RPC

Snapshots for Meta

SUMMER 2023

KEY UK AND EU DEVELOPMENTS FOR META'S COMMERCIAL LAWYERS

The EU-US Data Privacy Framework has landed

PLUS

The UK Government's approach to AI regulation

The Digital Markets, Competition and Consumers Bill – a gamechanger on UK consumer regulation

'Carbon neutral' and 'net zero' under greenwashing spotlight

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Welcome to the Summer 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
- Daniel Jackson
- Jess Kingsbury
- Nadia Tymkiw
- Mimosa Canneti
- Adam Williamson
- Aiswarya Nadesan
- Catriona McIntosh
- Chloe Shum
- Daniel Williams
- Elliott Davis
- Emily Snow
- Harpreet Kaur
- Jack McAlone
- Jake Cotterill
- Joshua Ajose-Adeogun
- Karolina Lewicki
- Klaudia Lapinska
- Laura Verrecchia
- Lauren Paterson
- Lewis Manning
- Mars Yeung
- Nancy Elesawe
- Nicci Da Costa
- Nick McKenzie
- Nneka Ezekude
- Pu Fang Ching
- Rebecca James
- Regina Gabbasova
- Sophie Hudson
- Sophie Yantian
- Tamara Hartmann
- Will Monaghan

EDITORIAL

Sub-editors Olly Bray, David Cran, Rupert Cowper-Coles, Praveeta Thayalan, Joshy Thomas, Anila Rayani

Design Rebecca Harbour

Contents

DATA

The EU-US Data Privacy Framework has landed

The question

What does the adoption of the EU-US Data Privacy Framework (**DPF**) look like and how did the European Commission (**EC**) get comfortable with the adoption of its adequacy decision for the DPF?

The key takeaway

Following changes to US intelligence-gathering, the DPF has been adopted by the EU as a lawful basis for trans-Atlantic data transfers between EU data exporters to US data importers, provided that those importers have certified that they comply with a prescribed set of data protection principles under the DPF. While this means that certain cross-border transfers of personal data to the US from the EEA now do not require the use of EU Standard Contractual Clauses (**SCCs**), it is almost inevitable that the DPF will come under heavy scrutiny and likely attack from activist groups. It remains to be seen if the DPF can keep standing where the Safe Harbour and Privacy Shield before it failed to do so.

The background

This is the third attempt by the EU in setting up a lawful framework for trans-Atlantic data transfers, after the Court of Justice of the European Union (**CJEU**) invalidated both the previous Safe Harbour and Privacy Shield following legal challenges by privacy campaigner Max Schrems. Since then, EU businesses have had to implement and rely on the SCCs.

In 2022, the European Commission and the US began to work on a replacement transfer framework and, at the end of last year, President Biden signed an Executive Order setting out the steps the US will take to meet its obligations under the DPF (see Winter 2022 Snapshots). Subsequently, the European Commission adopted an adequacy decision on 10 July 2023, recognising that the US had improved the protection of EU personal data and implemented a means for data subjects to enforce their rights.

The development

Following the publication of the draft adequacy decision in December 2022, the EC adopted a final version on 10 July 2023.

In order for a US business to certify under the DPF, it must (i) be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or a similar US body as approved under the DPF; (ii) publicly declare its adherence to the principles of the DPF; (iii) publicly disclose its privacy policies in line with those DPF principles; and (iv) fully implement them. The FTC and Department of Transportation will likely be the primary bodies responsible for enforcing certifying companies' compliance with the DPF framework going forwards.

"Following changes to US intelligence-gathering, the DPF has been adopted by the EU as a lawful basis for trans-Atlantic data transfers between EU data exporters to US data importers, provided that those importers have certified that they comply with a prescribed set of data protection principles under the DPF."

DATA

Businesses complying with the GDPR can transfer personal data to those certified US businesses without the use of the SCCs. If a business was previously certified under the Privacy Shield, it will need to update its privacy policies to comply with the DPF in order to certify under the new framework. A website listing US certified businesses which can import EU data will be made available.

Significantly, EU data subjects will be able to obtain redress for any illegal use of their personal data by US intelligence agencies directly in the US through a newly created Data Protection Review Court (**DPRC**). Data subjects can submit complaints to the DPRC which can issue binding remedial measures to be taken. This sits alongside other methods of redress available in US law including specific avenues to seek legal recourse against government officials for unlawful government access to, or use of personal data. This has been a particularly contentious topic in the discussions surrounding the draft adequacy decision.

Why is this important?

This new mechanism for EU to US data transfers will reduce the negotiating times between parties who would otherwise be required to incorporate the SCCs into their data sharing or processing agreements. Transfer impact assessments (**TIAs**), which can be time consuming and expensive exercises in themselves (sometimes requiring overseas counsels' advice), will not be required under the DPF. It is estimated that data flows support around €1 trillion worth of service exports to the US. The hope is that this will increase as more US businesses certify under the DPF and EU businesses start to make the most of the efficiencies gained.

Following the success of the legal challenges made to the Privacy Shield, it is clear that the DPF is going to be critiqued, scrutinised and, in all likelihood, legally challenged. The adoption was criticised immediately by noyb, the data protection activist group led by Max Schrems, which said it would challenge the DPF most likely at the start of 2024. Critics argue that the US has not significantly changed its intelligence-related laws meaning that the DPF still has the same fatal flaw as its predecessor. The EU is confident that the DPF will be able to withstand such a challenge as it was designed with the latest case law in mind.

The UK is expected to follow suit later this year with its much awaited "data bridge" announced on 8 June by Rishi Sunak and Joe Biden. It is likely to follow the structure of the DPF to avoid the UK risking the loss of its adequacy decision issued by the EU. UK businesses who engage in trans-Atlantic data transfers will need to keep a close eye on these developments.

Any practical tips?

EU data exporters wishing to transfer data under the DPF will need to ensure that the US importer is certified under the DPF. It would also be worth checking that the US importer has also reflected its commitment to the DPF in its privacy notices. In a similar vein, the EU exporter relying on the DPF will need to include the relevant information in its own privacy notices. While TIAs are not required under the DPF, existing TIAs should be reviewed to take into account the new amendments to US intelligence-gathering.

The big question is whether the DPF will withstand the almost inevitable legal challenges which will follow by the activist groups such as noyb, and whether it eventually bites the dust like the Safe Harbour and the Privacy Shield. And this in turn raises the question as to whether to include the SCCs in your data protection agreements as a fallback transfer mechanism, with express wording that they kick in if the DPF is eventually invalidated. This is a drafting point which deserves reflection when you are reviewing the next data protection agreement which lands on your desk.

DATA

EU Data Protection Board guidance on international data transfers

The question

How does the recent guidance issued by the European Data Protection Board (**EDPB**) assist businesses in complying with the EU GDPR when carrying out international data transfers?

The key takeaway

The EDPB has clarified the circumstances in which parties must take additional steps to ensure that personal data is safeguarded when it is transferred to data controllers or processors located outside the EEA.

The background

In February this year, the EDPB issued guidance (the **Guidance**) to help data controllers and processors comply with the EU GDPR when transferring data internationally. The official title of the Guidance is: "Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR".

Article 3 sets out the territorial scope of the EU GDPR. Under Chapter V of the EU GDPR, a transfer of personal data to a country outside the EU (a **Restricted Transfer**) may only take place if either (i) the third country is subject to an adequacy decision; or (ii) appropriate safeguards have been used (eg standard contractual clauses or binding corporate rules), which aim to create enforceable legal rights and effective legal remedies to ensure that data which is transferred outside the EU is kept safe. The provisions of Chapter V aim at ensuring the continued protection of personal data after it has been transferred to a third country or to an international organisation. However, there has since been some confusion as to what constitutes a Restricted Transfer and how the appropriate safeguards should be applied where the relevant parties (especially the data exporting party) are located outside the EU but subject to the EU GDPR.

The development

The EDPB has set out a three-stage test to enable parties to establish whether the intended transfer is a Restricted Transfer:

- a controller or processor (**exporter**) must be subject to the GDPR for the given processing
- the exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller or processor (**importer**).
- the importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3.

The Guidance also provides 12 examples to help readers understand what does and does not constitute a Restricted Transfer. If there is a Restricted Transfer then, unless a particular derogation or exemption applies, the parties must use one of the appropriate safeguards aimed at protecting the data after it leaves the EEA. These safeguards include seeking to address possible conflicting national laws and government access in the third country, as well as the difficulty to enforce and obtain redress against an entity outside the EU.

Interestingly, the Guidance also recommends safeguards that should be applied where technically no Restricted Transfer takes place, but personal data is still processed outside the EEA (for example, where an employee of an EU controller travels abroad and has access to the data in a third country). The EDPB reminds organisations that they are responsible for their data processing activities regardless of where these take place. As an example, the EDPB notes that, in some circumstances, it may be reasonable for a controller to restrict employees from bringing laptops to certain third countries.

For ease of reference, and to see how useful the 12 examples are, here they are (noting that the Annex to the Guidance analyses each in turn):

- **example 1:** controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR)
- **example 2:** controller in a third country collects data directly from a data subject in the EU (under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities
- **example 3:** controller in a third country receives data directly from a data subject in the EU (but not under Article 3(2) GDPR) and uses a processor outside the EU for some processing activities
- **example 4:** data collected by an EEA platform and then passed to a third country controller
- **example 5:** controller in the EU sends data to a processor in a third country
- **example 6:**processor in the EU sends data back to its controller in a third country
- **example 7:** processor in the EU sends data to a sub-processor in a third country
- **example 8:** employee of a controller in the EU travels to a third country on a business trip
- **example 9:** a subsidiary (controller) in the EU shares data with its parent company (processor) in a third country
- **example 10:** processor in the EU sends data back to its controller in a third country
- **example 11:** remote access to data in the EU by a third country processor acting on behalf of EU controllers
- **example 12:** controller in the EU uses a processor in the EU subject to third country legislation.

Why is this important?

The extra-territoriality provisions of the EU GDPR are far-reaching and, indeed, most multi-national companies are within scope of the EU GDPR in some way. The Guidance, therefore, is helpful in recognising the complex data flows that are typical for such businesses and clarifying which are Restricted Transfers and subject to additional obligations under the law. Businesses should note, however, that their duties do not fall away simply because the data transfer does not fall specifically within the "Restricted Transfer" definition under the GDPR and that they may be required to put in place additional safeguards and processes depending on the country in which the data is being processed. Furthermore, while the Guidance is only binding with respect to the EU GDPR, it is also likely to be instructive in interpreting the UK GDPR.

Any practical tips?

Businesses should assess to what extent the new Guidance would result in their data transfers being re-characterised as either a Restricted Transfer or not. None of the positions by the EDPB in the Guidance are controversial, however, and so it is likely that the Guidance aligns with businesses interpretation of the GDPR transfer restrictions to date. However, particular attention should be paid to the EDPB's recommendations regarding data processed in a third country that, whilst not a Restricted Transfer, may still be subject to access by national authorities in that country as this may affect businesses' internal processes and policies.

DATA

DATA

The new Data Act and the EU's vision for non-personal data sharing in Europe

The question

What does the proposed EU Data Act mean for the usage and sharing of non-personal data by businesses?

The key takeaway

The proposed EU Data Act (the **Act**) will govern the ownership, access, use and storage of non-personal data generated by connected devices and machinery such as smart appliances. Foreign products and services supplied to users in the EU will also be subject to the proposed Act.

The background

In February 2022, as part of the EU's 2020 Data Strategy, the European Commission proposed a new Act which sets out a framework to govern the use and sharing of non-personal data. The Act is not a replacement for the EU General Data Protection Regulation but is intended to focus on non-personal data generated by connected devices and services arising from such devices. Issues regarding the use of such data have been brought into sharp relief due to the rise in popularity of smart household appliances and industrial machinery as well as the rapid development of artificial intelligence.

The development

On 24 March 2023, the EU law-making institutions entered into trilogues – the last stage before the EU officially agrees on the text of the Act.

The Act is expected to apply extra-territorially so products and services which are supplied to the EU will also be within scope.

The Act introduces the following obligations:

- manufacturers and service providers must design connected products and services which allow users (both individuals and businesses) to access their data with ease
- users should be given the option to consent for their data to be shared with third parties
- data holders must implement measures to safeguard data
- data sharing agreements between businesses must be fair, and
- cloud operators and data processing service providers will be subject to interoperability requirements to facilitate customers' ability to switch between providers easily. The European Commission may adopt delegated acts or implement additional harmonised standards to introduce further interoperability requirements.

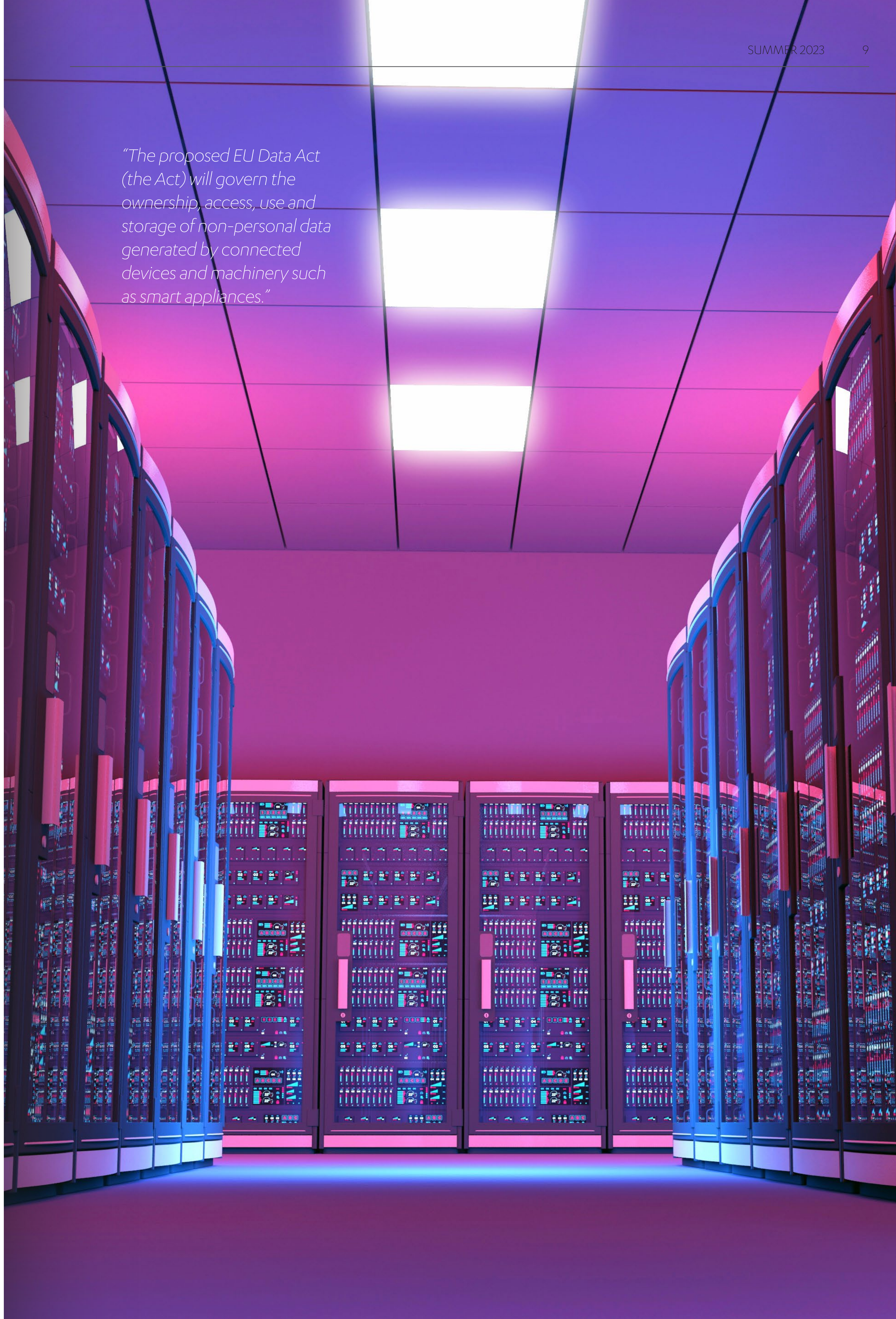
Regulators may impose administrative fines as per their discretion on manufacturers and data holders if they do not comply with the above measures.

Why is this important?

For businesses who invest heavily in collecting, analysing and monetising data collected through their products or services, the new Act is significant as it would require that such data be made accessible to users, other third parties and the public sector. The new interoperability requirements are also noteworthy as these will likely result in a compliance cost for cloud providers and may affect their customer base and market share.

Any practical tips?

Manufacturers of connected devices and data holders should review their data collection and data use strategies in light of the new obligations under the Act. New processes and systems would also need to be implemented to ensure that users are able to exercise their rights under the Act. Cloud providers and data processing service providers should review the interoperability and switching standards set out in the proposed Act as against their infrastructure and keep an eye on further requirements that may be issued by the European Commission in the future.



"The proposed EU Data Act (the Act) will govern the ownership, access, use and storage of non-personal data generated by connected devices and machinery such as smart appliances."

DATA

ICO updates its guidance on AI and data protection

The question

What are the key data protection principles which the Information Commissioner's Office (ICO) expects organisations to follow when integrating AI into their product and service offerings?

The key takeaway

Given the ICO's commitment to safeguarding vulnerable persons, and recent industry concerns in relation to the use of generative AI technology (eg ChatGPT, AlphaCode, Google Bard), the ICO believes these updates should provide clarity to the UK technology industry on how data protection can be appropriately embedded into those product and service offerings using AI. As such, the updated guidance provides a methodology for assessing AI applications, with a focus on processing personal data in a fair, lawful, and transparent manner.

The background

On 15 March 2023, the ICO published several updates to its "AI and data protection" guidance. These updates aim to deliver on the ICO's commitment (under ICO25) to assist organisations in adopting new technology, while safeguarding people, especially the vulnerable. The updates also demonstrate the ICO's support for the UK Government's "pro-innovation" approach to AI, as outlined by the Government's White Paper published on 29 March (see also our reaction to the UK government's White Paper on AI).

The development

Below is a breakdown of the ICO's key updates and the GDPR principles to which they relate:

- **accountability** – similar to many of the ICO's recent updates to its guidance, new content has been included which provides further clarity about what organisations using AI should consider when performing a data protection impact assessment (**DPIA**). As before, a DPIA should be conducted where an organisation's use of AI involves:
  - systematic and extensive evaluation of individuals based on automated processing, including profiling, on which decisions that produce legal, or similarly significant effects, will be made
  - large-scale processing of special category data
  - systematic monitoring of publicly accessible areas (eg internet forums) on a large scale, and
  - processing operations which are likely to result in a high risk to the rights and freedoms of data subjects (eg data matching, invisible tracking, or behaviour tracking).

Where the above conditions are met, the ICO now expects that an organisation's DPIA will assess whether it is "more or less risky" for the organisation to use an AI system. This means that the DPIA should demonstrate that the organisation has considered: (i) using alternatives to the AI system (if any) which present less risk to individuals, individuals' rights, the organisation, or wider society, and which achieve the same result; and (ii) why the organisation chose not to use any less risky alternatives which were identified. The ICO states that these considerations are particularly relevant where an organisation uses public task or legitimate interests as its lawful basis for processing personal data.

Additionally, when considering the impact of using a particular AI system to process personal data, the ICO has stressed that an organisation's DPIA should consider:

- **allocative harms** – harms caused by decisions to allocate goods and opportunities eg favouring male candidates in a recruitment process
- **representational harms** – harms caused by using an AI system which reinforces the subordination of groups based on identity factors eg an image recognition system which assigns labels reflecting racist stereotypes to pictures of a individuals from a minority group
- **transparency** – the ICO has added a new standalone chapter to its "Explaining Decisions Made with AI" guidance. This new chapter focuses on the importance of organisations being transparent with individuals where they process their personal data using AI systems. The key practical point under these updates is that, where an organisation collects data directly from certain individuals to train an AI model, or apply an AI model to those individuals, then the organisation must provide privacy information to them before their data can be used for that purpose. Further, where such data is collected from other sources, the organisation must provide privacy information to the individuals within a reasonable timeframe (no later than one month), or earlier, if the organisation contacts the individuals or provides their data to a third party
- **lawfulness** – here, the ICO has added two new sections to its chapter on "What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?". In these new sections, the ICO focuses on:
  - Using AI to make inferences – organisations may use AI to guess or predict details about individuals or groups, or use correlations between datasets to categorise, profile, or make predictions about such individuals or groups. The ICO states that such "inferences", can constitute personal data, or special category data in and of themselves. To constitute personal data, it must be possible to relate the inferences to an identified or identifiable individual. To determine if an inference constitutes special category data (triggering Article 9 UK GDPR), organisations should assess whether the use of AI allows them to: (i) infer relevant information about an individual; or (ii) treat someone differently based on the inference
  - Relationship between inferences and affinity groups – where inferences permit organisations to: (i) make predictions about individuals; (ii) create affinity groups from those predictions; and then (iii) link the predictions to specific individuals, the ICO stresses that data protection law will apply. Specifically, it will apply to: (i) the development stage of a product or service offering ie using personal data to train an AI model; and (ii) the deployment stage of a product or service offering ie applying an AI model to other individuals outside of the training dataset. Additionally, organisations must consider whether such processing may cause damage to the individuals whose data is being processed, whether data protection by design has been appropriately implemented in the offering, and the impact on society the offering will have once it's deployed
- **fairness** – the new content introduced by the ICO to its chapter on "Fairness in AI" states that organisations should only process personal data (including for an AI offering) in a manner which individuals would reasonably expect, and not use data in a way that would cause unjustified adverse effects on individuals. The guidance stresses that where organisations utilise AI, they should ensure that both the processing itself, and the decisions made based on that processing, are sufficiently statistically accurate such that they do not discriminate against individuals. In addition to highlighting that the fundamental principles of UK GDPR must be considered throughout the design and development of an AI offering, the guidance refers to the importance of data protection by design and default considerations, and of performing a comprehensive DPIA. Further, a new annex, "Fairness in the AI lifecycle", details the fairness considerations which the ICO expects AI engineers and key decision-makers to keep in mind throughout the development and use of their AI products and services.

Why is this important?

These updates provide AI engineers and key decision-makers with important reference materials when considering, designing, developing and deploying their product or service offerings which make use of, or which will make use of, AI technology. By following and implementing the fundamental principles of UK GDPR, as well as the specific recommendations detailed by the ICO, organisations can help ensure they mitigate the risk of future enforcement actions.

Any practical tips?

While these updates provide additional clarity, they should be viewed as a supplement to, not a substitute for, the ICO's original "AI and data protection" guidance, and the ICO's recommendations in its "Explaining Decisions Made with AI" guidance.

For a practical, step-by-step guide on how organisations can reduce the risk of enforcement action being taken against their products and services, the ICO has developed an "AI and data protection risk toolkit". This toolkit, when viewed together with the ICO's AI guidance, provides a template against which organisations can compare their internal AI design and development processes. It helps them ensure they are meeting the key points which the ICO expects from a data protection and privacy perspective on the integration and utilisation of AI in their products or services.

"Given the ICO's commitment to safeguarding vulnerable persons, and recent industry concerns in relation to the use of generative AI technology (eg ChatGPT, AlphaCode, Google Bard), the ICO believes these updates should provide clarity to the UK technology industry on how data protection can be appropriately embedded into those product and service offerings using AI."

ICO publishes new guidance on privacy in the product design lifecycle

The question

What are the key privacy considerations that the Information Commissioner's Office (**ICO**) expects organisations to implement in the design and development of their new products and services?

The key takeaway

Given the ICO's commitment to safeguarding vulnerable persons, and recent industry concerns in relation to the use of generative AI technology (eg ChatGPT, AlphaCode, Google Bard), the ICO believes these updates should provide clarity to the UK technology industry on how data protection can be appropriately embedded into those product and service offerings using AI. As such, the updated guidance provides a methodology for assessing AI applications, with a focus on processing personal data in a fair, lawful, and transparent manner.

The background

Previously, the ICO's "data protection by design and default" guidance provided controllers with a general framework for the safeguards they should consider when integrating data protection in their processing activities, and business practices. While this guidance was helpful, it did not provide organisations with any specific steps they could take to achieve data protection compliance. Instead, organisations were advised to implement "appropriate technical and organisational measures", adhere to fundamental data protection principles, and to remember that "what you need to do depends on the circumstances of your processing and the risks posed to individuals".

This new guidance fulfils the need for a more specific roadmap for achieving data protection compliance. It sets out the key privacy considerations across six distinct phases in the product development lifecycle. These are: (i) kick-off, (ii) research, (iii) design, (iv) development, (v) launch, and (vi) post-launch.

The development

Below is a summary of the key privacy considerations which the ICO states organisations must, and should, consider during each of these phases:

Kick-off phase

During this phase, the ICO stresses the importance of considering privacy, as early as possible, when scoping a new product or feature. This requires product designers and developers to consider:

- **ongoing collaboration** – project teams should introduce their projects to their colleagues, with expertise in data protection, as early as possible. This enables a lawful basis for the processing of any personal data to be identified. Further, once a lawful basis is identified, the ICO stresses the importance of recording this by preparing (i) a data protection impact assessment (DPIA), and (ii) a plan which contains milestones for raising any privacy issues which crop up with senior stakeholders. According to the ICO, these actions will assist organisations in demonstrating the data protection compliance of their products or services
- **data mapping** – project teams should consider the personal data, especially special category data, which their products or services might use across the product or service's entire range of features. They should also ensure that any processing meets the conditions set out under UK GDPR. Here, the ICO stresses that, where children are likely to access a service (even if they are not the target audience/user), the implications of the Children's code are key considerations (see our analysis of the ICO's guidance on compliance of game design with the Children's code)
- **any changes and risks** – the relationship between the organisation and the user should be reviewed to determine whether the data is provided directly by the user, or if it is inferred, or derived, another way. This will ensure that project teams are live to the risk that their new product or service could create "knock-on" privacy risks for existing features, potentially assisting bad actors, or cyber-attackers
- **responsibilities** – project teams should assign and agree responsibilities for privacy decisions with internal stakeholders. This ensures that anyone with final accountability for these decisions is aware of this. Further, all team members should be kept informed about key decisions and privacy risks/threats eg via an alert system, or audit trail.

ICO publishes new guidance on privacy in the product design lifecycle (cont.)

Research phase

In this phase, the ICO points out that "research" means user research, UX research, or design research, which designers and developers may use to understand users' needs, or to evaluate product choices. Project teams are expected to:

- **protect the privacy of research participants** – all research undertaken as part of a project (eg competitor, consumer, or market research), must be conducted ethically. This means ensuring that only the minimum amount of data about research participants is collected, any data collection is clearly explained, consent is sought (where appropriate) for collection, and any results are anonymised (where possible).

Design phase

The new guidance states that designers and developers "must consider privacy throughout the design process". This can be demonstrated by:

- **considering privacy throughout design activities** – this means designers should avoid using real user data when prototyping or mocking up interfaces
- communicating about privacy in an understandable way – all privacy information should be communicated in a concise, transparent, intelligible, easily accessible manner (ie using clear and plain language), and across a variety of mediums (ie not just through privacy notices)
- **being targeted** – while privacy information must be provided at the time the personal data is collected, project teams should consider providing such information when users might expect to receive it so that they are assisted in making reasonable, informed choices.
- **ensuring consent is valid** – where consent is required, it must be (i) freely given, (ii) specific, (iii) informed and (iv) just as easily withdrawn. Here, the ICO reiterates that pre-ticked opt-in boxes are specifically banned, and unnecessary consent popups should be avoided
- **empowering people** – organisations must allow people to exercise their rights (eg access, rectification, and data portability), and consider how to assist people in exercising their rights directly through the new product or service.

Development phase

During this phase, project teams are encouraged to bring forward all the privacy planning they have performed in the previous phases to engineer the finished product or service. This should involve:

- **collecting the minimum amount of personal data** – organisations should only collect the data they really need. This should be analysed by (i) reviewing the data maps from the kick-off phase, (ii) clarifying what the new product or service is trying to achieve, and (iii) ensuring that users can access as much functionality as possible before providing personal data
- **enhancing privacy and security measures** – this means that appropriate encryption, anonymisation, and other privacy-enhancing measures should be utilised
- **ensuring users can exercise their rights** – as in the design phase, this requires project teams to ensure that users can enter their personal data accurately and request its amendment
- **protecting personal data during development** – organisations must implement appropriate technical and organisational measures such as, setting up proper access controls, logging data interactions, and establishing retention policies.

Launch phase

Here, the ICO stresses the importance of reviewing any final privacy issues before launching a new product or service.
This requires project teams to:

- **mitigate privacy risks found in earlier phases** – project teams should run regression tests to determine if a new product feature could break old code. Further, they should remove, or replace, test data, before going live. The New Guidance also provides that there should be agreement from legal, and senior stakeholders, that a new product, or service, is ready for launch
- **factor privacy into rollout plans** – this requires project teams to have a rollback strategy, or contingency plan, where something goes wrong. The ICO specifically states that such plans are crucial because, if user access to the product, or service, is affected, it must be restored in a timely manner. Further, where an organisation stores, or accesses information on a user's device to assess novel privacy issues, user consent must be obtained
- **tell users what to expect** – this states that, if a change to the new product, or service, will affect the processing of personal data, this must be communicated to users in a clear and understandable manner.

DATA

Post-launch phase

During this phase, the ICO reminds organisations that the launch phase is not the end of data protection compliance. Instead, organisations must review how users are interacting with the new product, or service, and consider any fixes which may be required. This means:

- **monitoring and fixing issues, as required** – organisations should examine whether any unexpected privacy issues have arisen and run regression tests to determine if the new product feature has broken any old code
- **reappraising users' expectations and norms** – organisations should be live to how any changes to the features of the new product, or service, may significantly affect people's privacy expectations, or introduce new privacy risks. Further, organisations should assess any emerging privacy implications where they see significant new user behaviour.

Why is this important?

The new guidance is the latest move by the ICO to demonstrate its commitment to pragmatism and regulatory certainty. It provides designers, developers, product managers, and engineers with a new template for how they can embed data protection into their products and services. The guidance can now be used by organisations as an invaluable future-proofing tool, enabling them to review their policies, plans, internal Wikis, and playbooks, to ensure that they align with the key privacy considerations that the ICO has outlined.

Any practical tips?

While the guidance is instructive, it should be viewed as a supplement to, not a substitute for, the ICO's previous guidance on "data protection by design and default". As such, when reviewing any internal policies, plans, Wikis and playbooks, organisations should review both pieces of ICO guidance, together. Further, when designing and developing new products, and services, designers and developers can now supplement the new guidance with the ICO's new "Innovation Advice Service". While this service is currently in Beta, it provides a forum for organisations which are doing new or innovative things 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.

DATA

ICO's new draft guidance on "likely to be accessed by children" under the Age Appropriate Design Code

The question

When will an online service fall within the scope of the Age Appropriate Design Code?

The key takeaway

Assessing whether an online service is likely to be accessed by children is a continuous exercise. A service that at the outset did not fall within the scope of the Code, due to an insignificant number of children accessing the service, may find itself in scope.

The background

The Age Appropriate Design Code (also known as the "Code" or the "Children's Code") came into force on 2 September 2020 with the aim of ensuring that providers of online services "likely accessed by children", comply with their duties and responsibilities under different data protection laws, such as UK GDPR and The Data Protection Act 2018 (the **Act**), to protect children's personal data online.

The Code applies to "information society services likely accessed by children", meaning "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". This includes social media platforms, online marketplaces, online messaging platforms and search engines.

The development

In September 2022, the ICO published draft guidance which included FAQs, a list of factors and case studies, to assist Information Society Service (**ISS**) providers in assessing whether children are likely to access their services, after making it clear that adult-only services may fall within scope of this Code.

Under the ICO guidance, all ISS providers must determine whether children are likely to access their services, which includes adult-only services, services aimed at children and services that are not intended to be used by children but are accessed or are likely to be accessed by a "significant number of children" or individuals under the age of 18 years (ICO guidance provides that the actual identity of under 18s does not need to be established).

The "significant number of children" phrase stipulates that the ISS provider must determine whether "more than a de minimis or insignificant number" of children are likely to access the service provided, thus children must form a material group of users or likely users.

When a provider uses an age-gating page to restrict access by children, the page itself does not fall within scope, if the age-gating page is effective, robust and an extension of the adult site (however, this page must nevertheless be compliant with data protection legislation).

A list of non-exhaustive factors should be used by the ISS provider to determine whether the services are likely to be accessed by children, these include:

- the number of child users in absolute terms, or the proportion of all UK users or the proportion of all children in the UK that the child users of the service represent
- evidence of user behaviour
- information on the likely appeal of advertisements in use
- information about complaints received regarding children accessing the service
- content, design features and activities, which might draw children's attention
- research – public or commissioned independently
- understanding whether children are accessing services similar in nature and content, and
- whether the way the services are marketed, described, and promoted targets under 18s.

If the ISS provider concludes that children are likely to access the service and such service is not appropriate for children, the provider should apply age assurance measures to restrict access or ensure that services comply with the Children's Code in a "risk-based and proportionate manner".

Why is it important?

Although this guidance is in draft form and undergoing consultation, it is helpful for ISS providers when determining whether the services provided are "likely to be accessed by children". When finalised, this will be a welcome guidance for providers, who previously may have found it difficult to ascertain whether services fall in scope, given the lack of guidance in this area.

Any practical tips?

Every ISS provider should determine whether children are likely to access the services using the non-exhaustive list of factors prepared by the ICO.

Where an ISS provider determines that children are not likely to access the services provided, the provider should document the decision and provide evidence. The ICO provides several examples, which include "market research, current evidence on user behaviour, the user base of similar or existing services and service types and testing of access restriction measures".

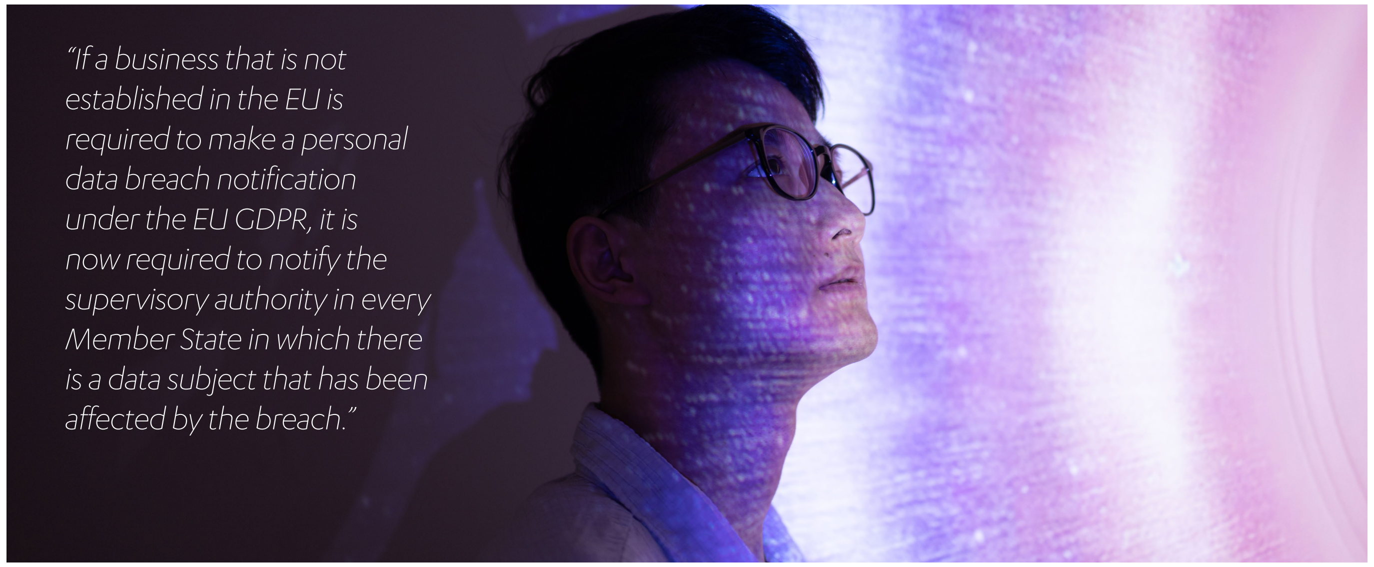
DATA

Assessing whether children access the services should be an ongoing exercise. Although it may seem that children are unlikely to access a service, or if it is found that in fact a "significant number of children" are accessing the service, the Code will apply. The Code also applies to new and existing services.

Simply stating in the terms of service section that individuals under the age of 18 should not access the service does not excuse the ISS provider from complying with the Code, when in reality, children access the service. As mentioned by the ICO, a self-declared age assurance method may not be effective in restricting children's access to content which is not children appropriate. If services are offered to children, a data protection impact assessment (**DPIA**), must be carried out and such should consider each factor from the non-exhaustive list provided by the ICO.

"A service that at the outset did not fall within the scope of the Code, due to an insignificant number of children accessing the service, may find itself in scope."

European Data Protection Board updates guidance on data breach notifications



The question

How does the recent update to the European Data Protection Board (**EDPB**) guidance impact data breach notifications for businesses?

The key takeaway

If a business that is not established in the EU is required to make a personal data breach notification under the EU GDPR, it is now required to notify the supervisory authority in every Member State in which there is a data subject that has been affected by the breach.

The background

EDPB Guidelines 9/2022 (the **Guidelines**) were originally adopted in October 2022 and set out guidance regarding a controller's obligations in the event of a personal data breach. When a breach occurs that is likely to result in a risk to the rights and freedoms of data subjects, Articles 33 and 34 of the GDPR require the controller to notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Previously, a controller not based in the EU who suffers such a breach would typically notify the supervisory authority in the Member State in which its EU representative is located.

The development

Following a consultation in October 2022, paragraph 73 of the Guidelines was amended and the updated Guidelines were adopted on 28 March 2023.

The amended paragraph 73 states that the mere presence of an EU representative (of a controller not based in the EU) does not trigger the one-stop shop system. Instead, in the event of a breach, the controller must notify every supervisory authority for which affected data subjects reside in their Member State.

Why is it important?

The update to the Guidelines places significant new obligations on data controllers in the event of a breach. It is particularly onerous given the timescales for notification set out in the EU GDPR and that failure to comply with the GDPR (as interpreted according to the Guidelines) may result in penalties such as fines.

Any practical tips?

Businesses should consider and identify the strategy they wish to adopt going forwards in light of the obligations of paragraph 73. Some businesses may take the view that, in the event of a breach, the safest approach is to notify all supervisory authorities in the Member States in which the business operates. Given the cost implications, others may look to review their internal processes so that, in the event of a breach, they can identify where the affected data subjects are located and thereby focus their efforts on notification in those Member States.

Italian Data Protection Authority issues fine for use of dark patterns

The question

How can companies ensure that their websites, apps and other online interfaces comply with regulations restricting the use of dark patterns when collecting consent to the processing of personal data?

The key takeaway

Companies must ensure that their online user interfaces are designed in a way that does not manipulate or push users into making a certain choice, for example, giving consent to the processing of their personal data in a way that they did not intend or understand.

The background

The term "dark patterns" describes the techniques used on websites, apps and other online interfaces that impact on a user's ability to make free and informed choices or decisions. European Data Protection Board (**EDPB**) guidelines Dark patterns in social media platform interfaces: How to recognise and avoid them, sets out the different categories of dark patterns that are typically used. For example, users may be "overloaded" with a large amount of information, requests or options which nudges them to share more data than they wish, the interface may be "fickle" in that it is hard for the user to navigate the web page and understand the purpose of the data processing, or users may be "left in the dark" on how their data is processed as the online interface is designed in a way that hides or distorts key information. Companies also use dark patterns to manipulate a data subject into giving consent for the processing of their personal data.

Companies may rely upon data subject consent as a lawful basis for processing under the EU GDPR. However, consent must be freely given, specific, informed, and unambiguous and requests for consent must be clearly presented in clear and plain language. Personal data must also be processed lawfully, fairly and in a transparent manner.

The development

The Italian Data Protection Authority (**Garante**) issued a €300,000 fine for the use of dark patterns in breach of the EU GDPR. The digital marketing services company in question designed its website and other interfaces in such a way that manipulated the consumer into giving consent. For example, if a user did not consent to the use of their data for marketing purposes and to their data being shared with a third party at the same time, a banner would open on screen containing a prominent consent button. The option for the user to continue on the page without providing consent was presented in a much less visible way, on a different part of the web page to the banner.

Users were also prompted to provide contact details for friends that might be interested in the services the user was signing up for. The font used to attract the user to do so was in bold and highlighted with an asterisk, but the option for the user to skip this stage during sign up was small and in italics. In this case, the Garante found that consent had not been properly obtained with respect to those individuals as neither the users nor their friends were provided adequate information regarding the processing of such data.

Why is it important?

This decision highlights the increasing focus on the use of dark patterns online, framed in the broader context of the EU's drive to improve consumer protections across the single market. In particular, by 17 February 2024 all digital services providers in scope of the Digital Services Act will be prohibited from designing, organising or operating online interfaces which deceive or manipulate the recipients of their service or materially distorts or impairs the ability of the recipients of their service to make free and informed decisions. In a wider context, the UK Competition and Markets Authority has also announced a new programme of enforcement focused on "Online Choice Architecture" ie dark patterns.

Any practical tips?

Companies should refer to the EDPB guidelines for helpful best practice recommendations that support EU GDPR compliant interface design on their online platforms. Companies should review their online data gathering and consent processes to ensure requests for consent are clear, not ambiguous and do not push users towards providing consent for use of their personal data.

Be aware also that "dark patterns" are now very much in the sights of consumer regulators also, such as the UK's Competition and Markets Authority. We anticipate that this may be one of the very first areas hit with fines by the CMA when it obtains its new fining powers proposed under the Digital Markets, Competition and Consumers Bill.

DATA

CJEU rules on right to compensation under Article 82 EU GDPR

The question

What must a data subject demonstrate to claim compensation for non-material damage (eg emotional distress/loss of confidence) under the EU General Data Protection Regulation (**GDPR**)?

The key takeaway

To receive an award of compensation for non-material damage under Article 82 GDPR, a data subject must demonstrate that (i) they have suffered damage, (ii) there has been an infringement of the GDPR, and (iii) the infringement is linked to the damage the data subject has suffered. As such, the Court of Justice of the European Union (**CJEU**) has confirmed that there is no "de minimis" level of damages under Article 82 GDPR but that the infringement must have caused some form of damage to the data subject. Infringement of the GDPR, by itself, is not sufficient for compensation.

The background

On 4 May 2023, the CJEU handed down its much-anticipated preliminary ruling in UI v Österreichische Post AG (Case C-300/21). A preliminary ruling is the mechanism by which the CJEU issues a binding decision on questions about the interpretation or validity of EU law. These questions are referred to the CJEU by national courts or tribunals in Member States.

This case concerned an algorithm which was applied to information by Austria's leading postal services provider, Österreichische Post. Österreichische Post's algorithm analysed various social and demographic criteria to predict the political affinities of the Austrian population. From these predictions, Österreichische Post created "target group addresses" and sold these to third parties, enabling those third parties to send targeted political advertisements to individuals.

In this case, Österreichische Post's algorithm predicted that the claimant had a high degree of affinity with a particular Austrian political party. The claimant had not consented to the processing of his personal data for this purpose. While this information was not communicated to third parties, the claimant was caused feelings of great upset, exposure, and loss of confidence, when he discovered that an affinity with this political party was attributed to him and retained by Österreichische Post. Given these feelings, the claimant sought (i) an injunction for Österreichische Post to cease its processing of his personal data for this purpose (granted at first instance and upheld on appeal), and (ii) compensation of €1,000 for the non-material damage he suffered (rejected at first instance and dismissed on appeal).

In particular, the claimant's claim for compensation was dismissed because Austria's Higher Regional Court found that Member States' laws supplement the GDPR. Under Austrian law, the right to compensation for non-material damage arising from a breach of data protection rules would only give the claimant a right to compensation where that damage reached a certain "threshold of seriousness", and "negative feelings" did not reach this threshold.

The development

When the case came before the Austrian Supreme Court, Österreichische Post appealed against the injunction imposed on it, but this was dismissed. As such, only the claimant's appeal against the rejection of his claim for compensation remained before the Supreme Court. The Supreme Court, in examining the concepts of damage, compensation, and effectiveness under EU law, decided to refer three questions to the CJEU. These were:

- is a claimant required to suffer actual harm before they can be awarded compensation under Article 82 GDPR, or is an infringement of GDPR, by itself, sufficient to allow the claimant to receive compensation?
- does EU law require that an infringement of GDPR must have a serious consequence, beyond "mere upset", before compensation may be awarded?
- should an award of compensation be considered in light of EU law requirements?

Question 1

In relation to this question, the CJEU analysed Article 82 GDPR which provides that any person who has suffered material or non-material damage, due to an infringement of GDPR, has the right to receive compensation. The CJEU found that to receive compensation, a claimant must show:

- they have suffered damage
- that there has been an infringement of the GDPR, and
- that the infringement of the GDPR is linked to the damage they suffered.

Further, because the words "damage" and "infringement" appear separately in Article 82 GDPR, the CJEU found that they should be considered different concepts. It found that only an infringement of the GDPR which causes a data subject to suffer damage, will be sufficient to give rise to an award of compensation. In relation to infringements by themselves, the CJEU found that they are covered by Article 77 and Article 78 GDPR which provide legal remedies to a data subject, before, or against, a supervisory authority where there has been an infringement of GDPR (ie administrative fines).

Question 2

Here, the CJEU stated that, according to settled case-law, a provision of EU law (ie Article 82 GDPR), which makes no reference to national Member States' laws, must be given (i) an independent, and (ii) uniform definition throughout the EU. The CJEU found that:

- Article 82 GDPR is independent, and does not refer to Member States' national laws as a way of determining how serious any material, or non-material damage must be to receive compensation, and
- the objective of GDPR is to ensure a consistent, high level of protection of individuals regarding the processing of their personal data in the EU.

As such, while a data subject is required to demonstrate that the consequences of an infringement of GDPR caused the non-material damage they suffered, the Austrian Supreme Court could not say that compensation for such damage should be subject to any set "threshold of seriousness". The CJEU stated that such a finding would undermine the autonomy and uniformity of GDPR, as a "threshold of seriousness" would be different in different Member States.

Question 3

In determining the amount of compensation which would be payable to a data subject, the CJEU found that the GDPR does not contain any provision intended to define rules for the assessment of damages to which a data subject may be entitled under Article 82 GDPR. As such, the CJEU found that individual Member States should prescribe such rules subject to the EU law principles of effectiveness and equivalence:

- **effectiveness** – the CJEU found that national courts should determine whether their national rules for assessing the amount of compensation payable under Article 82 GDPR make it impossible or excessively difficult for a data subject to exercise their rights under GDPR
- **equivalence** – the CJEU found that it would assess whether the legislation of Member States was less favourable to data subjects who are seeking to enforce their rights under EU law. However, there was no evidence of this in this case.

Why is it important?

While this case confirms that data subjects may claim compensation for non-material damage (ie feelings of upset) caused by an infringement of the GDPR, it provides more clarity to controllers on the situations in which a data subject may claim compensation under the GDPR. This ruling is not binding on the UK, but it still represents a persuasive authority, and is likely to inform how the UK courts and the Information Commissioner's Office deal with compensation claims from data subjects in respect of UK controllers going forward.

Any practical tips?

This decision could lead to an increase in non-material damage claims for a data breach linked to the GDPR, including "mere upset". That said, it does not set out what a claimant has to prove for such damage. It remains to be seen, therefore, quite where this decision will take the compensation argument for breaches of the GDPR.

DATA

DATA

Representative action in misuse of private information is struck out by the High Court

***Prismall v Google UK Ltd and another* [2023] EWHC 1169 (KB)**

The question

Can a representative claim in misuse of private information proceed on a "lowest common denominator" basis where it cannot necessarily be proven that all claimants have suffered the same level of harm?

The key takeaway

For a representative action to succeed, every member of the class must be able to show more than trivial loss and damage. Where some members cannot show a viable claim at all, not all members will have the "same interest" in the claim (as required under CPR 19.8), and the representative action is bound to fail.

The background

Andrew Prismall brought a representative claim on behalf of 1.6 million patients whose medical records were used for the purpose of clinical testing of a diagnostic app.

Mr Prismall claimed on behalf of each patient for wrongful interference with their private information, arguing that each Claimant should be awarded damages based on loss of control of their medical information.

A claim was originally brought under data protection legislation but was reissued as an action in misuse of private information after the Supreme Court in Lloyd v Google held that to succeed in data claims each Claimant needs to establish individual damage or distress. Misuse of private information was apparently considered a more effective route for representative actions given "loss of control" damages are available – which can more easily be demonstrated by the entire class.

The defendants sought to strike out the claim, alleging that the position of each member of the class was very different, meaning that the claimant could not adequately prove that the defendants misused the private information of each and every member. According to the Defendants, many of those represented would not have a valid claim at all, so without an individual assessment of entitlement for each of those represented (which would defeat the "same interest" requirement in a representative action), the claim must fail.

The decision

The defendants were successful in their application to strike out the claim and summary judgment was granted.

This was not a situation where it could be assumed that every member of the class was entitled to damages or could establish a reasonable expectation of privacy – each would have different privacy interests in the personal medical information processed by the defendants.

The Court established a list of lowest common denominator characteristics that every member of the Class would have – against which the question of whether every member of class had a reasonable expectation of privacy (and therefore had the "same interest" in the claim) would be assessed. These included: that limited information was transferred and stored; that the information transferred was anodyne in nature; that the extent of intrusion was the transfer of the data and its secure storage; and that there was no other impact save for the loss of control itself. Against these factors, the Court held that each member of the Claimant class did not cross the de minimis threshold for demonstrating a reasonable expectation of privacy in the information.

If, as in this case, individual assessments of damages are required to establish an entitlement to more than trivial damages, then the "same interest" test is not met, and the claim cannot be brought as a representative action.

Why is this important?

This judgment is a welcome indication that claimants cannot use class actions in misuse of private information to circumvent the recent decision in Lloyd v Google. A viable representative action claim will need to ensure that each member of the class can demonstrate they have the "same interest" in the claim and that this interest is more than trivial. Where individualised factors are relevant to demonstrating a viable cause of action, the result is that individual claims rather than class actions must be brought.

Any practical tips?

This decision reinforces the inherent difficulties for Claimants in forming viable opt-out data privacy actions under CPR 19.8.

Strike out and summary judgment applications will continue to be useful tools for Defendants when attempting to dispose of unmeritorious class actions at an early stage.

DIGITAL

Government White Paper sets out UK approach to AI regulation

The question

How is the UK Government looking to regulate AI?

The key takeaway

The UK Government plans to frame the regulation of AI in the UK around five key principles it believes will support innovation and foster public trust in the technology. The Government White Paper AI regulation: a pro-innovation approach, (the **White Paper**), published in March 2023 was the first step towards developing this new framework. And, in May 2023, we started to see regulator action as the Competition Markets Authority (**CMA**) launched an initial review of AI models in view of the five principles set out in the White Paper (the **May Review**) which was quickly followed in June by the CMA's response to the White Paper consultation (the **Response**).

The background

AI has been the hot topic since the end of 2022 as phrases like "language models", "training data" and "machine learning" have become common parlance. However, no AI-specific regulatory mandate exists in the UK. To date, the Government has relied on existing regulators to use their regulatory powers to address AI within their remit. This has created a web of regulation that is meant to cover the use of AI across the whole economy. This approach has inevitably led to gaps in the regulatory framework and uncertainty for businesses, consumers, innovators and even regulators.

The Government has been looking at AI and how it is regulated since it published the AI Sector Deal in 2018 (the **Sector Deal**). The Sector Deal established government funding for, and set out actions to promote, the development of AI in the UK. A number of papers and reports have since followed, including the AI Roadmap and an independent report setting out recommendations for the Government's approach to AI.

Following the release of the White Paper, the Government has called on regulators to review the use of AI within their remit to think about how it can promote innovation based on the five key principles.

The development

The White Paper

The Government describes the approach in its White Paper as "flexible", "pro-innovation", and "deliberately agile and iterative", clearly envisaging regulation to develop with AI. There are two key concepts in the White Paper which underpin the overall proposed regulatory framework: the five principles and the new central support function.

The five principles, the Government says, are fundamental to the safe and responsible design and use of AI. They will ensure that:

- AI systems are "safe, secure and robust"
- information concerning the decisions made by AI is "transparent" and "explainable"
- AI systems are "fair"
- those that supply and use AI have sufficient "governance and accountability", and
- decisions and outcomes produced by AI are "contestable" and "redressable".

Whilst, for now at least, regulators would not be under a statutory duty to enforce these principles, they would be encouraged to consider them when regulating and setting industry guidance.

The new central support function would tie the regulators together and help close the gaps, according to the White Paper. The central support function's role would be to monitor the use and effectiveness of the overall framework and incorporate feedback into further iterations of AI regulation. It would also be responsible for supporting businesses and innovators to understand the regulatory regime.

Following an initial period of implementation, the Government plans to review the effectiveness of the framework and take a view as to whether a statutory duty to have "due regard" to the principles needs to be imposed on regulators. For now, at least, the Government believes that not legislating allows regulation to remain agile, flexible and responsive to changes in AI and the market.

The CMA's review

The aim of the May Review is to develop an "early understanding of the market for foundation models" and to identify the risks and opportunities for consumers and competition associated with the use of AI. The May Review will focus on three themes:

- consumer protection
- competition and barriers to entry within the sector, and
- the impact of AI models on competition in the wider economy.

The CMA has clearly been busy thinking about AI regulation, and the Response, published in early June, was supportive of the Government's approach to AI regulation, agreeing with the five-principles model and the establishment of the central support function. The Response summarised how the CMA believes the five principles might be applied to its remit and how the principles could support the AI market whilst protecting consumers and competition.

The CMA has explicitly stated that it believes free and competitive markets are fundamental to innovation in emerging markets like AI, indicating that we could expect to see a light touch approach at this early stage. The findings of the May Review will be used by the CMA to identify which principles it feels are best suited to supporting the development of the AI market whilst protecting consumers and competition, ultimately informing how the CMA will implement the approach as set out in the White Paper. The Response has demonstrated clearly that the CMA thinks the White Paper is the right approach, and we can expect to see the findings published following the May Review echoing and building on its Response.

Why is this important?

The White Paper and subsequent regulator guidance will inform the decisions and processes of developers and users of AI technologies in the UK. As demonstrated by the May Review, we are starting to see regulators respond to the White Paper by thinking about what AI means for their sector and how they can implement the five principles. The positive response issued by the CMA may pave the way for other regulators to voice their opinions.

Any practical tips?

The White Paper represents the Government's first, but very cautious, step towards the regulation of AI. That being said, this is a guiding paper for regulators on how the Government expects them to act with regards to AI and what they should be considering when working within their remit. Equally, businesses that use AI technology now have a clearer understanding of the fundamentals of AI regulation and can use this as a toolkit when developing and using AI.

We can expect to see further developments in AI regulation over the course of this year. Regulators are likely to start to issuing guidance for businesses within the next 12 to 18 months, with the CMA in particular planning to publish a "short report" of its findings early September 2023.

Ethics in the age of AI: new Institute of Directors checklist

The question

What are the key considerations for boards regarding the ethical use of AI within their companies based on the Institute of Directors' (**IoD**) Checklist for Boards (**Checklist**)?

The key takeaway

Directors must understand and effectively mitigate AI-related risks. The Checklist highlights the importance of monitoring and audit measures, as well as board accountability and other oversight mechanisms. Additionally, compliance with data and privacy requirements is vital to meet these objectives. It will be imperative to conduct regular reviews and identify where corrective actions are necessary.

The background

The application of AI for commercial purposes is becoming increasingly relevant, revolutionising business operations and decision-making processes across organisations. However, as the use of AI expands, so does the need for ethical considerations linked to companies' ESG and CSR goals.

Recognising this imperative, the IoD, a professional organisation for directors and business leaders, has released a reflective checklist to guide boards in ensuring the ethical use of AI. The Checklist aims to address the gaps revealed by an IoD member survey, where a significant number of boards (80%) lacked AI audit processes and were unaware of existing AI implementation within their companies.

The development

The Checklist sets out several points to keep in mind during board meetings in respect of ethical AI considerations. The key takeaways are:

- boards should pay attention to how AI is implemented in their organisation and closely monitor the evolving regulatory environment
- organisations should focus on implementing robust auditing processes, guaranteeing the ongoing measurement and evaluation of AI systems
- impact assessments should be conducted to assess any potential negative effects of AI on employees and other stakeholders
- boards should assume accountability for the ethical use of AI and, where necessary, exercise their veto power over its implementation
- high-level goals aligned with organisational values should be established, focusing on augmenting human tasks, unbiased decision-making, and achieving better outcomes
- diverse and empowered ethics committees with veto powers should oversee AI proposals and safeguard ethical considerations
- organisations should prioritise data documentation and security, compliance with privacy requirements, and secure-by-design principles, and
- regular reviews and testing should be undertaken to monitor AI performance and rectify deviations as they arise.

Why is this important?

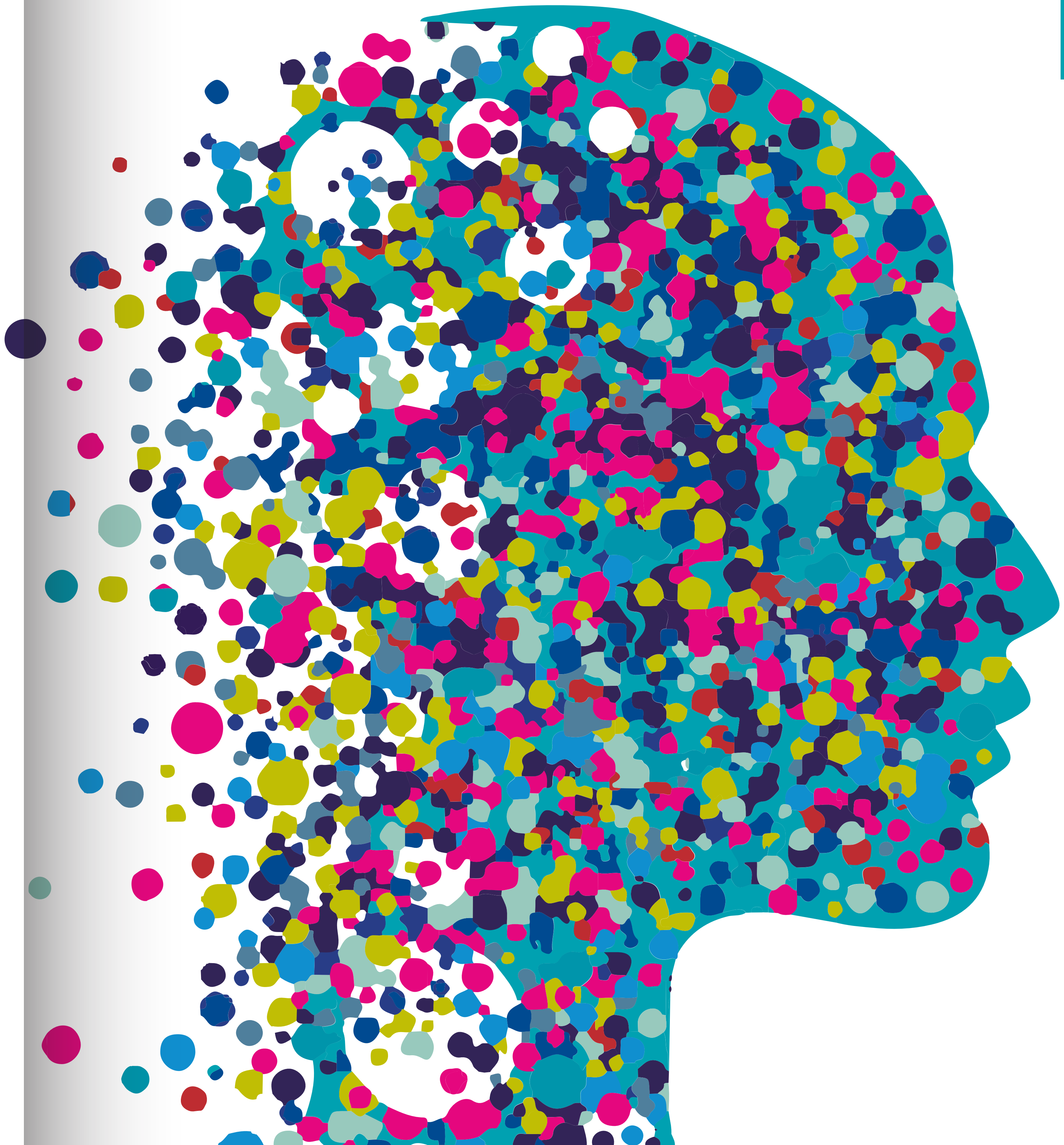
It is particularly crucial for businesses to keep a close eye on these developments to steer clear of potential regulatory risks. Seeing that the IoD's Checklist aligns with the growing regulatory landscape surrounding AI, including initiatives such as the UK Government's AI White Paper and the EU's AI Act, directors are well advised to take the IoD's suggestions into account.

Similarly, the Checklist emphasises compliance with data protection and privacy legislation, such as the GDPR. This ties in with guidance provided by regulatory bodies, like the ICO's AI and Data Protection Toolkit, and should be evaluated carefully to ensure compliance in the AI domain.

Any practical tips?

Organisations utilising AI-powered solutions in their day-to-day operations should reflect on any associated ethical implications of doing so. Board-level accountability and oversight are necessary to ensure responsible decision-making in this regard. AI impact assessments can help address any risks head-on, and auditing processes allow for the evaluation of AI systems and their performance. Setting high level goals for a business's use of AI can help ensure that it is properly utilised in line with the company's goals, which in turn will help to ensure that its use is internally regulated. It is also advisable to document data sources, implement strict measures to detect AI bias and ensure compliance with data privacy regulations.

By following these practical tips, organisations can navigate the legal landscape surrounding AI, promote ethical practices, and mitigate potential risks and liabilities.



Digital Markets, Competition and Consumers Bill opens door for stricter regulation of news platforms

The question

How might the proposed Digital Markets, Competition and Consumers Bill (the **Bill**) affect news reporting by digital platforms?

The key takeaway

The new rules present an avenue for the UK Government to designate large scale tech companies as having a "strategic market status", and thus create tailored rules for them to pay for news services on their platform.

The background

The UK has introduced legislation that could pave the way to compelling Google, Facebook and other tech companies to pay to distribute news content by as early as 2024. The long-awaited Bill's proposed changes have now been presented to Parliament and raise significant new developments in this area. The Bill seeks to improve competition online while affording consumers greater protections online.

This development is a key part of promoting competition by ensuring that bargaining power is restored to media outlets and that they are not left behind in terms of the means by which consumers access the news. The proposals are reminiscent of legislation that has already been introduced in other jurisdictions (most notably in Canada and Australia).

The development

The legislation would allow the Competition and Markets Authority's Digital Market Unit (**DMU**) to designate certain platforms as having "strategic market status". A classification of this kind would give the DMU the authority to create codes of conduct for these businesses as well as customise specific conduct rules for the business's interactions with users and content providers. According to the Department for Digital, Culture, Media and Sport (**DCMS**), companies could be forced to alter their interactions with news publishers in order to ensure that publishers are "paid fairly for their online content" by using these behaviour criteria as a legal requirement. These rules are somewhat vague and arguably allow the DMU the power to create rules as they see fit.

Why is this important?

This change is a huge step up in the power of the DMU, who were set up with no powers beyond the CMA's basic enforcement options. Through creating these tailored rules for "strategic market status" companies, the DMU has been given freedom in what it requires such a company to do, including paying for news. Alongside the other large-scale reforms that the Bill proposes for the UK, the change will have profound impacts on online platforms. Many of these platforms vehemently opposed Australia's version of the legislation, believing that it could distort digital market competition and leave publishers uncertain about which companies would financially support the news publishing ecosystem. As a result of the opposition, commercial agreements were reached between publishers and online platforms before the Australian legislation was passed.

Any practical tips?

Tech companies which may fall within the DMU's remit should start assessing how they may be designated once these proposals become law next year and start thinking hard about how they may limit the impact it may have on them. Considering a commercial deal, similar to those pursued in other jurisdictions, may provide a shield from the most extreme of these effects.

DIGITAL

Criminal sanctions for senior managers under the Online Safety Bill

The question

What criminal sanctions will senior managers face under the Online Safety Bill?

The key takeaway

The Online Safety Bill (**OSB**) will introduce criminal sanctions to hold senior managers of in-scope services personally liable in certain circumstances for the company's non-compliance with obligations within the OSB. Officers and directors of tech companies should familiarise themselves with these provisions and consider what steps can be taken at this stage to ensure personal and corporate compliance once the Bill comes into force.

The background

The UK government published the first draft of the OSB in May 2021. After passing through several iterations, it is now making its way through the House of Lords. The aim is that the OSB will come into force this Autumn, though it is likely to be some time before many of its provisions take effect.

The OSB seeks to improve user safety online by ensuring the most harmful content is identified and removed by search engines and providers of user-to-user services. Key aims include the protection of children and tackling illegal content such as that which promotes terrorism. A "systems-focussed" bill, it will require companies to implement appropriate procedures and processes to tackle illegal and harmful content and will grant extensive powers to the new online safety regulator, Ofcom, to oversee and enforce the new rules.

RPC last covered this topic here and here.

The development

The OSB introduces potential criminal liability for senior managers and other officers of in-scope companies in some key areas.

First, if an entity fails to comply with an information notice issued by Ofcom, knowingly or recklessly provides false information in response to an information notice, or intentionally destroys or alters information, senior managers may be held personally liable if they have failed to take steps to prevent that offence from being committed. The same applies to senior managers who fail to ensure compliance with audit notices issued by Ofcom.

Perhaps even more significant is the introduction of criminal liability for individual officers if, through their consent, connivance or neglect, the company fails to comply with a confirmation notice requiring it to take steps to ensure it acts in accordance with a child safety duty in the OSB. The upshot is that individual directors could face up to two years' imprisonment for alleged failure to prevent children from encountering harmful content even where they are not internally responsible for moderation decisions or the response to Ofcom's confirmation notice.

Why is this important?

This legislation will fundamentally change the criminal and regulatory landscape for tech companies in the UK and will introduce personal criminal liability in relation to a key focus of the OSB: child online safety. The consequences of non-compliance for both the corporate entity and for individuals are extremely serious and should be grappled with as soon as possible in order to ensure compliance once the OSB comes into force.

Any practical tips?

In-scope services should consider who may be deemed an "officer" of the company under clause 182 of the OSB to understand to whom personal liability could attach. Companies should also undertake a detailed review of the processes and practices they currently have in place relating to children's online safety and should implement any necessary adaptations now, to ensure they are well-placed to engage robustly with the regulator in relation to any investigations or provisional notices once the OSB comes into force.

Singapore's Online Criminal Harms Bill

The question

What is the current shape of Singapore's Online Criminal Harms Bill?

The key takeaway

The Online Criminal Harms Bill (the **Bill**) looks set to grant the Singaporean Government a wide range of new powers against providers of online and internet services in an attempt to prevent online criminal activity and malicious cyber activities.

The background

According to the Singaporean Ministry of Home Affairs (**MHA**), the prevalence of online crime, scams and malicious activity has increased considerably in recent years. The MHA has reported that these online crimes include child sexual exploitation and the sale of drugs over chat apps, and that online scams led to over S$600m (c. £355m) being lost in 2022.

To combat these and a variety of other online activities, the Singaporean Government has begun to introduce a 'suite' of legislation. Previously introduced pieces of legislation in this suite include the Online Falsehoods and Manipulation Act, the Foreign Interference (Countermeasures) Act, and (recent amendments to) the Broadcasting Act. The Singaporean Government is now in the process of introducing the next piece of legislation, the Bill, which had its Second Reading in the Singaporean Parliament on 5 July 2023.

The development

The Bill as it currently stands has set a lower threshold for the Government to be able to issue 'Directions' for "scam or malicious cyber activity offences" (i.e. scam activities) than it has for "specified offences" (i.e. criminal activities), though it should be noted that some scam activities are effectively also treated as criminal activities under the Bill.

Examples given by the MHA of criminal activities include offences relating to terrorism, racial harmony, violence, drugs, sexual offences and others, including scams and malicious cyber activities. Examples of scam activities include loan and phishing scams.

DIGITAL

The Government will have the power to issue any of the following 'Directions' where, for criminal offences, there is a "**reasonable suspicion** that an online activity is being carried out to commit a crime" (emphasis added) and, for scam activities, when it is "**suspected** that any website, online account, or online activity **may** be used for scams or malicious cyber activities" (emphasis added):

- **Stop Communication** (requirement to stop communicating specified online content to people in Singapore)
- **Disabling** (requirement for online service providers to disable specified content from the view of people in Singapore)
- **Account Restriction** (requirement for online service providers to stop an account using their service from interacting or communicating with people in Singapore)
- **Access Blocking** (requirement for internet service providers to block a website from the view of people in Singapore)
- **App Removal** (requirement for app stores to remove an app from its Singapore storefront).

Why is this important?

Social media websites, internet service providers, app stores and more will fall within the scope of the Bill, meaning its effects are likely to be felt across much of Singapore's digital footprint.

The Bill grants the Singaporean Government a wide range of powers to stop what it deems to be inappropriate online behaviour. Such powers range from ordering that certain content no longer be communicated, through to the complete blocking of access to websites through an internet service provider, and the removal of an app from an app store. The broad wording of "when there is reasonable suspicion", and even broader wording of where it is "suspected" that a site "may be used" for scams, that is used to justify the issuing of Directions means that appeals against such orders are likely to have a high hurdle to overcome.

Any practical tips?

While the Bill must still go through a Third Reading before it becomes law, those who are likely to be caught by the legislation should begin to put the necessary measures in place to ensure that, when the Online Criminal Harms Act 2023 takes effect, they are not on the receiving end of a Direction from the Singaporean Government. Such measures include steps to prevent users from communicating illegal or malicious content, removing non-compliant apps from app stores and blocking access to non-compliant websites on internet services.

DIGITAL

UK Government's draft Media Bill is published

The question

How will the Government's new draft Media Bill (Bill) affect UK broadcasters?

The key takeaway

The draft Bill is a key change in the media landscape, particularly affecting Public Service Broadcasters (**PSB**) and streaming companies through implementing consistent standards across traditional broadcasting and video on demand (**VOD**) services. However, its impact is slightly up for debate, with many of these companies already complying with Ofcom and UK regulation voluntarily.

The background

Following a White Paper published in April 2022, the UK Government's objective to modernise broadcasting law, including reshaping the regulatory environment for public service broadcasters, is being put into practice with the publication of the Department for Digital, Culture, Media and Sport's (**DCMS**) draft Bill.

The development

There are several key developments which will have a significant impact on UK broadcasters. However, the most significant is that Ofcom will be empowered to create and implement a new Video-on-Demand Standards Code (**VOD Code**). The VOD Code will apply to VOD services domiciled in the UK as well as non-UK VOD providers that engage a sizable UK audience (such as Netflix). The Government anticipates that the VOD Code will bring VOD services in line with the requirements already in place for linear programming under the Ofcom Broadcasting Code. This includes robust requirements relating to providing adequate protections for members of the public from harmful and/or offensive material, ensuring that news is reported with due accuracy, preventing unfair treatment of individuals in programming, and preventing unjustified invasions of privacy.

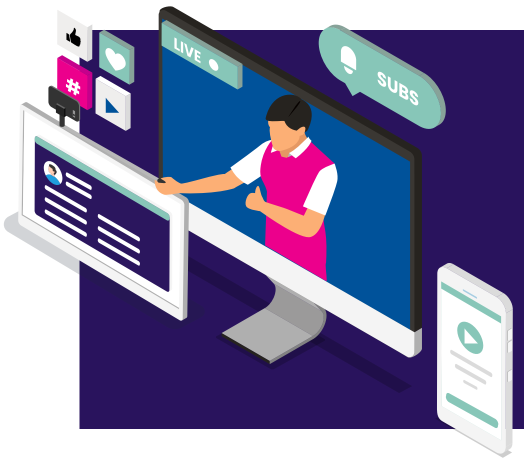
Ofcom will have a wide range of enforcement and investigative powers under the envisaged VOD Code, including the ability to levy fines of up to £250,000 or 5% of the relevant worldwide revenue, whichever is higher. In the most severe circumstances, Ofcom will be able to restrict the accessibility of VOD services in the UK.

Significant legislative changes include:

- giving PSBs more freedom in how they fulfil their public service requirements, including the ability to use content from VOD services
- ensuring that public service content is given enough prominence on a variety of television platforms, including smart TVs, set-top boxes, and streaming sticks, and
- regulating the commercial relationships between radio stations and radio selection services to ensure, amongst other things, that platforms cannot charge to host and/or distribute live UK radio. This reflects the fact that radio listeners are increasingly moving away from traditional means of tuning into radio broadcasts to listening via the internet on smart speakers.

Why is this important?

This update is long awaited due to the significant changes the broadcast environment has undergone. The addition of VOD services as well as significant technological change has changed the landscape of broadcasting whilst the legislative framework has not been updated since 2003. The draft Bill will bring current legislation in line with the reality of broadcasting in 2023 and beyond. The regulation of VOD services is a significant development and will have a significant impact on how VOD services are able to provide their content to UK audiences, regardless of whether they are established in the UK.



Any practical tips?

VOD services, as well as PSBs that also offer a VOD alternative, should be mindful of the draft Bill and be ready to implement changes so as to ensure compliance. PSBs and VOD services alike should start planning how to implement any necessary changes to their operations or programming to ensure compliance but to also make sure that there is no drop in their offering. Whilst complying with relevant laws is paramount, ensuring customer satisfaction remains key in an extremely competitive industry.

"The draft Bill is a key change in the media landscape, particularly affecting Public Service Broadcasters (PSB) and streaming companies through implementing consistent standards across traditional broadcasting and video on demand (VOD) services."

DIGITAL

"DSIT is a new, stand-alone department for Science, Innovation and Technology, created by the UK Government. The new department is responsible for putting technological innovation at the core of the UK economy and delivering key legislative and regulatory reforms relating to cyber security and the UK's digital industries."

UK's new Department for Science, Innovation and Technology

The question

What is the Department for Science, Innovation and Technology (**DSIT**) and what is it responsible for?

The key takeaway

DSIT is a new, stand-alone department for Science, Innovation and Technology, created by the UK Government. The new department is responsible for putting technological innovation at the core of the UK economy and delivering key legislative and regulatory reforms relating to cyber security and the UK's digital industries.

The background

The creation of four new departments was announced by the Government on 7 February 2023. DSIT will be responsible for technology-related policies previously split between the Department for Culture, Media and Sport (**DCMS**) and the Department for Business, Energy and Industrial Strategy (**BEIS**). DSIT's purpose is to put the UK at the forefront of global scientific and technological advancement whilst simultaneously attracting significant investment in the UK as part of the Government's plan to make the UK the next "Silicon Valley".

DSIT has six outlined priorities suggesting exciting advancements in the UK digital space to come, as well as a focus on digital and cyber regulation implementation, including to:

- "promote a diverse research and innovation system that connects discovery to new companies, growth and jobs, including by delivering world-class physical and digital infrastructure (such as gigabit broadband), making the UK the best place to start and grow a technology business and developing and attracting top talent"
- "deliver key legislative and regulatory reforms to drive competition and promote innovation, including the Data Protection and Digital Information Bill, the Digital Markets, Competition and Consumers Bill and a pro-innovative approach to the regulation of AI", and
- "pass the remaining stages of the reformed Online Safety Bill to keep British people, especially children, safe online".

The development

The key point to note is that DSIT now has responsibility for the implementation of the Government's National Cyber Strategy (2022). Whereas the strategy itself has not changed with DSIT's inception, methods of implementation are expected to. The shake-up of governmental departments will see changes in approaches to fulfilling government policy. DSIT's aims revolve around innovation, sustainable technological advancement, increasing physical and digital infrastructure and optimising research and development when delivering the National Cyber Strategy to "ensure the UK is a science and technology superpower". DSIT are responsible for the five pillars of the UK National Cyber Strategy, outlined below, being reached by 2025:

- strengthening the UK cyber ecosystem
- building a resilient and prosperous digital UK
- taking the lead in the technologies vital to cyber power
- advancing UK global leadership and influence for a more secure, prosperous and open international order, and
- detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace.

It will be interesting to see how quickly DSIT can establish itself and bring changes in this area, when compared to its predecessors, DCMS and BEIS.

Why is this important?

The creation of DSIT as a stand-alone department focusing on science and technology highlights a clear government endeavour to boost innovation in the UK economy and push resources in to the digital and cyber space. Having one department concentrating on science and technology will help to streamline the practical implementation of new technological innovations but also digital and cyber security regulation/legislation; notably the Data Protection and Digital Innovation Bill and the Online Safety Bill, as well as the priorities set out by the National Cyber Strategy 2022. The expectation is that DSIT will eliminate the potential competing priorities that might have hindered progress when these policies were the responsibility of DCMS and BEIS. This offers opportunities to businesses in this sphere to take advantage and work with new systems and infrastructures implemented by DSIT.

Any practical tips?

The Government's focus on innovation and technology and the aim to make the UK economy one of the most innovative in the world is an exciting prospect for many businesses in this sector. DSIT's updates and projects should be reviewed closely for opportunities for involvement, investment, and growth.

Bitcoin developers may owe fiduciary duties: Tulip Trading

The question

Can Bitcoin developers owe fiduciary duties to Bitcoin owners and, if so, in what circumstances?

The key takeaway

In the case of *Tulip Trading Limited v van der Laan and others* [2023] EWCA Civ 83, the Court of Appeal found that the developers looking after Bitcoin arguably owed fiduciary duties in tort to an owner of Bitcoin. Whether such a duty did arise in the specific proceedings would depend on the facts established at trial.

The background

The claimant company Tulip Trading is controlled by Dr Craig Wright, who claims to be Satoshi Nakamoto, the inventor of Bitcoin. Tulip allegedly lost access to a significant amount of Bitcoin because of a cyber-attack in which the private keys needed to access a significant amount of Bitcoin were deleted.

Tulip brought proceedings against the developers and controllers of the relevant Bitcoin networks seeking, amongst other things, to compel them to implement a software patch that would enable Tulip to regain control of its Bitcoin. Tulip argued that the defendants were obliged to do so as a result of fiduciary and/or tortious duties owed to it.

Tulip was initially granted permission to serve the various defendants out of the jurisdiction, but a number of the defendants successfully challenged jurisdiction and the relevant order was set aside. The High Court held that there was no good arguable case – the (reasonably low) standard required for permission to serve out of the jurisdiction to be granted – that the defendants owed either fiduciary duties to Tulip or a tortious duty of care to include in their software the means to allow those without access to their private keys to access their Bitcoin. Tulip was denied permission to appeal by the High Court Judge but was subsequently granted permission by the Court of Appeal.

The development

The Court of Appeal overturned the High Court decision, finding that Tulip's case on fiduciary duties was arguable. The Court of Appeal did not consider whether the defendants also owed tortious duties to Tulip as well because, on Tulip's case, such a duty could only arise in circumstances where the defendants also owed a fiduciary duty, and the issues were so closely related that if the fiduciary duty appeal succeeded the right course was to allow the appeal regarding the tortious duty as well.

The Court of Appeal's reasoning is set out at paragraphs 70 to 88 of the judgment. In summary, the court considered that a realistic argument could be made that the defendants owed fiduciary duties along the following lines:

- the developers of a given Bitcoin network were a sufficiently well-defined group to be capable of being subject to fiduciary duties. The court observed that this was fact sensitive and a contentious point between the parties and found that the first instance judge, in finding that the developers were a "fluctuating and unidentified body", had erroneously accepted a highly contested fact as a premise
- the developers were fiduciaries because they had undertaken a role which involved making discretionary decisions and exercising power for and on behalf of Bitcoin owners, in relation to the owners' Bitcoin, which had been entrusted into the developers' care. Such trust was said to arise because the developers could decide what software changes would be implemented for the relevant Bitcoin networks, which enabled them to make decisions on behalf of all the participants in those networks, and
- the fiduciary duty owed by the developers comprised both a "negative" duty not to act in their own self-interest as well as a duty to act in positive ways in certain circumstances, such as fixing code errors. The court observed that identifying what actions might fall into the "positive" category was fact sensitive and it would not always be straightforward to delineate from actions falling into the "negative" category. Of the duty to act in positive ways, the court also remarked that it:
  - would be a "significant step to define a fiduciary duty in that way" but considered it was arguable because on Tulip's case the developers had, via their exclusive access to the relevant password for the Bitcoin software account, the practical ability to prevent anyone else from amending the source code, and
  - might realistically include, in the circumstances alleged by Tulip, a duty to act to introduce code so that an owner's Bitcoin could be transferred into a safe account controlled by the true owner or otherwise safeguard it.

The Court of Appeal also did not accept what the High Court regarded as a "fundamental difficulty" with Tulip's case – a tension between the obligation of undivided loyalty to a class (which characterises fiduciary relationships) and the fact that the action sought by Tulip was for its own benefit, which might be to the detriment of other users of the Bitcoin networks such as rival claimants to the relevant Bitcoin. In its conclusion, the Court of Appeal accepted Tulip's submission that it was arguable that such a duty would be owed only to the "true owners of the property", removing the conflict.

Why is this important?

The upshot of this decision is that the issue of whether Bitcoin developers owe fiduciary and/or tortious duties to users of the network remains very much live. It will need be determined at trial in the proceedings.

However, although Tulip's claim lives to fight another day, it faces formidable legal and factual challenges. The Court of Appeal acknowledged that, for Tulip's case to succeed, a significant development of the common law on fiduciary duties was needed, and that while the established categories in which fiduciary relationships arose were not closed, it is exceptional for fiduciary duties to arise outside of them. Tulip will also need to make good on its factual arguments regarding the extent to which the developers do control the operation of Bitcoin and the extent to which they are a sufficiently well-defined group.

Any practical tips?

Regardless of whether Tulip is ultimately successful in establishing a fiduciary duty for the developers to take the positive steps it seeks, the decision will be of particular comfort to holders of cryptoassets who might wish to take action against relevant developers in respect of negative steps. This is because the Court of Appeal was far less hesitant about finding that negative duties may arise, including a duty not to take actions for their own advantage at the expense of the participants in the relevant network.

DIGITAL

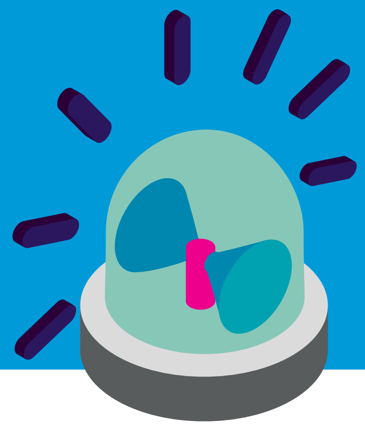
New development – Keeling Schedules published for the Data Protection and Digital Information Bill

The UK Government published a set of Keeling Schedules on 10 May 2023 for the Data Protection and Digital Information Bill version 2 (the **Bill**).

A Keeling Schedule is usually included as an appendix to an amendment. The name comes from the MP E.H. Keeling who introduced these types of schedules to help show how an existing statute will read if a proposed amendment is adopted.

The new schedules effectively redline the changes proposed by the Bill against the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, thus making it far easier to review and consider the impact of the proposed changes on existing law.

See our previous coverage of the Bill in the Autumn 2022 and the Spring 2023 Snapshots.



CONSUMER

The UK's Digital Markets, Competition and Consumers Bill – a first look at the new regime

The question

What are they key legislative developments proposed by the first draft of the new UK Digital Markets, Competition and Consumers Bill?

The key takeaway

The Bill contains a number of significant legislative amendments in relation to digital markets, competition law and consumer protection. Most notably, in relation to: direct enforcement powers for the CMA; power for the CMA to issue fines; revisions to the Consumer Protection from Unfair Trading Regulations 2008; regulation of subscription traps; insolvency protection for consumer saving schemes; and alternative dispute resolution options for consumers. It is also anticipated that there will be further regulation in respect of fake reviews.

The background

As well as signalling changes to the consumer protection landscape, the Bill contains important new provisions relating to digital markets and competition law. It gives the CMA powers to regulate, investigate and impose conduct requirements on digital business with strategic market status (think: Big Tech), with fines for non-compliance of up to 10% of global annual turnover. And it reforms the UK competition law regime more widely.

The Bill is born into a world where the EU has already set in motion a major, modernising uplift to the consumer, digital and competition landscape, with the Omnibus Directive (enhancing consumer protection for the digital world), and the Digital Markets Act and Digital Services Act (aimed at creating fair and open markets and better user safety and content moderation, respectively). From a UK perspective, it will join the ranks of legislation such as the Online Safety Bill (which has recently been saved from lapsing from the Parliamentary legislative agenda), which together work towards curating a legislative backdrop fit for the modern day and the increasingly digital online lives we lead.

The development

So, what does the Bill mean for UK consumer law?

- **Direct enforcement powers for the CMA.** Under the Bill, the CMA will be able to directly enforce consumer protection law avoiding the need to go through the court system. Such powers may prove to be a meaningful deterrent for businesses who repeatedly breach consumer protection law but have to date managed to avoid sanctions because of the timeframes and process involved in the CMA taking court action. It should also help to "level the playing field", a bonus for law-abiding businesses that may previously have had to watch their less well-behaved competitors enjoy an extended competitive advantage whilst enforcement action proceedings trundle slowly through their process.
- **Power for the CMA to issue fines.** The Government has itself acknowledged that the UK is the only G7 country not to have any civil penalties for common consumer protection breaches. To address this, the Bill grants the CMA the ability to make determinations on whether breaches of consumer law have occurred, and to impose monetary penalties directly (similar to the ICO in their enforcement of data protection legislation). There are several tiers of possible fines, but for the most serious breaches, the CMA may impose penalties of up to £300,000 or 10% of global annual turnover (if higher). The CMA will also be able to issue fines for breaches of undertakings, non-compliance with notices given by a consumer protection officer and breaches of an administrative direction given by the CMA.
- **The CPRs v2.0.** The Bill revokes and then restates, with some tweaks, the provisions of the Consumer Protection from Unfair Trading Regulations 2008 (**CPRs**). In terms of call outs, there is a newly created "omission of material information from an invitation to purchase" offence which joins the list of offences that we have become used to since the CPRs came into force in 2008 (misleading acts, misleading omissions, aggressive practices, blacklisted practices and practices contravening the requirements of professional diligence). The "blacklist" of practices which are in all circumstances considered unfair remains intact, and appears at Schedule 18 to the Bill (with a couple of tweaks to the ordering and certain instances where practices have been reframed to be clearer and/or broader).
- **What about fake reviews?** We were also expecting to see provisions in the Bill adding certain fake review activities to the famous blacklist. These have been noticeably absent from the first draft of the Bill, but this doesn't mean they won't be coming. The Bill enables the list of blacklisted practices to be updated speedily by Parliament through secondary legislation, in order to reflect new business practices and emerging consumer harms. The Government has also confirmed that, during the passage of the Bill through parliament, it plans to consult on adding the following "fake review" practices to the blacklist: (a) commissioning or incentivising any person to write and/or submit a fake consumer review of goods or services; (b) hosting consumer reviews without taking reasonable and proportionate steps to check they are genuine; and (c) offering or advertising to submit commission or facilitate fake reviews.
- **Subscription traps.** As expected, the Bill will also give new rights to consumers entering into subscription contracts. Businesses will now need to provide certain pre-contract information prominently and clearly. They will also need to allow both an initial 14-day cooling off period and further 14-day renewal cooling off periods whenever a subscription is renewed (during which time subscribers may cancel). The protections are further reinforced by requirements to remind consumers when any free or discounted trial period is ending, and/or where the subscription is about to renew, and to make it easy for subscribers to exit their subscriptions (ie via a single communication).
- **Insolvency protection for consumer saving schemes.** The Bill sets out requirements on traders operating certain consumer saving schemes (such as Christmas saving clubs, which are not, by their nature, FCA-regulated or protected by the Financial Services Compensation Scheme) to make insurance and trust arrangements to protect consumer pre-payments in the event of the trader becoming insolvent.
- **Alternative Dispute Resolution (ADR).** Finally, the Bill will help to empower consumers to be able to resolve disputes directly with businesses by the introduction of ADR provisions. These include a duty on businesses to notify consumers about any ADR arrangements applicable to the business where a consumer is dissatisfied with the outcome of any complaint, and imposes obligations on ADR providers (including a prohibition on acting as an ADR provider without accreditation, unless exempt, and a prohibition on charging fees to consumers).

Why is this important?

The Bill marks the beginning of a new era of enhanced consumer protection, with a regulator that is set to cast off any previous reputation it may have picked up for having a bark that was worse than its bite. The Bill itself runs to almost 400 pages and covers a plethora of new and updated law and consequential legislative amendments on its core topics: digital markets, competition law and consumer protection.

Any practical tips?

The Bill is the biggest change to UK consumer legislation in years. The CMA's new powers to fine should make all businesses sit up and take note. At this stage, this includes keeping track of the progress of the Bill through Parliament and beginning to prepare for its implementation. On that note, most businesses already know when they are sailing close to the wind from a consumer fairness perspective. Taking early steps to amend riskier trading practices, including changing risk mindsets internally, may well pay dividends later once the CMA begins to use its new financial claws.

CONSUMER

The Digital Markets, Competition and Consumers Bill and its impact on digital markets

The question

What impact will the Digital Markets, Competition and Consumers Bill (**DMCC**), and the new Digital Markets Unit of the Competition and Markets Authority (**DMU**), have on the regulation of UK digital markets?

The key takeaway

The DMCC will have a significant impact on the regulation of Digital Markets. The DMCC proposes extensive enforcement powers for firms with a Strategic Market Status (**SMS**). Such firms are proposed as those with a SMS in relation to one or more digital activities which are linked to the UK and where the firm has substantial and entrenched market power and a position of strategic significance in respect of a digital activity, subject to certain turnover thresholds. Where a firm is designated as having a SMS, this will result in conduct requirements, Pro-Competitive Interventions (**PCIs**) and mandatory merger reporting.

The DMCC is also a further step towards implementing the Digital Markets Unit's formal statutory powers to police digital markets through corporate fines and implications for individuals.

The background

The long-anticipated DMCC has now begun its parliamentary journey following its introduction on 25 April 2023. Described as a "flagship bill" by the CEO of the Competition and Markets Authority (the **CMA**), the DMCC not only introduces major landscape reforms to the UK's consumer protection regime and significant enhancements to the CMA's competition law powers, it also ushers in a new regime for digital markets. The DMCC has the potential to be a "watershed moment" in how UK digital markets are regulated.

The CMA established the DMU in shadow form in 2021, so the DMCC marks a crucial step towards it gaining formal statutory powers to police digital markets. The main aspects of the new regime and the DMU's extensive enforcement powers are summarised below.

The development

SMS designation

The Government's stated purpose of the new regime is to regulate "the largest and most powerful digital firms to ensure effective competition that benefits everyone" and "to address the far-reaching market power of a small number of tech firms". To this end, the CMA, and therefore the DMU (an administrative unit within the CMA), would have the power to designate a firm as having SMS in relation to one or more digital activities which are linked to the UK and where the firm has substantial and entrenched market power and a position of strategic significance in respect of a digital activity, subject to certain turnover thresholds:

Digital activities

- Their scope is set out in the form of three broadly defined categories of activities rather than a specific list (in contrast, the EU's Digital Markets Act (**DMA**) lists ten "core platform services"). The proposed categories are:
  – the provision of a service via the internet
  – the provision of digital content, or
  – any other activity carried out for the purpose of either of the above.

Linked to the UK

- A jurisdictional nexus with the UK is required. A digital activity would be considered to be linked to the UK if:
  – it has a significant number of users
  – it is likely to have an immediate, substantial and foreseeable effect on trade in the UK, or
  – the undertaking which carries out the digital activity carries on business in the UK in relation to the digital activity.

Substantial and entrenched market power

- The DMCC sets out that a firm would be in such a position if one or more of the following conditions were met:
  – the undertaking has achieved a position of significant size or scale in respect of the digital activity
  – the digital activity carried out by the undertaking is used by a significant number of other undertakings in carrying on their business
  – the undertaking's position in respect of the digital activity would allow it to extend its market power to a range of other activities, or
  – the undertaking is in a position to be able to determine or substantially influence the ways in which other undertakings conduct themselves in respect of the digital activity (or otherwise).

Turnover thresholds

- Only if a firm (and its group) is estimated by the DMU to have turnover, arising in connection with **any** of its activities, in excess of £25bn globally or in excess of £1bn in the UK (from UK users or customers) over usually the last twelve-month period could it be designated as having SMS. With such high turnover thresholds envisaged, the scope of the new regime would be limited to only the largest digital firms.

In terms of process, prior to making a SMS designation, the DMU would be required to conduct an SMS investigation. It must first give notice to the firm in question setting out the reasonable grounds it has for considering that it may be able to designate the firm as having SMS and the purpose and scope of the SMS investigation, amongst other requirements. The DMU has up to nine months to conclude this investigation and decide on SMS designation (subject to possible extension) and is required to carry out a public consultation on its proposed decision. An SMS designation is then in place for a period of five years.

Consequences of SMS designation

There would be three main consequences of SMS designation for firms. It is envisaged that the DMU would have two new tools, one to prevent harm by setting out tailored conduct requirements and the other to impose targeted pro-competition interventions to address the root causes of competition issues in digital markets. Thirdly, there will also be a mandatory merger reporting requirement for SMS-designated firms where certain thresholds are met.

Conduct requirements

- To seek to mitigate the effects of market power, the DMU would be able to impose an enforceable Code of Conduct, tailored to the SMS-designated firm, to regulate its conduct in relation to a relevant digital activity. As with SMS designation, the DMU must give notice and consult on the proposed conduct requirements. The conduct rules would set out how the firm should treat consumers and other businesses based on three overriding principles: fair dealing (eg on reasonable terms); open choices (eg ease of ability to switch providers); and trust and transparency (eg sufficient information to make informed decisions).
- The DMCC sets out an extensive list of the permitted types of conduct requirements. Conduct requirements would need to be kept under review and could be varied, revoked and added to by the DMU.
- In contrast with the obligations under the DMA which apply equally to all designated "gatekeepers", the DMCC empowers the DMU to prescribe bespoke conduct requirements targeted at the SMS-designated firm in question. While the UK's novel approach enables more flexibility in regulating dynamic digital markets, the breadth of the DMU's discretion to impose conduct requirements across wide-ranging conduct categories provides much less legal certainty for SMS-designated firms.
- If the DMU has reasonable grounds for suspecting that a SMS-designated firm has breached a conduct requirement, it would be able to carry out a conduct investigation and would have six months within which to notify the firm of any infringement finding. The DMU would be able to impose enforcement orders (including on an interim basis) and would also have the power to accept commitments instead. An SMS-designated firm would be able to put forward evidence that its conduct benefited from a countervailing benefits exemption (broadly equivalent to the section 9 criteria for an exemption from the Chapter I prohibition on anti-competitive agreements under the Competition Act 1009 where the benefits outweigh the potential harm).
- In addition, under the proposed a final offer mechanism, the DMU would have the discretionary power to act, where a SMS-designated firm has failed to agree "fair and reasonable terms as to payment" in its dealings with a third party, by choosing between the respective final offers of the parties. It has been designed as "a tool of last resort" available in only certain circumstances.

Pro-Competitive Interventions (PCIs)

- The DMCC enables the DMU to investigate where it has reasonable grounds to consider that a factor (or combination of them) relating to a relevant digital activity may be having an adverse effect on competition (an AEC Finding). In the event of an AEC Finding, the DMU would have the power to make a PCI. The DMU must provide the SMS-designated firm with notice of the investigation and then would have nine months within which to notify the firm of its final decision (as opposed to the usual eighteen-month timeframe for Market Investigation References (MIRs) following a market study). There is also an obligation to consult publicly. The DMU would then have four months from giving notice within which to make a pro-competition order and would have broadly equivalent powers as under MIRs, ranging from imposing behavioural remedies through to structural remedies and divestments. The DMU would also have the power to accept commitments in place of pro-competition orders.

Mandatory merger reporting

- In a departure from the UK's voluntary merger regime, the DMCC proposes a mandatory advance reporting obligation on a SMS-designated firm in relation to transactions where:
  – it (or its group) has "qualifying status", ie it is to increase its shares or voting rights in a "UK-connected body corporate" target:
    – from less than 15% or 15% or more
    – from 25% or less to more than 25%, or
    – from 50% or less to more than 50%
  – the target carries on activities in the UK or supplies goods or service to a person in the UK so

CONSUMER

CONSUMER

The Digital Markets, Competition and Consumers Bill and its impact on digital markets (Cont.)

  - as to be a "UK-connected body corporate", and
  - the consideration is at least £25m.
- This obligation also captures joint ventures. Details of the form and content of the report to be submitted are to be published in due course. The purpose of the report is to provide sufficient information so that a decision can be made as to whether a merger investigation should be launched.
- In addition to this prior reporting mechanism before a deal can complete, a new jurisdictional threshold will be introduced (amongst other changes to the merger regime proposed by the DMCC). The new threshold will be met where one of the parties supplies at least 33% of the goods or services of a particular description in the UK (or substantial part of it) and has UK turnover in excess of £350m and the other party has a UK-nexus. This is likely to impact on acquisitions by SMS-designated firms.

Enforcement, Appeals and Damages Claims

Whilst it is the Government's stated intention that the "DMU will seek to resolve concerns through informal and cooperative engagement with firms", the DMCC proposes that the DMU would have significant and far-reaching fining powers.

Corporate fines

- The DMU would have the power to fine an SMS-designated firm up to 10% of global (group) turnover for breaches and/or to impose daily fines of up to 5% of daily global (group) turnover for certain ongoing infringements. Fines could be imposed for failure to comply with a conduct requirement or an enforcement order, pro-competition order, final offer order or commitments or merger-related obligations.
- The DMU's proposed investigatory powers under the new digital markets regime would be similar to the CMA's powers under the Competition Act 1998. The DMCC sets out that failure to comply with investigative requirements "without reasonable excuse" could lead to significant penalties (a fixed fine of up to 1% of annual worldwide turnover and a daily fine of up 5% of daily worldwide turnover).

Implications for individuals

- The DMCC also places obligations on individuals with potential consequences for non-compliance.
- The CMA already has the power to seek director disqualifications of up to 15 years in connection with competition law infringements. However, the DMCC proposes this power would be extended to cover involvement in breaches of conduct requirements and PCIs.
- An SMS-designated firm is required to nominate an appropriate senior manager to have responsibility for monitoring compliance with conduct requirements and any orders and/or commitments; co-operating with the DMU regarding compliance; and reporting on compliance. The DMU could impose a penalty on the nominated officer for failure "without reasonable excuse" to ensure that the compliance reporting obligation is duly met.
- In addition, the DMU could require a SMS-designated firm to nominate a senior manager as having responsibility for ensuring compliance with an information request notice and the individual could also be fined in the event of non-compliance "without reasonable excuse".

Appeals

- The SMS-designated firm (or another person with sufficient interest) may challenge a decision by the DMU by means of an appeal before the Competition Appeal Tribunal (**CAT**), but only on judicial review grounds (with a limited exception for certain penalty decisions). Therefore, the review on appeal is not on the merits of the decision itself, but on the legality of the decision-making processes.

Damages Claims

- The new regime also sets out the basis on which third parties affected by certain breaches by a SMS-designated firm would be able to bring a damages claim, seek an injunction or any other appropriate remedy or relief. The DMCC proposes that third parties would be entitled to bring civil proceedings where they suffer loss or damage as a result of an infringement of a conduct requirement, pro-competition order or a commitment. To this end, it is envisaged that the High Court and the CAT would be bound by a DMU infringement decision once it has become final.

Why is this important?

It will take some time for the final legislation and requisite guidance to be in place. As part of the wider preparations for the new regime, on 4 May 2023, the Department for Business and Trade (**DBT**) and Department for Science, Innovation and Technology (**DSIT**) issued a proposed framework to assist in the monitoring and evaluation of the proposed regime. Those anticipating SMS-designation will also be preparing for the new regime and carefully scrutinising further developments, including the extent to which the UK regime may differ from other jurisdictions, such as under the EU's new DMA.

The DMA is now already in force and the European Commission's "gatekeeper" designation process has just begun. Last month, the Commission issued implementing rules covering guidance on many practical aspects including time limits, format and length of documents, access to file and information for the purposes of the DMA's quantitative thresholds. The DMA provisions apply with effect from 2 May 2023, including the gatekeeper designation procedure. By 3 July 2023, providers of "core platform services" must self-assess whether they qualify as gatekeepers and notify the Commission.

Any practical tips?

With the DMCC only having been recently introduced as a Bill in Parliament for debate, the UK's proposed solution to regulating digital markets is playing catch up with the DMA. It remains to be seen whether the heavy-hitting and extensive enforcement powers proposed under the DMCC will remain unchanged from their current form and, ultimately, how quickly the legislation will reach the statute books. The CMA's DMU will still have to wait some time for its formal powers to then take effect. Digital firms firmly in its sights best speed up their preparations in the meantime.

"The DMCC will have a significant impact on the regulation of Digital Markets. The DMCC proposes extensive enforcement powers for firms with a Strategic Market Status (SMS)."

CONSUMER

EU proposal for all distance contracts to include a withdrawal button

The question

How will the EU's proposed withdrawal button impact businesses?

The key takeaway

The EU is seeking to impose a withdrawal button for all distance contracts entered into by consumers. This expands its initial proposal which only required a withdrawal button for financial services contracts. If approved, this proposal will apply to a wide range of businesses, including many who now sell online, who they will face strict requirements for implementing a withdrawal button or a similar function.

The background

On 11 May 2022, the European Commission (**EC**) proposed a new Directive intended to improve how financial services are provided to EU consumers (the **EC Proposal**). This includes strengthening the right to withdraw from financial services that are agreed electronically as distance contracts, such as those agreed online, by requiring providers to set up a withdrawal button on the interface that consumers use.

However, On 24 February 2023, the Council of the European Union (the **Council**) responded to the proposal setting out their support for its expansion by requiring that all consumer contracts agreed at a distance include a withdrawal button or similar function.

The development

The EU's consumer agenda

The EU has an ongoing obligation to ensure high levels of consumer protection. It has been implementing this over several years beginning with the Consumer Rights Directive of 25 October 2011 (**CRD**) which initially established the right for EU consumers to withdraw from many types of distance contracts.

The EC Proposal takes this further by recommending amendments to the CRD, including the withdrawal button, to ensure consistent rules for governing consumer financial services throughout the EU. Similarly, the Council's suggested expansion of the EC Proposal to all distance contracts is intended to ensure that it is just as easy to withdraw from distance contracts as it is to sign up. Both the EC Proposal and the Council's suggested expansion aim to implement the EU's New Consumer Agenda, adopted on 13 November 2020, which set out a strategic framework for modernising EU consumer protection.

Strict requirements

The EC Proposal prescribes how businesses should implement the withdrawal button. This includes:

- clearly labelling the button with the words "Withdraw from Contract" or equivalent wording
- placing the button in prominent view and ensuring it is available as soon as the distance contract is agreed and throughout the entire withdrawal period
- ensuring that activating the withdrawal button creates an instant confirmation notice that a consumer has exercised their withdrawal right, including the date and time it was exercised, and
- requiring businesses to retain detailed records on how the button is used.

The Council's expanded proposal also specifies that the button or withdrawal function should:

- allow consumers to withdraw by providing their name, identifying the contract they agreed; and stating the electronic method that will be used to send them a withdrawal confirmation
- provide an extra confirmation step to prevent accidental, one-click, withdrawals
- enable consumers to withdraw from only part of their contract if it includes multiple goods or services, and
- increase consumers' awareness of their right to withdrawal, especially for remote consumers who do not have the chance to test or inspect what they are buying in person.

The expanded EC Proposal will now be negotiated between the European Parliament and the Council where the current wording may be approved or changed further. Once approved, the final proposal will enter into force on the 20th day following publication in the Official Journal of the European Union.

Why is this important?

If approved, the expanded EC proposal will impose wide reaching requirements on EU retailers who sell online. Industry response so far has been negative, with 17 trade associations submitting a statement rejecting the Council's extension of the proposal to all distance contracts.

Businesses are also likely to be concerned that compliance may incur significant costs, limit flexibility and stunt growth potential as well as undermine their ability to offer distance contracts in flexible ways.

Any practical tips?

EU businesses should be aware of the requirements of the EC Proposal and be ready to make adjustments in order to implement it. Businesses should also be mindful that the proposal will only apply to distance contracts which offer a right to withdraw and will not apply to excluded contracts, such as those involving cryptoassets. Businesses should also keep up to date on national legislation which may impose similar requirements. For example, recent German legislation has imposed a cancellation button for subscription services offered on websites.

CONSUMER

European Commission proposes new rules on repairing defective goods

The question

How will the new rules proposed by the European Commission (**EC**) in the Right to Repair Directive affect producers and consumers of goods?

The key takeaway

The EC has proposed new rules which aim to prevent defective goods from being prematurely discarded and replaced. Manufacturers will have to repair goods deemed reparable under EU law and must inform consumers of their repair obligations in a clear and accessible manner. Put another way, the EC is saying repair, don't replace, defective goods in its latest Net Zero effort.

The background

Consumers are currently entitled to a replacement or repaired product under the legal guarantee in the EU Sale of Goods Directive, if their product is defective. Consumers are often also discouraged from opting for a repair because of poor repair options and conditions. Due to this, reparable products are often prematurely replaced, causing increased waste and a greater demand for resources with the need to manufacture additional products from scratch.

On 22 March 2023, the EC proposed the Right to Repair Directive (the **Proposed Directive**), which modifies existing EU legislation (including the Sale of Goods Directive, the Representative Actions and the Consumer Protection Cooperation Regulation) to promote repairing goods rather than replacing them. This will mean that consumers will only be able to choose a replacement, when it is cheaper than a repair.

The EC's overarching goal is to deliver on the European Green Deal, a package of climate, energy, tax and transport policies striving to reduce net greenhouse gas emissions by at least 55% by 2030. This proposal seeks to contribute to this by reducing greenhouse gas emissions caused by throwing products away as soon as they show a slight defect, despite the products still having a lot more life left in them, if repaired properly.

The development

The Proposed Directive recommends the following obligations for manufacturers and EU Member States:

Producers must:

- repair goods deemed reparable under EU law
- inform consumers as to which products they are obliged repair whilst providing easily accessible, clear and comprehensible information on the repair services offered
- provide consumers seeking repair with a standardised European Repair Information Form (ERIF) setting out the price and key conditions of a proposed repair.

Member states must:

- establish national matchmaking online repair platforms where consumers can easily find a repairer based on different search criteria, including location
- ensure adequate and effective means are implemented to make their country compliant
- incorporate the Directive into national laws within 24 months of it being codified.

Member states can:

- set their own penalties, ensuring that they are effective, proportionate and dissuasive
- choose precisely how to incorporate the Directive into their national law.

The same final text of the Right to Repair Directive will need to be adopted by the European Parliament and the Council. Once this is agreed, the legislation will be published in the Official Journal of the European Union and will enter into force. Member States will then have 24 months to adopt the Directive into domestic law, with measures applying 24 months from then.

Why is this important?

The Proposed Directive follows on from the Digital Services Act and Digital Markets Act (see our previous Snapshot here) and ultimately shows an ongoing trend by the EC of stricter legislation which imposes new duties on companies. Whilst Member States have discretion as to how they incorporate directives in national law, they must give effect to the Proposed Directive once it becomes legislation. Member States will be able to set their own penalties for noncompliance.

Any practical tips?

Producers manufacturing or supplying reparable goods in EU Member States will need to assess potential liabilities under the Directive and should monitor developments in the Member States in which they operate; there may be differences in how each Member State chooses to enforce the Directive. It is also likely that other countries, such as the UK, will follow suit.

Producers will not only need to ensure existing products are repaired, but also that they are built with repairability in mind and that they are able to complete a fast and efficient repair, if anything goes wrong. They will also need to source the right parts and ensure employees are properly trained to complete the repairs.

"The EC has proposed new rules which aim to prevent defective goods from being prematurely discarded and replaced."

CONSUMER

CONSUMER

2023 Gambling Act White Paper: The new age of gambling regulation

The question

How far reaching are the proposed reforms of the Gambling Act and how will they impact digital platforms?

The key takeaway

The UK Government has introduced major proposals for the digital gambling space, including financial risk checks, transaction blocks for payments, restrictions on advertisements and raising the age limit for gambling both offline and online. These changes are seen to target businesses in the tech space and are expected to impact which advertisements are displayed, how payments are made and how age verification takes place online.

The background

The Gambling Act first came into effect in 2005. The gambling landscape has since changed substantially, marked by the introduction of multinational tech businesses into the space. On 27 April 2023, the Government published its White Paper on reform of the Gambling Act.

The White Paper proposes a series of changes pursuant to a review conducted by the Department for Culture, Media and Sport (**DCMS**). In this review, the DCMS highlights its aim to balance consumer freedom on one hand, and the protection from harm (especially of those at risk of addiction and the younger population) on the other.

The development

The White Paper introduces a multitude of proposals. Amongst other changes to land-based gambling, the following key changes are brought in specifically targeting the digital space:

- **protections in place targeting online gambling** – the main proposal is a system to conduct affordability checks on individuals losing £1,000 within a day or £2,000 within 90 days. There are also proposals for the implementation of stake limits for online slot games, reviews of game speed for online games, an extension of gambling transaction blocks to online payment, as well as regulation over digital prize draws and competitions
- **tougher restrictions on gambling advertising, sponsorship and branding** – the White Paper suggests a further review from the Gambling Commission (Commission) of incentives such as free bets and bonuses and for online advertising of gambling to be directed away from children
- **increase of the Commission's power** – there are also suggestions that the Commission's licence fees should be increased and statutory levies be introduced for gambling operators so that the Commission has adequate resources to exercise extended powers, including compelling internet service providers and payment providers to stop providing their services to black market websites
- **raise in age limit for gambling** – following an increase in the age limit for the National Lottery to 18 years, the Government plans to increase the minimum age for other forms of gambling, including those online.

A further consultation is to follow which seeks contributions from industry stakeholders and participants in gambling during Summer of 2023.

Why is this important?

Though the series of reforms put forward by the White Paper are still subject to consultation and legislation pending Parliamentary timetable, the Government's intention to regulate the online realm of the gambling industry is clear. Future legislation is likely to follow, putting the onus on businesses to implement practices in line with the directions of the Government.

Any practical tips?

Digital platform providers are also likely to be directly impacted by the tightening of regulations over gambling related advertisements and sponsorships and may become responsible for age verification online. They may also find themselves in positions where they may be asked to impose blocks on large transactions pursuant to the White Paper proposals. Providers should keep a close eye on this developing area of law and when the consultation opens, should consider communicating their perspectives.

CONSUMER

New ICO guidance on direct marketing and regulatory communications

The question

When is a regulatory communication (ie a message sent in compliance with a regulator's request) likely to be considered direct marketing?

The key takeaway

On 28 March 2023, the UK's Information Commissioner's Office (**ICO**) issued new guidance for those operating in a regulated sector. The guidance aims to help organisations determine when regulatory communications could be considered direct marketing, which should help them comply with the relevant rules.

The background

Data protection laws (the UK GDPR and Data Protection Act 2018) and the Privacy and Electronic Communications Regulations 2003 (**PECR**) impose limitations on direct marketing carried out by organisations. Specific messages sent to people in compliance with a regulator's request (referred to as "regulatory communications" in the guidance) are unlikely to count as direct marketing, unless such communications promote a particular product or service.

The development

The guidance applies to organisations operating in regulated industries such as finance, pensions, communications, or energy. A regulatory communication is unlikely to be considered direct marketing if it is:

- conveyed in a neutral tone, without active promotion or encouragement
- solely for the people's benefit
- against the interests of the sender, and
- only motivated by the need to comply with a regulatory requirement.

For example, a regulatory communication message that provides prior notice of changes to terms and conditions or reminds customers of contact information if they are struggling with payments is less likely to be direct marketing.

However, the ICO emphasised that it is important to assess the specific circumstances and details of the message rather than adopting a 'one size fits all' approach. If marketing is not the main purpose of communication but the communication contains elements of marketing, then it would still be deemed as direct marketing.

Why is this important?

Even though regulators consider people's interests when requiring their sectors to send regulatory communications, the ICO guidance highlights that organisations have the responsibility to assess whether a message constitutes a direct marketing message and comply with appropriate rules. They must allow people the absolute right to opt out of communication and ensure that electronic messages comply with PECR provisions.

Any practical tips?

When delivering a regulatory communication, businesses must assess necessity and proportionality. They should consider if a specific purpose of the message can be achieved via "less intrusive means" such as displaying it on a website or social media. Additionally, organisations can choose to communicate the message to customers if they call their helpline, through television, radio or streaming services. The hypothetical examples are helpful in deciding whether a regulatory communication is likely to be direct marketing.

New development – Product Security and Telecommunications Infrastructure Bill

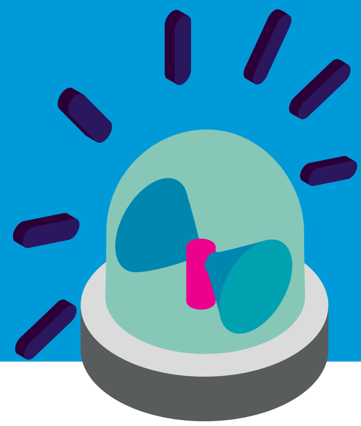
The Product Security and Telecommunications Infrastructure Bill received Royal Assent and became law on 6 December 2022.

The new law requires device manufacturers, importers and distributors to guarantee that their products meet minimum security standards during all design stages.

Businesses could face fines of up to £10m or 4% of global revenue (whichever is higher) for non-compliance.

Details of the security requirements will be laid out in the supporting regulations which are yet to be published.

See our previous coverage in our Autumn 2022 Snapshots.



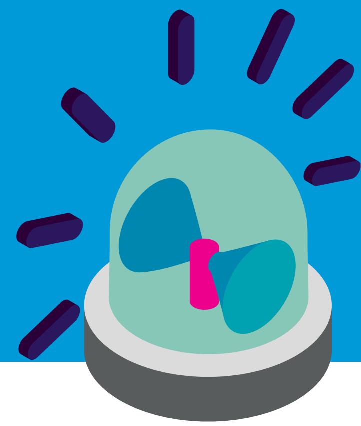
New development – General Product Safety Regulation

The General Product Safety Regulation (EU/2023/988) (**GPSR**) was entered into the Official Journal of the European Union on 23 May 2023.

The GPSR came into force on 12th June 2023 and will apply from 13 December 2024, replacing and revoking the General Product Safety Directive (2001/95/EC) (**GPSD**) on non-food consumer products and Directive (87/357/EEC) on food imitating products.

The GPSR addresses potential safety issues associated with new technologies sold online by increasing obligations on providers of online marketplaces, translating to possible operational changes for providers to ensure compliance. Under the GPSR authorities have enhanced enforcement powers and can take swift action to remove dangerous products from online marketplaces. Goods placed on the market before 13 December 2024 and which were compliant with the GPSD will not be prohibited from being sold.

See our previous coverage of the GPSR in the Spring 2023 Snapshots.



"For obvious reasons, the aviation industry needs to take particular care over green claims. From a wider perspective, absolute green claims are always hard, if not impossible, to justify."

ADVERTISING

ASA ends Etihad Airways' "sustainable aviation" campaign

The question

What went wrong with Etihad's claim about their commitment to "sustainable aviation" and why did the ASA hold it in breach of the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (the **CAP Code**)?

The key takeaway

For obvious reasons, the aviation industry needs to take particular care over green claims. From a wider perspective, absolute green claims are always hard, if not impossible, to justify. Specific, narrow claims are the way to go, especially from a substantiation viewpoint.

The background

In October 2022, Etihad Airways posted two ads on Facebook. They included pictures of plants and the Earth to promote their "louder, bolder approach to sustainable aviation" campaign.

In the first ad, the text stated: "We understand the impact flying has on the environment" and "With Etihad you'll earn Etihad Guest Miles ... every time you make a Conscious Choice for the planet".

The second ad included the same text, as well as further text explaining that Etihad are "cutting back ... on single-use plastics ... and are flying the most modern and efficient planes. Flights with a smaller footprint".

Both ads declared that Etihad were "Environmental Airline of the Year for 2022 in the Airline Excellence Awards".

The ASA investigated whether the campaign was misleading, on the basis that the environmental benefits of flying with Etihad were exaggerated. In response, Etihad argued that "sustainable aviation" was not to be interpreted as the only solution to aviation-caused environmental damage – it was merely part of their wider aspirations to reach "net zero" carbon emissions by 2050.

The development

The key takeaways from the ASA's investigation were that:

- the CAP Code stipulates that "absolute" environmental claims must be substantiated to a high level
- the first ad needed further context or explanation as to how "sustainable aviation" was being achieved
- the second advert failed to provide sufficient "qualifying information"
- the ads were aimed at the general public, so clearer language was needed to explain the claims
- no initiatives or technologies currently in operation by the aviation industry would have sufficient effect to fully substantiate an absolute claim such as "sustainable aviation", and
- overall, the ad campaign exaggerated the impact that flying with Etihad would have on the environment.

The CAP Codes breached were: rules 3.1 (Misleading advertising), and 11.1, 11.3 and 11.4 (Environmental claims).

The ASA advised Etihad to prevent making misleading claims in their future advertisements, and to ensure that environmental claims are fully substantiated.

Why is this important?

This decision follows the ASA's September 2021 statement, in which they committed to taking decisive action against misleading environmental claims in advertising.

In March, ASA banned ads from Lufthansa in which the airline stated they were: "Connecting the world. Protecting its future". Other big brands to have fallen foul of the ASA on green claims recently include Ryanair, Oatly, Shell and HSBC. The ASA is showing no sign of softening their approach against greenwashing.

Any practical tips?

Businesses must of course continue to prioritise initiatives to improve their impact on the environment. However, UK businesses must ensure they communicate these objectives in line with the ASA's guidelines. See our Spring 2023 snapshots for more on this. Essentially, and as demonstrated in the Etihad ruling, robust substantiation of all greens claims is essential. It is always easier to substantiate specific, narrow claims than broad or "absolute" green claims. The aviation industry, in particular, must maintain a sense of perspective when communicating green claims, in light of the industry's overall impact on the environment.

Lufthansa ad campaign to protect the environment fails to fly with the ASA

The question

Can an airline claim to be protecting the environment?

The key takeaway

The ASA has ruled that an ad for the German airline Lufthansa gave a misleading impression of the extent of the airline's environmental impact. The decision underlines just how hard it is for businesses in non-environmentally friendly industries to make green claims, and how broad, absolute environmental claims are almost always impossible to substantiate.

The background

A poster ad for the German airline Lufthansa included an image of the top half of a plane which was in flight, with half of a globe at the bottom half and carried the line "Connecting the World. Protecting its Future. #MakeChangeFly". The ASA sought to investigate whether the ad gave a misleading impression of Lufthansa's environmental impact.

In its response to the ASA's investigation, Lufthansa said the purpose of the ad and wider #MakeChangeFly campaign was to address the need to reduce the impact of air travel on the environment and to raise awareness amongst consumers of how Lufthansa is achieving this. It said that the website, which consumers were directed to through the ad via a hyperlink to www.makechangefly.com, was the primary source for this awareness, rather than the ad itself.

Lufthansa also argued that the slogan "Connecting the World. Protecting its Future" was open to interpretation but would not be understood by consumers as an absolute promise that their service caused no harm to the environment. It emphasised that "Connecting the World" was not an absolute claim and insisted that it could therefore be extrapolated that the second half, "Protecting its Future", was not an absolute claim either. It explained that the slogan would be seen as a mission statement intended to draw people to the website, which provided more context for the ad, in order to raise awareness of the environmental impact caused by air travel and the steps Lufthansa was taking to address them.

The development

The ASA acknowledged Lufthansa's view that the claim, "Connecting the world. Protecting its future" in isolation was ambiguous and not clearly linked to the environment. However, it considered that the claim "Protecting its future" was likely to be interpreted by consumers as an environmental reference to how Lufthansa's approach to aviation was protecting the future of the world, given that this text appeared immediately after the text "connecting the world" and was superimposed on a picture of the globe.

The ASA understood that the campaign was based on steps Lufthansa was taking as part of its aspirations to become more environmentally friendly at targeted points in the future. However, viewing the ad without the context of the accompanying website was likely to be interpreted by consumers as meaning that Lufthansa had already taken significant steps to mitigate the net harmful environmental impacts of its operations on the environment. The fact that the ad directed consumers to the website was therefore not sufficient to substantiate its claims given the fact that the ad could and would still be viewed in isolation by consumers.

The ASA also pointed out that air travel produces high levels of climate changing CO_2 as well as non-CO_2 emissions and that there are currently no environmental initiatives or commercially viable technologies in the aviation industry which could substantiate the absolute green claim that Lufthansa is protecting the future of the planet

Why is this important?

This is yet another example of a brand who has fallen foul of the ASA's rules on environmental claims, after the watchdog made promises in 2021 to crackdown on greenwashing. In 2022 the number of ads banned for environmental claims that could not be substantiated tripled from the previous year; those involved included HSBC, Innocent Drinks Oatly, Pepsi's Lipton and Unilever's Persil detergent. Miles Lockwood, the director of complaints and investigations at the ASA, gave the reminder that advertisers should not make environmental claims that mislead consumers about their green credentials which they cannot substantiate with robust evidence.

Any practical tips?

It is imperative that companies understand the ASA's CAP Guidance in its entirety. Of particular importance in this arena is the Advertising Guidance titled "The environment: misleading claims and social responsibility in advertising".

Failure to comply with the rules surrounding substantiated claims can give rise to immense wasted costs on advertising campaigns that ultimately get banned. There is also a significant risk of reputational damage when both a company's actual environmental impact and its overall integrity and authenticity are brought into question.

ASA guidance on "Carbon Neutral" and "Net Zero" as part of a greenwashing crackdown

The question

What does CAP's updated advertising guidance mean for businesses who wish to use green claims in marketing materials?

The key takeaway

Advertisers must be mindful of using the claims "carbon neutral" and "net zero" as well as consider their social responsibility when it comes to using green claims as part of their marketing materials. Transparency and clarity for consumers is key.

The background

In 2021, the ASA's Climate Change and the Environment project identified that the general understanding of certain advertising claims, including "carbon neutral" and "net zero" by consumers was an area requiring further understanding. This was against the backdrop of increased use by businesses of these claims as part of their marketing materials. The research found that:

- there is significant consumer engagement on environmental issues, affecting their understanding of, and reaction to, environmental claims
- "carbon neutral" and "net zero" were the most commonly encountered claims, but there was little consensus as to their meaning. There were calls for significant reform to simplify and standardise the definitions of such terms and for claims to be policed by an official body, such as government
- participants tended to believe that carbon neutral claims implied that an absolute reduction in carbon emissions had taken place or would take place. When the potential role of offsetting in claims was revealed, this could result in consumers feeling that they had been misled
- claims in air travel, energy and automotive advertising tended to attract more attention, and the potential role of offsetting, when revealed, could result in greater disappointment. Participant reactions suggested the need for transparency is potentially greater in those sectors, and
- participants called for more transparency about offsetting and target dates in ads.

The development

Based on the outcome of the research which identified a generally low understanding around the meaning of "carbon neutral" and "net zero" amongst consumers, the ASA released updated guidance for marketers on 10 February 2023. The guidance takes into account the core principles of the relevant Competition and Markets Authority (**CMA**) guidance. The updated guidance can be summarised as follows:

- marketers must avoid using unqualified carbon neutral, net zero or similar claims and information explaining the basis for these claims must be included
- marketers should ensure that they include accurate information about whether they are actively reducing carbon emissions or are basing claims on offsetting, to ensure that consumers do not wrongly assume that products or their production generate no or little emissions
- claims based on future goals relating to reaching net zero or achieving carbon neutrality should be based on a verifiable strategy to deliver them and details of this strategy should be easily accessible
- where claims are based on offsetting, they should comply with the usual standards of substantiation for objective claims and marketers should provide information about the offsetting scheme they are using, and
- where it is necessary to include qualifying information about a claim, that information should be sufficiently close to the main aspects of the claim for consumers to be able to see it easily and take it into account before they make any decision. The less prominent any qualifying information is, and the further away it is from any main claim being made, the more likely the claim will mislead consumers.

The ASA will conduct monitoring for up to six months and also gather information to assess how claims are being substantiated.

Why is this important?

This new guidance forms the basis of the regulatory crackdown on greenwashing. Under the plans, the ASA will take a strict enforcement approach against any businesses that mislead consumers regarding the effectiveness of their products in helping stop climate change - unless they can actually demonstrate that they really are effective. Recent ASA rulings against Shell, Petronas and Repsol SA highlight the ASA's zero tolerance approach to greenwashing, particularly with regard to the use of "net zero". In each of these cases, the ASA challenged whether the ads exaggerated the total environmental benefit of the products which therefore rendered the ads misleading.

Any practical tips?

The ASA guidance shows that transparency and clarity is key when making these types of green claims. Consider sharing the guidance with the marketing team if your business is looking at making green or sustainability claims based on carbon offsetting.

Avoiding a subscription trap: CAP issues enforcement notice on online ads for subscription services

The question

What do traders need to do to ensure online ads for free trials or promotions to subscription services comply with the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (the **CAP Code**)?

The key takeaway

Online ads promoting free trials or promotional offers for subscription services must ensure that the significant conditions of the free trial or promotion which are likely to influence the consumer's decision to subscribe are displayed with "sufficient prominence" and that the information is clearly visible, legible and identifiable from other information. Since 27 April 2023, CAP is actively targeting enforcement in this regard.

The background

CAP published its "Guidance on 'free trial' or other promotional offer subscription models" in 2017 (the **Guidance**) in support of the CAP Code which sets out the rules that subscription ads must comply with. For online ads relating to free trials and promotions of subscription services, CAP states that traders must ensure:

- the ad does not (or is unlikely to) mislead the consumer (Rule 3.1)
- qualifications to the service or promotion are clearly presented (Rule 3.10)
- the ad is clear about the length of commitment the consumer must make to benefit from the promotion (Rule 3.23)
- the ad clearly communicates all "significant conditions or information", where omission of said information would likely mislead the consumer (Rule 8.17), and
- where the ad is limited in time or space, as much information about the significant conditions is provided as possible and the consumer is clearly directed to another page or source where all significant conditions and information are available (Rule 8.18).

The Digital Markets, Competition and Consumers Bill (the **Bill**) will replace the existing rules in the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 for subscription services and will establish a separate set of rules for pre-contract information and cancellation that must be presented to consumers. For more information on the Bill see this Summer 2023 Snapshot.

The development

In response to the growth of the subscriptions market and the apparent non-compliance with the Guidance by advertisers, CAP has issued an enforcement notice (the **Notice**) providing further support to advertisers.

The Notice is targeted at online ads for subscription services which use free trials or promotional offers which require consumers to enrol onto an "ongoing payment arrangement" which continues, unless cancelled, after the free trial or promotion ends. Such ads must:

- ensure all significant conditions or information which are likely to influence the consumer's decision to enter into the subscription are clearly communicated and displayed with "sufficient prominence". It must be clear to the consumer if the subscription automatically continues after the end of the free trial or promotion, or if they need to cancel, the financial commitment if the subscription is continued, and
- ensure that all significant conditions follow directly from the free trial or promotion and are "immediately visible, prominent and distinct" from the rest of the information in the ad. This requires the wording to be in legible font.

For ads which are restricted in time or space, the Notice reminds advertisers that they must include as much information about the significant conditions to the free trial or promotion as is practicable. The ad must then clearly direct consumers to a secondary source where they can find all the information, which again complies with the CAP Code and the Notice.

The Notice states that CAP will be targeting enforcement from 27 April 2023.

Why is this important?

The Notice is a clear signal to advertisers that the ASA will specifically target advertisers of subscriptions services which do not comply with the CAP Code. Advertisers need to be aware of the advertising rules, especially as the Bill progresses through to implementation.

Any practical tips?

Online advertisers of subscription services should review their current marketing assets as well as any planned future campaigns against the Notice and the CAP Code to ensure any subscription ads are fully compliant. This is a clearly an area of focus for the ASA, and with the CMA about to obtain its direct enforcement powers under the Bill, now is the time to check and double-check that there are no gaps in the required information.

"Online ads promoting free trials or promotional offers for subscription services must ensure that the significant conditions of the free trial or promotion which are likely to influence the consumer's decision to subscribe are displayed with "sufficient prominence" and that the information is clearly visible, legible and identifiable from other information. ."

CMA open letter to businesses on urgency and price reduction claims

The question

What are urgency and price reduction claims and when will they breach consumer protection laws?

The key takeaway

"Sneaky" sales tactics (such as urgency claims and misleading price reduction claims) are likely to constitute a breach of consumer protection laws and constitute a criminal offence. Businesses that sell online should be aware of the sorts of practices prohibited by consumer protection law and ensure that they are not utilising these tactics.

The background

The Competition and Markets Authority (**CMA**) has become increasingly concerned that businesses are using "pressure selling tactics" to encourage consumers into buying their products or services online. Such practices can amount to a criminal offence under the Consumer Protection from Unfair Trading Regulations 2008 (**CPRs**) – which are soon to be updated and republished in the statute books within the Digital Markets, Competition and Consumers Act 2023 (**DMCC**).

On 29 March 2023 the CMA published an open letter to all UK online businesses that sell or advertise their goods and services online. The letter reminds businesses what their obligations are under the law in respect of urgency and price reduction claims and what may constitute an infringement of the law. At the same time a number of examples have also been published clearly showing the sorts of messaging and imagery that is likely to fall foul of the CPRs.

The development

The open letter focuses on two types of tactics that businesses may use: (i) urgency claims and (ii) price reduction claims. The key point is that businesses should not use these tactics where they are misleading, untrue or put pressure on consumers. This means that merely stating "only five left in stock" will not in itself be unlawful, as long as there are indeed only five of the relevant product available for sale to consumers.

Urgency claims

- Time limited claims, such as "offer ends in X days, X hours and X minutes". This is a tactic used where the business tells consumers that a specific offer will expire in a specified time. If, when the time runs out, the offer does not expire, this is likely to be unlawful as it is untrue and was only used to pressure the consumer into buying the product at that time on the basis that it would not be available at that price after such time.
- Popularity claims, such as "Hurry, 10 people have now purchased this item" or "20 people are viewing this item now". The idea behind these claims is to demonstrate to the consumer that there is a lot of interest in the product. These will be unlawful where the business' algorithm that produces the claims are not providing accurate data for that moment in time. For example, it might be that 10 people purchased the item yesterday or that 20 people viewed the item within the past 2 hours, but not at that exact moment in time.
- Scarcity claims, such as "limited availability left". This tactic encourages impulsive and fast purchasing decisions by consumers by implying that stock levels are low so if the consumer does not act with urgency, they will not be able to purchase the product. This is likely to be unlawful where stock levels are not low, or are at least high enough to mean the business can fulfil its contracts for that day (including in the event where stock is low but more is due to arrive).

Price reduction claims

- Any discount, special offer or reduction that refers to a higher comparison price, such as "Was £100, now £45". One example of a price reduction claim that would be unlawful is where the comparison prices are inaccurate because the business no longer sells the product at that price. As an example, a business might advertise that it is selling its product for £50 down from £80. However, if the business has actually been selling the product at £50 for several months, this means the "higher" comparison price the business is using is not the product's everyday selling price anymore. This gives the consumer the false impression of the price advantage they are getting on the product.

The CMA has also launched a new phase of its "Online Rip-Off Tip-Off" campaign which aims to enable consumers to report businesses that are engaging in misleading sale tactics (including those outlined above, as well as fake reviews, concealed charges or fake subscriptions). The campaign was introduced following a survey which showed that 67% of the 3,700 UK adult participants say the pressures associated with the cost-of-living crisis have made them more desperate to find cheaper, more affordable deals. It was also found that 24% of UK consumers have been subject to misleading online sale tactics. The online report form also offers advice on how to identify any sneaky sales tactics.

Why is this important?

In a day and age where e-commerce forms such a large percentage of retail sales, the CMA needs to ensure businesses are not employing unfair sales tactics, particularly given the current cost of living crisis where consumers are more interested that ever in getting "a good deal" on their purchases.

With the DMCC set to give the CMA direct enforcement powers and the ability to fine businesses directly where it determines there has been a breach of consumer protection law, it is clear we are entering a new era of enhanced consumer protection in the UK, which all traders need to be ready for.

Any practical tips?

Businesses should be reviewing their current sale tactics to ensure that they are not employing urgency and price reduction claims that put unfair pressure on consumers. All sale tactics must be compliant with the CPRs (or DMCC once this is in force – likely to be Spring 2024), as well as taking guidance from the promotions section of the CAP Code more generally and the Chartered Trading Standards Institute Pricing Practices Guidelines.

OFCOM consultation on advertising "less healthy" food and drink products

The question

How are new restrictions on the advertising of less healthy food and drink products under the Health and Care Act 2022 (**HCA 2022**) likely to be implemented?

The key takeaway

Although the position will be confirmed in OFCOM's response to its consultation, OFCOM's current approach suggests that the ASA will be designated as the primary regulator for the new advertising restrictions and that the restrictions will not replace existing restrictions on the advertising of HFSS products.

The background

In 2018 the UK Government set a target to halve childhood obesity by 2030. As part of measures to achieve this aim, the Government developed restrictions on the advertising of products that are high in fat, salt or sugar (**HFSS**). In June 2021, following a consultation period, it published a formal consultation response on policy, and proposed a series of restrictions. These included a 9pm watershed for the advertising of HFSS products on TV and on-demand programme services (**ODPS**) between 5.30am and 9pm, as well as a complete prohibition on paid-for online advertising of HFSS products (as set out in further detail in our blog here), restrictions on the placement of HFSS products in stores at aisle ends, store entrances, near checkouts, and at queuing areas, and restrictions on the volume price promotion of HFSS products.

Whilst the placement restrictions came into force in October 2022, in the face of the growing cost of living crisis, the volume price promotion restrictions were subject to a last-minute delay by the Government and are now set to come into force in October 2023.

The Government also delayed the introduction of the watershed for the advertising of HFSS products on TV and ODPS, as well as the prohibition on paid-for online advertising of HFSS products from January 2023 to October 2025. In the meantime, the Government's consultation seeking views on draft secondary regulations (the Advertising (Less Healthy Food Definitions and Exemptions) Regulations) on products within the scope of the advertising restrictions (and the extent of exemptions for small and medium-sized enterprises (**SMEs**)) closed on 31 March 2023. Separately, Ofcom launched its own consultation on 21 February 2023 to seek stakeholder views on its proposed approach to implementing the new advertising restrictions, which closed on 21 April 2023 (the **OFCOM Consultation**).

The development

Here are some of the key points to note:

- whilst OFCOM is the statutory regulator with overarching responsibility for TV and ODPS advertising, its existing co-regulatory relationship with the Advertising Standards Agency (**ASA**), Broadcast Committee of Advertising Practice (**BCAP**) and Broadcast Standards Board of Finance (**BASBOF**) should continue in respect of the regulation of the new restrictions on TV and ODPS advertising. Further, the ASA is likely to be designated by OFCOM as the primary regulator for online advertising. This suggests that the ASA's usual sanctions will be used to achieve compliance in relation to online, TV and ODPS advertising where necessary and if compliance is not achieved, OFCOM's powers will be utilised. In OFCOM's view this process of regulation will create consistency for consumers and advertisers alike
- the new advertising restrictions will not replace existing rules on the advertising of HFSS products, for example, rules on the targeting of children (ie those under the age of 16) and scheduling. Instead, the new restrictions will sit alongside existing restrictions and only apply to "less healthy" food and drink ie those which are both: (i) classified as HFSS according to the Department of Health and Social Care's Nutrient Profiling Model, and (ii) fall within the specified categories of food and drinks products detailed in the Food (Promotion and Placement) (England) Regulations 2021 – the existing rules only apply to the former. Further, any exemptions in respect of the new advertising restrictions, such as the proposed exemption for SMEs, will not automatically apply to existing HFSS advertising restrictions, and
- OFCOM is proposing a number of changes to the BCAP Code (for TV adverts), the Broadcasting Code (for TV sponsorship adverts) and the CAP Code (for ODPS advertising) to reflect the new restrictions. Amendments include an appropriate definition for HFSS products and to ensure that the advertising restrictions in the Broadcasting Code also cover the sponsorship of less healthy food and drinks between 05:30 and 21:00.

Why is this important?

Once the Government publishes its responses to both the Government and OFCOM consultations, we expect to see more clarity for brands about the boundaries and scope of the new advertising restrictions. However, as matters stand, the proposed advertising restrictions will apply to most brands selling HFSS products and are therefore likely to impact a wide range of brand owners.

Any practical tips?

Although the delays to HFSS advertising restrictions have not been well received by those who are in the healthcare sector or otherwise at the sharp end of the health implications of rising rates of obesity, businesses should make use of this period of delay to assess their marketing of HFSS products, and the steps required to comply with the proposed restrictions. They should also consider whether there may be value in developing alternative non-HFSS product lines in order to bypass the proposed restrictions.

Although the most recent consultations do not appear to address the issue, brands should bear in mind that the advertising restrictions will bite on influencer marketing, to the extent the relevant content represents "paid-for" advertising (ie where an influencer posts content about HFSS products having received payment or another kind of benefit from the advertiser).

"Once the Government publishes its responses to both the Government and OFCOM consultations, we expect to see more clarity for brands about the boundaries and scope of the new advertising restrictions."

> *"The draft Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023 (the **Order**) will mean qualifying cryptoasset promotions are regulated in the same way as traditional financial promotions."*

ADVERTISING

New legislation proposed to bring FCA regulation to cryptoasset promotions

The question

What will the Government's new legislation mean for the promotion of cryptoassets?

The key takeaway

The draft Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023 (the **Order**) will mean qualifying cryptoasset promotions are regulated in the same way as traditional financial promotions. There will also be an exemption allowing some FCA-registered businesses who would not otherwise be eligible to make cryptoasset promotions.

The background

Cryptoasset advertising has concerned the UK Government for several years. Consumers are often faced with advertising which presents cryptoassets of all kinds as low-risk and high-reward. Cryptoasset promotions to date have not been subject to the stringent rules governing conventional financial promotions, being overseen only by the ASA, not the FCA. Although the ASA has taken action at times (for example, banning two crypto "fan tokens" promotions by Arsenal FC in 2021), recent cryptoasset market instability has underlined the need for more effective regulation of cryptoasset promotions to protect consumers from harm and allow them to make informed decisions on cryptoasset investments.

The development

On 27 March 2023 HM Treasury published the draft Order and an accompanying explanatory memorandum. When it comes into force, the Order will bring the promotion of "qualifying cryptoassets" into the financial promotion restriction under Section 21 of the Financial Services and Markets Act 2000 (**FSMA**).

Qualifying cryptoassets are defined as those which are fungible and transferrable. This includes common cryptocurrencies such as Bitcoin or Ether. Notably it does not include non-fungible tokens (**NFTs**) on the basis that "these have so far tended to be used in a way more akin to digital collectibles than financial investments".

In-scope cryptoassets will become "controlled investments" and therefore subject to strict rules governing their promotion. This will prohibit a person from communicating invitations or inducements to invest in these cryptoassets in the course of business unless:

- the promoter is an authorised person under Part 4A of FSMA
- the content of the communication has been approved by an authorised person, or
- an exemption applies.

Very few current cryptoasset promoters can meet these criteria, so the draft Order also creates a limited, temporary exemption, discussed in more detail in our Spring 2023 Snapshots.

The FCA will become the regulator and supervisor of these promotions and will act against any non-compliant promotions. Making an unlawful financial promotion is a criminal offence with a maximum sentence of 2 years imprisonment and an unlimited fine.

If Parliament approves the draft Order it will come into force after a four-month implementation period, reduced from the anticipated six months due to the need to protect consumers as soon as possible whilst the crypto market remains volatile. Further regulation in this area is almost certain, including in relation to stablecoins and unbacked cryptoassets.

Why is this important?

The draft Order represents a clear choice to bring cryptoasset promotions into the established financial promotions regulatory regime rather than establishing a bespoke crypto regime. This FSMA regime is well-understood by the major FCA-regulated financial institutions and their professional advisers. They should welcome the decision to use this familiar framework rather than creating a bespoke regime for cryptoasset promotions. Crypto promoters should also welcome it as a sign that the Government is likely to reject calls to regulate cryptoasset trading as gambling, rather than financial services.

Any practical tips?

Affected business must take advice to ensure they fully understand the new rules and requirements before they make financial promotions of qualifying cryptoassets. Given the high profile of the issue, the FCA is likely to take its new regulatory responsibilities very seriously. Penalties for non-compliance may well be severe.

ADVERTISING

CMA and CAP issue stronger joint guidance on influencer marketing

The question

What can we learn from the new edition of the joint CAP and CMA "Influencers guide to making clear that ads are ads"?

The key takeaway

It is clear that influencer marketing remains firmly on the regulators' radars for 2023 and beyond. In this new iteration of the joint guidance, brands and agencies, as well as influencers, are reminded of the advertising disclosure obligations. Whilst the updated guidance is not substantively ground-breaking, it represents a concerted effort by the Committee of Advertising Practice (**CAP**) and the Competition Markets Authority (**CMA**) to make it absolutely crystal clear both when the requirement to disclose arises (including clarification as to who/what constitutes an "influencer") and how to make such a disclosure when the requirement is triggered.

The background

CAP and the CMA first published joint guidance in 2018 to help social media influencers understand their obligations when posting content online which advertises a brand, product or service. Since then, CAP and the CMA each have produced further guidance to keep up with changes in industry practice and to better engage with influencers. However, influencers are still consistently falling foul of the advertising rules and despite the existing body of guidance and the steady stream of upheld rulings handed down by the Advertising Standards Authority (**ASA**), it feels like influencers are either not aware of, or simply not following, the rules.

In previous Snapshots we have commented on recent key influencer ASA rulings against the likes of MailOnline, Laura Whitmore and Binky Felstead, as well as the three-part set of guidance published in November 2022 to support influencers, advertisers and social media platforms with complying with consumer protection law and protecting consumers from hidden ads. In this Snapshot we look at the new joint CAP and CMA guidance, which landed at the end of March 2023.

The development

The updated guidance has a marked change in tone and language, which makes it more reader-friendly compared to its predecessor. It is clear that CAP and the CMA are aiming to ensure that all influencers, including those perhaps without agency representation or ready-access to legal advice, understand what they need to do to comply with the advertising disclosure rules.

In case there was any doubt previously, the guidance now confirms that all of the following fall within the definition of "influencer": "any human, animal or virtually produced persona that is active on any online social media platform", regardless of any label that they or any platforms use to describe them (eg "content creator", "celebrity" etc). Pets on Instagram, be warned – the rules apply to you too.

The guidance explicitly confirms some specific situations where a disclosure requirement arises:

- where an influencer is not receiving money directly from a post, but the post includes a discount code or affiliate link allowing the influencer to receive commission
- (following in the footsteps of the CMA's November 2022 guidance) where an influencer has received a gift with no obligation to post about it, but the influencer does opt to feature it in their content, and
- where an influencer is promoting their own business/product or that of a friend or family member.

CAP and the CMA have also updated their list of acceptable and unacceptable disclosure labels. In the previous edition, the guidance stated that the usual "ad" label could be used with or without a hashtag. Now it is clear that omitting the hashtag will only be acceptable if the "ad" label is clearly prominent from the rest of the text in the caption or post.

The new guidance also removes the list of labels marked as "usually recommend staying away from" and strengthens the position by stating examples of labels they explicitly "advise against using". This stronger approach is also seen in the decision tree towards the end of the guidance. This has been updated to be more direct as to when a post needs to be disclosed as (eg "your content is advertising and needs to disclose that upfront" has become "you need to label it").

Why is this important?

The ASA, CAP and the CMA are doubling-down on their approach to influencer marketing. The string of upheld influencer marketing ASA rulings in the last few years have seen brands and influencers attempting to run a couple of typical defences (lack of awareness of the requirement and/or that it was obvious that the post was an ad even without a disclosure). The regulators are clearly fed up with this line of argument, and this new guidance feels like a last-ditch attempt to make the rules so clear and simple that there is no place left for influencers to hide when it comes to disclosures.

What this means for the future of enforcement activity in relation to influencer marketing, given the CMA is on the verge of receiving harsher direct enforcement powers for breaches of consumer protection laws under the forthcoming Digital Markets, Competition and Consumers Bill, remains to be seen.

Any practical tips?

As always, influencers should take a maximum-transparency approach to creating and publishing marketing or promotional content. However, now more than ever, advertisers using influencers should also be taking a proactive approach to disclosure compliance, and include strict requirements on its influencers to ensure they make the necessary disclosures. For now, it is clear, the safest approach for disclosing ads within influencer marketing content is to clearly include #ad and to avoid any other labels that have not been endorsed by the ASA, CAP or the CMA.

ASA slams KSI and JD Sports for omitting #ad in online post

The question

What if a social media post is clearly a piece of marketing? Do you still need to prominently label it with #ad?

The key takeaway

Predictably, the Advertising Standards Authority (**ASA**) upheld a complaint against popular social media figure KSI when he did not use #ad to obviously identify his Instagram video for JD Sports as a marketing communication. The ASA's message is simple. Whenever influencers make a marketing post in connection with a brand, they must almost always use #ad.

The background

Olajide Olayinka Williams "JJ" Olatunji, known professionally as KSI, is a well-known YouTuber, rapper and boxer from the UK. In November 2022, he posted a video on his Instagram account of himself and others playing games at a bowling alley and arcade with modern electric music playing in the background. The video included close-up shots of the pair of trainers worn by KSI. KSI also drew attention to his trainers during the video. The other people in the video were depicted wearing sports clothing from popular brands, such as Adidas, North Face and Nike. The end of the video showed the JD Sports logo, below which was the text: "King of the Game". The caption which accompanied the video stated: "Welcome to the JD Arcade [devil emoji] Head over to the @jdofficial YouTube channel to watch the full-length film #kingofthegame". The video tagged the Instagram accounts of @jdofficial and @adidasoriginals. Importantly, the post did not feature the hashtag #ad.

The ASA adjudication

The complaint was made on the grounds that the Instagram video was not obviously identifiable as a marketing communication for JD Sports. In response, JD Sports' stated that their understanding of social media marketing was that the inclusion of hashtag #ad was only required where a post was not already obviously identifiable as a marketing communication. They argued that various aspects of their ad, such as the caption directing viewers to their YouTube channel and mentioning a full-length version, along with the high production value and involvement of 28 celebrities, made it clear that it was created for the purpose of being a marketing communication. They also emphasized that the video had gained significant exposure through prior appearances on TV, billboards and social media, and had been widely discussed due to the numerous celebrity cameos. JD Sports also confirmed that they had a contractual agreement with KSI, which was founded through a third-party agency, to post ads on their behalf. They had agreed on the ad schedule and content with KSI's representatives, including the specific ad in question.

KSI stated that, at the time at which the Instagram video was posted, he believed that the references to JD Sports in the video's caption, and the brand's logo featuring at the end of the video, made clear to consumers that the video was a marketing communication. However, when he became aware of the complaint, he added the hashtag #ad into the caption.

In the ASA's consideration of the complaint, they looked at a number of key elements, including the contractual relationship between KSI and JD Sports, the elements of the video's caption and the content of the video itself. In conclusion, the ASA considered that these elements did not amount to a clear statement of the commercial relationship between KSI and JD Sports, which would be immediately understandable to consumers.

Therefore, the ASA ruled that KSI's Instagram video must not be used again in its current form, ie without the inclusion of hashtag #ad in the video's caption. Both JD Sports and KSI were warned that any future social media marketing communications must be clearly identifiable as such, for example by utilising the hashtag #ad, as soon as a video is posted, in a clear and prominent way.

Why is this important?

This decision is one in a growing line of upheld adjudications by the ASA against social media posts failing to properly identify themselves as marketing communications, and many of those adjudications relate to situations where the brand and influencer involved believed it was screamingly obvious that the post was an ad. The decision is important because it reinforces that pretty much every marketing communication you can conceive of which is made by a social media influencer needs a prominent and clear #ad disclaimer.

Any practical tips?

If we said it before, we'll say it again: use #ad when making marketing communication posts by social media influencers, however obvious you think it is that it is clearly an ad.

If you need more on this, see the ASA's "An Influencer's Guide to making clear that ads are ads", which provides a plethora of advice for any social media influencer to ensure that any posts they make for the purpose of marketing communication are clearly identifiable to the consumer.

ASA rules against use of filters to promote beauty products

The question

How careful should advertisers and influencers be when using in-app filters for beauty products? And is "#myownbrand" helpful from an advertising disclosure perspective for an influencer's own products?

The key takeaway

While the ASA does not particularly see an issue with using filters in general, they should not be used in conjunction with the promotion of cosmetic or beauty products as this may mislead over the effect of such products. Separately – and hopefully this goes without saying – anything other than #ad won't wash with the ASA as an advertising disclosure.

The background

Influencer Charlotte Dawson was found to be in breach of the UK Code of Advertising and Direct & Promotional Advertising (the **CAP Code**). The complaints stemmed from several Instagram stories she posted about fake tanning products. The products were from Ms Dawson's own "Dawsylicious Tanning" range. Despite inserting "#myownbrand" to each Instagram story, complaints were submitted that it was unclear that her posts were in fact ads, especially to Instagram users who are not familiar with her branding and products. A second group of complainants believed that the Instagram filters used (in relation to the same stories) were misleading as they embellished the efficacy of the products being promoted.

The ASA adjudication

The ASA held that the posts were not obviously identifiable as marketing communications, despite all the ads including the handle "@dawsylicioustanning", her Instagram username "charlottedawsy", and the URL "dawsylicioustanning.co.uk". These references were not sufficiently clear to make the posts obviously identifiable as ads. There was nothing in their content, such as "#ad" placed upfront to indicate to users that the posts were marketing communications. The ASA also commented that the #myownbrand text was not in any event sufficiently clear and prominent, given its placement, colour and font size.

As for Instagram's in-app beauty filters, the ASA considered that the use of filters in ads was not inherently problematic, but that advertisers of cosmetic products need to take particular care not to exaggerate or otherwise mislead consumers regarding the product advertised. As Ms Dawson's ads conveyed a tanning and smoothing effect of the product, the ASA considered that the application of the filters to the images was directly relevant to the claimed performance of the product and gave a misleading impression about the performance capabilities of the product.

The ASA therefore upheld both complaints.

Why is this important?

There is nothing new in the ASA's call for clear and prominent use of ad disclosures by social media influencers when they are posting marketing communications. The ASA's approach to the use of filters in ads is helpful though, in that they have confirmed that filters can be used in ads provided they are not relevant to the performance of the product or service in question.

Any practical tips?

Don't use filters in ads for beauty products if they are in any way relevant to the claims about their performance. And always, always use #ad in influencer marketing posts!

Social media influencer criticised by ASA for not clearly identifying a TikTok video as a marketing communication

The question

What should social media influencers include in their TikTok content to ensure they are obviously identifiable as marketing communications?

The key takeaway

A social media influencer did not correctly identify her TikTok video as a marketing communication for a music brand, despite using the wording "soundad" in the video's caption. The Advertising Standards Authority (**ASA**) banned the video from being used in the same form again, giving a warning that any future videos of this nature, including where the audio content was part of a marketing communication, must clearly be labelled with #ad, as a minimum, to avoid any potential confusion.

The background

Tasha Ghouri, a social media influencer and contestant on series 8 of ITV's Love Island, posted a video on her TikTok channel documenting a day in her life, which featured the song "Hold Me Closer" by Elton John, Britney Spears and Joel Corry playing in the background. The caption of Ghouri's video stated: "[heart emoji] #TinyDancer #HoldMeCloser soundad" and below the caption, the video stated: "[music note symbol] Hold Me Closer - Joel Corry Remix – Elton John & Britney Spears".

The development

The complaint on Ghouri's content was made on the grounds that the TikTok video was not obviously identifiable as a marketing communication for Universal Music Operations Ltd (**EMO**), despite the caption containing "soundad".

EMO stated that the standard practice when they collaborated with influencers on TikTok was to request that either "musicad" or "soundad" was included within the video's caption. According to EMO, this was sufficient to identify such content as a marketing communication and they provided examples of where other influencers had used the #musicad or #soundad in their posts of the same nature. Moreover, according to EMO, after a "quick scan" of TikTok, there were over 450m uses of #musicad and / or #soundad, which they felt highlighted that the use of such hashtags clearly indicated such content as marketing campaigns to TikTok consumers. Ghouri's management, who commented on her behalf, stated that her TikTok caption clearly displayed "soundad" in the first line, and that this should have been more than sufficient in identifying her video as a marketing communication. TikTok also confirmed that the video appeared to be branded content, given that Ghouri had used their 'Branded Content' disclosure tool, which was a requirement for marketing communications under their Terms of Service and Branded Content Policy.

However, the complaint was upheld. The ASA held that, firstly, for the purposes of the CAP Code, the TikTok video was a marketing communication, because there was a contractual agreement between Ghouri and EMO, under which Ghouri was being paid to promote the track "Hold Me Closer" in her TikTok post. The ASA then assessed whether the video was obviously identifiable as a marketing communication. They held that the use of "soundad" alone was not sufficient to identify the video as a marketing communication, as it may have been confused by TikTok users as a misspelling of "sounded" and the "ad" part of the label was insufficiently prominent. Therefore, the ASA concluded that the TikTok video was not obviously recognisable as a marketing communication and was in breach of the CAP Code.

It was ruled that Ghouri's TikTok video must not be used again in its current form, with the ASA warning her and EMO that any future TikTok marketing of this nature must be obviously identifiable as such, for example by utilising the hashtag #ad in a clear and prominent way.

Why is this important?

It is of upmost importance to ensure that any social media post, whether on TikTok, Instagram or other platforms, created for the sole purpose of being a marketing communication, is clearly identifiable as such. This is particularly important for influencers, because if a post isn't clearly labelled as an ad, fans or followers may be led to believe that the brand or product endorsement portrays the influencer's own view, rather than it being paid promotion. Transparency is key to ensure posts fall within the remit of the CAP Code.

Any practical tips?

Influencers and brands alike must err on the side of caution when producing social media marketing content. In short, the best way for influencers to ensure their marketing communications do not breach the CAP Code is to display hashtags such as #ad in a clear and prominent way within the caption of a post. The ASA's "An Influencer's Guide to making clear that ads are ads" is a useful resource, providing comprehensive advice for social media influencers to ensure that any posts with the purpose of promoting a brand or product are clearly identifiable as such.

ASA upholds ban on BetVictor ad featuring football stars with "strong appeal" to under 18s

The question

What are the rules on including sports stars with strong appeal to under 18-year-olds in gaming and lottery ads?

The key takeaway

Businesses must ensure that all gambling or lottery ads do not have a "strong appeal" to those under 18 years old before they are published. The ASA can be seen to be taking both a wide and strict approach to the interpretation of the words 'strong appeal', so great care must be taken whenever the marketing team seeks to include sports stars in advertising.

The background

In a paid-for Facebook ad, BetVictor, next to an image of its logo, featured an image of two FC Barcelona players, Jodie Alba and Sergio Busquets, with the caption "Who is the most underrated player at the club you support?" As both are active players for a prominent team, the ASA challenged whether the ad included individuals who were likely to have a strong appeal to under-18s and therefore breached the UK Code of Advertising and Direct & Promotional Marketing (the **CAP Code**).

In response, BetVictor challenged the decision, claiming that even though the players played for FC Barcelona, they were not that popular or well known in the UK. Their objection included comparisons against other well-known stars such as Ronaldo, Messi and Mbappe whose UK searches far exceeded those of Alba and Busquets. Additionally, BetVictor confirmed that neither Alba, nor Busquets held goal-scoring or attacking positions, or have recently hit news headlines.

The arguments were rejected by the ASA and both players were considered to be "stars" and therefore were likely to be of "strong appeal" to under 18s. The ASA further commented that "because Facebook is a media environment where users self-verified on customer sign-up and did not use robust age-verification, [it] considered that Bet Victor had not excluded under-18s from the audience with the highest level of accuracy required for ads the content of which was likely to appeal strongly to under-18s".

The development

In October 2022, CAP and BCAP accepted recommendations to amend the rules in respect of the content of gambling and lottery advertisements. These rules state that any marketing communications related to gambling or lottery products must not be likely to appeal to children or young adults. An update was published by CAP entitled "Don't gamble on what appeals to kids", which drew attention to this issue.

Examples of how content can have a "strong" appeal to minors include the following:

- activities that are very popular or common amongst younger people
- characters or real people who are under 25 or dress/behave in a young manner (to avoid 18s identifying with them), and
- the use of music, graphics or animation which is closely connected to youth culture.

There is an exception to the rules where the underlying activity itself has a strong appeal to minors, such as football or video games. In this case, gambling products can still be advertised but only if "appropriate steps" have been taken to limit the ad's strong appeal to under 18s. For lotteries advertising, no person or character with a strong appeal to under 18s can be used unless that person is directly associated with the lottery for a good cause (eg an athlete who has received lottery funding). A number of other conditions must also be met.

While the term 'strong appeal' is subjective, this case demonstrates the ASA's strict approach to its interpretation. This case was the first time that the ASA has had to rule on players who play for teams outside of the UK, demonstrating a wider and stricter scope of interpretation.

Why is this important?

Advertisers involved in producing these types of ads must be highly tuned in to these rules. This involves reviewing available data and investigating the target audience of those they have sponsorship deals with, in order to ensure that their ads are responsibly targeted.

Any practical tips?

Gaming and betting businesses need to pay particular attention to this decision. Using football and other sports stars in ads is a common and obvious marketing tactic. Of course, the rules don't just apply to sports stars. Using anyone (including famous influencers) who may have a strong appeal to under-18s will be caught. It's well worth reviewing previous ASA rulings and, if you proceed, collating sufficient evidence to help demonstrate to the ASA that an ad does not have a "strong appeal" to minors. If you are unable to reach a firm conclusion on this point, it is best to play it safe and not publish – at least not without first seeking legal advice.

Valid incorporation of terms dealing with software error in online contract using click-wrap acceptance

***Parker-Grennan v Camelot UK Lotteries Ltd* [2023] EWHC 800 (KB)**

The question

When using the "click-wrap" method to accept terms in an online contract, what issues should be considered to ensure that the terms are properly brought to the consumer's attention?

The key takeaway

Where standard terms and conditions in an online contract are clear, balanced and set out with some thought, the click wrap method will generally be effective to incorporate them. Unusual or onerous terms may require additional signposting in order to be validly incorporated.

The background

In 2015, Ms Parker-Grennan purchased a £5 ticket for an online National Lottery Instant Win Game (**IWG**) operated under licence by Camelot UK Lotteries (**Camelot**). To win the IWG, players had to match the numbers in the "Your Numbers" section of the screen to those in the 'Winning Numbers' section, where each of the 'Winning Numbers' corresponds to a monetary prize. Prizes ranged from £5 to £1m.

After Ms Parker-Grennan had pressed the "play" button on her screen and then clicked on all of the numbers as instructed, her screen changed, and she was told that she had won £10. This was because the number "15" was matched and it was flashing white, and the prize for that combination was £10. However, on closer scrutiny she could see that she had also matched the number "1", the prize for which was £1m. There was no corresponding message to the effect that she had won that amount, and no flashing lights.

In 2009, in order to open her National Lottery account, Ms Parker-Grennan was required to tick a box to confirm that she had read and accepted Camelot's applicable terms. These account terms, rules and game procedures were accessible via a series of hyperlinks or drop-down menus. Notable updates to these terms were alerted to Ms Parker-Grennan from time to time who was again required to indicate her acceptance through clicking an 'accept' button or ticking a box.

Under these terms, it was stated that the results of IWGs are pre-determined and that only one prize may be won per game. The terms also stated that Camelot had the right to validate each win before any prize was paid out and that its decision as to whether a play is a winning play is final. According to Camelot's list of winning plays, Ms Parker-Grennan's play had been assigned a prize value of £10.

Ms Parker-Grennan issued proceedings against Camelot claiming she was entitled to the £1m prize in addition to the £10 prize which the screen display had told her she had won. Camelot refused to pay out, saying that she did not win the £1m and that a coding issue had generated an error in the software responsible. The £10 prize was the one the computer had "predetermined" would be won in conjunction with the ticket she had purchased. Further, it was the £10 prize only that was automatically recorded on Camelot's official list of winning plays.

Ms Parker-Grennan argued that either the above terms were not validly incorporated into the contract, or that they were unenforceable under the Unfair Terms in Consumer Contracts Regulations 1999 (**UTCCR**).

The decision

The High Court dismissed the application, finding that the applicable terms had been validly incorporated into the agreement with Ms Parker-Grennan and were enforceable.

The court considered three key issues: what were the applicable terms (incorporation); were any of these terms unenforceable under the UTCCR (enforceability) and, following on from this, did Ms Parker-Grennan win £1m (construction)?

The court acknowledged that it was not necessary for standard form conditions to be read by the receiving person and that the method of acceptance used by Camelot is common practice on the internet – consumers are familiar with the requirement to accept terms by ticking a box or clicking "accept". Subject to the other issues on enforceability, Camelot's use of drop down menus and hyperlinks to display the relevant terms was sufficient to incorporate them.

Reviewing the relevant terms against what would reasonably be expected in the given scenario, the court found that the rules were not particularly unusual or onerous so as to require additional signposting in order to be validly incorporated. In a more general comment, the court held that the rules were clearly drafted, set out in a logical order with reasonably prominent headings, obviously drafted by a lawyer and easy to follow.

On the enforceability of the relevant terms under UTCCR (which applied because the circumstances of the case arose before the Consumer Rights Act 2015 came into effect), the court found that while some of the relevant clauses contained terms that created an imbalance between the parties, it was not a significant imbalance so as to render the terms relied on by Camelot to be unfair and unenforceable or contrary to the requirement of good faith.

In particular, Camelot's requirement for it to validate a prize before paying out was not considered to be unusual for online games even though this gave more power to the supplier than the consumer.

Consequentially, Ms Parker-Grennan was found not to have won £1m.

Why is this important?

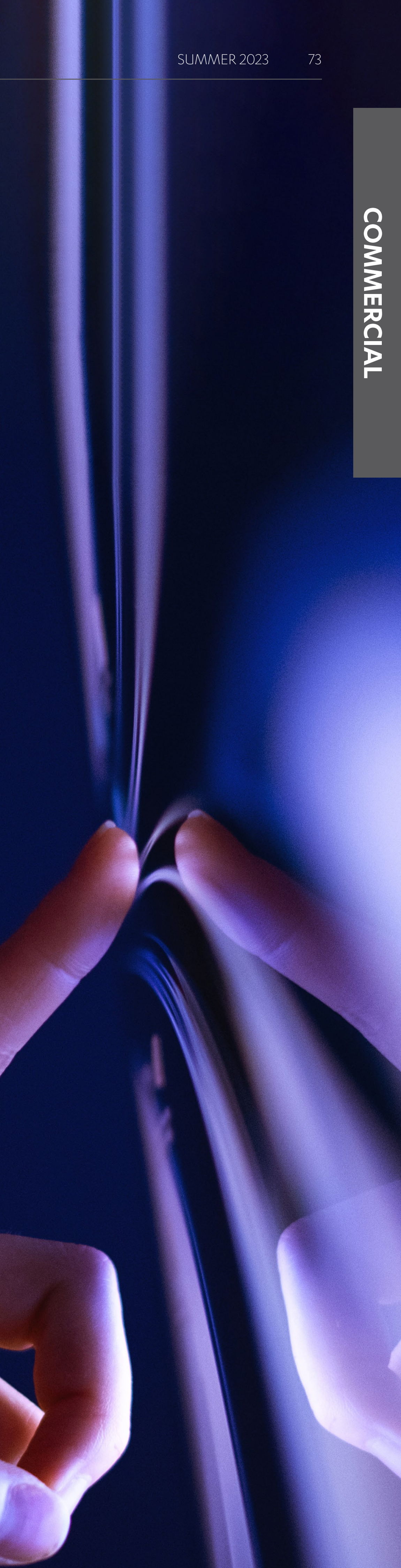
This decision highlights that for clear and balanced online standard terms and conditions, the click wrap method will generally be effective but that reasonable steps must be taken to draw onerous and unusual terms to the notice of those who are to be bound by them to ensure that the terms and conditions are incorporated and do not fall foul of consumer rights legislation.

Any practical tips?

In online contracts, the click-wrap method of accepting terms is well established and will usually be sufficient to incorporate standard terms and conditions as long as the terms themselves are not unusual or onerous. Unusual or onerous clauses should be specifically signposted to consumers but clauses dealing with the supplier's ability to step in to deal with issues such as the results of software errors will not necessarily be considered to be onerous or creating an unfair imbalance between the parties.

Terms must be accessible – in this case the court commented favourably on the use of hyperlinks, drop down menus and the use of three separate sets of terms (account terms and conditions, rules and game procedures) for the services offered.

The general rules of drafting also apply: keep key terms short and written in a way consumers can understand, use plain English and include short summaries of clauses, and use bullet points and headings to allow consumers to more easily navigate long form contracts.



Court of Appeal considers key requirements for an enforceable dispute resolution clause

***Kajima Construction Europe (UK) Ltd v Children's Ark Partnership Ltd* [2023] EWCA Civ 292**

The question

What form of wording and/or omissions in drafting may result in a Dispute Resolution Procedure (**DRP**) clause being held to be unenforceable?

The key takeaway

Courts will generally try to uphold a commercial agreement where possible. However, if the DRP clause is not sufficiently clear and certain, then it is liable to be held unenforceable.

The background

In 2004, the Children's Ark Partnership (**CAP**) entered into a contract with the Brighton and Sussex University Hospital NHS Trust to redevelop the Royal Alexandra Hospital for Sick Children in Brighton. Schedule 26 of the contract set out the dispute resolution procedure (**DRP**) between the parties.

On the same day, CAP entered into a contract with Kajima Construction where Kajima was engaged to design, build and commission the hospital (the Construction). The Construction Contract stipulated that proceedings were not to be brought against Kajima after the end of a 12-year period from the 'Actual Completion Date of the Works'. The works were originally completed in 2007 so the limitation period expired in April 2019.

CAP alleged that there were defects in the design and/or construction of the hospital. In late 2018, Kajima agreed to conduct remedial works. A standstill agreement between the parties was agreed extending the limitation date and expressly referring to the DRP set out in Schedule 26.

After a breakdown in the relationship between the parties and without first submitting to the DRP, CAP issued proceedings against Kajima. In response, Kajima applied for CAP's claim to be set aside or struck out due to CAP's lack of compliance with the DRP. In particular, CAP had not sought to refer the dispute to a 'Liaison Committee', as required under Schedule 26. Kajima claimed that the referral of the dispute to the Liaison Committee was a condition precedent and CAP's failure to do so meant the court had no jurisdiction over Kajima.

At first instance, the court found that the DRP provided for in the contract was not enforceable because:

- the DRP did not contain a "meaningful description" of the process to be followed
- there was no unequivocal commitment to engage in any particular procedure. Kajima was not a party to the Liaison Committee (but could be invited) so Kajima was not obliged to take part in the process, consequently it was impossible to see how the process could be said to provide a means of resolving disputes or disagreements between the parties amicably
- it wasn't clear how the dispute should be referred to the Liaison Committee, in fact the parties did not agree that the issue had in fact been referred to the Liaison Committee
- it was unclear whether any decision of the Liaison Committee would have a binding effect on Kajima
- it was not clear when the process of referral to the Liaison Committee came to an end (ie whether resolution or a decision was required before litigation could be commenced), so it was unclear when the condition precedent was satisfied.

The court rejected Kajima's application and Kajima appealed to the Court of Appeal.

The decision

Agreeing with the lower court, the Court of Appeal dismissed the appeal.

Referring to a number of authorities on general principles relating to enforceability of DRP clauses the court emphasised that wherever possible, the court should endeavour to uphold the agreement reached by the parties. However, where there is a dispute about the enforceability of alternative or bespoke dispute resolution provisions which are being relied on to defeat or delay court proceedings, the courts will be prepared to find that these provisions are not enforceable, because clear words are needed to remove the jurisdiction of the court, even if only on a temporary basis.

The Court of Appeal found that Kajima's absence from the Liaison Committee, their lack of ability to see documents and make representations, together with the Liaison Committee's inability to resolve a dispute amicably or provide a decision binding on Kajima made it "fundamentally flawed". The parties making up the Liaison Committee had interests contrary to Kajima's, resulting inevitably in actual or apparent bias in any dispute resolution procedure.

The Court of Appeal also agreed with the lower court on its finding that under the DRP in Schedule 26, it was not clear when the condition precedent might be satisfied.

Why is this important?

Where there is an enforceable DRP clause in a contract, but a party has declined to activate that clause and instead has commenced proceedings, a court will usually stay the proceedings until the dispute resolution procedure has been completed. In this case, if Kajima had been able to rely on the dispute resolution procedure being found to be a condition precedent to court proceedings, they may have been successful in striking out CAP's claim and not just staying it. On the facts, any fresh claim against them would have been outside the limitation period.

However, Kajima failed to do this because the dispute resolution clause was not drafted to be sufficiently clear and certain as to the obligations of the parties in the event of a dispute. It did not adequately provide for when the obligations were to be triggered or whether or not they were to be followed before proceedings could be begun.

Any practical tips?

When drafting an DRP clause, you should ensure that:

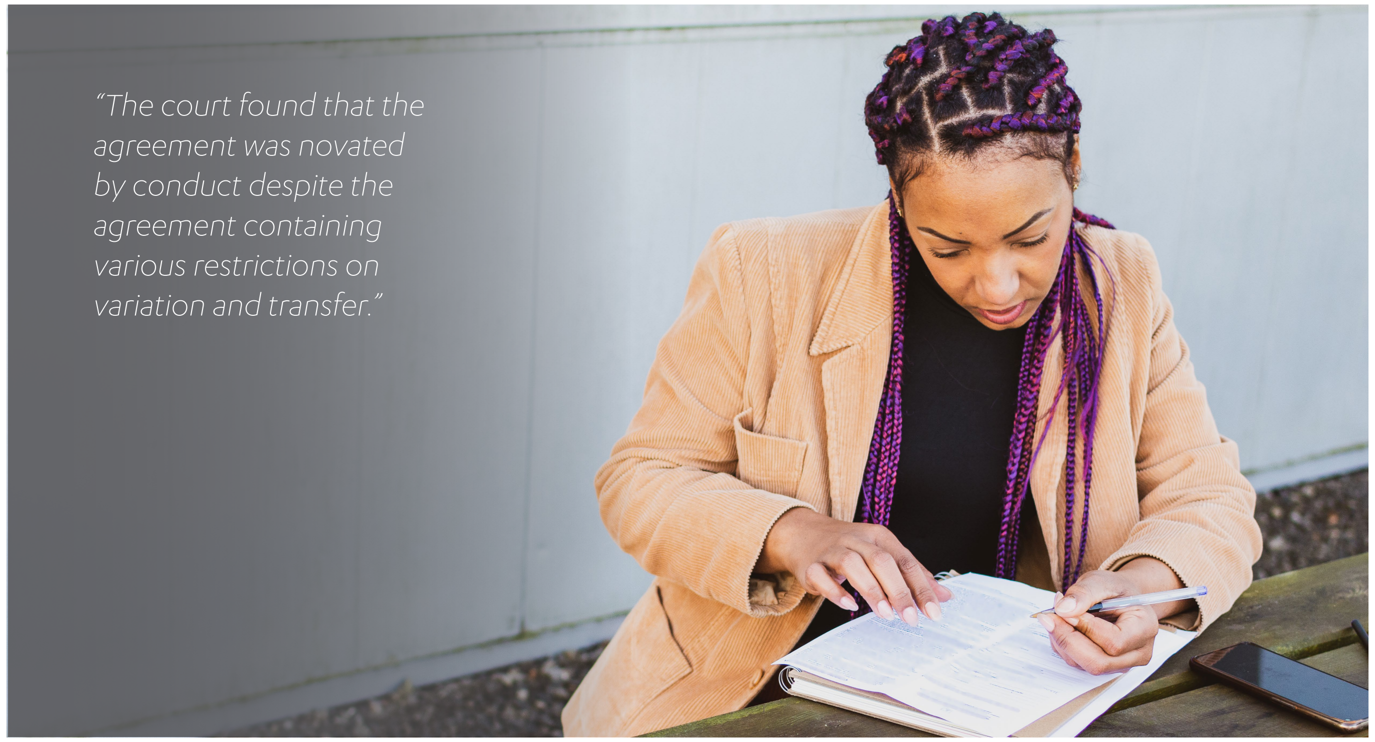
- there is an unequivocal commitment to engage in a particular dispute resolution rocedure
- there is a meaningful description of the process to be followed
- the order of the process is clear, including what triggers it and how it is satisfied
- details of the (senior) representatives who have knowledge of the agreement/ project and will be key in resolving the dispute are included
- it includes set time periods for serving the notice of request and for completing each stage before the parties move on to the next stage.

It specifies what stages of the process must be completed before litigation can be commenced (except perhaps in certain circumstances, such as where the limitation period would expire during the process or where urgent relief is required).

COMMERCIAL

"Courts will generally try to uphold a commercial agreement where possible. However, if the DRP clause is not sufficiently clear and certain, then it is liable to be held unenforceable."

Contract novation – consent inferred by conduct despite written restrictions in contract



***Musst Holdings Ltd v Astra Asset Management UK Ltd* [2023] EWCA Civ 128**

The question

Where consent for novation has not been provided for explicitly in a contract, how may courts approach inferring consent by conduct?

The key takeaway

The court found that the agreement was novated by conduct despite the agreement containing various restrictions on variation and transfer. The requirement for prior written consent for a transfer was considered to be waived by the remaining party who provided retrospective consent by subsequent correspondence.

The background

Mr Mathur developed a new business in 2012 involving attracting investors to invest in "synthetic" asset backed securities. Mr Siddiqi's role in this was to introduce contacts, provide his own technical expertise and to coordinate distribution activity through his company, Musst Holdings Ltd (**Musst**).

Mr Mathur intended to provide these investment services under two companies (collectively known as **Astra**). These companies did not have the necessary regulatory approvals to conduct business so Mr Mathur traded under two, already approved, companies (**Octave**). In practice, Astra did the work on behalf of Octave, but Octave were the contracting party.

In 2013, Octave entered into an introduction agreement (**Octave Contract**) with Musst. By this agreement Musst introduced investors to Octave and received a 20% share of the management and performance fees. Just over a year later, Astra obtained FCA authorisation and agreed in correspondence that, for a nominal amount, they would take over Octave's investment management responsibilities and receive the fees direct. The Octave Contract was not mentioned in this correspondence, however, in separate correspondence, Musst agreed to invoice Astra. Thereafter, Astra paid Musst's invoices.

In 2016, Astra began to experience financial difficulties and stopped payments to Musst. Musst brought a claim for breach of the Octave Contract, which it claimed had been novated to Astra. It sought an order for payment of the revenue share to which it claimed it was entitled either contractually or on the basis of unjust enrichment. Astra denied the contract was novated because a draft contract was sent to Musst but it was never agreed.

The court at first instance acknowledged that there was no express agreement on novation, that the language of novation had not been used and that it would be wrong lightly to infer a novation. Instead, the court focused on the parties' conduct – Astra and Octave were closely related entities working from the same address and were evidently seen by the parties as such. There was an overlap of staff between Octave and Astra and they shared the same offices at the date of the novations. The lack of formality was therefore not surprising – both parties anticipated that Mr Mathur would "spin out" of the Octave umbrella. Astra replacing Octave was no different from a name change. Further, the request on the part of Astra to Musst to be invoiced the money instead of Octave was not administrative but substantive. Astra was not acting as agent for Octave, it was acting for itself as a consequence of the transfer of business from Octave to Astra.

The High Court found that the contract had been novated by conduct. Astra appealed.

The decision

Denying Astra's appeal, the Court of Appeal (**CA**) found that the court at first instance was right in its finding that the contract had been novated by conduct.

The CA specified that consent will only be inferred from conduct if that inference is required to give business efficacy to what happened. Repeating many of the points made by the court of first instance (see above), the CA emphasised that the parties knew that Octave was being used because Astra was not initially authorised and that Astra presented the change as the name changing exercise which, from a commercial perspective, it was. When the income steam transferred to Astra, Octave dropped out of the picture and had no continuing role. The judge held that a novation was not just necessary to give business efficacy, it was the only rational explanation for the parties' conduct.

The court focused on three clauses of the Octave Contract as relevant to the issue of novation. The first was clause 9.4 which provided that Octave must do "everything within their power" to retain responsibility for management of the funds. Despite this, Octave handed over control to Astra in 2014 without seeking Musst's consent. However, Musst waived this breach by continuing the arrangement with Astra. The draft written novation agreement was then simply an attempt to formalise what had already been agreed by conduct.

The court then turned to clause 16, a "no oral modification" (**NOM**) clause which provided that the contract could not be varied unless the variation was in writing and signed by the parties. The court dispatched this point promptly on the basis that a novation is not a variation because a varied contract remains in place whereas a novation replaces the contract with a new contract between different parties.

Clause 17 of the Octave Contract imposed an obligation on Octave not to "assign or transfer… or deal in any other manner" with any of its rights and obligations under the agreement without prior written consent. The CA held that it was open to Musst to waive the requirement for prior consent and instead provide consent after that dealing occurred. The correspondence between Astra, Octave and Musst amounted to the provision of consent to the transfer.

Why is this important?

Where there is a clause which prevents a party from being able to novate the agreement without prior written consent from the other party, a court may find on the facts that a breach of such a provision is capable of waiver by the injured party, in the form of retrospective consent. The case also acts as a reminder that provisions covering a variation to the agreement will not, as a matter of course, apply to novation.

Any practical tips?

Ensure that novation is considered when drafting, in terms of potential consequences for the remaining, incoming or outgoing party, understand what obligations and liabilities may transfer, and keep in mind the requirements for a valid novation. Consider whether other options to a novation such as assignment, subcontracting, termination or variation may be more appropriate.

Consider specifying in the contract how a waiver of the novation requirements must be met. NOM clauses, or any other clauses which seek to limit a party's ability to vary, transfer or deal with the contract, should refer explicitly to novation (or other dealings) if this might be relevant to the transaction.

Contract interpretation – informality of contract does not overturn text with obvious and clear meaning

***Contra Holdings Ltd v Bamford* [2023] EWCA Civ 374**

The question

Where an informal, brief and home-made agreement has been drafted without lawyer input, will the ordinary rules of contractual interpretation apply?

The key takeaway

Where an agreement is informally drafted without the input of lawyers, the courts will still look to interpret the contract as a whole, giving the words used their natural and ordinary meaning in the context of the agreement, the parties' relationship and all the relevant facts. Informality cannot be used as a trump card that can overturn wording that carries an obvious and clear meaning.

The background

Following the death of Joseph Cyril Bamford, founder of the JCB group of companies (**JCB Group**) in 2001, negotiations took place regarding the future ownership of the JCB Group. Mark Bamford and his brother Anthony Bamford were principal beneficiaries of several Trusts which owned the JCB Group through shares and interests in principal holding companies.

Richard Bamford, CEO of Contra and second cousin of Mark and Anthony, provided advisory services to Mark in relation to the negotiations and in connection with multi-jurisdictional litigation related to the JCB Group. In June 2011, Anthony and Mark agreed, in principle, a settlement of all disputes.

The proceedings centred around an unsigned agreement (the **Touch Agreement**) between Mark and Contra (formerly Touch Worldwide Holdings Ltd) dated 1 July 2011 which the court took to be legally binding. The Touch Agreement was drafted by Richard and entered into by both parties without the assistance of external (legal or other) advisors.

The agreement included two express terms relating to two separate success fees. One was for the services provided up to and including the settlement in June 2011. This success fee was paid. A second success fee was due on completion of "Project Crakemarsh". Project Crakemarsh referred to the proposed sale of the JCB Group. No sale of JCB Group took place in 2012 or subsequently.

Contra commenced proceedings against Mark for the payment of the unpaid success fee, claiming breach of the Touch Agreement. Contra claimed that the contract was to be interpreted (including on the basis of an implied term) to provide for payment of the second success fee if the divestment of the assets or the separation of the interests of Mark in the trusts took a different form than the anticipated sale of the JCB Group, arguing that the payment would also be due if the JCB Group was in some other form restructured rather than sold.

The court of first instance looked first at the express terms of the Touch Agreement and as a matter of textual analysis concluded that there was no doubt that payment of a "success fee on the completion of Project Crakemarsh" referred to the proposed sale of the JCB Group, and that there were no implied terms that would provide for the payment of the success fee without the sale of the JCB group. The court also bore in mind that the agreement was drafted by a professionally qualified person (Richard was a chartered accountant) who was capable of performing services, in relation to complex matters, worth several million pounds.

Contra appealed on the basis that the clear commercial purpose of the (informal) Touch Agreement was to reward Contra for achieving Mark's long-held intention to separate his interests in JCB.

The decision

The Court of Appeal (**CA**) dismissed the appeal essentially on the same reasons identified by the court of first instance.

The CA pointed out that Contra's claim was a breach of contract claim only, rather than a claim for rectification or estoppel and was solely based on the Touch Agreement. The Touch Agreement, while not drafted by lawyers was "nevertheless a logically structured and (largely) clear document". The ordinary rules of contractual interpretation in the context of the relevant factual matrix applied to it and "informality is not a trump card that can overturn a text that carries an obvious and clear meaning. There are also degrees of informality, and the Touch Agreement was a careful, albeit brief, document, drafted by a qualified accountant".

When carrying out the exercise of interpretation against the relevant factual matrix, the court did not consider that there was anything in the relevant factual matrix which detracted from the clear meaning of the language of the Touch Agreement.

On the question of implied terms, the court held that the Judge's conclusions at first instance that the proposed implied terms were not sustainable either as a matter of obviousness or business efficacy were unimpeachable.

Why is this important?

An informal or home-made agreement will not automatically lead a court to overturn the natural and ordinary meaning of the words used. The CA did acknowledge that it is right that context may have greater than usual weight when interpreting a more informal document, but in this case the Judge at first instance had properly taken this into account. The express terms of the Touch Agreement did not, on their true construction, provide for payment of the success fee in circumstances where there had been no sale of the JCB Group.

The terms sought to be implied by Contra were not necessary to make the contract work – neither so obvious that they went without saying, nor necessary to give the contract business efficacy.

Any practical tips?

For contracts of significant value (here the potential success fee was very substantial) that may well result in proceedings in the event of non-payment or lack of performance, ensure legal professionals are involved at the drafting stage.

This should assist with the parties' deal being properly reflected in the written agreement, and provide a clearer and more certain outcome. The commercial purpose of the agreement should be stated (for example, in recitals) and ensure, in particular, that any payment triggers and terms are clear. A well drafted agreement, prepared with the benefit of legal advice, may make it more difficult to challenge on the basis that the context must be given greater weight when interpreting the wording (as a matter of contractual interpretation), that it does not properly record the parties' deal (as a matter of rectification) or that certain terms must be implied into the agreement (as they are so obvious or are required to make the contract work properly).

"Where an agreement is informally drafted without the input of lawyers, the courts will still look to interpret the contract as a whole, giving the words used their natural and ordinary meaning in the context of the agreement, the parties' relationship and all the relevant facts."

Breach of warranty claim notification fails to comply with notice clause

***Drax Smart Generation Holdco Limited v Scottish Power Retail Holdings Limited* [2023] EWHC 412 (Comm)**

The question

What principles will a court consider when construing notification of claim clauses in a share purchase agreement to determine whether a party has given valid notice of loss?

The key takeaway

In determining whether a notification of claim is valid under a contractual notice clause that requires "reasonable detail", a court will consider whether the notice includes sufficient detail to allow a reasonable recipient of the notice to understand the claim against it and the type of losses claimed (although specific amounts need not be identified).

The background

The proceedings relate to the content and timing of Drax's notice of claim for breach of warranty, an indemnity and other contractual breaches under a share purchase agreement (**SPA**) between it and Scottish Power.

In summary, Drax purchased the shares in a company (the **Company**) which owned a potential location for an as yet unbuilt power station. In order for the power station to be built, the site needed to be connected to the national electricity grid, via cables that would run over a key piece of land. Rights under an option agreement, that gave Scottish Power the right to require the grant of an easement over the key land to run the cables, were improperly transferred. As a result, the Company was not entitled to exercise these rights under the option agreement.

Under the SPA, Scottish Power had warranted that the benefit of the option agreement would be assigned to the Company prior to completion and agreed to indemnify Drax for all losses suffered in relation to the option agreement as a result of Scottish Power failing to implement an internal reorganisation of its group fully and correctly before completion.

A pre-condition was included in the SPA stating that the Scottish Power's liability for certain claims necessitated a notification of claim setting out "in reasonable detail the nature of the claim and the amount claimed (including the Buyer's calculation of the Loss thereby alleged to have been suffered)".

Drax only discovered that the option had not been effectively assigned to the Company, and was of no effect, after the expiry of the option period. On the last day of the relevant time limit for Drax to provide notification of a claim, it served a notice of claim alleging breach of warranty, other contractual breaches and an indemnity claim. In terms of the nature and amount of loss suffered, Drax changed its case from that submitted in its notice of claim to its pleaded case in the proceedings, and then sought to amend its particulars at a later date alleging that Drax, not the Company, had sustained loss in that the Company's value (and therefore the shares acquired by Drax) were less than they would have been had Scottish Power complied with its contractual obligations.

In relation to the breach of warranty claim, Scottish Power contended that the claim as notified did not give reasonable detail of the nature and amount of the claim brought in the particulars or draft amended particulars of claim. More importantly, Drax was now claiming for a different type of loss than that which it had specified in its notice (ie claiming for a loss suffered by Drax, rather than a loss suffered by the Company as notified) – Drax had therefore failed to comply with the notice requirements set out in the SPA and the notice was therefore invalid

Scottish Power argued that the requirement that the notice give reasonable details of the amount claimed had also not been fulfilled in relation to the indemnity claim because under the SPA the claim notified had to be for an ascertained sum.

The decision

The key issue before the High Court was whether Drax's notice was adequate in relation to its breach of warranty and other claims and in particular whether it gave reasonable detail of the nature of the claim in respect of the loss suffered, and in relation to the amount claimed and its calculation.

The court acknowledged that part of the purpose of a notification clause is certainty for the party being notified. It concluded that a reasonable recipient would understand from the notice of claim that the loss being claimed was heads and items of loss which the Company would suffer and for which Drax bore a liability. There was no reference in the notice of claim to a diminution in value of the shares in the Company, although this was how the claim was later pleaded in the draft amended particulars of claim.

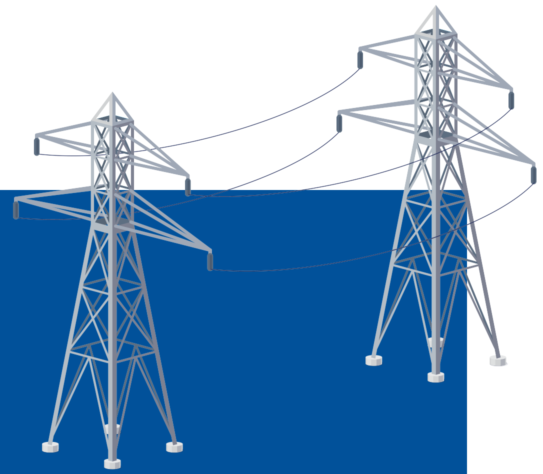
The notice had to include sufficient detail to allow the seller to understand the claim against it in at least outline terms. The diminution in value of the shares in the Company should therefore have been included in the notice of claim. As it had not been included the notice did not comply with the SPA in relation to the warranty claim or other breach claim and there was therefore no real prospect of Scottish Power being liable for that claim.

In relation to the indemnity claim, the court reasoned that a requirement that the indemnity claim must be precisely ascertained within the timeframe given in the SPA would be uncommercial and not the intention of the parties. It would deprive Drax of a chance to bring a claim. As the full extent of the loss had not been ascertainable, stating the amount claimed in reasonable detail did not require identifying an ascertained sum.

There was sufficient information in the notice of claim, in terms of identifying what loss had been suffered and what was likely to be suffered, including the giving of figures where they could be given (and in some places estimates of figures), to allow Scottish Power to understand what was being claimed against it and for what amounts, and (where specific amounts were not identified) the types and categories of costs and liabilities in respect of which an indemnity would be claimed. The commercial purpose of the clause, including the level of certainty the clause sought to provide to Scottish Power, was satisfied.

Why is this important?

The case highlights that problems can arise where a clause requires notice of a claim to include specific information which might not be obvious, easy to ascertain or indeed might be omitted in error at the time the notice is served, especially if it is being served close to the deadline. This notice of claim was nine pages long and still, on the breach of warranty claim, failed to satisfy the SPA's requirement to state the nature of the claim and the amount claimed (including a calculation of loss suffered) in "reasonable detail". This was because Drax later changed its claim to a different type of loss depriving Scottish Power, as the party being notified, from the certainty and clarity it expected from the SPA's notification clause.



Any practical tips?

Consider whether the notice clause should specify precisely what information the notice should contain such as the nature of the claim, the type of loss and the amount claimed (if known, or estimated), or whether it should be more general. A notice requiring "reasonable detail" is likely to be interpreted as providing enough information to allow "the vendor to know in sufficient detail what he is up against (not least because it might then enable the parties to settle without recourse to litigation)".

When preparing notices, bear in mind the various contractual (and other) claims that may be available, and that they may differ both in their nature and in the losses that may be claimed. Consider taking an 'over-inclusive' approach to the notice (and/or multiple notices) to keep these options available if appropriate. Where detail is not available, provide estimates where possible or explain why information is not yet available. If possible, do not leave notices until the very end of time limits so as to mitigate risks of ineffective notices or defective service.

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

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

Global Expertise.
Local Connections.
Seamless Service.

TerraLex

www.terralex.org

rpc.co.uk