RPC

Snapshots for Meta

AUTUMN 2023

KEY UK AND EU DEVELOPMENTS FOR META'S COMMERCIAL LAWYERS

New data bridge to allow for UK – US data transfers

PLUS

UK ICO publishes draft guidance on biometric data and technologies

European Parliament publishes draft report on the addictive design of online services

ASA updates on environmental claims

Welcome to the Autumn 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

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

WITH THANKS TO OUR FANTASTIC CONTRIBUTORS

- Hettie Homewood
- Nicole Clerk
- Tom James
- Dan Jackson
- Lauren Paterson
- Anila Rayani
- Laura Verrecchia
- Ben Jeffries
- Courtney Brotherson
- Nick McKenzie
- Rebecca James
- Sofia Gofas

EDITORIAL

Sub-editors Olly Bray, David Cran, Joshy Thomas, Praveeta Thayalan, Anila Rayani, Laura Verrecchia

Design Rebecca Harbour

Contents

4 DATA

5 New data bridge to allow for UK-US data transfers

6 UK ICO and CMA release joint position paper on harmful design in digital markets

8 UK ICO publishes joint statement on data scraping and the protection of privacy

10 UK ICO publishes draft biometric data and technologies guidance for public consultation

11 New development: updated ICO guidance on "likely to be accessed by children"

12 DIGITAL

12 Ofcom publishes new report on video-sharing platforms

14 Amazon appeals its EU designation as a VLOP

15 Thumbs-up if you agree: emoji can represent contractual agreement according to Canadian judge

16 UK Government publishes first MaaS (mobility as a service) Code of Practice

18 CONSUMER

18 European Parliament publishes draft report on the addictive design of online services

19 The Retained EU Law (Revocation and Reform) Act 2023 – a happy new year?

20 UK Government u-turns on phasing out "CE" product safety marking

22 Government consults on improving price transparency and product information for consumers

24 ADVERTISING

24 ASA updates guidance on misleading environmental claims

26 The ASA's "Active Ad Monitoring" AI tool: nowhere to hide for green claims

27 New advertising laws to tackle illegal ads and protect children online

28 COMMERCIAL

28 Financial claim caught by clause excluding liability for loss of anticipated profits

30 Terminating software agreements when they fail to deliver software deliverables on time

32 Limitation of liability clauses in software development projects – financial caps

34 Pre-contractual documents – when heads of terms are legally binding and enforceable

"The new data bridge, an extension to the EU-US Data Privacy Framework (the DPF), will allow UK businesses to transfer personal data to certified US organisations without needing to put in place the typical safeguards (eg Standard Contractual Clauses) or performing a transfer risk assessment."

DATA

New data bridge to allow for UK-US data transfers

The question

How will the recently approved data bridge impact transfers of personal data from the UK to the US?

The key takeaway

The new data bridge, an extension to the EU-US Data Privacy Framework (the **DPF**), will allow UK businesses to transfer personal data to certified US organisations without needing to put in place the typical safeguards (eg Standard Contractual Clauses) or performing a transfer risk assessment.

The background

On 10 July 2023, the European Commission adopted an adequacy decision in respect of the DPF. US businesses may certify themselves with the DPF thereby committing to comply with certain GDPR-style privacy obligations (eg purpose limitation and data minimisation). Transfers from the EU to these US businesses may then be freely carried out without the need to establish safeguards like the EU Standard Contractual Clauses or carry out a transfer impact assessment. EU data subjects may obtain redress in the US for any non-compliant use of their personal data by national intelligence agencies through a new Data Protection Review Court. See previous coverage on this in our Summer Snapshots.

At the same time as this decision, the UK Government had indicated that it was working towards a data bridge that would "piggyback" on the DPF and allow for transfers to be similarly made from the UK to certified US businesses under the UK GDPR.

The development

On 21 September 2023, the UK Government published the Data Protection (Adequacy) (United States of America) Regulations 2023 for the UK Extension to the EU-US Data Privacy Framework. These regulations state that under the UK GDPR and the Data Protection Act 2018, the US is an adequate country for the purposes of data transfers from the UK provided: (i) the transfer is to a US business certified under the UK Extension to the DPF; and (ii) the recipient complies with its obligations under the DPF. The US Attorney has also designated the UK as a "qualifying state" under US Executive Order 14086 that implements arrangements to complement the DPF (see our Winter Snapshots 2022 for more details) and would allow UK data subjects to access the Data Protection Review Court.

Businesses may start relying on the data bridge from 12 October 2023. Note, however, that only US organisations subject to the jurisdiction of the US Federal Trade Commission or Department of Transportation may certify with the DPF. Businesses not subject to these regulators (eg banks, insurers, telecommunications providers) are not eligible.

The Department for Science, Innovation and Technology have said that they will continue to monitor the DPF and the data bridge.

Why is this important?

The new data bridge should significantly cut down time taken for businesses to agree and implement data transfers to the US by eliminating the need for transfer risk assessments and Standard Contractual Clauses. It should also provide UK data subjects with confidence that their data transferred to the US will be protected in line with requirements in their home country. However, there have been many indications that the DPF will be challenged and, if so, this could potentially affect the validity of the data bridge. For this reason, whilst these transfer mechanisms are in their infancy, businesses should consider adopting a "belts and braces" approach to its important contracts and agreeing Standard Contractual Clauses as a fallback should the DPF fall away.

Any practical tips?

Before initiating any transfer to a US entity under the data bridge, UK businesses must complete the following steps:

- check that the recipient is certified under the DPF list on the data privacy framework website (www.dataprivacyframework.gov/s/participant-search)
- check on that list that the recipient is separately signed up to the UK Extension to the DPF
- review the recipient's privacy policy linked to via the DPF list to confirm that it reflects the recipient's commitment to the DPF. If intending to transfer HR data, this needs to be specifically referred to in the privacy policy.

UK organisations should also update their own privacy policies and record of processing activities as necessary to reflect any transfers to US businesses pursuant to the data bridge.

Finally, keep an eye on the transfer of "sensitive" personal data under the UK Extension. This is because the definition of sensitive data under the DPF and the UK GDPR is the same on one level, being personal data revealing racial or ethnic origin; political opinions; religious beliefs; trade union membership; and data concerning health or an individual's sex life. However, the DPF definition is slightly narrower than the definition of special category data under Article 9(1) of the UK GDPR and, unlike the UK GDPR, does not include genetic data, biometric data (for the purpose of uniquely identifying a person) or sexual orientation data. Businesses intending to transfer such data should specifically identify the data as being sensitive to the US recipient to ensure it is properly protected under the DPF.

DATA

UK ICO and CMA release joint position paper on harmful design in digital markets

The question

What are the impacts of the ICO and CMA joint position paper on "Harmful Design in Digital Markets" and what action should companies take in light of its guidance?

The key takeaway

The ICO and CMA have provided clear guidance on what they jointly consider to be harmful design of digital products and services, in particular harmful nudges and sludge, confirmshaming, biased framing, bundled consent and predefined default settings. Empowering user choice and control and the testing and trialling of design choices is now a must for all businesses in the digital sphere, especially those likely to appeal to children.

The background

On 9 August, the UK Information Commissioner's Office (**ICO**) and the Competition and Markets Authority (**CMA**) published their joint position paper on harmful design in online markets. The paper focuses on the ways in which information and choices are presented to users (referred to as Online Choice Architecture or **OCA**) and its effect on user's choice and control over their personal information. The paper provides five examples of potentially harmful design practices which can risk infringing data protection, consumer and competition laws. It also offers guidance on good practices that companies are expected to adopt in relation to the design of their OCA.

This publication follows both the CMA's 2022 Discussion Paper "OCA: How Digital Design Can Harm Competition and Consumers" and the 2021 Joint Statement by the CMA and ICO "Competition and Data Protection in Digital Markets" and is the latest example of the ICO continuing the implementation of its strategy as set out in the ICO25 plan.

The development

The CMA and ICO highlighted in their 2021 Joint Statement that user choice and control over personal data are fundamental to data protection. OCA plays a major role in shaping users' decision making online. Poorly designed or misused OCA can undermine user data protection by causing users to share more information than they would otherwise volunteer and depriving them of meaningful control over their personal information.

The paper highlights the five potentially damaging OCA design practices which firms must avoid in order to ensure compliance with data protection, consumer and competition laws:

Harmful nudges and sludge

This is where a company makes it easy for users to make inadvertent or ill-considered decisions ("harmful nudge") or creates the same effect by creating excessive or unjustified friction which makes it difficult for users to get what they want or do as they wish ("harmful sludge"). For example, using a cookie pop-up which contains an option to accept all non-essential cookies, but which does not contain an equivalent option to reject them. The use of harmful nudges and sludge may infringe both Article 5(1)(a) of the GDPR and Regulation 6 of PECR. It is expected as a minimum that users must be able to refuse non-essential cookies with the same ease as they can accept them. Where an accept all option is offered, there must be an equivalent option to reject all and both options must be presented with equal prominence.

Confirmshaming

Applying pressure or shaming users into doing something by making them feel guilty or embarrassed if they do not, eg through the use of language which suggests that there is a good or a bad choice. The example provided is a pop up which asks users to provide an email address and phone number in exchange for a discount which includes a reject button which states "Nahh, I hate savings". The use of Confirmshaming is likely to infringe Article 5(1)(a) of the GDPR.

Biased framing

Presenting choices in a way that either emphasises the supposed benefits of a particular option in order to make it more appealing to the user ("positive framing") or alternatively the negative consequences of an option to dissuade the user from selecting the option ("negative framing"). This can highly influence users' decision making and impede users' ability to assess information independently and accurately. Biased framing may infringe Article 5(1)(a) and Article 7 of GDPR. Additionally, if the practice is misleading to users, it may breach Regulation 3 and 5-7 Consumer Protection from Unfair Trading Regulations 2009.

Bundled consent

Requesting that users consent to their personal information being used for several separate purposes or processing activities via a single consent option. This can make it harder for users to control what their data is used for. The effect of this is that consent is unlikely to be specific or informed and as such risks infringing Article 5(1)(a) GDPR.

Default settings

Where a predefined choice of settings is provided to users which they then must actively take steps to amend. Users can be deterred from amending default settings due to the difficulty of altering them. The example provided refers to social network post settings, which are set by default to being public (ie the post is viewable by everyone with an account on the platform). The user would be required to take steps to amend the settings to make their content more private. Most users are unlikely to do this and therefore this increases the risk of their personal data being available more widely and used without their knowledge or understanding. Where a company's settings are by default intrusive it will be difficult for them to justify such an approach. This potentially risks infringing Article 5(1)(a) and 5(1)(c) of the GDPR and Regulation 6 of PECR. If users are likely to be children, settings should be set to "high privacy" by default following the ICO's Age Appropriate Design Code (unless the business can demonstrate a compelling reason for a different default setting taking into account the best interests of the child).

Why is this important?

The positions outlined in the paper are based on existing guidance and publications by the ICO and CMA and do not supersede or reopen existing legal guidance. The paper emphasises that companies are expected to make improvements to their design of OCA in light of the guidance provided.
If companies fail to meet expectations, the ICO makes it clear that that it will take formal enforcement action where it is deemed necessary to protect people information and privacy rights, particularly where this involves risks or harms for people at risk of vulnerability (including children). Additionally, the CMA is currently investigating both the Emma Group and the Wowcher group in relation to the use of wider OCA practices.

Any practical tips?

Well-designed OCA can help users to make informed choices which are aligned with their goals, preferences and best interests with regard to the use of their personal information. To achieve this the ICO and CMA expect that companies have regard to the following factors which should be used to guide their OCA design:

- users should be placed at the heart of design choices: OCA and default settings should be built around the interests and preferences of users
- design should empower user choice and control: users should be helped to make effective and informed choices regarding their personal data and put users in control of how their data is collected and used
- design choices should be tested and trialled: testing should be carried out to ensure design choices are evidence based
- compliance with data protection, consumer and competition law: companies should consider whether OCA practices could be unfair to users or anti-competitive.

Where products or services are likely to accessed by children, companies should also ensure that they adhere to the standards provided in the ICO's Age Appropriate Design Code and follow the ICO's Children's Code Design Guide.

The ICO and CMA welcome further participation and feedback from interested stakeholders. A joint ICO and CMA workshop on good practices for the design of privacy choices online is scheduled to take place during the Autumn.

DATA

UK ICO publishes joint statement on data scraping and the protection of privacy

The question

What are the key privacy risks that the UK Information Commissioner's Office (**ICO**) expects organisations to consider when hosting publicly accessible personal data and how can those privacy risks be mitigated?

The key takeaway

The joint statement is an invaluable blueprint on the steps that social media companies and other websites should take to protect the publicly available personal data which they host.

The background

On 24 August 2023, the ICO, along with eleven other national data protection authorities, published a "Joint Statement on Data Scraping and the Protection of Privacy". The joint statement sets out a series of recommendations outlining how social media companies (**SMCs**), and operators of websites hosting publicly accessible personal data (other websites), can ensure that they adequately protect personal data in accordance with their obligations under data protection laws. The joint statement encourages SMCs, within 1 month of the statement's issuance (24 September 2023), to provide feedback on it to their national data protection authority. Where SMCs and other websites do decide to provide such feedback on the joint statement, they are also encouraged to demonstrate their compliance with the expectations outlined therein.

Given this call for feedback, it appears that the recommendations contained within the joint statement are intended to form the basis of a guidance note which SMCs, and other websites, should follow.

The development

In the joint statement, it is confirmed that, while individuals and organisations which scrape publicly accessible personal data are responsible for ensuring that they comply with data protection laws, SMCs and other websites also have data protection obligations with respect to third-party scraping from their publicly accessible websites.

The joint statement also provides that scraped personal data can be exploited for numerous purposes. It follows that SMCs and other websites must carefully consider the legality of different types of data scraping in their jurisdictions so that they can implement measures to protect against data scraping which is unlawful.

Below is a summary of the key privacy concerns raised in the joint statement and the national data protection authorities' recommendations for how they may be mitigated:

Key privacy concerns

The joint statement stresses that many national data protection authorities are seeing increased reports of mass data scraping from SMCs and other websites. These reports have raised concerns with respect to how this personal data is being used. The key privacy concerns identified by the national data protection authorities in relation to mass data scraping are:

- **targeted cyberattacks** – where scraped identity and contact information is posted on hacking forums so that it can be used by malicious actors in social engineering or phishing attacks
- **identity fraud** – where scraped personal data is used to submit fraudulent loan or credit card applications, or to impersonate an individual by creating fake social media accounts
- **monitoring, profiling and surveilling individuals** – where scraped personal data is used to populate facial recognition databases and provide unauthorised access to authorities
- **unauthorised political or intelligence gathering purposes** – where scraped personal data is used by foreign Governments or intelligence agencies for unauthorised purposes.
- **unwanted direct marketing or spam** – where scraped personal data, including contact information, is used to send bulk unsolicited marketing messages.

In addition to the above, the joint statement also provides that where data scraping leads to a loss of control by an individual over their personal data, either without their knowledge or which causes the personal data to be used in a way in which that individual would not expect, this is of particular concern as it undermines the trust which individuals have in SMCs and other websites, and has the potential to have a detrimental impact on the digital economy.

Steps SMCs and other websites should take to combat unlawful data scraping

The joint statement emphasises that because techniques for data scraping and extracting value from publicly accessible personal data are constantly evolving, SMCs and other websites need to take a dynamic approach to data security. To demonstrate this, the joint statement provides that SMCs and other websites should implement proportionate multi-layered technical and procedural controls aimed at mitigating the privacy concerns listed above, namely:

- **designate a team** – assign specific roles to assist in the identification and implementation of controls to protect against, monitor for, and respond to, data scraping activities
- **rate limiting** – consider capping the number of visits which one account can make to another account per hour or per day, thereby limiting access where unusual activity is detected
- **monitoring** – track how quickly and aggressively a new account searches for other users. If abnormally high activity is detected, this could be an indicator of unacceptable usage
- **identify patterns** – take steps to detect data scraping by identifying patterns which are specific to "bot" activity
- **block "bots"** – make use of CAPTCHAs and block IP addresses where data scraping activity is identified
- **legal action** – where data scraping is suspected or confirmed, take legal action to stop it or enforce terms and conditions which prohibit it eg by requiring the deletion of scraped personal data
- **notification** – where the data scraping constitutes a data breach, notify affected individuals and supervisory authorities where required under data protection laws.

The joint statement also provides that SMCs and other websites should inform their users about the steps they have taken to protect against unlawful data scraping and enable their users to engage with their platforms in a manner which protects user privacy. This can be achieved by actions such as assisting users to make informed decisions about the sharing of their personal data, or raising awareness about the privacy settings which are available to them.

In addition, SMCs and other websites are encouraged to routinely stress-test their procedural controls to ensure they remain effective and analyse any data scraping incidents, to identify areas in need of improvement.

Steps users can take to combat unlawful data scraping

The joint statement sets out the steps which users can take to empower themselves to better protect their personal data. The steps outlined are:

- **review** – read the information provided by SMCs or other websites about how they share users' personal data (eg the privacy policy)
- **limit sharing** – consider limiting the amount of personal data, particularly sensitive personal data, which is posted online
- **manage privacy settings** – use privacy settings to control the personal data which is shared and limit the personal data which can be made publicly accessible
- **consequences** – be aware that despite the tools which SMCs and other websites use to delete or hide personal data, it can live forever on a website if it has been indexed, scraped, and onward shared.

In addition, the joint statement provides that where users are concerned that their personal data may have been unlawfully scraped, they can contact the SMC or other website, and if dissatisfied with the response, file a complaint with their national data protection authority.

Why is this important?

The joint statement is another demonstration by the ICO of its commitment (under its ICO25 strategic plan) to safeguarding vulnerable persons while addressing recent global industry concerns on the utilisation of generative AI technology (such as those which arose during the Clearview AI investigation – see our Autumn 2022 Snapshot).

While the joint statement recognises that there are steps which individual users can take to combat the risk of unlawful data scraping, many of the obligations outlined in the joint statement remain with SMCs and other websites. Even though the joint statement requires SMCs and other websites to implement multi-layered technical and procedural controls, it also clearly sets out the key privacy concerns of several national data protection authorities. This presents an opportunity for SMCs and other websites to effectively address and mitigate those concerns and reduce the risk that their platform, website or service will become the subject of unlawful data scraping, and by extension, regulatory enforcement action.

Any practical tips?

The expectations in this joint statement set out key areas for SMCs and other websites to focus on with a view to ensuring that they protect the personal data which is publicly accessible on their platforms, websites, or services from unlawful data scraping.

By clearly setting out their expectations, national data protection authorities have provided SMCs and other websites with an invaluable future-proofing tool which they can use to ensure that they remain compliant with data protection laws. As such, when reviewing any internally or externally facing policies, plans, and Wikis, these organisations should review them in conjunction with the concerns raised, and the mitigation steps outlined, by the national data protection authorities in the joint statement.

Given the importance of trust in the regulatory as well as user relationship, SMCs and other websites may well want to consider providing feedback to the ICO on the joint statement to set out clearly how they comply with the expectations outlined therein.

UK ICO publishes draft biometric data and technologies guidance for public consultation

The question

What are the key considerations which the Information Commissioner's Office (**ICO**) proposes organisations should be aware of when implementing biometric recognition systems?

The key takeaway

The ICO's draft guidance on biometric data and biometric technologies (**Draft Guidance**) outlines the ICO's proposal for how it will regulate the use of biometric data and biometric recognition systems in the future. It follows that any organisation with a vested interest in the development and regulation of biometrics should review the Draft Guidance and consider providing feedback to the ICO's public consultation by 20 October 2023.

The background

On 18 August 2023, the ICO published the first phase of the Draft Guidance and opened it up to public consultation. The Draft Guidance aims to build on the ICO's two previous reports on biometric technologies which were released on 26 October 2022. The ICO's two reports entitled: "Biometrics: Insight" and "Biometrics: Foresight", examined recent trends and developments in biometric technologies and explored the opportunities and challenges which various sectors (eg finance, wellness, and education) could face over the course of the next five to seven years due to the predicted increase in their use of biometric technologies. The reports raised concerns about the impact that the increased use of biometric technologies could have on the ability of these sectors to comply with the fundamental principles of UK GDPR.

The reports also highlighted key areas which required further clarification with respect to biometric data and biometric technologies including definitions and terminology, the management of "high risk" biometric systems, and the processing of "ambient data".

The development

The first phase of the Draft Guidance examines key data protection concepts, explores "biometric recognition systems" and sets out the key data protection requirements which the ICO expects organisations to consider when implementing biometric recognition systems.

Key data protection concepts

In order to determine whether "personal data" can be categorised as "biometric data" under UK GDPR, the Draft Guidance provides that "personal data" is only "biometric data" where it:

- relates to someone's behaviour, appearance, or observable characteristics (eg their face, fingerprints, or voice)
- has been extracted or further analysed using technology (eg an audio recording which is analysed using software to detect tone or pitch, and
- allows the individual to be uniquely identified (recognised) from it.

The Draft Guidance notes that, even where the data being processed does not meet the above criteria, it is still necessary to determine if it constitutes "personal data", as data protection requirements will still apply in that instance. The Draft Guidance also draws a distinction between the definitions of "biometric data" and "special category biometric data". "Biometric data" allows an individual to be uniquely identified from it, whereas "special category biometric data" is when biometric data is used for the purpose of uniquely identifying an individual.

According to the Draft Guidance, this means that, where the purpose (ie the intention) behind processing personal data related to an individual's characteristics is to uniquely identify that individual (eg by comparing it to other individual's biometric data as part of an identification or verification process), then it constitutes "special category biometric data".

Biometric recognition systems

The Draft Guidance sets out what it means when referring to "biometric recognition systems". It states that "biometric recognition" is where an individual's biometric data is used for identification or verification purposes. Further, the Draft Guidance provides that:

- **identification** refers to a one-to-many matching process where the biometric data of one individual is compared to that of many to find a match, and
- **verification** refers to a one-to-one matching process where the biometric data of one individual is compared against a stored biometric record to verify that they are who they claim to be.

Given the above definitions of "biometric data" and "special category biometric data", the Draft Guidance provides that, whenever an organisation uses a biometric recognition system, it will:

- initially be processing personal data
- then it will, by default, be processing biometric data as the personal data collected will obey the three-pronged criteria under "Key data protection concepts" above, and
- lastly, it will process special category biometric data from the moment it intends to use the biometric data it has collected to perform an identification or verification process.

Key data protection requirements

The Draft Guidance details the data protection requirements which controllers and processors must comply with when processing biometric data and special category biometric data. In particular, the Draft Guidance notes that, when using this data:

- data protection laws must be complied with, and this must be able to be demonstrated
- a data protection by design approach must be adopted such that biometric data is protected in all systems, and only processors which provide sufficient guarantees of their adoption of data protection by design, should be utilised
- a data protection impact assessment (**DPIA**) should be carried out before using a biometric recognition system as it is highly likely that its use will result in a high risk to the rights and freedoms of individuals, and
- it is likely that the only valid condition for processing special category biometric data is explicit consent, but this will depend on the specific circumstances and justification being relied upon.

To assess whether an organisation needs to conduct a DPIA, the Draft Guidance refers to the ICO's "examples of processing likely to result in high risk". Further, when considering how to adopt a data protection by design approach, see our analysis of the ICO's guidance on "privacy in the product design lifecycle" in our Summer 2023 Snapshot.

Why is this important?

The Draft Guidance is another demonstration of the ICO's commitment, under its ICO25 strategic plan, to empowering organisations to use information responsibly, enabling them to invest and innovate in the adoption of new technologies. As this is the first phase of the ICO's guidance on biometrics, and it is open to public consultation, this presents organisations with a vested interest in biometrics with an important opportunity to feed into how the ICO will regulate the use of biometric data and biometric recognition systems in the future. Organisations can respond to the consultation by completing the ICO's MS Forms survey, or emailing their responses to biometrics@ico.org.uk. The consultation is open until 20 October 2023.

Any practical tips?

All organisations which are using, or considering the use of, biometric recognition systems should consider the key data protection requirements flagged by the ICO in the Draft Guidance. In tandem, it is worth reflecting on the importance of data protection by design, and the ICO's new "Innovation Advice Service". While this service is currently in Beta, it provides a forum for organisations which are trying new or innovative steps with personal data, to ask the ICO specific questions with a view to solving any data protection issues that are holding up their product's or service's development. Lastly, it is important that those considering implementing innovative biometrics technologies take a holistic view of the technologies they are looking to implement, and consider these in light of the ICO's other guidance such as the ICO's guidance on AI and data protection (see our Summer 2023 Snapshot).

New development: updated ICO guidance on "likely to be accessed by children"

Following consultation, the ICO has updated its guidance "Likely to be accessed' by children – FAQs, list of factors and case studies". The guidance supports Information Society Service (ISS) providers to ascertain whether the service they provide falls within scope of the Age Appropriate Design Code (the Code). ISS providers should review the guidance, which includes a checklist, FAQs and context specific case studies (such as social media and gaming), to assess scope and compliance with the Code.

If the ISS provider concludes its service is "likely to be accessed by children" and the service is not appropriate for children, it must apply age-based measures to restrict access to the service. If the ISS provider concludes children are not likely to access the service, the reasoning for and evidence in support of this conclusion must be documented.

For our coverage on the consultation, see our Summer 2023 edition of Snapshots.

DIGITAL

Ofcom publishes new report on video-sharing platforms

The question

What does Ofcom's new report, entitled "Regulating Video-Sharing Platforms" (**VSPs**), consider good practice in respect of user policies and terms and conditions of video sharing platforms?

The key takeaway

Ofcom's new report sets out its observations and recommendations following its review of six VSPs' user policies and T&Cs. Key examples of good practice highlighted by Ofcom include: clarity and accessibility; specifying which content is prohibited; comprehensive guidance for internal moderators; explaining the consequences of breach; and keeping T&Cs and policies under review. Ofcom is expected to publish further reports on VSPs over the coming months.

The background

The Communications Act 2003 (the **Act**) introduced Ofcom as the regulator of telecommunications, radio, post and television broadcasting. Developments in the media and communications markets, including the rise in user-generated content, led to the EU's Audio-Visual Media Services Directive in 2018, a subsequent amendment to the Act and the start of a VSP regulatory regime.

In November 2020, Ofcom's powers were extended to include the regulation of VSPs. Ofcom's role is to ensure that VSP providers have appropriate safety measures in place to protect users from harmful online videos. Relevant videos include content which may impair the development of children, incite violence and hatred, or which display acts of terrorism, child sexual abuse, racism or xenophobia.

VSP providers are legally obliged to notify Ofcom of their platform if the VSP meets specific legal criteria. At the time of writing, 20 VSPs, including Snap, Twitch and TikTok, are notified to Ofcom as being caught within the UK VSP regulatory regime.

The development

On 9 August 2023, Ofcom published its first 2023 report, "Regulating Video-Sharing Platforms", which sets out observations and recommendations on VSPs' T&Cs and user policies. The report follows a review of six notified VSPs' policies, namely Snap, TikTok, Twitch, BitChute, Brand New Tube, and OnlyFans, and the different approaches taken to implement the policies.

Ofcom's research identified several issues with current T&Cs ranging from poor accessibility and readability to a lack of clarity on the consequences of breach. The report also raises concerns about the quality of internal training and guidance for moderators on how to enforce T&Cs effectively.

Against this background, the report sets out examples of good practice for VSP providers to help them improve their approach to writing and implementing T&Cs. In summary, it recommends that:

- **T&Cs should be clear, easy to locate and accessible** – this may mean tailoring the language or location of the T&Cs on the platform to match the likely comprehension level of the user. It may also mean exploring different techniques to measure how users engage with and understand T&Cs
- **T&Cs should specify which type of content is prohibited** – T&Cs should be clear about the type of videos which will likely cause harm, particularly to children. They should indicate circumstances where content should be tagged as being sensitive, mature or graphic
- **moderators should have comprehensive internal guidance to help them apply T&Cs effectively** – Ofcom recommends that VSP providers provide moderators with definitions of key terminology, audio and/or visual case studies and detailed guidance to demonstrate how to assess a potential violation of the T&Cs and to determine appropriate responses to harmful content
- **T&Cs should clearly explain the consequences of any breach** – this may include setting out the content which is, and is not, permitted on the VSP and the range of potential action that could be taken against a user
- **VSP providers should keep T&Cs and internal guidance under review** – Ofcom recommends taking a regular and proactive approach to conducting reviews and taking a reactive approach when a new risk emerges. The development of processes for reviewing and testing polices should involve experts and should strike the correct balance between user safety and users' rights. Changes to guidance and T&Cs should be communicated in a timely manner.

Ofcom is expected to publish further reports on VSPs over the coming months, including a report on VSPs' measures to protect children and Ofcom's plan for the next phase of the VSP regime.

Why is this important?

The report highlights the importance Ofcom places on T&Cs and how moderators are implementing T&Cs to protect users from online harms. The examples of good practice provide VSP providers with insight into the potential safety issues which may arise from their own user policies and what providers should be doing by way of preventative action. The VSP regime will eventually be replaced by an all-encompassing online safety regime when the Online Safety Bill receives Royal Assent (as discussed in our Spring 2023 edition of Snapshots). Ofcom will become a key regulator under the regime and has confirmed that it will use its experience of VSP regulation to inform the approach taken to regulating online safety.

Whilst the regimes place different obligations onto service providers, the recommendations help VSPs prepare for compliance with future duties under the new online safety regime.

Any practical tips?

VSP providers should take a holistic approach to reviewing the T&Cs on their platforms to ensure that they are clear, accessible and specific. Where necessary, providers should consider whether to involve internal and/or external experts in the policy development process when preparing T&Cs and guidance for moderators.

The examples of good practice set out in the report are a helpful starting point for VSPs when considering improvements to user safety whilst still striking the right balance with users' ability to create, upload and view content on platforms. With the Online Safety Act round the corner, and Ofcom about to get its new powers, now is the time to pay particular attention to its recommendations.

Amazon appeals its EU designation as a VLOP

The question

What are the implications of Amazon's recent legal challenge against its designation as a "Very Large Online Platform" (**VLOP**) by the European Commission under the new Digital Services Act (**DSA**)?

The key takeaway

Following Amazon's challenge regarding its designation, the EU's General Court is set to issue a decision as to whether Amazon is a VLOP and to what extent it is required to comply with certain onerous obligations under the DSA. This decision will be of key interest to other businesses designated as VLOPs currently and in the future.

The background

The EU has recently passed the Digital Markets Act (**DMA**) and the DSA which together create a single set of rules applicable to digital services across the EU. See our ongoing coverage on the DSA and DMA in previous editions of Snapshots.

The DSA imposes far-reaching responsibilities on "very large online platforms", which it classifies as those with more than 45m active users per month. 19 platforms have so far been designated as VLOPs, including the Apple app store, Booking.com and Wikipedia. Rules that apply specifically to VLOPs include auditing, monitoring and data sharing with authorities to reduce systemic risk in the EU.

The development

On 5 July 2023 Amazon filed an appeal at the EU's General Court against its ruling as a VLOP. In its legal challenge, Amazon said that the VLOP rules, aimed at safer content and dissemination of information, are more appropriate for social media and search engines than for retailers. Amazon also asserts that it has been unfairly singled out, highlighting the fact that it is not the largest online retailer in any EU state but that none of its rivals have been designated as VLOPs.

Amazon's challenge follows a similar challenge by German online retailer Zalando, which is also pursuing legal action against its classification as a VLOP. Like Amazon, Zalando pointed out that the nature of its retail business means it does not pose a risk in terms of spreading harmful or illegal content from third parties. Zalando also alleged inconsistencies with the methodology used to calculate user numbers, which it argues have been significantly overestimated.

Most recently, the General Court agreed to suspend the obligation on Amazon to provide information on ads in a repository, which would otherwise have gone into effect on 25 August 2023. Amazon is still waiting for a final decision from the court as to whether it will remain designated as a VLOP.

Why is this important?

It remains to be seen whether Amazon's push-back on its classification as a VLOP will be successful. Or alternatively if the court adopts a more flexible approach to applying the DSA with certain obligations being waived but others upheld. If the classification is successfully resisted entirely, Amazon will still be subject to the wider DSA rules. This (and Zalando's) appeal will be an interesting test of the new rules for businesses that provide digital services.

Any practical tips?

All providers of online platforms and search engines have already been subject to certain obligations (eg reporting number of active users) since the DSA came into force in November 2022. VLOPs and Very Large Online Search Engines (**VLOSEs**) will separately need to comply with their own specific obligations within four months of their designation by the European Commission. The remaining provisions in the DSA will then come into force in February 2024, by which time all businesses within scope of the DSA must implement necessary measures to meet the requirements applying to their business. Any business that considers it falls within the DSA's reach should prepare for compliance by this date. Separately, designated VLOPs and VLOSEs might well wish to track Amazon's appeal through the courts, as any final decision may be helpful in clarifying the application of the DSA to their business operations.

Thumbs-up if you agree: emoji can represent contractual agreement according to Canadian judge

The question

Can an emoji be used to accept and form a legally binding contract?

The key takeaway

A Canadian court has decided that a thumbs-up emoji was used to validly accept and create a legally binding contract. This decision shows that using emojis and informal messaging tools to conduct business poses a risk that contracts could be accepted when they may not be intended to be.

The background

On 8 June 2023, the Canadian provincial court of Saskatchewan ruled that Mr Chris Achter had used a thumbs-up emoji to validly agree a contract to deliver 86 tonnes of flax for a price of $669.26 per tonne.

The court found that Mr Achter's use of the thumbs-up emoji meant that he had accepted the contract according to an "uncontested" process that both parties had previously used to agree similar contracts. Mr Achter had previously accepted contracts by texting succinct phrases, such as "looks good" and "yup", to confirm potential orders after receiving an initial "text blast" and phone call setting out the proposed terms.

The development

Agreeing by emoji

The court reached its conclusion by deciding that the meaning of the thumbs-up emoji should be considered according to what an "informed objective bystander would understand" rather than the subjective intention of Mr Achter in sending the thumbs-up, or the understanding of the person receiving the emoji. This included considering that a thumbs-up emoji is now widely defined in dictionaries to "express assent, approval or encouragement in digital communications" and finding that the emoji was "an action in electronic form" capable of being used to accept legally binding contracts according to Canadian legislation.

Emojis as signatures

The court also found that a thumbs-up emoji, whilst non-traditional, was a valid electronic signature under Canadian legislation and fulfilled the two purposes of signatures, namely, to identify the person signing and to express acceptance of a contract. This recognition follows previous Canadian case law which similarly found that emails could stand as signatures that can legally bind contacts.

The court also stated that it should not "attempt to stem the tide" of modern-day use of technology to accept contracts when it was asked during the proceedings to consider whether this decision would open the "flood gates" for further claims addressing the meaning of many other emojis, such as the fist-bump and handshake emojis.

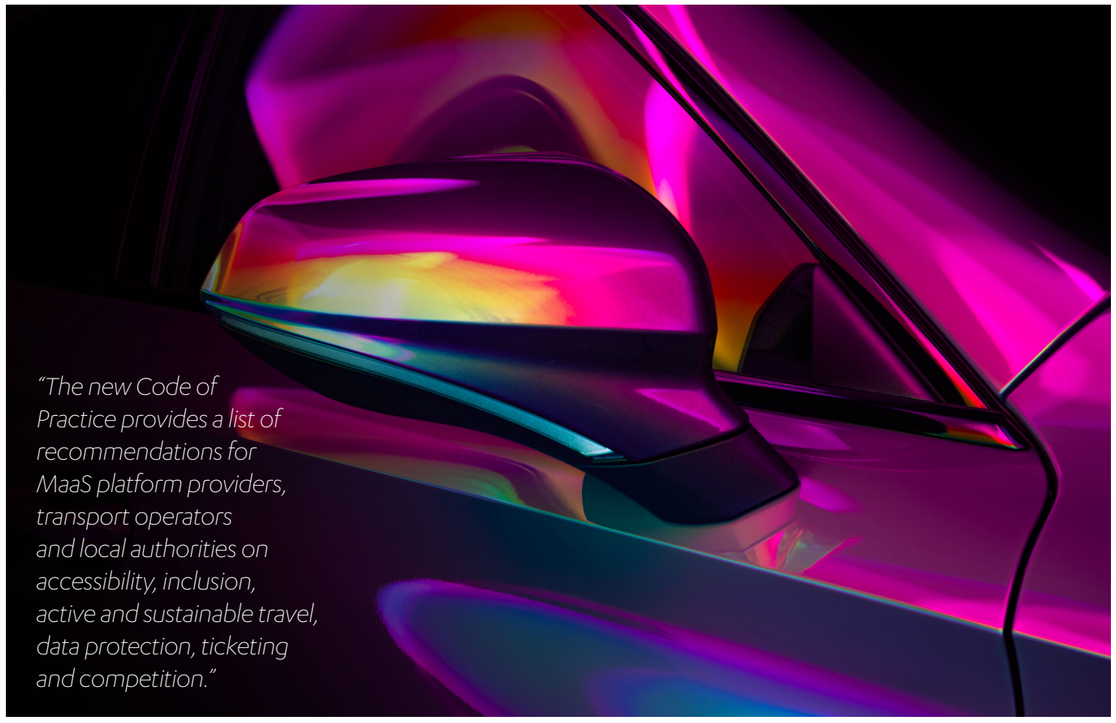
Why is this important?

Whilst this decision will not bind courts in England and Wales, similar decisions are likely to emerge in other jurisdictions that also feature legislative regimes that are attempting to keep up with emerging technologies and the different ways they are used in digital commerce. Businesses may be concerned by the uncertainty this presents and should consider whether their employees' actions could unintentionally create legally binding contracts.
This concern is likely to be exacerbated by the normalised use of emojis throughout internal and external workplace communications, the variety of messaging and communication platforms that remain in the post-Covid world of remote work, and when business is conducted across both personal and business devices.

Any practical tips?

Businesses should be aware of this decision and the possibility for courts across various jurisdictions to make similar decisions. They should be mindful of the risks inherent in using unclear and informal methods of agreeing contracts, as well as have a thorough understanding of the extent to which their contractual negotiations may be being made over digital messaging platforms. It goes without saying that establishing clear procedures for agreeing contracts, and ensuring this is followed by all employees, is a sensible precaution for any business.

UK Government publishes first MaaS (mobility as a service) Code of Practice



The question

Why is the UK Government's new code of practice for "mobility as a service" so useful for MaaS platforms?

The key takeaway

The new Code of Practice provides a list of recommendations for MaaS platform providers, transport operators and local authorities on accessibility, inclusion, active and sustainable travel, data protection, ticketing and competition. Although the guidance is voluntary, those involved in the deployment of MaaS technologies should review the Code to check that they are adopting best practice and to potentially improve the quality of their users' experience.

The background

The UK Government has identified that the emergence of various online platforms and mobile apps using data analytics and digital capabilities to provide seamless, multimodal transport planning information has made transport planning easier for consumers and businesses. Such technological solutions have been described as "mobility as a service" (MaaS), defined by the Government as "the integration of various modes of transport along with information and payment functions into a single mobility service" and typically uses innovation to simplify the planning and payment processes associated with making journeys. In 2022, the UK Government's Department for Transport (DfT) ran a consultation on a MaaS code of practice to better understand how it could support this emerging industry. The consultation was its third consultation on MaaS, commissioned as part of various commitments made by the Government surrounding its overarching plan to decarbonise the British transport system.

The development

Following the responses to its consultation, the DfT introduced a Code of Practice for MaaS in August 2023, which is primarily aimed at organisations producing MaaS schemes, MaaS platform providers, transport operators and local authorities. Under the Code, the DfT makes 34 recommendations to address issues identified through public consultation, categorised as below:

- **improvement of user accessibility and inclusion** – providers should consider accessibility requirements and the inclusion of all platform users with protected characteristics. These considerations apply across the user experience whilst interacting with a platform, when suggesting routes for users and when testing platform features. The needs of users in rural areas should also be taken into account, particularly where internet connectivity could be an issue
- **enabling active and sustainable travel** – platforms should provide users with information regarding CO2 savings that could be made by taking alternative modes of transport and should display health benefits (such as calories burned) associated with taking more active routes that involve walking or cycling
- **improvement of ticketing experience** – providers, transport operators and local authorities should collaborate to offer a consistent ticketing experience that is convenient and provides users with value for money
- **protecting consumers** – providers should offer transparent and consistent information for multimodal journeys and should inform users of relevant points of contact for feedback on their journeys, claiming compensation for delays or cancellations or requesting ticket refunds. Platforms should also make clear where a journey, mode, or operator is being promoted or prioritised as part of a commercial arrangement. Additionally, all organisations should ensure user personal data is processed in accordance with data protection legislation and that a data protection impact assessment is conducted prior to the processing of high-risk data
- **promoting a competitive environment** – commercial agreements entered into should be fairly priced, should avoid exclusivity of services and should encourage data sharing. MaaS apps should also show all available public transport options and services in an area.

Why is this important?

There are various technical, commercial and regulatory challenges associated with the development of MaaS solutions. The DfT supports the growth of the MaaS industry which has societal benefits, including the potential to improve the British transport network experience for passengers and aligns with its broader strategy to promote more active and sustainable ways to travel. According to the DfT, using a code of practice approach at this stage ensures that the industry is supported without the imposition of seemingly premature regulation which could negatively impact innovation. The DfT also believes that the deployment of the Code of Practice will increase its understanding of where regulation might be needed in future.

Any practical tips?

Although the Code of Practice contains voluntary guidance, all stakeholders involved in MaaS products and schemes would do well to review it and look to implement any improvements in line with its recommendations. The content should be regularly reviewed as the DfT will be updating the guide to reflect the latest developments within the industry. Keeping in line with the guidelines will help platforms comply with any regulations which may be introduced down the line.

European Parliament publishes draft report on the addictive design of online services

The question

How is the European Parliament looking to combat the exploitation of psychological vulnerabilities through the addictive design of online services?

The key takeaway

The European Parliament has published a draft report (the Report) on the addictive design of online services and consumer protection. They are concerned with the harmful impact of internet-use-related addiction and have invited the European Commission to regulate online services to curtail their addictive nature and prevent platforms from using addictive design features.

The background

The European Parliament has issued the Report in the wake of the comprehensive digital services package passed by European legislators as well as the heightened focus on consumer protection in the region. The Rapporteur was Dutch MEP Kim van Sparrentak who presented the own-initiative Report at a recent meeting of the Committee on the Internal Market and Consumer Protection. The Rapporteur was alarmed that platforms and tech companies exploit psychological vulnerabilities and called for EU legislation protecting users from harm by addictive design.

The development

The Report contends that platforms are designed to be as addictive as possible, using "psychological tricks" to keep users engaged. Some digital services have been found to exploit psychological vulnerabilities (similar to those involved in online gambling addictions) and deploy "gamification" techniques. The Report refers to a number of addictive design features, including infinite scroll, pull-to-refresh page reloads, auto-play functions and personalised recommendations (amongst others). The Report concludes that these addictive design techniques have created the issue of "internet-use-related addiction".

Of particular concern to the European Parliament is the effect of digital addiction on children and young people. The Report finds that 16–24-year-olds spend an average of seven hours per day online, that "one in four children and young people display 'problematic' or 'dysfunctional' smartphone use" and "the rise in mental health problems in adolescents might be related to excessive social media use".

The Report calls on the European Commission (the **Commission**) to legislate on addictive design. Specifically, the European Parliament have requested a review of the Unfair Commercial Practices Directive (**UCPD**), the Consumer Rights Directive and the Unfair Contract Terms Directive, with a particular focus on addictive and manipulative design of online services. They have requested that the Commission prohibits the most harmful practices, as these are not currently blacklisted in the UCPD or other EU legislation. They further call on the Commission to impose a fair/neutral design obligation on platform providers.

In addition, the Report specifically calls for a ban on interaction-based recommender systems, particularly hyper-personalised systems which are designed to be addictive and keep users on the platform for as long as possible. Further proposals include a digital "right not to be disturbed", a list of good practices of design features, and a specific focus on the impact of addictive design features on children and young people.

Why is this important?

The Report indicates a possible shift in attitudes towards online services with the idea that these may be as addictive as other products that are subject to legislative controls (eg tobacco and HFSS food and drink). If the proposals are adopted, these could have wide-reaching consequences, as the Report suggests controls on not just social media sites but a number of other online service platforms, including streaming services, dating apps and online shops. It's too early to call whether the proposals in the Report will carry through to legislation, and whether all types of online service will be treated the same for regulatory purposes. Curtailing the addictive features within online platforms will also significantly impact advertisers who benefit from users remaining on a platform for as long as possible.

Any practical tips?

It will be some time before any of the Report's proposals are reflected in regulations, if at all. However, considering the potential impact on platforms, businesses should be aware that these discussions are taking place in Brussels. Businesses should track the progress of this Report and be ready to take proactive steps, including participating in any consultations held by the EU institutions. It may also be prudent to consider if more can be done through product and service design to assist users who wish to have more control over their screen time and platform usage.

The Retained EU Law (Revocation and Reform) Act 2023 – a happy new year?

The question

How will the Retained EU Law (Revocation and Reform) Act 2023 (the **Act**) impact UK businesses?

The key takeaway

31 December 2023 will mark the beginning of the UK's divergence from EU law. Under the Act, around 600 pieces of legislation across 16 Government departments will be revoked and some key EU law principles will no longer be applicable. The Act represents more of a post-Brexit tidying up exercise than a wide-scale reform as had initially been planned, meaning more certainty for businesses as the legislation that is due to be revoked has now been specified. However, further change is on the horizon as the Government looks to redefine the legal landscape post-Brexit and businesses should stay alert to wider reform plans.

The background

From September 2022, when the Act was first introduced into parliament as a bill, the Government faced mounting pressures and waves of criticism from a broad spectrum of people, companies, and bodies about its approach to post-Brexit legislation. In bill form, the Government had initially planned to sunset all retained EU law, meaning thousands of pieces of EU legislation on the statute books on 31 December 2023 would have been automatically repealed unless actively assimilated into UK law by MPs. These plans, originally dubbed the "Brexit bonfire" would have seen seismic changes to consumer law, employment law and product regulation through the proposed revocation of the Consumer Protection from Unfair Trading Regulations 2008, Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (**CCRs**), Business Protection from Misleading Marketing Regulations 2008, Weights and Measures (Packaged Goods) Regulations 2006 and the Commercial Agents Regulations 1993, for example.

The development

The Act received Royal Assent in June 2023. Following a U-turn by the Government, the Act will facilitate more of a tidying-up exercise, not a "bonfire". Now, under the Act almost 600 pieces of legislation, which are considered obsolete or no longer needed, will be revoked on 31 December 2023. All other retained EU law will remain in force unless and until reformed by the relevant Government department (see the Government's Keeling Schedule for more detail, as reported in our Summer 2023 Snapshots edition).

Why is this important?

Whilst the Act will not implement sweeping deregulation at the end of the year, businesses should keep an eye on the Government's wide-reaching programme of reforms. In particular, the Digital Markets, Competition and Consumers Bill will represent substantial reform due to enhanced consumer protections, particularly around subscription services (again, see our Summer 2023 Snapshots edition for more on this) as well as the Government's product safety review, which launched at the start of August 2023.

Any practical tips?

Compliance departments should reflect on the list of regulation to be revoked and assess the potential consequences relevant to their operations. Businesses operating in the food, agricultural products and chemicals industries may wish to further assess the impact of the Act, as there are a number of patchwork EU regulations which relate to these industries being revoked.

CONSUMER

UK Government u-turns on phasing out “CE” product safety marking

The question

What product safety marks can be used on products in the UK?

The key takeaway

The “CE” safety mark will continue to be recognised in the UK beyond the original cut-off date of December 2024. This marks a shift in policy which aims to ease the burden on businesses and create more certainty that will allow for continued innovation and growth.

The background

The “CE” product safety marking appears on many products traded on the extended Single Market in the European Economic Area (**EEA**). The mark signifies that products sold in the EEA have been assessed to meet high safety, health and environmental protection requirements. In January 2021, following Brexit, the UK Conformity Assessment (**UKCA**) mark replaced the “CE” product safety marking on products being sold in the UK. However, the CE marking would continue to be recognised until December 2024 in order to ease the transition for businesses.

The development

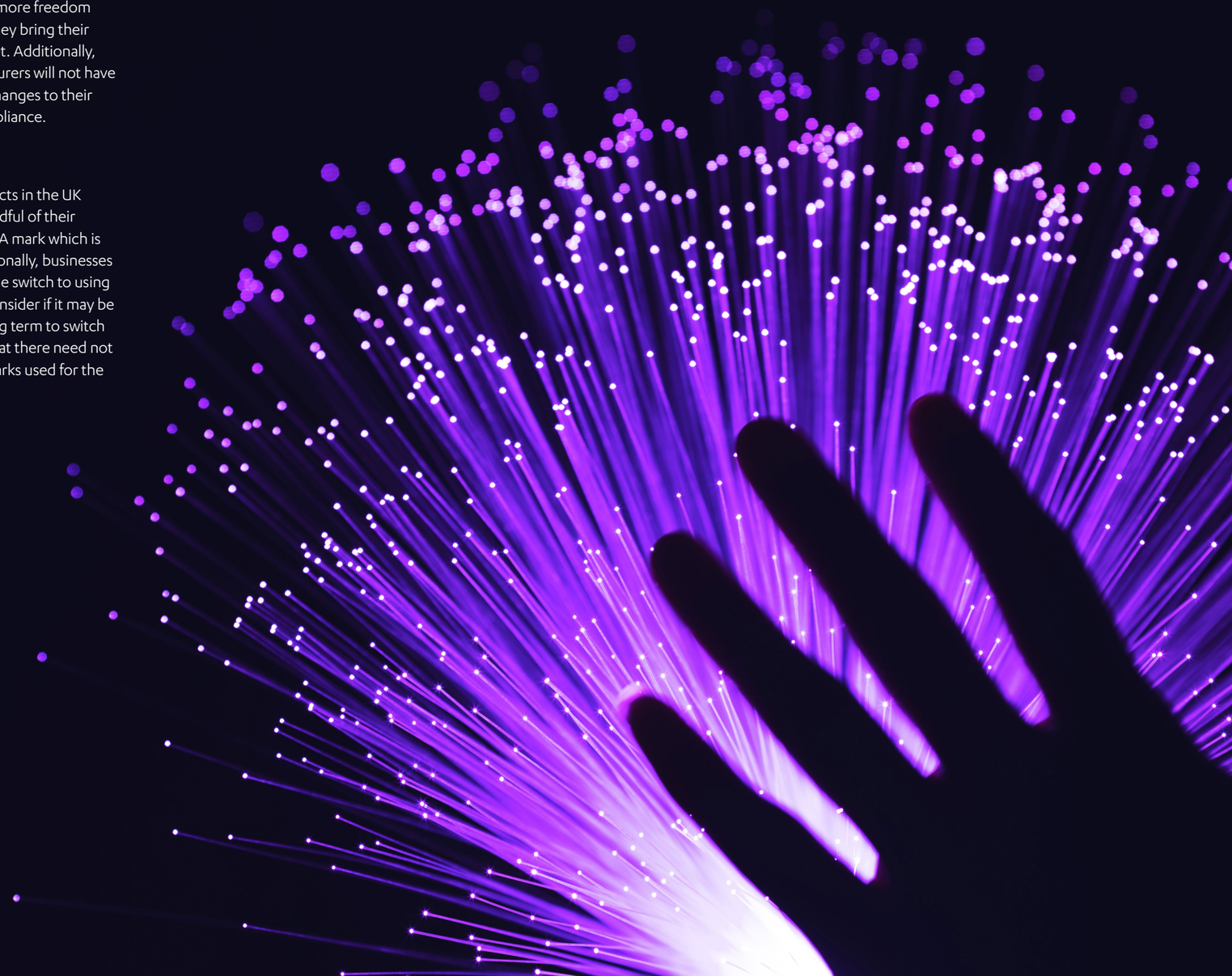
In August of this year, following detailed engagement with UK industry the UK Government announced an indefinite extension to the recognition of the “CE” product safety marking in Great Britain. UK businesses highlighted that no longer recognising the CE mark would likely lead to regulatory uncertainty as well as higher costs. The Government hopes that the extension will ease the burden on businesses by cutting barriers and red tape which will then allow for a continued focus on innovation. This development means that businesses placing products into the EU market are no longer required to use the UKCA mark but can still choose to do so (for example if there manufacturing processes have already been updated to include the new mark). Going forward businesses will have more flexibility regarding how they certify that their products meet the appropriate standards for the UK market. This also means that businesses can continue to be aligned with the EU.

Why is it important?

This development highlights the UK Government’s continued commitment to easing the regulatory burden on businesses in an effort to foster innovation. Businesses will now have more freedom and flexibility as to how they bring their products to the UK market. Additionally, this means that manufacturers will not have to make any significant changes to their processes to ensure compliance.

Any practical tips?

Businesses that sell products in the UK and the EU should be mindful of their continued use of the UKCA mark which is not valid in the EU. Additionally, businesses that have already made the switch to using the UKCA mark should consider if it may be more beneficial in the long term to switch back to the CE mark so that there need not be two separate safety marks used for the UK and the EU.



Government consults on improving price transparency and product information for consumers

The question

What does the UK Government's consultation on Improving Price Transparency and Product Information for Consumers (the Consultation) signal about online choice architecture, and what businesses should be doing now to avoid the risk of fines next year?

The key takeaway

The Consultation highlights the Government's fixation on protecting consumers from manipulative practices, in particular from the harms of being misled into making purchasing decisions. Businesses should be mindful of this focus, especially as the Competition and Markets Authority (the **CMA**) will be gaining new fining powers under the Digital, Markets Competition and Consumer Bill (**DMCC**) early next year. They should start reviewing their own selling practices right now to see whether any significant updates are required to their consumers' online experiences, especially those that directly or indirectly influence their transactions.

The background

The draft Digital Markets, Competitions and Consumer Bill (the **Bill**), published in April 2023 (see our Summer 2023 Snapshot) marked a seismic shift in UK consumer law with a significant enhancement of the UKs consumer protection regime. Whilst the Bill seeks to address inadequacies in the current consumer protection regime, a primary focus is the enhancement of consumer information transparency.

The development

The Consultation was launched on 4 September 2023 and seeks input on some of the key consumer protection elements of the Bill. These include:

- display of pricing information
- hidden fees and drip pricing
- fake and misleading reviews
- online platforms, and
- online interface orders.

The aim is to ensure that consumers are provided with timely and relevant information when making purchasing decisions, which in turn will give them greater visibility of the options available to them.

Fake reviews

A key facet of the consultation is to seek industry opinions on how the Government's policy to add practices relating to fake reviews to the "blacklist" of automatically unfair commercial practices at schedule 18 of the Bill should work in practice. The Government currently proposes adding the following to the "blacklist":

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

Businesses that utilise customer reviews will have an obligation to ensure that consumers are not misled and will be required to take reasonable and proportionate steps to prevent customers from encountering fake reviews. It is not yet clear what "reasonable and proportionate" steps will mean in practice and the Consultation also seeks input on definitions that will underpin any updates to the legislation. It is likely that the Government will not seek to place overly onerous obligations on businesses but will also keep consumers front of mind when enacting any legislation regarding fake reviews.

Drip pricing

Drip pricing, which is the practice of stating a base price and then gradually introducing additional fees as consumers work their way through the transaction process, is also front of mind for the Government in this current overhaul of UK consumer law. Research suggests that this practice is problematic when used to entice a customer to what appears to be a low price, which is in fact misleading when the additional fee/costs are added. The Consultation seeks views on how this practice should be managed and which specific practices should be outlawed.

Display of pricing information

Finally, following Brexit, the regulations governing the display of pricing information (Price Marking Order (**PMO**) 2004) are being considered under the Consultation to ensure that they remain fit for purpose. In particular, the Government wants to ensure that consumers are provided with all the information that is required to understand the pricing of products so that they can make informed choices. The Government aims to tweak the PMO so that it better suits the needs of consumers as well as helping ensure clarity for businesses. The key proposals the Government is consulting on are:

- mandating the consistent use of unit pricing measures for products so businesses can more easily comply, and consumers can compare similar items more easily
- improving the legibility of pricing information through adopting consistent standards that businesses can easily comply with rather than having to invent their own
- whether the current small shop exemption should be revised for clarity in any way
- strengthening and clarifying the requirement to provide promotional unit pricing for promotional offers, such as loyalty schemes or multibuys of similar items, and
- how the "deposit return scheme" (eg for redeeming empty drinks containers) should be displayed on pricing labels.

Why is this important?

The Consultation underlines the Government's goals of ensuring that UK consumer law is fit for purpose and is effective in practice. Importantly, it highlights that whilst the consumer is front of mind, the Government does not seek to be restrictive, instead attempting to curate an ecosystem in which consumers and businesses are able to thrive.

Any practical tips?

Whilst the Bill is not yet formally law, the core elements are unlikely to undergo any significant amendments. However, there may well be some refinements to some of the more specific aspects relating to transparency. Businesses should keep track of the Bill's progress through Parliament as well as the output of the Consultation. Come what may, it's clear that the CMA has a keen eye on this topic. With the CMA finding itself with new fining powers early next year under the DMCC, businesses would be wise to review their online choice architecture to ensure that consumers are presented with clear information and can make purchasing decisions without being subtly manoeuvred towards a purchase.

ASA updates guidance on misleading environmental claims

The question

What additions have been made to the guidance on misleading environmental claims issued by the Committee of Advertising Practice (**CAP**) and what additional factors should businesses be taking into account now when considering green marketing campaigns? And are the rules beginning to push businesses into "greenhushing" for fear of greenwashing?

The key takeaway

The ASA has issued updates to its guidance on green claims in advertising, demonstrating a continuing intention to clampdown on misleading environmental claims. Businesses should carefully consider the rules, guidance and steady flow of ASA rulings on this issue before making any green claim, particularly if the business is in an environmentally harmful or high emissions sector. This continues to be a high risk area, with marketing departments regularly stumbling into high profile mistakes, which often have a disproportionately high negative PR impact especially from a consumer trust perspective.

The background

In December 2021 the ASA published guidance on the interpretation of the CAP and BCAP rules on making environmental claims in advertising (the **Guidance**). The ASA made their first update to the Guidance in February 2023 in relation to the use of "carbon neutral" and "net zero" claims in advertising (see our Summer 2023 napshot).

The regulatory crackdown on misleading environmental claims has continued apace, with the ASA issuing a number of rulings in recent months. Claims against energy companies Repsol, Shell and Petronas were all upheld on the basis that their ads omitted material information and were misleading to customers. Anglian Water were also found to have misled customers when one of their ads omitted material information on their poor track record in relation to their Environmental Performance Assessment (**EPA**) by the Environment Agency.

The development

The ASA has sought to provide extra clarity on the issue in a new section of the Guidance entitled "Claims about initiatives designed to reduce environmental impact". The new section draws on the principles established within the recent ASA rulings as well CMA guidance on environmental claims in goods and services.

The Guidance highlights a number of factors which make ads more or less likely to comply with the rules on environmental claims, including the following key principles:

- if an environmental claim relates solely to a specific product, this should be made clear to avoid consumers linking the claim to the business as a whole
- if a business has a particularly harmful impact on the environment, an ad which highlights positive environmental activities is likely to be misleading if it does not include "balancing information" on the business's environmental harm. This balancing information is likely to be more necessary in high emission sectors and sectors where consumers are likely to be less aware of the business's negative environmental impact
- if an ad refers to lower-carbon activities without including information on a business's overall harmful impact this may create a misleading impression of the proportion of that business's activities that are low-carbon
- the ASA will likely consider a business's EPA in determining whether an ad is misleading. If a business has a low EPA rating, it is likely to be considered material information which contradicts a positive environmental claim and so should be disclosed
- "Imagery of the natural world" may be seen as giving an environmentally positive impression depending on context, and therefore may be misleading without balancing or qualifying information
- absolute environmental claims such as "sustainable" or "environmentally friendly" must be backed up by a high level of substantiation
- a suggestion that a business is already taking steps to reduce emissions and/or environmental harm should be accompanied with any material information about the balance of current emissions and activities
- if an ad suggests that a business's negative environmental impact is a thing of the past this is likely to be misleading if the business is still having a negative impact
- if an ad details initiatives aimed at achieving net zero, the customer should be given context on how those initiatives form part of the net zero plan and how and when net zero will be achieved. Timescales for a net zero plan are likely to be seen as material information to be included in an ad.

Why is this important?

The ASA is clearly cementing their position on misleading environmental claims in advertising. The rulings and further updated Guidance demonstrate a continuing intention for the ASA to clampdown on misleading green claims. It is clear from the recent ASA rulings and new Guidance that if you are in a sector which has a particularly harmful environmental impact, you are likely to need to give more balancing information when making a green claim. Some have publicly said that the ASA's approach is likely to lead to companies "greenhushing" so as to avoid any possible accusation of greenwashing. However, the ASA has also made it clear that it does not view environmental claims issues as so binary, and that it is not fair to say that businesses must essentially choose between "greenwashing" and "greenhushing". Businesses, including those in a harmful sector, can still make green claims provided that the required balancing information is given.

Any practical tips?

Businesses should familiarise themselves with the rules and Guidance (and the CMA's Green Claims Code) before making any green claim. If you are in a sector which has a particularly harmful environmental impact, you may need to ensure that any green claim in an advertisement acknowledges these less-climate-positive activities. The ASA has advised that this does not need to dominate the advertisement, but it cannot be hidden away. It's also important to keep up to date with ASA rulings on this issue to keep track of their current reasoning and approaches.

ADVERTISING

The ASA's "Active Ad Monitoring" AI tool: nowhere to hide for green claims

The question

What does the ASA's targeting of its AI monitoring and targeting tool at green claims mean for businesses interested in spotlighting the role they play in the environment?

The key takeaway

The ASA is using its Active Ad Monitoring artificial intelligence tool to identify ads that make green or environmental claims, no longer solely relying on complaints made by the public. This highlights just how high a priority the ASA is viewing green claims. More than ever, businesses looking to make green, environmental or sustainability claims should think extremely carefully about how to frame these in a way which complies with what has quickly become a highly, and very tightly, regulated area.

The background

The ASA's "climate change and the environment" project is well underway. In September 2021, the ASA announced its programme dedicated to cleaning up green advertising, and since then, we have seen a steady stream of activity and guidance. In October 2022, the ASA published its Climate change and the environment – consumer understanding of environmental claims report. It has used the findings from this report to inform its guidance note on misleading environmental claims and social responsibility (see our Snapshot in this Autumn 2023 edition) and launched an e-learning module to help advertisers understand the key principles to bear in mind when making green or environmental claims. The ASA has also been working in partnership with the Competition and Markets Authority (**CMA**) which published its own Green Claims Code in 2021 and began enforcing it in earnest in 2022 (see our Autumn 2022 Snapshot CMA investigates ASOS, Boohoo and Asda over "greenwashing").

To support its proactive approach to regulation, the ASA has developed an Active Ad Monitoring system (**AAM System**) which uses AI to actively seek out and identity ads in "high-priority" areas which may be non-compliant and which flag these to the ASA for "expert review". So far, we have seen at least four ASA rulings for ads which have been identified for investigation by the AAM System (including the one referenced below). With "climate change and the environment" clearly remaining a hot topic (pun intended) for the ASA, it is no surprise that the AAM System has started to pick up sustainability and green claims.

The development

On 30 August 2023, the ASA published an upheld ruling against 4AIR, a company that provides services that assist businesses operating in the aviation space to meet emission targets and industry standards and implement sustainability initiatives. The ad in question, which was identified by the AAM System, contained claims such as:

- "Eco-Friendly Aviation – Future of Sustainable Aviation", and
- "Learn How To Turn Flying Into A Force For Good With A 4AIR Rating. Industry-Leading Standard For Sustainability In Private Aviation. Sustainability. Aviation Industry".

Unsurprisingly, the ASA stated that absolute environmental claims such as these require a "high level of evidence" to substantiate the claims and must be provided from across the entire life cycle of the products and services in question. 4AIR argued that the claims were substantiated by: (i) its service offering which used "sustainable" aviation fuel made from non-fossil fuel sources to reduce carbon emissions by up to 80%; and (ii) donations to a non-profit organisation (set up by none other than 4AIR itself), Aviation Climate Fund, which researches new technologies to support the transition to low-carbon in the aviation industry. However, 4AIR failed to convince the ASA that the high bar for substantiation had been met and so the ASA concluded that the ad was likely to mislead consumers.

Why is this important?

This ruling not only signals (once again) that the ASA's dedicated project, "climate change and the environment", remains a high priority but the use of the AAM System also represents a gear change by the ASA. Consequently, we can expect to see a levelling up of enforcement by the ASA in this space – so there really is no place for misleading or unsubstantiated green claims to hide.

Any practical tips?

Businesses and advertisers looking to make green or sustainable claims, or wanting to refer in some way to the environment, should carefully consider all elements of what is now a substantial amount of ASA guidance as well as the fact that it no longer requires a complaint to be made to the ASA for an investigation to be launched. Before publishing green claims and other advertising or marketing materials that include any environmental credentials, businesses will need to ask themselves the basic compliance questions to ensure they have framed the claim properly. These include:

- is the claim specific enough, taking into account the full cycle of the product/service, and
- do we hold robust enough documentary evidence to substantiate the exact claim being made)?

New advertising laws to tackle illegal ads and protect children online

The question

What measures are the Government planning to implement to protect consumers, specifically children, from illegal adverts online?

The key takeaway

The UK Government has announced plans to implement new rules to crack down on illegal ads and influencer scams, with the objective of safeguarding consumers and protecting children online.

The background

In January 2020, the Government initiated an inquiry into the regulation of online advertising, focusing on the effectiveness of the existing self-regulatory framework managed by the Advertising Standards Agency (**ASA**). Then in March 2022, the Government launched the Online Advertising Programme (**OAP**) to revamp the regulatory framework for paid online advertising, addressing both illegal and harmful ads and issues of transparency and accountability. Three options for future regulation were considered:

- continuing self-regulation with ASA oversight through the CAP Code
- introducing a statutory regulator to support self-regulation, and
- a fully statutory approach with a new regulator handling both regulation and enforcement.

Online advertising accounted for £26.1bn of the £34.8bn spent on UK advertising in 2022, making its regulation of upmost importance.

The development

On 25 July 2023, the Department for Digital, Culture, Media, and Sport (**DCMS**) unveiled its response to the OAP consultation. The Government's plan involves the introduction of new legislation aimed at addressing specific issues in online advertising, with the proposed laws honing in on advertisements that facilitate illegal activities, including fraud, illegal products, malware and human trafficking. Platforms and publishers alike will have to implement measures to prevent the dissemination of such content and advertising platforms may be compelled to share information with regulators and act proactively to prevent the spread of harmful content. They will also safeguard under-18s from exposure to ads for products and services they cannot legally purchase.

The new laws will apply only to paid-for online advertising, with social media firms, online publishers, apps, websites, adtech intermediaries and social media influencers (in relation to paid content) all falling within scope. The measures are intended to complement other digital regulatory reforms, such as the Digital Markets, Competition and Consumers Bill, the Data Protection and Digital Information Bill and the Online Safety Bill. The Government will continue to enforce other consumer protection laws through existing legislation, such as the Consumer Protection from Unfair Trading Regulations. The legislation will not affect the ASA's jurisdiction over legitimate paid-for online advertising.

Why is this important?

The introduction of new laws in online advertising is very significant and means that anyone involved in this industry will now have statutory obligations to combat illegal ads and shield under-18s from exposure to restricted products. That said, these laws are narrowly focused on addressing the most egregious forms of illegal advertising and the overall advertising framework will remain largely unchanged.

Any practical tips?

More than three years have passed since the initial call for evidence and actual legislative changes are still pending. However, it's still worth being alive to the proposed changes to come – namely the creation of statutory responsibilities to remove online ads for illegal activities and prohibit under-18s from exposure to products which they are unable to legally buy. So while detailed rules, player involvement and scope will be determined in a subsequent consultation, those involved in the online ad industry should begin to think now about the steps they can take to combat the harm of illegal ads.

Financial claim caught by clause excluding liability for loss of anticipated profits

EE Limited v Virgin Mobile Telecoms Limited **[2023] EWHC 1989 (TCC)**

The question

How did the court approach the construction of an exclusion clause to determine whether the claimant's financial claim for breach of an exclusivity provision was properly described as a claim for "anticipated profits" and as such was excluded by that clause?

The key takeaway

In line with a number of recent cases, the court's decision in this case shows that parties generally cannot avoid clear wording contained in exclusion clauses in order to recover losses that have been expressly excluded (in this case, loss of profits).

The background

Under a telecommunications supply contract, Virgin Mobile Telecoms (**Virgin Mobile**) contracted with Mobile Network Operator EE to access its radio access network. EE was required to supply Virgin Mobile with various services that would enable Virgin Mobile's customers to be provided with 2G, 3G and 4G mobile services. This arrangement was subject to an exclusivity clause in the contract.

Other than in certain limited circumstances, the liability clauses in the contract expressly excluded liability for "anticipated profits".

The initial arrangement wasn't applicable to the provision of 5G services but 5G was added subsequently and the contract was amended accordingly. The amendments provided for potential agreement between EE and Virgin Mobile in relation to the provision of 5G services using EE's network or, in the absence of such agreement, for Virgin Mobile to be entitled to provide 5G services to its customers from a different network owned by one of EE's competitors.

Virgin Mobile put some of its customers on Vodafone's and O2's networks believing it fell within that "5G services" exception to the exclusivity clause. EE considered that by doing so Virgin Mobile had breached the exclusivity clause and issued proceedings, claiming damages of c.£25m in revenue that it would otherwise have earned in respect of liability for additional charges payable by Virgin Media to EE under the contract had Virgin Mobile's customers been kept on EE's network instead.

Virgin Mobile accordingly applied for strike out and/or reverse summary judgment of EE's claim, contending that regardless of breach (which it denied) the claimed losses fell within the clear and natural meaning of the words "anticipated profits" in the exclusion clause.

The key question for the court was whether that interpretation was correct. While bearing in mind that the court should hesitate about making a final decision without trial, the court decided that it had all the evidence necessary to determine this key point of contractual construction summarily.

The decision

TThe court revisited the well-established general approach to contractual interpretation, as well as the purposive and contextual principles applicable to the interpretation of exclusion clauses.

Given the clear and unambiguous language of the exclusion clause, the court found that EE's damages claim fell within the natural meaning of "anticipated profits" and was therefore excluded.

There was no difference in meaning between "lost profits" and "anticipated profits". The agreement was a bespoke, lengthy and detailed contract negotiated by two sophisticated parties operating in the field of telecommunications, which had been negotiated on a level playing field. Although that admittedly left EE without a financial remedy if Virgin Mobile breached the exclusivity clause, EE would still be paid the substantial contractually agreed minimum revenue payments in any event, and EE could still seek effective non-financial remedies (such as injunctive relief), so the result could not be said to render the contract an "illusory bargain" or "a mere declaration of intent".

The court therefore gave summary judgment in Virgin Mobile's favour.

Why is this important?

The meaning ascribed to the phrase "loss of profits" will depend on the context and drafting of the relevant contract – this case highlights that despite the wording in the claim referring to "charges unlawfully avoided" the court found the damages sought were for loss of profit, and thereby excluded, on the grounds that the wording of the clause was clear.

The judgment also includes a useful summary of key case law showing the court's approach to the interpretation of exclusion clauses.

Any practical tips?

It is important to identify in the contract exactly which losses the parties intend to limit or exclude and under what circumstances. If it is intended that certain losses are not to be excluded (for example, charges) consider including a (non-exhaustive) list of losses that are recoverable. If particular risks or liabilities are being allocated to a particular party in specific circumstances, consider describing the commercial rationale in recitals or acknowledgments in the contract or the specific provisions.

COMMERCIAL

COMMERCIAL

Terminating software agreements when they fail to deliver software deliverables on time

Topalsson GmbH v Rolls-Royce Motor Cars Limited **[2023] EWHC 1765 (TCC)**

The question

How did the court determine: (1) whether a software implementation timeline agreed by the parties was binding; (2) when implementation was considered complete; and (3) in what circumstances did failing to complete implementation by the contractual deadlines entitle the customer to terminate the contract?

The key takeaway

In this particular case, the court found that milestone dates contained in an agreed implementation plan (revised from those contained in the tender documentation implementation plan) constituted contractually binding delivery dates. While there was no express definition of "Technical Go-Live" in the contract, based on wording contained in the contract and the sequencing of project activities set out in the agreed implementation plan, the court found that Technical Go-Live required the successful completion of systems integration and user acceptance testing, and not just delivery of broadly functioning software.

The background

In October 2019, following a tender process, Rolls-Royce contracted with software developer Topalsson to develop a new digital visualisation tool allowing prospective customers to see photo-realistic renderings of Rolls-Royce cars with different custom configurations, before purchasing.

Under the services agreement (the **Agreement**), Topalsson was obliged to meet milestone dates contained in an agreed implementation plan, which gave a detailed breakdown of the project programme (the **December Plan**). It soon became evident that the December Plan dates could not be achieved. A revised plan was agreed, with later delivery dates for "Technical Go-Live" (the **March Plan**). Technical issues and delays continued and Rolls-Royce lost confidence in Topalsson's ability to deliver the project to the new agreed timeline. Despite agreeing the revised March Plan, Rolls-Royce served a termination notice on Topalsson (the **First Termination Notice**) relying on Topalsson's repudiatory breach for its failure to meet the December Plan dates. Topalsson rejected the First Termination Notice and affirmed the Agreement, denying that the December Plan dates were contractually binding.

Rolls-Royce then served a further notice (the **Second Termination Notice**), again purporting to terminate the Agreement both: (i) for repudiatory breach, but this time for missing the March Plan deadlines; and (ii) under clause 13.11 of the Agreement, which permitted immediate termination if Topalsson failed to meet the agreed delivery or milestone dates. Topalsson rejected the Second Termination Notice too, alleging that Rolls-Royce was itself in repudiatory breach of the Agreement and purporting to accept that repudiatory breach to bring the Agreement to an end.

Topalsson brought proceedings against Rolls-Royce, asserting that Topalsson was not in breach, as it had achieved Technical Go-Live for some deliverables and would have completed the others but for Rolls-Royce's termination; or alternatively there were no contractually binding delivery dates and time was not of the essence, and Rolls-Royce was partly to blame for the delays.

Rolls-Royce counterclaimed, arguing that the December Plan and subsequently the March Plan dates were contractually binding, and Topalsson was responsible for having missed them.

The decision

There were several key issues to be decided:

Did Topalsson just have to deliver and install the software within a "reasonable time", or did it have to comply with specific milestone dates?

The court found that the December Plan dates were contractually binding on Topalsson. Topalsson itself had proposed the December Plan timeline to Rolls-Royce, it knew that the timeframes were commercially sensitive and that the software was needed in time for the planned launch, and the parties had agreed those dates.

The court also held that, properly construed, the express terms of the Agreement made time of the essence in respect of the dates in the December Plan.

As to the March Plan, Topalsson asserted that the dates had no binding contractual effect and it just had to deliver within a "reasonable time". The court disagreed: Topalsson had agreed to the March Plan dates in circumstances where it had already failed to meet the December Plan and where Rolls-Royce had expressly stated that Topalsson meeting the March Plan dates was "a condition of our ongoing contractual relationship". Accordingly, the March Plan was a relaxation and/or extension of time under the binding December Plan. The March Plan dates were therefore binding on Topalsson and time was also of the essence in achieving them.

Had Topalsson met the contractual milestone dates?

By the time Rolls-Royce sent its Second Termination Notice, the Technical Go-Live milestone dates for two deliverables had passed and it was accepted that the third milestone date was not going to be met. There was, however, no express definition of "Technical Go-Live" in the Agreement and Topalsson asserted that it had either achieved Technical Go-Live or would have but for Rolls-Royce terminating the Agreement, on the basis that not all testing had to be completed and that the existence of open defects did not preclude Technical Go-Live being achieved. In other words, delivery of broadly functioning software was sufficient.

Based on the wording of the Agreement and the sequencing of project activities set out in the December Plan, the court again disagreed: Technical Go-Live required the successful completion of systems integration and user acceptance testing. The court also found that Topalsson had accordingly failed to achieve Technical Go-Live by the March Plan deadlines that had already passed and was so far behind schedule that it would not have met the final deadline even if the Agreement had continued.

Was Topalsson responsible for failing to meet the March Plan milestones, or was it impeded by Rolls-Royce?

Topalsson argued that the delays were not its fault because:

- its subcontractor, to which it had been introduced by Rolls-Royce, had performed poorly
- Rolls-Royce itself had delayed the start of the project and failed to provide Topalsson with the necessary systems access and software licences
- Rolls-Royce had introduced changes to the requirements and/or scope creep
- Rolls-Royce had imposed a waterfall project management methodology, despite Topalsson having strongly pushed for a purely agile approach.

The court rejected those arguments, finding that Topalsson's own commercial decisions were the most likely cause of the delays including that Topalsson had chosen to engage the subcontractor and was responsible for its performance, and that Topalsson had contractually agreed to a hybrid agile/waterfall methodology. Ultimately, either "Topalsson took on a project that simply was beyond its capabilities, or… it struggled to recruit and retain the necessary staffing levels".

Was Rolls-Royce in repudiatory breach by giving the Termination Notices?

The court found that Rolls-Royce's First Termination Notice was erroneous because it relied on Topalsson missing the original December Plan deadlines, when the revised March Plan deadlines had already been agreed. This was, however, ultimately immaterial as Topalsson had affirmed the Agreement in response.

As to the Second Termination Notice, this was based on Topalsson's failure to achieve the milestone dates set out in the March Plan and relied upon:

- a contractual right to terminate for failure to meet milestone dates pursuant to clause 13.11 of the Agreement, and/or
- the common law right to terminate for repudiatory breach on the basis that time was of the essence in respect of achieving the milestone dates and Topalsson had breached this obligation.

There was a key difference between the two termination avenues available to Rolls-Royce: case law is clear that the contractual termination right under clause 13.11 could only be exercised in respect of a significant or substantial breach justifying termination; whereas under clause 5.8, the parties had agreed that time for delivery deadlines was "of the essence", ie a condition of the Agreement, any breach of which (irrespective of severity) would in principle amount to a repudiatory breach and justify termination. On the facts, the court found that Rolls-Royce had been entitled to rely on either avenue as Topalsson's delays were significant and "could not be described as a 'near miss'". The Second Termination Notice was therefore valid.

Why is this important?

The decision highlights that key requirements and deadlines should be clearly defined and recorded in the contract (or it should provide clear mechanisms for agreeing them later) to avoid subsequent confusion and disputes arising as to whether deadlines are binding and when they have been achieved. It also underlines the need for careful consideration when drafting termination notices to ensure they are not defective and in themselves repudiatory.

Any practical tips?

Parties should define and make use of contractual change control mechanisms – whether relating to scope, delivery dates or other requirements – to give clarity about the contractual status of any variations agreed.

Parties seeking to terminate for repudiatory breach or based on a contractual right should, in the notice of termination, take care to rely on valid legal and factual bases to do so, or else risk being in repudiatory breach themselves. For example, if contractual timelines or scope have been varied by agreement, failure to meet the original requirements may no longer justify termination. In addition, specific requirements for written notices as set out in the contract should be strictly observed.

While a minor breach of a condition (ie a term which "goes to the root of the contract") may be enough for termination, breaches of other contractual terms giving rise to an express right to terminate may still need to be sufficiently significant in the circumstances to warrant termination.

Consider whether time is expressed to be of the essence in the contract. Making time of the essence for performance is (usually) sufficient to constitute a term essential and render any delay (even if only by a few hours) repudiatory. The repudiation can be accepted by the innocent party and they can seek damages for loss of the bargain resulting from the termination of the agreement even where the failure to perform the obligation on time is relatively minor.

COMMERCIAL

Limitation of liability clauses in software development projects – financial caps

***Drax Energy Solutions Limited v Wipro Limited* [2023] EWHC 1342 (TCC)**

The question

Was the limitation of liability clause in the Master Services Agreement construed by the court to provide for a single aggregate cap to be applied to the customer's pleaded claims (limiting the claim to £11.5m from a pleaded claim of £31m), or separate caps for each claim?

The key takeaway

Where there is more than one possible interpretation of the wording of an ill drafted clause, with "linguistic quirks" and where there is an inconsistent choice of wording throughout the contract, the courts will use their tools of linguistic, contextual, purposive and common-sense analysis to discern what the clause really means, respecting that commercial parties are entitled to allocate between them the risks of something going wrong in their contractual relationship, in any way they choose.

The background

Drax and Wipro entered into the MSA in January 2017. Under the MSA and its seven related Statements of Work (**SOWs**), it was envisaged that Wipro would design, build, test and implement a new Oracle-based IT system for Drax – including customer relationship management, billing and smart metering functionality, as well as software encryption, ongoing maintenance and related IT services.

However, milestones were repeatedly missed and the project ended in failure: less than eight months in, Drax terminated the MSA for Wipro's alleged repudiatory breaches and sued Wipro for damages. Drax claimed total losses of around £31m (more than four times the fees payable in that first year).

Clause 33.2 (the **Clause**) of the MSA contained the following limitation of liability:

"Subject to clauses 33.1, 33.3, 33.5 and 33.6, the Supplier's total liability to the Customer, whether in contract, tort (including negligence), for breach of statutory duty or otherwise, arising out of or in connection with this Agreement (including all Statements of Work) shall be limited to an amount equivalent to 150% of the Charges paid or payable in the preceding twelve months from the date the claim first arose. If the claim arises in the first Contract Year then the amount shall be calculated as 150% of an estimate of the Charges paid and payable for a full twelve months."

Ahead of the main trial in this case, scheduled for October 2024, the court was asked to determine two preliminary issues:

- did the Clause provide for separate liability caps for each claim, or did it provide for one single aggregate cap?
- if the Clause did provide for multiple liability caps for different claims, what were the different claims to which the cap applied?

The decision

Issue 1: One cap or multiple caps?

Perhaps unsurprisingly noting the use of phrases such as "total liability", and "the claim" (rather than "a claim" or "for each claim"), the court held that the language of the Clause and related provisions were a "clear indicator" that the Clause imposed a single aggregate cap, not multiple caps.

As to business common sense and contextual considerations, including the purpose of limitation clauses:

- Drax argued that there were multiple SOWs under the MSA, and more SOWs could have been executed in future by other group companies, in respect of other projects – so it didn't make business sense for there to be a single aggregate cap, which Drax would be stuck with in respect of any and all claims that might arise under any SOWs in the future. The court dismissed that argument as unrealistic – Drax had termination rights it could utilise under the MSA if the project was proving or threatening to be a disaster
- Drax also argued that if the Clause provided for a single aggregate cap, that would result in its claims being limited to just £11.5m – a third of their potential £31m value, which would make no business sense. The Court disagreed. Balancing the parties' competing perspectives, the court's view was that, although it was true that a single aggregate cap would significantly limit Drax's claims, the Clause still left Drax with potential and not insignificant damages, while at the same time operating as an effective limit on Wipro's liability, without being "so high as to be devoid of any real purpose" as a limitation clause.

Ultimately, the court recognised that "it may be that Drax did not… protect itself in terms of claims to be made as it could or should have done [but that] is quite different from saying that the Clause makes no commercial sense".

Accordingly, the court found that Drax's total claim of £31m was effectively limited to £11.5m by the single liability cap under the Clause.

Issue 2: One claim or multiple claims?

Despite its conclusion for Issue 1 effectively closing off the second issue, the court answered Issue 2, accepting neither party's primary cases about the meaning of "claim":

- Drax's contention that "claim" meant "cause of action" (resulting in 16 "claims") simply couldn't be right, as "there would be a total cap of £132m for the first 12 claims and then a further cap for the remainder". The Clause had to operate as an effective limitation on Wipro's liability.
- Wipro's position that "claim" meant "liability", however, would have been too restrictive, depriving Drax of the ability to bring multiple claims under the MSA: that would be an "artificial" interpretation which would mean "there could never be more than one operative claim".

Instead, the court adopted a middle ground that involved "construing a claim in the context of and for the purposes of the operation of the Clause". The court considered that Drax's alternative case, that "claim" should be interpreted in accordance with the four broad categories of claim included in its particulars of claim, was a sensible approach and would not lead to an "odd outcome" as to the applicable liability caps under the Clause. Even though the court accepted that Drax's four categories were somewhat arbitrary, the parties' chosen contractual wording was not entirely clear as to what "claim" meant, and their primary arguments were not workable within the purpose of the Clause, and therefore the court explained that "some other meaning must be given".

Why is this important?

The decision provides a useful illustration of the court's approach when interpreting a limitation of liability clause and highlights the dangers of poor and inconsistent drafting. Where there is ambiguity in the contractual wording, the court is entitled to prefer the construction that is consistent with commercial common sense but will not seek to relieve a party from a bad bargain.

Any practical tips?

Consider that the courts may take a narrow and purposive approach when construing limitation of liability clauses (within their factual and commercial context). Key words like "claim" will be interpreted based on context and may not equate to "cause of action" or "liability".

Software developers, IT service providers and others that typically operate within an MSA/SOW contractual framework should take care to consider and agree allocation of risk effectively before entering into any MSA or SOW (including considering whether each SOW should contain its own specific limitations of liability that override any general limitations in the MSA).

Clauses containing financial caps can use a variety of ways to ensure certainty and enforceability for example by fixing an overall sum for the cap or by limiting the amount to the sums paid to the supplier. When referring to "paid" sums it is important to define "paid" as opposed to "payable".

As well as dealing with the value of the cap it is important to carefully describe what the cap applies to: a single cap may apply to all claims made "under" or "in connection" (much wider) with the agreement, a defined period such a calendar year, or per claim. In some circumstances, it may be advisable to apply different limits for different kinds of loss, accepting that the more complex the arrangements the more likely that arguments may ensue.

Pre-contractual documents – when heads of terms are legally binding and enforceable

Pretoria Energy Company (Chittering) Ltd v Blankney Estates Ltd **[2023] EWCA Civ 482**

The question

Was a signed document marked "heads of terms" but not marked "subject to contract" a binding agreement for lease?

The key takeaway

The label heads of terms (**HoT**) is not indicative of whether a document has contractual effect. It is the interpretation of the document as it stands, based on a number of factors including intention of the parties to create legal relations, the provision of essential commercial terms and, in the case of an agreement for a lease, certainty as to the start date that determines whether a contract is binding.

The background

Pretoria Energy (**Pretoria**), develops and operates anaerobic digestion (**AD**) plants. Farming business Blankney Estates (**Blankney**) owned commercial land suitable for operating an AD plant.

In proceedings for breach of contract, Pretoria contended that the parties entered into an agreement in November 2013 under which Blankney agreed to grant it a 25-year lease of a site in Lincolnshire for the purpose of developing and operating an AD plant. This agreement was contained in a document called "Heads of Terms of Proposed Agreement between Blankney Estates, Lincolnshire and Pretoria Energy Company Limited Subject to Full Planning Approval and appropriate consents and easements" (the **HoT**).

It was Pretoria's case that Blankney repudiated that contract, and became liable for damages, while Blankney contended that there was never a binding contract by which it agreed to grant Pretoria a lease. Its case was that the only enforceable contract between it and Pretoria to be found in the HoT was an exclusivity or "lockout" arrangement (the **Lockout Provision**), by which the parties agreed, until 31 July 2014, not to enter into negotiations with third parties.

In the High Court, the judge ordered that the following issue be tried as a preliminary issue:

"Is the document titled 'Heads of Terms of Proposed Agreement' a binding and enforceable agreement between the parties other than in respect of the Lockout provision?".

At first instance the court agreed with Blankney and decided that the parties did not objectively intend to bind themselves to a contract by the HoT, other than in respect of the lockout provision.

Pretoria appealed.

The decision

The Court of Appeal (CA) dismissed the appeal, finding that the HoT was not a binding and enforceable contract, but took a different view to the trial judge with regards to why.

In giving its judgment, the CA observed that:

- the fact that the HoT provided for a formal contract to be drawn up within one month of receipt of planning permission, was of considerable significance
- the HoT were not headed "subject to contract" which would have put it beyond doubt that the parties did not intend to be contractually bound by any part of the HoT. But since it was common ground that the parties did intend to be bound by the lock-out agreement, the omission of the phrase "subject to contract" was of less importance than it might have been
- the inclusion of the lockout provision, providing for an exclusive negotiating period, was incompatible with a binding agreement
- no commencement date was specifically expressed, and it was not possible to deduce from the terms of the agreement, with reasonable certainty, when the term was intended to begin. If the time from which the lease is to begin is uncertain, this made the agreement incomplete and not binding. An uncertain start date is a very powerful objective indicator that the parties did not intend to be bound
- in the HoT, the parties agreed that the lease would be outside of the Landlord and Tenant Act 1954 but the formalities, necessary for contracting out of the 1954 Act, had not been completed.

Why is this important?

The judgment confirms that where an agreement is vague and uncertain it is less likely to be deemed by a court to be legally binding. It goes on to give helpful examples relevant generally to determining whether heads of terms are legally binding.

Whether a particular set of heads of terms is legally binding is a matter of construction and will depend on the intention and conduct of the parties and whether evidence of these leads objectively to a conclusion that they intended to create legal relations and had agreed all the terms which they regard, or the law requires, as essential for the formation of legally binding relations. The whole course of the parties' negotiations will be considered.

Any practical tips?

Heads of terms are a helpful set of documented principles or commercial terms that can form the basis of an agreement between the parties.

When drafting HoT, to show intention and provide for contractual certainty, parties should consider the following:

- marking a document "subject to contract" helps to avoid ambiguity about contractual intention but may not be fully determinative
- expressing explicitly whether or not the HoT are intended to be legally binding or separating out binding terms from non-binding terms and placing them into different paragraphs or documents
- including a statement that the heads of terms are not exhaustive to allow for change and further negotiation.

If it is intended to have a (short form) binding agreement ensure that all of the essential terms are included, and the document meets the minimum requirements for an effective contract.

COMMERCIAL

"The label heads of terms (HoT) is not indicative of whether a document has contractual effect."

rpc.co.uk