important?

The EU has taken an authoritative stance by encouraging member states to sanction companies guilty of greenwashing. Sanctions have been effective at encouraging organisations to change environmental communications across their wider groups, as opposed to solely adjusting their communications in the country they were sanctioned in (for example, H&M and Decathlon were sanctioned by Dutch authorities and enacted EU-wide change). The new Directive represents an important step in ensuring environmental claims are substantiated and independently verified across the EU.

Whilst the UK will not be subject to the new Green Claims Directive because of Brexit, the FMCG market review shows the CMA's commitment to combatting greenwashing. As the CMA is on the verge of receiving new direct enforcement powers, via the Digital Markets, Competition and Consumer Bill, we are likely to see an uptick in enforcement action as the CMA flexes its new muscles.

Any practical tips?

Businesses operating in the EU should closely examine the new rules from the Directive and see how their current environmental communications align with the rules. Adjustments may be needed both in relation to claims being made and the methodology for substantiating those claims.

In the UK, all businesses (not just those in fashion or FMCG) should be looking at their claims to ensure they give the CMA no reason to come knocking at their door. Remember that specific, narrow claims are always easier to substantiate than broad green claims, which are almost always found to be misleading when placed under the regulatory spotlight.

CONSUMER

New EU General Product Safety Regulation to offer more safety for online shoppers and vulnerable consumers

The question

How will the proposed General Product Safety Regulation (GPSR) impact the obligations of providers of online marketplaces?

The key takeaway

The proposed GPSR will overhaul the general legal framework around product safety by addressing potential safety issues associated with new technologies sold on the online marketplace. This includes increased obligations on providers of online marketplaces to facilitate communication with consumers regarding concerns they may have surrounding product safety issues as well as giving more power to authorities so they can take swift action in removing dangerous goods from the market place.

The background

On 28 November 2022, the EU Parliament and EU Council agreed to update existing product safety rules relating to non-food consumer products. This political Provisional Agreement was further supported on 24 January 2023 by the Internal Market and Consumer Protection Committee, thus paving the road for a more harmonised system which may be implemented by all EU states across the board.

If the new proposal is agreed by the EU Parliament, the existing General Product Safety Directive would be transmuted into a Regulation. The vote is expected to take place in March 2023. The proposal for the new GPSR targets rules surrounding the safety of non-food consumer products with a particular focus on protecting online shoppers.

The development

The proposed regulation is expected to contribute significant changes to online marketplaces with several provisions under Article 20 of the draft GPSR expected to bolster buyer confidence when purchasing goods online. In summary:

- Providers of an online marketplace must provide a single point of contact which consumers and national surveillance authorities may contact electronically to voice concerns in relation to product safety issues.
- Providers must inform their consumers regarding the available interfaces of communication (eg email, webchat etc).
- Providers must communicate their business' basic information as well as information relating to the products they are selling.
- Providers must use the Safety Gate Portal to communicate with the authorities in relation to issues concerning product safety.
- Providers must cooperate with market surveillance authorities especially where the removal of dangerous products is concerned.
- Providers must take reasonable measures to conduct random checks for dangerous products.
- National authorities will be given the power to disable access to and/or remove dangerous content from online marketplaces without undue delay/ within two working days.

Furthermore, the proposals under Articles 31-35 provide increased buyer protection by solidifying a consumer's right to information and remedies, which seeks to protect vulnerable consumers in particular, such as those with disabilities. These include:

- Providers must clarify information surrounding a consumer's right to repair, replacement, or an adequate refund.
- Consumers will be entitled to file complaints.
- Consumers will be entitled to launch collective actions.

The draft GPSR is now in its final stage and is therefore ready to be debated in March 2023 by the EU Parliament and the EU Council. Once formally agreed, the Regulation will be published in the EU Official Journal and will enter into force. To note, according to Article 47, the GPSR will only apply 18 months following formal agreement, so enforcement is likely to be effective around late 2024.

Why is this important?

Despite being in the draft stage, if approved and enforced, the new GPSR is likely to impose significant legal obligations on providers of online marketplaces which may require operational changes to ensure compliance.

When the General Product Safety Directive was first implemented in 2001, the subsequent amount of buying and selling in the online marketplace was not pre-envisaged. Online sales are notoriously difficult to monitor, which has encouraged the EU regulators to adopt the proposed requirements as a Regulation, thereby increasing cohesive enforcement. Furthermore, although the new rules directly affect EU member states, the EU accounts for 50.4% of all imports in the UK thus allowing UK consumers to benefit from the Regulation vicariously.

Separately, the UK is currently carrying out its own review of applicable product safety legislation which will naturally be influenced by developments in Europe.

Any practical tips?

The GPRS will require significant, long-term changes to online marketplaces, making it important for their operators to start considering its impact now. This includes relatively simple steps like establishing a single point of contact (so there is a clear line of communication between the business, the authorities and consumers) through to more complicated steps such as measures to undertake regular and random safety checks on products and to enable cooperation with national authorities where the safety of a product is questioned. Importantly, consumers must be informed of their rights to repair, refunds and adequate replacement, as well as have the right to file complaints or launch collective actions.

CONSUMER

CONSUMER

Court of Justice of the EU – Amazon may be found liable for marketing third-party counterfeit products

The question

Can online marketplaces be held directly liable for trade mark infringement when marketing counterfeit, third-party products on their online marketplaces?

The key takeaway

The Court of Justice of the European Union (CJEU) has ruled that Amazon may in certain circumstances be held accountable for trade mark infringement for the marketing of third-party counterfeit, red-soled Louboutin shoes on its platform. The issue is now with the Belgian and Luxembourg national courts to decide.

The background

In 2019, Christian Louboutin initiated a claim for trade mark infringement against Amazon in the national courts of Brussels and Luxembourg. The legal action aimed to establish that Amazon is liable for displaying advertisements for third-party counterfeit, red-soled shoes sold through its online marketplace. In June 2022, the Advocate General gave an opinion that features of Amazon's business practices did not support the finding that the sign had been "used" by Amazon for the purposes of establishing trade mark infringement.

The development

Departing from the reasoning in the Advocate General's opinion, the CJEU concluded that Amazon, and any other operator of an online marketplace that utilises a similar sales model, may be held liable for trade mark infringement when marketing counterfeit third-party goods.

The CJEU outlined that the key test for establishing whether Amazon might be in breach was where a "well-informed and reasonably observant user" of the website would establish a link between Amazon's services and the sign at issue. Important factors when determining a connection between the online marketplace's services and the offerings included:

- The online marketplace's logo being used when displaying advertisements, including on those relating to goods offered by third-party sellers.
- Where services (such as shipping the product and handling returns, storage and dealing with customer queries) are offered for the third-party products and its own goods.
- Offerings from the online marketplace and third parties being described as "bestsellers" or "most popular".

Next steps

Now that the CJEU has issued its preliminary ruling, the case has been sent back to the national courts in Belgium and Luxembourg to decide whether Amazon has infringed Louboutin's trade mark.

Why is this important?

The implication of this ruling leaves operators of online marketplaces who utilise a hybrid model (such as Amazon) more vulnerable to being held directly liable for third-party sales of counterfeit products on their platforms. In turn, it will make it easier for brand owners to safeguard their intellectual property rights by allowing them to pursue legal action against the online marketplace itself for trade mark infringement instead of targeting individual counterfeiters.

Any practical tips?

In light of this ruling, online marketplaces should exercise caution in the way that they promote the products sold on their platforms. It is important for them to clearly differentiate between their own product listings and those of third-party vendors, to enable consumers to easily identify the actual seller of the goods.

CONSUMER

UK's new Extended Producer Responsibility regime increases waste packaging responsibilities

The question

How will the Extended Producer Responsibility (EPR) regime alter the way businesses deal with waste packaging?

The key takeaway

The cost to businesses of dealing with waste packaging will increase significantly under EPR. Obligations regarding collecting data on packaging handled and supplied and reporting that data to the Government came into force on 28 February 2023, and will be followed up in 2024 with ongoing reporting requirements along with registration and fee payment obligations and a continuing requirement to purchase Packaging Recycling Notes (PRNs) and Packaging Export Recovery Notes (PERNs).

The background

As part of its Resources and Waste Strategy released in late 2018, the UK Government committed to working towards the objectives of the EU's Circular Economy Package. This involves a series of legislative reforms which include implementing EPR in relation to packaging waste. EPR aims to create an incentive for waste packaging producers to: (i) use less packaging overall and (ii) use packaging that is easier to recycle.

Many retailers and brand owners will likely already be registered as a "producer" under the current Packaging Waste Regulations 2007 system and this position may not change under EPR. However, businesses will need to take stock of how EPR may impact their obligations as a household packaging producer.

The development

One of the main changes under EPR is that the full cost of collecting, sorting, recycling and disposing of household packaging waste will be placed on packaging producers rather than the taxpayer. Currently the UK's waste packaging regime operates on a shared producer responsibility basis and it is estimated that packaging producers pay around just 10% of the cost of dealing with packaging waste. Under EPR, the focus will be on having a single point of compliance within the waste management chain – with the party that has the most influence on packaging choices – and it is envisioned that the cost of compliance for packaging producers will rise from approximately £350m to £1.7bn.

There are two phases to implementing EPR:

5. 2023: The Packaging Waste (Data Reporting) (England) Regulations 2023 (and equivalents for Wales, Scotland and Northern Ireland) (Reporting Regulations) came into force on 28 February 2023. These impose data collection and reporting obligations on packaging producers in the UK. The results of this reporting will feed into calculations for fees that, in turn, will herald the implementation of the second phase.
6. 2024: Fee payment obligations will be introduced (based on calculations facilitated by the requirements under the Reporting Regulations) as well as ongoing data reporting requirements and PRNs and PERNs by producers will be needed.

Next steps

A key step for businesses in evaluating the impact of EPR is determining whether their organisation is caught by the Reporting Regulations and, if so, if it is as a "small" or "large" producer.

Producers who have a turnover of less than £1m annually and/or handle less than 25 tonnes of packaging will not currently have obligations under the Reporting Regulations. Producers who have an annual turnover of £1m to £2m and handle 25-50 tonnes of packaging annually will fall within the definition of "small" producers. "Large" producers are those who have a turnover of more than £2 annually and handle more than 50 tonnes of packaging or packaging materials a year. The Reporting Regulations also confirm that each company in a group of companies will be considered a "small" or "large" producer if the aggregate of the annual turnovers and packaging tonnage thresholds handled by the companies in the group meet the relevant "small" or "large" producer thresholds.

Why is this important?

Small producers (that are not also an online market operator or seller) will only be subject to data collection retention and reporting obligations regarding the type and weight of their waste packaging. Conversely, large producers, aka "fully obligated producers" (that are not also an online market operator or seller) will be subject to more detailed data collection, retention and reporting. They will then also have further fee payment and recycling obligations, discharged via purchasing PRNs or PERNs, as applicable.

Any practical tips?

Organisations which are unsure whether they are caught by EPR can check via an online questionnaire the Government has provided to confirm the roles/responsibilities of organisations: https://www.gov.uk/guidance/check-if-you-need-to-report-packaging-data.

Businesses already registered with a registered compliance scheme under the existing producer responsibility regime should engage with their provider to understand the practicalities of getting ready for EPR, as they will be able to provide operational and practical assistance.

From 1 January 2023, businesses will need to have started collecting and recording the data which EPR requires in order for it (or its compliance scheme) to report at the applicable times.

Business would also do well to start reviewing current packaging practices and considering options in terms of both reducing the amounts of packaging used and whether any aspects of the packaging can be made easier to recycle.

The Department for Environmental, Food and Rural Affairs (DEFRA) is currently developing an EPR digital platform (which should be operational from July 2023) that will allow producers to register and report their data.

Social influencers and gifts: ASA lowers bar for #ad marketing disclosures

The question

Does a social media influencer still need to make an advertising disclosure using #ad when receiving free tickets to an event, even where there is no obligation to post and no contract in place with the relevant sponsor?

The key takeaway

Even if there is no actual obligation to make a post about a gift (here, tickets to Wimbledon), the mere suggestion that the influencer makes a post using a specified hashtag in connection with the gift was enough for the Advertising Standards Authority (ASA) to deem that there was a level of "editorial control" over the post – thereby requiring the need for a #ad marketing disclosure.

The background

Social media influencer and reality TV star Alexandra "Binky" Felstead was invited by Vodafone to attend the prestigious Wimbledon Tennis Championships at the All England Lawn Tennis Club in July 2022. Whilst there was no formal agreement between Felstead and Vodafone, she was given free tickets to the event, accompanied by access to their highly "instagrammable" hospitality suite. This was considered "payment" under the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (the CAP Code). In return, it was hoped that Felstead would utilise this as an opportunity to promote Vodafone on her social media channels. Albeit not a requirement of the free tickets and hospitality access, the PDF provided to Felstead's agent regarding provision of the tickets simply encouraged guests to share their Wimbledon experience using hashtag #FeelTheConnection and tagging @VodafoneUK. Vodafone's Head of Social Media and Content Brand Marketing reiterated that there was no expectation for Felstead to post anything on social media during the day, nor did Vodafone have any approval over what Felstead chose to post. This was confirmed by Felstead's agency. She was not paid by Vodafone nor was she required to post anything on social media.

Felstead subsequently posted an Instagram post, containing three images: herself and husband, Max Darnton, wearing Vodafone lanyards, in front of a wall made of plants and flowers; herself, again wearing a Vodafone lanyard, pointing at the Vodafone logo on the same plant and flower wall; and herself holding a bowl of Wimbledon's iconic strawberries and cream, with the Vodafone lanyard in the background. Felstead also posted an Instagram story, containing two images: a bartender pouring a drink, wearing a Vodafone apron; and Felstead in front of the plant and flower wall, with the Vodafone logo. The first image was tagged with @VodafoneUK and #FeelTheConnection, with a location marker for Wimbledon.

The ASA decision

A complaint was made on the grounds that the Instagram post and story were not clearly identifiable as marketing communications for Vodafone. The ASA agreed and banned Felstead from using the posts again, warning her and Vodafone that any future social media marketing of this nature must be obviously identifiable as such, for example by utilising the hashtag #ad in posts, in a prominent and clear way, so that they comply with the CAP Code.

Why is this important?

Ensuring that social media posts created for the purpose of marketing communications are explicitly identifiable as such is nothing new. The ASA, and indeed the Competition and Markets Authority (CMA), have been banging this drum for years. What is new, however, is the ASA's broad interpretation of "editorial control" which allows it to treat as within its remit any content that previously may have been within the CMA's remit only. The mere suggestion of posting using a specified hashtag (#FeelTheConnection and @VodafoneUK) was enough in this case to bring the content within the classic definition of an advertorial (payment plus editorial control) and therefore bring it within the remit of the ASA. In practice what this means is that influencer gifting no longer occupies a grey area where a #ad disclosure ought to be made but the chances of enforcement action being taken are slim (the CMA is not active on a day-to-day basis enforcing influencer disclosures). It is also a sharp reminder to follow the CMA guidance on this topic, which was published in November 2022 and was the first time the regulators had expressly provided guidance indicating that even in gifting situations, a #ad (rather than #gifted or other kind of disclosure) should be used – see our Winter 2023 Snapshot on the CMA's guidance on influencer marketing.

Any practical tips?

Influencers and brands alike must err on the side of caution when producing social media marketing content. The ASA's "An Influencer's Guide to making clear that ads are ads" provides comprehensive advice for social media influencers to ensure any posts with the purpose of promoting a brand or product are clearly identifiable.

In short, influencers should ensure that the hashtag #ad is clear and prominent within any social media post which is intended as a marketing communication – and to look to do this even where that post relates to a pure gift (ie there is no obligation on the influencer to make a post about it). This ruling reminds brands and social influencers alike of the need to take a very cautious approach to advertising disclosures, with the safest course being to use #ad in almost every promotional scenario.

"Even if there is no actual obligation to make a post about a gift (here, tickets to Wimbledon), the mere suggestion that the influencer makes a post using a specified hashtag in connection with the gift was enough for the Advertising Standards Authority (ASA) to deem that there was a level of "editorial control" over the post – thereby requiring the need for a #ad marketing disclosure."

FCA gets tough on illegal financial promotions on social media

The question

What steps is the UK's Financial Conduct Authority (FCA) taking to combat the spread of illegal financial promotions through social media channels?

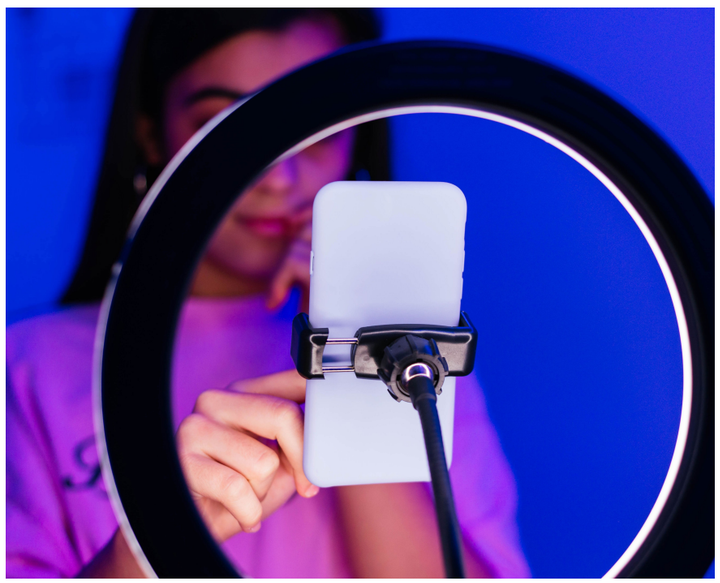
The key takeaway

The FCA has published an analysis of its financial promotions data for 2022. The data relates to action taken by the FCA against authorised firms in breach of financial promotion rules. Additionally, the regulator has reprimanded unauthorised firms and individuals. The report highlights the FCA's active involvement in ensuring that quality marketing information is being delivered to consumers, with the regulator prepared to intervene in instances that pose potential harm to them. The role of online platforms and social media companies will increasingly be called into question as the FCA progresses its fight against online financial misinformation.

The background

The FCA has spent the past year increasingly scrutinising advertisements on social media platforms in relation to financial products and services. This comes amidst broader concerns regarding the impact of the rising cost of living to consumers, with the UK's most vulnerable consumers at risk of being exploited.

Through its report, the FCA aims to illustrate the work being undertaken alongside social media platforms to improve standards across the market. The aim is to ensure that consumers are provided with clear, fair and trustworthy financial promotions which enable them to make informed decisions.



The development

The FCA report focuses on three broad stakeholders, being authorised firms, social media influencers and social media platform providers.

Action against authorised firms in numbers

FCA intervention over the course of 2022 led to 8,582 promotions being either amended or withdrawn altogether. This represents an increase of 1,398% when compared against 2021, which saw 573 amendments/withdrawals in comparison. These figures are indicative of the FCA's increasingly stringent approach to authorised firms who flout its rules relating to financial promotions and referrals. Whilst it remains the case that the FCA itself has no powers to require sites to be taken down, there has been ongoing cooperation from platform hosting providers who have assisted the regulator in removing potentially harmful content. Moving forward, it is likely that the FCA will continue its approach of requesting assistance from platform providers in tackling illegal promotions.

Warnings issued to influencers

The FCA has flagged the growing impact of social media bloggers and influencers in the promotion of financial products. Particularly concerning to the FCA is the promotion of access to credit and investment products, on behalf of unauthorised third parties, to younger age groups. Coming under the colloquial title of "fin-fluencers" (influencers who publicise content on financial matters), the FCA plans to collaborate alongside external regulators to educate financial influencers of their responsibilities when promoting financial products and services.

The FCA has indicated that it will not hesitate to refer for criminal investigation individuals who haphazardly publicise illegal financial promotions. Companies should therefore be increasingly alert to the potential perils of aligning themselves with influencers who choose to promote financial material.

Working alongside platform providers

The FCA seeks to establish a network of support and co-operation between itself as the regulator and social media companies as platform providers. "More needs to be done by tech companies to protect consumers", with a growing onus on platform providers to help combat the spread of illegal financial promotions. Recent commitments from tech companies to change their advertising policies to ensure that ads for financial products on their platforms are limited to regulated firms represents a key step. However, with an increasing concern regarding the vulnerability of consumers, the FCA will undoubtedly demand more from platform providers over the next few years.

The FCA will continue to remain actively engaged in the review of online material to ensure that authorised firms are complying with its rules.

Why is this important?

The FCA has increased its capability of performing cross-platform searches across social media platforms to identify illegal financial promotions in larger volumes. We can therefore expect to see it being ever more vigorous in its monitoring of social media platforms and whether they are actively engaging in blocking

illegal promotions. Those who take a lax approach to engagement are likely to face the risk of reprimand and the ramifications of being seen to facilitate fraudulent and illegal promotions could be significant. Of course, this is against the backdrop of the UK Government's evolving Online Safety Bill, which is primarily aimed at the protection of young and vulnerable people.

Any practical tips?

There is growing pressure on social media platforms to adopt a more proactive approach in tackling illegal financial promotions, as well as monitoring influencer compliance in line with FCA requirements. With the FCA doubtlessly expecting platforms to utilise their capabilities to identify and remove illegal financial promotions as an issue of high priority, it makes sense for them to proactively engage with the FCA to help combat misleading information and to educate users of the risks associated with financial promotions. This expectation will only increase due to the current macroeconomic outlook and the heightened financial vulnerability of online consumers.

HMRC sending “nudge” letters to social media influencers to encourage tax compliance

The question

How is HMRC ramping up its efforts to increase compliance yield in the context of the digital sales space?

The key takeaway

Social media influencers might find that at least one of their new “followers” engages with their content over the coming months. Unfortunately for them, that follower is HMRC. HMRC is sending “nudge” letters to social media influencers and online sellers to remind them about their tax obligations. Nudge letters are an increasingly important part of HMRC’s armoury and are used to “encourage” tax compliance behaviour. In the past, HMRC has sent nudge letters in respect of cryptocurrency and offshore companies that own UK property.

The background

HMRC has announced that it is starting a new nudge letter campaign and will be writing to individuals who have sold goods or services through online platforms or created content on digital platforms. The letters remind individuals of their legal obligation to declare their profits and suggest that they make use of HMRC’s Digital Disclosure facility to put things right if they have not reported their profits or earnings.

The development

It appears that HMRC has gathered seller details from several online platforms and is using this information to guide its nudge letter campaign before a new system of transaction reporting by online platforms begins. HMRC has data on individuals using sales platforms as well as influencers, vloggers and other content creators using online platforms.

Later this year, HMRC will be publishing regulations that will require online platforms to report on the transactions carried out through their sites. This is part of a global initiative, organised through the Organisation for Economic and Cooperation Development (OECD), for tax authorities to share information on online trading and platforms.

Why is this important?

Regularising your tax arrears can be costly but the longer you leave it the more expensive it is likely to become, particularly when HMRC’s late payment interest is 6.5%. Over time, the risk of being prosecuted by HMRC increases. Once HMRC starts to get regular transaction reports from online platforms it is expected to launch tax enquiries and tax fraud investigations into online sellers and influencers whose tax affairs are not up to date. HMRC has wide tax enforcement powers – everything from charging

Any practical tips?

If you live in the UK and make a profit from selling goods online or earn an income from online activity then, subject to a small de minimis limit (£1,000 a year), that profit is taxable and must be reported to HMRC through a tax return. Income from creating content on digital platforms is also taxable. Even if this is not your main source of income, it must be declared and any tax due paid to HMRC. HMRC’s nudge letters suggest that individuals make disclosure through its Digital Disclosure facility. However, making a mistake on a disclosure can have serious consequences and, depending on your personal circumstances, there may be a better way to make an appropriate tax disclosure.

ASA slams social media post for breaching rules on alcohol advertising

The question

How much care do brands and influencers alike need to take when promoting higher risk products like alcohol on social media? And what does this ASA ruling tell us about the appropriate targeting of posted content?

The key takeaway

It goes without saying that combining social media influencers and the promotion of alcohol (or any other sensitive product/service for that matter) is a risky activity, at least unless everyone involved (especially the influencer) has a clear understanding of the relevant rules and what is, and what is not, permissible. Added to this must be clarity over how and when to make an advertising disclosure and who (ie which audience) will see it from a demographic perspective, not least given the need to protect minors.

The background

In July 2022 Laura Whitmore, TV presenter and social media influencer, posted a video to both Instagram and TikTok that featured The Muff Liquor Company (MLC). The video in question (which was removed within 24 hours of being posted) showed Ms Whitmore dancing in a manner which became progressively "more energetic" as her drink changed from non-alcoholic drinks to "Muff and Tonic". Dancing to a song with the lyrics "I'll be fu**ed up if you can't be right here", the video caption read: "If drinks were dance moves @muffliquorco #makemineamuff #muffboss #irishowned".

The complainant challenged whether the video was easily identifiable as marketing communication and whether the ad was inappropriately targeted at under 18s. Additionally, the ASA challenged whether or not the ads encouraged responsible drinking, due to the implication that alcohol can enhance confidence and mood.

The ASA ruling

It was noted that the video was clearly intended to be a marketing communication as it was "directly connected to the supply of goods" and promoted MLC alcoholic drinks. As the ideo did not contain a "#ad" identifier or engage with TikTok and Instagram's advertising identifier tools, the video was not obviously identifiable as a marketing communication. MLC highlighted that Ms Whitmore was an investor in the company and as such it was clear that the post was marketing content. They also claimed that the inclusion of the hashtags "#muffboss" and "#irishowned" further made it clear that Ms Whitmore was commercially involved with the product. The ASA disagreed, noting that the hashtags were insufficient to identify her status to viewers. Additionally, because Ms Whitmore's social media accounts were public, the video could be viewed "in isolation" to her previous posts in which she referred to MLC and her involvement with the brand.

The ASA also ruled that the video was not socially responsible in that it suggested that alcohol could change mood or enhance confidence. The ASA concluded that in the video Ms Whitmore danced "more confidently and enthusiastically" when drinking the alcoholic drink, "Muff and Tonic", compared to when drinking non-alcoholic drinks, implying to consumers that drinking Muff and Tonic would enhance their confidence and improve their mood. The ASA also found that the content and the caption implied that "sobriety was boring". This was also compounded when combined with the lyrics of the song "I'll be fu**ed up" which was also deemed to promote excessive alcohol consumption.

Finally, as to whether the ads were inappropriately targeted towards children, the ASA noted that the Instagram video would have been "primarily seen by Ms Whitmore's followers" with the video pulling through to the "Explore" feed of anyone who had interacted with similar posts. The percentage of users under 18 deemed likely to have seen the video was significantly below the 25% audience share stipulated by the CAP Code (rule 18.15), given that Ms Whitmore's followers under the age of 18 is such a small proportion of her total followers. The ASA did not have data available about the demographic of Ms Whitmore's TikTok followers. Instead, they considered TikTok's interface and algorithm along with Ms Whitmore's previous role as presenter of Love Island, the "fifth most watched programme by those aged 4 to 15 years old" in the summer of 2022. On this basis, the ASA deemed the video to be directed at people under the age of 18. Contributing to this decision was TikTok's policy on banning the advertisement of alcohol on the platform. As a result, only the ad as it appeared on TikTok was in breach of the relevant rule (ie rule 18.15) in the CAP Code.

Why is this important?

The ruling highlights several key points around the engagement of social media influencers, especially when they are involved in the promotion of restricted products such as alcohol. It shows that brands need to fully control, and keep a close ongoing watch of, their influencers in this space. This goes to the extent to which the influencer displays a marketing disclosure as well as the actual activities they engage in as part of the promotional activity for the product in question (noting the higher levels of care needed for alcohol and other restricted products/services). An understanding of the demographics of the influencer's followers is also critical for these types of products – not just where the demographics can be cleanly assessed through follower numbers, but also on those channels where they cannot be where the ASA may look to the influencer's wider appeal (such as here with Ms Whitmore's Love Island fame).

Any practical tips?

When featuring any products on social media, influencers must use the hashtag "#ad" if they have any commercial interest in the product, even if they have not received direct payment for the post. The CMA's guidance: "Hidden ads: Being clear with your audience" and CAP's guide: "Influencer's guide to making clear that ads are ads" are both helpful here. And remember that with higher risk products and services, like alcohol and gambling, it's critical to ensure compliance with the specific advertising rules which govern them. Otherwise, it is almost inevitable that the promotional activity will fall foul of the (critical) eye of the regulators.

"It goes without saying that combining social media influencers and the promotion of alcohol (or any other sensitive product/service for that matter) is a risky activity, at least unless everyone involved (especially the influencer) has a clear understanding of the relevant rules and what is, and what is not, permissible."

The ASA's strict approach to affiliate marketing links and the need for advertising disclosures

The question

What does the ASA's ruling on several MailOnline articles tell us about its approach to affiliate marketing?

The key takeaway

The ASA has affirmed its stance on affiliate marketing where commercial intent is not obviously identifiable. Both affiliate marketers and the brands they promote hold joint responsibility for compliance with the CAP Code and both need to ensure that affiliate marketing communications are always obviously identifiable. In this case, the "short articles" on the MailOnline homepage which linked to "long-form articles" (that were advertising in their entirety) needed to make clear that the content to which they were linked were ads. The "long-form articles" were advertising in their entirety and also needed to be clearly labelled as such.

The background

Various articles containing affiliate links were published on the MailOnline website. The ASA received five complaints regarding the articles which challenged whether the articles were obviously identifiable as marketing communications.

The articles complained of were a mixture of headlines, short-form articles, and long-form articles, all focused on Amazon products (save for one, which focused on the fashion choices of an influencer, with the articles of clothing available to purchase via Skimlinks). Readers who clicked on the short-form articles were taken to the long-form article, which included a review of a product and several affiliate links leading to its purchase.

Associated Newspapers, the owner of MailOnline, responded by arguing that the content complained of was not within the remit of the ASA as the articles were largely editorial and therefore were not subject to CAP rules to identify marketing communications.

The development

The ASA rejected Associated Newspapers' response. It reported that the inclusion of affiliate links meant that the articles were subject to ASA regulation as MailOnline agreed to be an affiliate marketer. It was not essential for the affiliate marketer to have direct control over the content of the article to fall in the remit of the ASA and to be subject to the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (the CAP Code).

As the long-form articles primarily focused on the Amazon or Skimlinks products, and the short-form articles only served as a preview of the long-form articles, their marketing purpose must have been obviously identifiable to avoid violating the CAP Code. On this point, it was found that the ads were not obviously identifiable as marketing communications. The headlines, format, style, and layout of the articles were all akin to editorial articles, hiding the commercial focal point. Additionally, the wording used was unclear in relation to commercial arrangements.

MailOnline claimed "Products featured in this Mail Best article are independently selected by our shopping writers...". This wording was deemed insufficient by the ASA, as the products featured were selected from a list curated by Amazon, so therefore were not independently selected. Further, the ASA deemed the statement "...[we / MailOnline] may earn an affiliate commission" confusing, as barring an administrative error, MailOnline would always receive commission after a purchase via the link.

The ASA stated that had there not been a marketing arrangement, it was unlikely that the editors would have chosen to write these articles. Therefore, as all the articles were primarily focused on the sale of goods and did not make their marketing communications clear, the ASA found them in breach of the CAP Code (sections 2.1 and 2.3, namely "Recognition of marketing communications") on five separate occasions by including affiliate links without making it obvious that the catalyst of the articles was through affiliate marketing partnerships.

Why is this important?

The ruling was the first violation of the CAP Code's rules on the recognition of marketing communications against a news site after nearly four years. This affirms the strong responsibility on affiliate marketers and brands alike to ensure compliance with marketing disclosures and to ensure that affiliate articles are clearly labelled or constructed in a way to make clear that they are in fact advertising.

Any practical tips?

Businesses need to be careful when treading the fine line between ads and editorial content. Whilst recent actions under the CAP Code have largely focused on social media campaigns and influencers, it is an important reminder that all content is under possible scrutiny by the ASA, including affiliate links.

“Up to 50% off” Carpetright saving claim deemed misleading by ASA

The question

What does the ASA’s recent ruling on Carpetright’s banner ads tell us about its approach to “up to” or “from” price promotions?

The key takeaway

Traders need to take care when using “from” or “up to” pricing announcements in a promotion. A significant proportion of the products in the promotion must benefit from that maximum saving and the discounted product must have a sufficiently established prior price. In this ruling, the ASA ruled that eight Carpetright banner ads claiming that certain products were up to 50% or 20% off were misleading because they exaggerated the amount that customers would likely save.

The background

In January and February 2022, Carpetright launched a campaign promoting discounts on a range of products. All the ads were a variation of the following information: “Up to 50% off a choice of floors and beds + extra 20% off a huge range of floors when you buy underlay”.

Two rival companies challenged whether these savings claims were misleading because they understood that only a small proportion of products were available at these maximum discounts, and that the products which were discounted had never actually been sold at the stated higher, undiscounted price.

The ASA ruling

As part of its investigation, the ASA first considered how consumers would interpret the ads. They determined that consumers would draw the following key conclusions:

- that a significant proportion of the products would be discounted “up to” the amounts stated
- that the maximum discounts referred to would be spread across the different price ranges of products, and
- that the higher undiscounted prices were the genuine original prices.

Carpetright provided the ASA with price and sales data divided into three categories: beds, hard flooring and soft flooring. The ASA reviewed the data provided by Carpetright and considered the pricing history as well as which savings claims were made in relation to which products or product categories at the various stages of the 10 week long promotion. They noted that the figures Carpetright referred to showed the percentage of product lines discounted, rather than the percentage of product lines that were discounted by the maximum possible percentage.

The ASA considered that the use of the maximum discount in the ads (50% and 20%) was misleading because that maximum discount had not been applied to a significant proportion of the products and maximum discounts were not evenly distributed across different price ranges of products. For example, for hard flooring only 2-8% of the product lines were discounted by the maximum amount.

In deciding whether the advertised savings were genuine savings, the ASA considered whether the higher undiscounted prices were the usual selling price, and took three key principles into account. Firstly, the Chartered Trading Standards Institute’s Guidance for Traders on Pricing Practices states that savings are more likely to be considered genuine if the discounted price is used for a period of time which is the same or shorter than the period of time that the reference price is used. In this case, although Carpetright had a policy of ensuring that over a rolling 52 week period, no product was discounted more than 26 weeks, from the six months’ sales data provided “there were certain products that had been discounted for more than half that time and so at that particular point in time, those products had been at the discounted price for longer than they had been at the higher price”. Secondly, Carpetright used a pricing model whereby products were given essentially two prices over the year. The ASA concluded that rather than one being the genuine price and the other being a discounted price, the product had two prices and consumers who were aware of the pattern would know that neither was the usual selling price. The final relevant factor was the volume of sales at the higher price. Here, the ASA pointed to the fact that a large proportion of beds had not been sold at their higher price because consumers knew that they would be discounted in the future.

The ASA found that the ads were misleading because consumers would understand that a significant proportion of products would be discounted by the “up to” amounts, when they were not, and the advertised savings were not against a genuine usual selling price.

Why is this important?

This decision highlights the care that must be taken with a common promotional technique, namely “up to X% off” and how this can become misleading. In this case, it was not enough for Carpetright to show that some of its product lines were discounted by the maximum amount of the discount (50% or 20%). The maximum discount had to be across a significant proportion of products and across the various categories of products which were advertised. The ruling also serves as useful reminder to advertisers of the importance of genuine price establishment and that juggling with prices may result in consumers being misled.

Any practical tips?

Retailers should ensure that when the term “up to” is used in a sale advert, they need to be able to show that a significant proportion of products (with a good distribution across product categories and price ranges) have the maximum saving. They must also be able to demonstrate that a genuine usual selling price has been established to ensure that any discount represents a genuine saving for the consumer.

“Traders need to take care when using “from” or “up to” pricing announcements in a promotion.”

ASA rules against Match.com on portrayal of offensive gender stereotypes

The question

When do ads depicting small gestures between couples cross the line into gender stereotyping?

The key takeaway

The ASA is continuing to clamp down on ads that may cause harm and offence by perpetuating negative gender stereotypes. Great care must be taken whenever ads depict the interplay between men and women, whatever the background context.

The background

In June 2022, Match.com posted a TikTok which depicted a woman carrying out gender stereotypical acts for her male partner. The woman was seen making a protein shake for her partner, whilst he was sitting down with his feet up, and a female voiceover in the background stated, "things that make him realise I'm a keeper. I will make him his protein shake after the gym". The female voice went on to say, "I always make sure he has a fresh towel and socks after his shower" whilst she was shown arranging a towel and pair of socks in the bathroom.

Match.com explained that it was their intention to portray that small gestures between couples were an important part of all successful relationships. Whilst the focus was small acts of kindness in a relationship, they clarified that they had contacted real couples and asked them about everyday gestures they did for each other.

Match.com also emphasised that this was one ad of a three-part series featuring the same couple, all posted on the same day, further adding that all ads could have been viewed consecutively. Although all the ads were told from the woman's perspective, the other two featured alternative perspectives of the same theme: "things that make me realise he's a keeper" and "small gestures we do for each other that make me realise he's a keeper". Nonetheless, the ASA held that it was not self-evident that the ad was part of a wider series of ads and therefore, in isolation, "the title, when viewed in the context of the ad, reinforced the idea that women should be subservient to men in order to maintain a successful relationship".

The development

The ASA understood that the ad sought to highlight small gestures of kindness performed in relationships and that the ad in question centred on the actions carried out by a woman for her male partner in their relationship. However, it was also noted that all gestures performed by the woman were domestic chores and one-sided: they were not reciprocated by the man.

The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing Practice (the CAP Code) states that ads must not include gender stereotypes likely to cause harm, or serious or widespread offence. CAP guidance also makes it clear that ads should be careful to avoid suggesting stereotypical roles or characteristics are always uniquely associated with one gender.

The voiceover of the ad was considered by the ASA as well as the title and visuals. They found the wording used suggested habitual gestures regularly undertaken by women. Meaning, it was not obvious that the woman's actions were "one-off" acts distinguishable from chores. The acts were also viewed as being undertaken solely for the benefit of the man, not the woman. As a result, the ASA concluded that the ad was likely to cause harm and widespread offence due to its perpetuation of negative gender stereotypes.

The ad has been removed and Match.com has since acknowledged that it would have been more appropriate to portray a couple having more equal roles in their relationship.

Why is this important?

Society has for some time now been shifting away from entrenched mindsets that particular genders have particular roles without overlaps or crossovers. As such, self-regulatory organisations (such as the ASA) take such issues seriously in playing their part to break down gender stereotyping. It is therefore important to keep up with the most up-to-date rules and guidance on these issues, especially when attempting to depict real life issues such as family and/or relationships within an advertising context.

Any practical tips?

Gender stereotyping and allegations of sexism are not labels that brands will want to associate themselves with. Therefore, careful consideration should be given to the rules surrounding such important and live sensitive issues. Despite clearly outlining their intentions, Match.com were still found to be in breach of the CAP rules because the execution of their ideas perpetuated harmful gender stereotypes.

"The ASA is continuing to clamp down on ads that may cause harm and offence by perpetuating negative gender stereotypes."

Contractual right to terminate – determining whether there has been a material breach

RiverRock European Capital Partners LLP v Harnack **[2022] EWHC 3270 (Comm)**

The question

What factors will a court consider when determining whether a breach is "material" in the context of contract termination?

The key takeaway

A termination right which is triggered by a "material breach" will only be effective if the breach has a serious effect on the benefit the innocent party would otherwise derive from performance of the contract. The court will consider the character of the breach, the breaching party's explanation for the breach and the consequences of the breach in the context of the agreement.

The background

RiverRock brought proceedings in the High Court claiming its entitlement to certain payments on termination of a consultancy agreement and other allied agreements, made with Deutsche Real Estate Asset Management Limited (DREAM).

RiverRock had, under the consultancy agreement, appointed DREAM as its FCA Appointed Representative for the purpose of providing FCA-regulated activities in connection with an investment fund. Mr Harnack and Mr Mörsdorf (H and M) were responsible for the day-to-day operation and management of the fund.

From its launch in around 2016, the fund encountered problems raising and sourcing investments. DREAM was obliged to file a confirmation statement with Companies House in July 2017. This had not been done which resulted in DREAM being struck off and dissolved in November 2017. Consequently, RiverRock terminated the consultancy agreement and brought a claim against H and M.

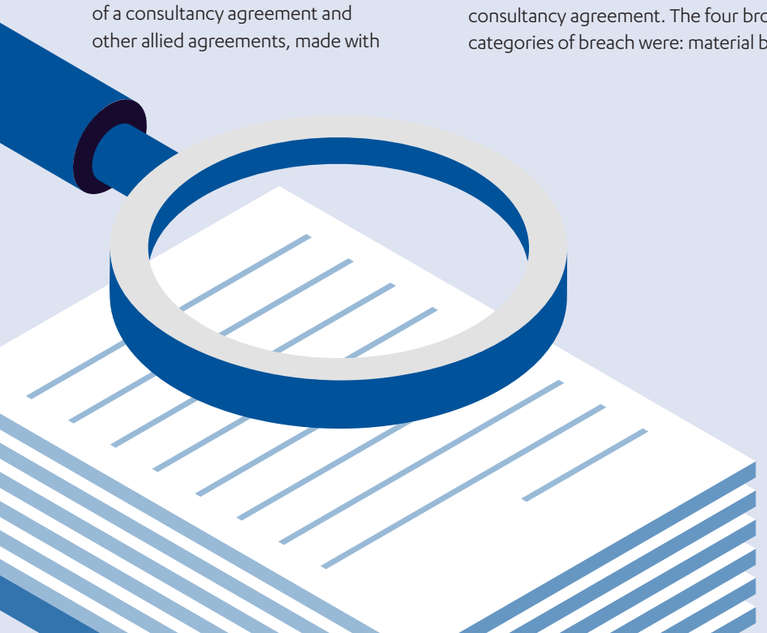
RiverRock claimed that the striking off of DREAM from the Register of Companies, and its dissolution had put DREAM in breach of various terms of the agreements giving rise to a right to terminate the consultancy agreement. The four broad categories of breach were: material breach of the agreements, breaches of FCA rules, acting in such a way as to bring the parties and the fund into disrepute and breach of implied terms.

A key issue for the High Court was whether any of the breaches said to result from the striking off and dissolution of DREAM were material.

The decision

The court dismissed RiverRock's claim.

The court acknowledged that the concept of a "material" breach is not easy to define – whether there was a material breach is often dependent on the context and may be dictated by the consequences that flow from a finding that it had occurred. The court also equated words like "substantial", "more than trivial, but not repudiatory" and "a serious matter" with "material". Factors to consider on materiality included the actual breaches, the consequence of the breaches to the innocent party, the guilty party's explanation for the breaches and the breaches in the context of the agreement between the parties continuing or coming to an end.



Applying this to the facts, the court reasoned that the consultancy agreement was expected to continue for some time and, if terminated, might result in the waste of years of work by H and M. In these circumstances, while a repudiatory breach was not required, there had to have been a substantial breach involving serious consequences for the innocent party.

The judge held that there was no such breach citing the following reasons, among others:

- The breaches were the result of a mistake. One of the defendants had moved house and therefore did not receive the notification that they needed to file their confirmation statement.
- The breaches were readily capable of remedy. DREAM could have been restored to the register in a very short period and with little difficulty allowing the arrangements between the parties to continue.
- On the facts, RiverRock were not concerned by the dissolution of DREAM and used the breach as a means of justifying the termination of the agreements. It was apparent from email correspondence and oral evidence that the fund was underperforming and RiverRock sought its end before the dissolution was known to it.
- The breach caused no loss to the fund or its investors or any complaints or claims against RiverRock.
- The FCA took no action against RiverRock as a result of the breaches and it suffered no penalty.
- RiverRock failed to identify any other practical consequences arising from the dissolution.

Why is this important?

Contractual termination which is triggered by a material breach will be effective only if the breach has a serious effect on the benefit the innocent party would otherwise derive from performance of the contract. If the agreement is to continue for a long time and the offending party has invested a lot into the agreement, the breach will need to be more significant to justify termination.

Any practical tips?

Courts are likely to find material breach arguments unattractive where it is clear that the apparently injured party is simply using the clause to prematurely exit the agreement.

There is no definition of "material" in case law – each case turns on its facts. If an express provision giving a party or the parties the right to terminate for material breach is included in the contract, at the drafting stage consider what substantial breaches may arise that may seriously impact the innocent party (ignoring those that may result from mistake or a lack of understanding). The parties should then consider specifying that certain breaches or breaches of certain clauses will always be material.

Those drafting contracts should also keep in mind that contractual material breach should largely be treated as separate to and not the same as the common law right to terminate for repudiatory breach. Not all material breaches will be considered to be repudiatory.

The courts have been prepared to accept a right to terminate for any breach and for specific contracts this might be a better option than a provision for termination in the event of a "material breach".

Contract termination – obligation to engage during notice period

AMT Vehicle Rental Ltd v Volkswagen Group United Kingdom Ltd **[2022] EWHC 2934 (Comm)**

The question

In a contract for the supply of vehicles, was the customer required to inform the supplier of its requirements during the contractual notice period?

The key takeaway

In a contract to supply hire vehicles, the customer had a duty to engage with the supplier by informing the supplier of its need for vehicles and allowing the supplier to offer hire vehicles based on the customer's needs during the notice period.

The background

AMT Vehicle (AMTV) contracted with Volkswagen Group UK (VWUK) to supply them with hire vehicles to replace their customers' vehicles when they were unable to be used because of breakdown or other need for investigation or repair.

In order to facilitate the booking process, AMTV was given daily access, via a third party intermediary, to a spreadsheet (the booking master sheet) showing VWUK's demand for vehicles. AMTV could then match VWUK's need with one of its vehicles.

In September 2019, VWUK gave notice to terminate the contract – It had decided that it would be more efficient to have a single supplier of vehicles and AMTV was not a viable contender because it was not large enough. VWUK decided to terminate its agreement with the third party intermediary and AMTV. VWUK's notice expired in March 2020 and it was common ground between the parties that the notice was effective from that date.

From October 2019 to March 2020, VWUK removed AMT's access to the booking master sheet and did not otherwise inform AMTV of its needs for replacement vehicles. This made it impossible for AMTV to meet VWUK's needs and supply vehicles. AMTV contended that this placed VWUK in breach of the terms of the contract. It claimed damages by way of lost profits for the hires that VWUK would have made from it, but for the breach.

The decision

One key issue for the court was whether VWUK owed a contractual obligation to notify AMTV of its requirements (ie allow it access to the booking master sheet or similar) and allow it the opportunity to respond to vehicle requests during the notice period. In its judgment, the court reasoned that knowledge of that need was central to the performance of the contract and that the commercial efficacy of the contract depended on there being a contractual obligation on VWUK to give this notification.

The court focused on clause 2.1 of the contract which stated that "... VWG engages the Provider to provide the services to VWG ..." and, in particular, the meaning of the word "engage". The court found that the clause was worded to be a term of the contract, not simply background to it, suggesting that it was meant to have some operational significance and also that the presumption against surplusage would favour the clause having some meaning beyond simple repetition of the background section. While there was no requirement for VWUK to engage AMTV in respect of any particular vehicle need, that did not mean there were no contractual obligations as to how the parties should deal with each other.

The court accepted AMTV's pleaded case that VWUK was obliged to engage with it during the course of the contract. On whether VWUK had breached the contract, the court found that VWUK was in breach of clause 2.1 in not informing AMTV of its need for replacement hire vehicle services or giving it an opportunity to offer its services in response to such information from October 2019 until the termination of the contract in March 2020.

The court awarded AMTV its losses by assessing what hires it would probably have obtained from VWUK, disregarding any possibility that VWUK would simply have refused to propose any hires, then discounting from the sums received for the hires the costs that AMTV would have incurred.

Why is this important?

During a contractual notice period, contracting parties should continue to perform their obligations under the contract. Just because notice to terminate has been given, this does not mean that the obligations under the contract cease.

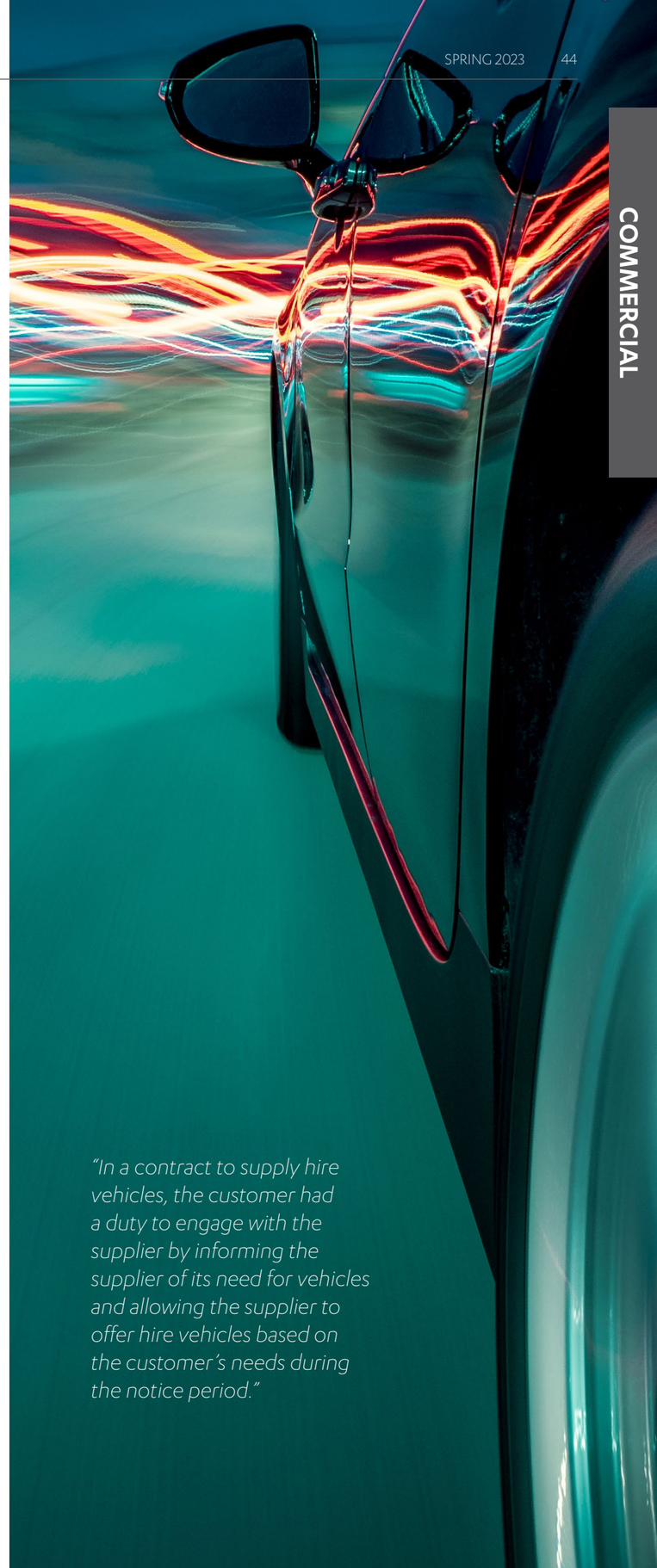
Any practical tips?

During the proceedings, VWUK argued that the use of the word "engage" in clause 2.1 was more consistent with the word "involved" which had been used elsewhere in the contract. The court noted that, in VWUK's examples of use elsewhere in the contract, the word "engage" was used passively whereas in clause 2.1 the use was active and transitive. The parties and court had also examined dictionary definitions of the word "engage". This forensic approach to interpreting key terms is worth noting.

When drafting contractual provisions, consider that the courts took seriously AMTV's reliance on the presumption against surplusage in the construction of a contract, quoting previous case law: "Surplusage is by no means unknown in commercial contracts, of course, but it is unusual for parties to include in the operative part of a formal agreement of this kind a whole clause which is not intended to have contractual effect of any kind. One starts, therefore, from the presumption that it was intended to have some effect on the parties' rights and obligations". If a particular clause is intended to have some significance to the parties' obligations rather than simply to restate the background to the contract, then its inclusion in the operative part of an agreement is compelling evidence that it is intended to have contractual effect.

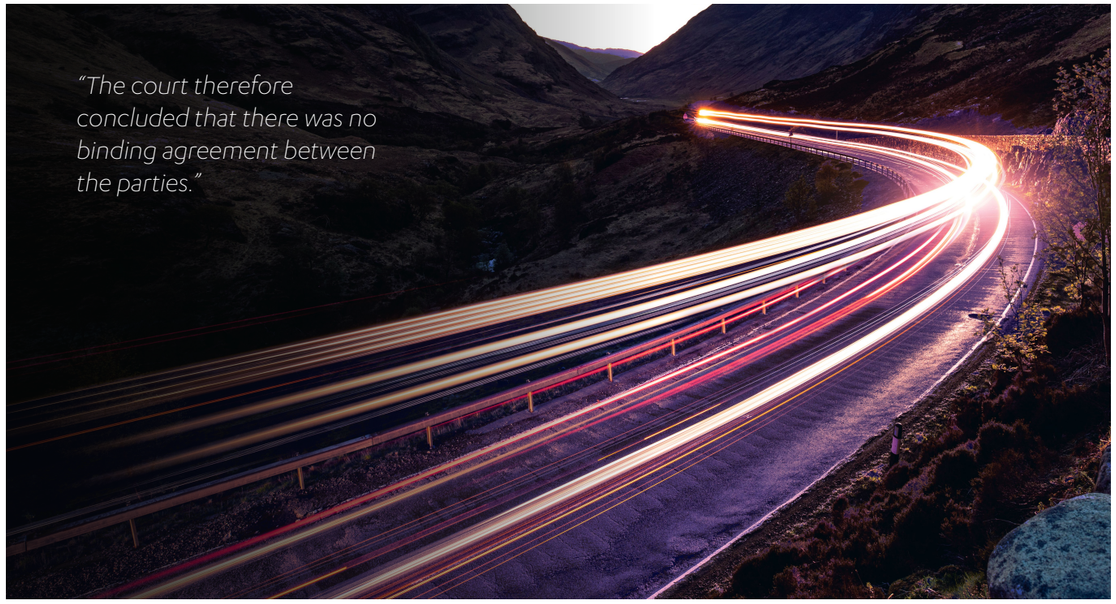
The court also considered that the commercial efficacy of the contract depended on there being a contractual obligation on VWUK to notify AMTV of their vehicle requirements.

COMMERCIAL



"In a contract to supply hire vehicles, the customer had a duty to engage with the supplier by informing the supplier of its need for vehicles and allowing the supplier to offer hire vehicles based on the customer's needs during the notice period."

Contract formation during contract negotiations



***Fenchurch Advisory Partners LLP v AA Ltd* (formerly AA PLC) [2023] EWHC 108 (Comm)**

The question

Can a contract negotiation, which has broken down before all of the contract terms have been agreed, nevertheless result in a binding agreement?

The key takeaway

Whether there is a binding contract between the parties and, if so, on what terms, depends on what was agreed in the parties' communications (words or conduct), the wider context and whether that leads to an objective conclusion that the parties intended to create legal relations, have agreed all the essential terms required for a legally enforceable contract and there is valid consideration.

The background

A claim for fees was bought by an investment banking and corporate finance advisory firm, Fenchurch Advisory Partners (Fenchurch), in respect of the advice and assistance it provided in the potential sale of the insurance division of the AA. The terms of engagement of Fenchurch were extensively negotiated between the parties but no engagement letter was ever signed and the sale of the insurance division did not go ahead.

For about 11 months, while the engagement letter negotiations were taking place, the Fenchurch team worked on the potential sale project: attending working group and steering committee meetings, co-ordinating the work of other advisers, scoping the various workstreams, assisting in the preparation of a financial model and drafting key documentation.

Fenchurch pleaded that the fact that work had been done by them was highly relevant to their position that the parties had intended to enter into a binding contract. It was argued that the combination of the exchanges (many by email) and the carrying out of the work agreed in those exchanges gave rise to a binding contract.

The AA, on the other hand, submitted that a binding contract should only come into being when contractual documents were signed by the parties (and this was particularly the case where solicitors were involved on both sides). The AA argued that the way the engagement letter was negotiated envisaged the requirement of signatures and drew the court's attention to the fact that there was an entire agreement clause. This reinforced their case that the parties wanted a written agreement which set out all of the terms of their bargain.

The decision

Two main issues for the court to decide were whether a binding contract had been agreed between the parties and, if not, whether there was an implied contract.

In considering whether a binding contract had been formed, the court firstly accepted the AA's case that not all of the terms of the contract had been agreed by the time the project was dropped.

The court then considered whether there had been a binding agreement "with some details left over". While it is possible for parties to reach a binding agreement when there are still unfinished negotiations, this was not true in the present case. Email exchanges between the parties dealt specifically with the fee arrangement (ie the commercial negotiation) and not the outstanding points relating to the detailed terms of the engagement letter (the legal negotiation). Although these workstreams had been separated out, the expectation was that both workstreams would be completed and then the final engagement letter signed.

It was also clear that at all stages, the parties envisaged that the terms of their agreement would be contained within a signed engagement letter – there was never any suggestion that a binding agreement would come into being at any earlier stage. There was also no other external sign that the parties were taking a different course to a legally binding agreement.

The court therefore concluded that there was no binding agreement between the parties.

Fenchurch argued in the alternative that there existed an implied contract that it would be paid a reasonable fee for its services. In fact, it was "commercially absurd" to suggest that it was acting on the basis that it did not expect to be paid should the AA unilaterally refuse to progress the negotiation of the contract.

The High Court also rejected this argument. As evidenced by the extensive negotiations, it was never contemplated by the parties that the AA would pay a "reasonable fee"; they expected to agree a specified fee. Additionally, Fenchurch began work on the understanding that its engagement terms would be agreed in due course, not that there was already an agreement in place.

Fenchurch's other alternative argument for a claim in restitution for unjust enrichment in respect of the services that it had provided to the AA, was successful. However, crucially, this did not include any success fee element and was limited to a "progress payment" in relation to the services provided.

Why is this important?

It is not uncommon for a party to start performing some of its obligations before a written agreement is signed. The case illustrates the importance of ensuring clarity during negotiations. If parties mean to create a legally binding agreement before all terms are agreed this should be dealt with explicitly. Whereas, if parties are negotiating one specific aspect, it should be made clear that agreement on that aspect is not a binding contract on its own and that agreed terms are subject to the final contract being agreed and signed.

Any practical tips?

When negotiating and agreeing individual aspects of an overall deal, particularly important ones such as fees, specify whether agreement is subject to the signing of the entire contract embodying all terms or whether the parties intend to be bound on that specific aspect.

The key question is what the parties objectively intended, having regard to their communications and the wider context. Use of the phrase "subject to contract" usually indicates that there is no intention to be bound until there is a signed agreement, but it is not determinative, and so the communications and the basis on which any work is being carried out should be made clear.

A party to contract negotiations who is undertaking progress work should ensure this is provided for expressly and separated out from the overall transaction. Create a clear formula which can be applied to all potential outcomes to calculate the market value of the services.

Although a claim in restitution for unjust enrichment in respect of goods or services provided may provide some level of compensation, it is a much more uncertain outcome and may not cover all of the consideration that a supplier may wish to contract for.

Oral commission agreement for sale of property silent on consideration for actual service provided – legal remedies

Barton and others (Respondents) v Morris and another in place of Gwyn-Jones (deceased) (Appellants) **[2023] UKSC 3**

The question

In an oral agreement in which a vendor expressly agreed to pay an individual a set introduction fee on the sale of a property sold at a certain price, did the vendor have to pay the introducer (and how much?) where the property sold for a lower sum than that expressly provided for in the contract?

The key takeaway

In the absence of price manipulation to avoid a contractual payment obligation, even if the terms of a contract provide for a bad bargain for one party when the factual scenario plays out, courts will be reluctant to imply a term on payment that contradicts the express terms agreed or oblige a party under the law of unjust enrichment to pay a fee.

The background

Foxpace wanted to sell one of its properties – Nash House. Mr Barton entered into an oral agreement with Foxpace regarding the sale of the property where, if Mr Barton introduced a buyer to Foxpace who then bought Nash House for £6.5m, Mr Barton would receive a commission of £1.2m for his efforts.

This figure reflected the amount Mr Barton had already expended in trying (unsuccessfully) to purchase the property himself. Nothing was said about what Mr Barton would be paid in the event the property sold for less than £6.5m.

Mr Barton found a buyer for the property. While the contract of sale initially was for £6.55m, the property sold for only £6m following the discovery that it was on land earmarked for HS2 construction work. Foxpace then fell into liquidation. Mr Barton brought a claim to challenge the decision to value his debt at £1 in the liquidation, and instead sought to prove the debt was worth £1.2m.

Mr Barton claimed that Foxpace was liable to him in contract, on the grounds that the contract expressly stipulated that he would be paid £1.2m if he introduced a buyer for Nash House to Foxpace (regardless of the purchase price). In the alternative, he brought a claim for unjust enrichment, on the grounds that Mr Barton had provided a service to Foxpace (ie the introduction of the buyer) which Foxpace knew it would have to pay for.

At first instance, the judge held that since the contract said nothing about the fee that Mr Barton would receive if the property sold for less than £6.5m, Foxpace did not have to pay Mr Barton anything for finding the buyer. In case this was wrong, the judge assessed the commercial value of the services provided by Mr Barton at £435,000.

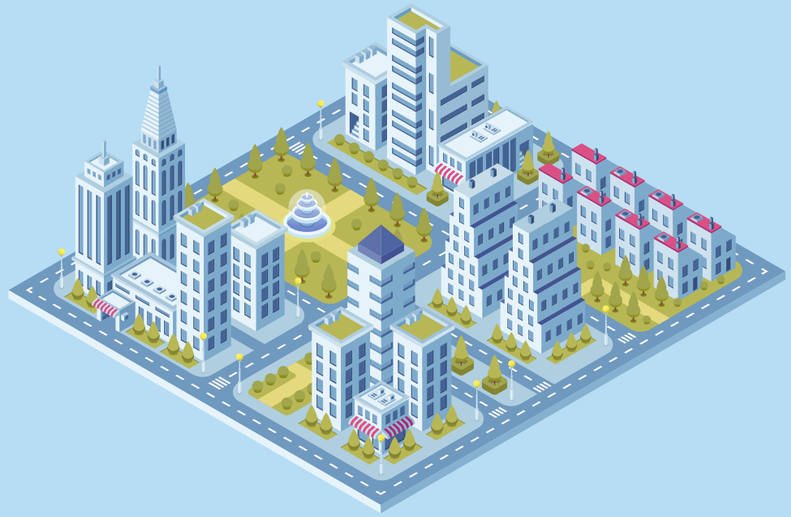
The Court of Appeal disagreed, allowing Mr Barton's appeal and ordering that he be paid a reasonable sum for his efforts (£435,000). Foxpace appealed.

The decision

The Supreme Court considered the ways in which Foxpace was obliged to pay something to Mr Barton. As well as considering the express terms of the contract and the claim of unjust enrichment, it also considered whether a term for payment could be implied into the agreement.

All the arguments were rejected, resulting in no order for payment to Mr Barton, on the following grounds:

- The oral agreement was silent on what Mr Barton would be paid if the property sold for less than £6.5m. Therefore, there was no express term requiring Foxpace to pay Mr Barton anything upon the sale of Nash House.
- A term requiring Foxpace to pay Mr Barton a specific sum in the event that Nash House sold for less than £6.5m could not be implied into the contract. This was because it was not necessary to imply this term to give the agreement business efficacy nor was it possible to determine what sum Foxpace would have agreed to pay



Mr Barton in the situation where the property sold for less than the £6.5m agreed. Such an implied term would run contrary to the express term of the contract which restricted payment to the instance where the property sold for £6.5m.

- Section 15 of the Supply of Goods and Services Act 1982, provides that, where under a "relevant contract" for the supply of a service, the consideration for the service is not determined by the contract, there is an implied term that the party contracting with the supplier will pay a reasonable charge. The court found that this did not apply since the consideration for the introduction was in fact determined by the contract. It was also doubtful whether the agreement would be considered to be a "relevant contract" as it was not a services agreement but a "unilateral contract by which Mr Barton's making of the introduction was what brought the contract into existence".
- The unjust enrichment claim was based on a "failure of basis" argument, ie where the benefit incurred by a defendant is intended to be conditional and so the defendant must return the benefit if the condition is not fulfilled. The court rejected this argument finding that it was unlikely that the parties simply did not contemplate a lower sale price such that a sale for £6m constituted a failure of that basis for the purposes of founding a claim for unjust enrichment.

Why is this important?

In terms of its application of underlying legal principles, the court was emphatic in its finding that the claim for unjust enrichment could not conflict with an express term in the contract covering the same ground and events (although two judges provided dissenting judgments). Although narrow in scope, the express term provided a complete statement of the circumstances in which Mr Barton was promised some reward under the agreement. The court concluded: "unjust enrichment mends no-one's bargain".

Any practical tips?

For an agreement of this value, an oral agreement was inadvisable. However, the oral nature of this agreement was not the issue. It was the narrowness of the agreed terms for payment that provided such an unsatisfactory outcome for Mr Barton. To reduce uncertainty, ensure that the express terms of the contract (especially concerning payment and the services to be provided) address all relevant scenarios.

To bring a claim for unjust enrichment the defendant must have been enriched at the claimant's expense – these two elements are often relatively straightforward to prove. The third element is that the defendant's retention of the enrichment must be found to be unjust. In cases involving failure of basis, the failure must be total not partial, and the test is not whether the promisee has received a specific benefit, but rather whether the promisor has performed the duties in respect of which the payment is due.

As a general drafting consideration, be mindful that the courts will be reluctant to alter a contractual relationship by implying terms or provide for restitution for unjust enrichment. If risk has been allocated between the parties by the contract (even if this is by omission of a term), the courts will usually choose not to interfere.

Audit clauses – true construction and implied terms

***Pixdene Ltd v Paddington and Company Ltd* [2022] EWHC 2765 (IPEC)**

The question

How did the court construe the wording of an audit clause when the parties to a royalty distribution agreement disagreed on who was entitled to inspect the relevant documents and what could be done with the documents?

The key takeaway

To avoid disputes about the true construction of audit clauses, parties should ensure that the audit clause is tailored to the specific transaction and factual background and that the scope of their respective obligations is clearly set out. A party seeking audit rights will want to focus on having broad rights to access data, information, systems, equipment and the premises. A party granting audit rights, however, will aim to limit disruption to their business, costs and will be looking to restrict access to confidential and commercially sensitive information.

The background

Pixdene had entered into a royalty distribution agreement (RDA) giving it a right to a 10% share of the net merchandising income from the worldwide exploitation of the Paddington Bear merchandising rights. The other party to the agreement, Paddington and Company Limited (Paddington), owns the intellectual property rights to Paddington Bear. A dispute arose between the parties which focused on the proper contractual interpretation of the RDA's audit clause which provided:

"5. Audit

During the term of this Agreement a third party auditor may, upon prior written notice to Paddington and not more than once per every two year period, inspect the agreements and any other business records of Paddington with respect to the relevant records or associated matters during normal working hours to verify Paddington's compliance with this Agreement.".

Audits took place in 2014 and 2017 with no issues raised. However, in 2019, Pixdene appointed a different auditor, and the dispute arose concerning what the audit clause entitled Pixdene and the auditor to access.

Pixdene sought an order for specific performance requiring Paddington to perform its obligations under the audit clause. It also sought a declaration from the ourt on the general interpretation of the audit clause.

It was Pixdene's case that the audit clause should be construed to require Paddington to send to Pixdene in advance of inspection all the documents which it was required to make available for inspection (effectively giving Pixdene a right to inspect) and to provide it with copies of inspected documents. Paddington submitted that the audit inspection was limited to a physical on-site inspection of documents in Paddington's offices, during normal working hours and only in the presence of Paddington's representatives.

The decision

The court dismissed Pixdene's submission that the audit clause entitled it to inspect or receive copies of inspected documents from Paddington in advance of any inspection. The drafting very specifically covered only a third party auditor and this excluded Pixdene.

The court agreed with Paddington on the place and timing of the inspection but did not agree that the clause obliged the third party auditor to inspect only in the presence of Paddington's representatives.

On the question of what information the third party auditor was entitled to share with Pixdene, the court found that the clause did not give Pixdene a blanket right to copies of inspected documents from the auditor but the auditor would be permitted to disclose information gained from inspecting documents that would enable it to report to Pixdene.

The court then considered whether Paddington was entitled to redact documents to be reviewed by the auditor. Paddington submitted that it should be permitted to redact "those parts of the said agreements and other business records which do not relate to the Claimant's entitlement under the Agreement …". The court disagreed, even in relation to confidential information, because the clause was silent on redaction and the limited disclosure permitted by the auditor (a professional with professional obligations to treat confidential information confidentially) under the clause provided adequate protection to Paddington. The court did, however, imply a term that Paddington could withhold legally privileged information from inspection.

The court also made useful findings on a number of other points. While it did not specify exactly how long the prior written notice of the audit should be, it confirmed that this notice should be given within a "reasonable time". This should not be less than 10 clear business days before the proposed audit and must identify the relevant period for the audit inspection.

Why is this important?

Audit clauses that fall to be interpreted by the courts will have the usual rules of contractual construction applied to them. This case is particularly helpful in summarising the court's approach to construction of audit clauses and to implying terms into them.

There was no great departure from the court's normal approach of placing great importance on the natural meaning of words in contractual provisions (even if a term that is very imprudent for one of the parties has been agreed) and a reluctance to imply terms unless this is necessary to give business efficacy to the contract or on the basis of the obviousness test.

Any practical tips?

Where the audit clause provides for the auditing party to undertake audits via a third party, but the auditing party wishes to include its own right to inspect or receive copies of documents, this should be stated explicitly in the provisions of the agreement. There should also be clear reasons for it to do so because invariably this will be resisted by the party granting audit rights due to concerns about confidentiality and access to commercially sensitive information (which is one of the reasons why a third party auditor is often specified).

Cases relating to audit clauses and disclosure of information are generally fact specific, but a common theme is courts refusing to grant an order for access where an audit clause does not specify the access required, or provide sufficient information about the purpose of the audit and what will be done after access has been obtained. To avoid this, ensure audit provisions fit the type of transaction and individual circumstances, and encompass the scope of information and access required.

Where appropriate, consider stipulating the period of advance notice required to be given prior to inspection, to avoid any debate around what constitutes reasonable notice. Also consider exercising audit rights on a regular basis, as envisaged by the contract, rather than only in circumstances where a dispute has already arisen or an underpayment or non-compliance issue has been raised.

"To avoid disputes about the true construction of audit clauses, parties should ensure that the audit clause is tailored to the specific transaction and factual background and that the scope of their respective obligations is clearly set out."

COMMERCIAL

Global Expertise.
Local Connections.
Seamless Service.

TERRALEX

www.terralex.org

rpc.co.uk