Contents

Commercial

Contractual interpretation: the dangers of inconsistency between formulae and worked examples

Altera Voyageur Production Limited v Premier Oil E&P UK Ltd [2020] EWHC 1891 (Comm)

The question

If a contract includes both a written formula and worked examples, which method of calculation will a Court uphold if they produce different results?

The key takeaway

Worked examples are helpful to include in contracts, but should always be double-checked for consistency with the underlying terms.

The background

The Defendant (**Premier**) hired an oil vessel from the Claimant (**Altera**). Under the terms of their charterparty contract (**Contract**), Premier were required to pay a daily hire rate to Altera. The daily rate was adjusted on a yearly basis, depending on the proportion of time when certain systems on the vessel were available. Whether the adjustment was upwards or downwards, depended on whether availability met the target of 95%.

As set out in the Contract, the adjusted hire rate was to be calculated as follows:

- If actual availability of the system was more than 95%, the formula was: "*(100% + (Actual Availability % - 95%) x2) x Weighted Factor)*"
- If actual availability of the system was less than 95%, the formula was: "*(100% + (Actual* Availability *% - 95%) x1) x Weighted Factor)*".

An appendix to the Contract contained two worked examples of the hire adjustment formula: However, these included a number of steps that were not set out in the written formula – namely:

- **Step 5:** adding the figures for the different systems together to provide a total percentage, and
- **Step 6:** dividing the actual availability figure by the target availability.

The parties agreed that Step 5 was intended to have been part of the formula, however they disagreed about the inclusion of Step 6 (which would have a significant impact on the adjusted hire rate). Altera sought to enforce the worked example interpretation of adjusted rate and brought a claim against Premier for the resulting amount.

Premier highlighted a clause that stated the main body would prevail over the appendix in the event of a conflict. Premier asserted that it would be commercially irrational for Altera to get an uplift in the daily rate as a result of the worked examples in the appendix, given that they were facing penalties under the main contract.

The decision

In the High Court, Mr Salter QC upheld Altera's claim and ruled in favour of the method of calculation set out in the worked examples. He did so despite:

- the clause which said that the main body of the contract (in which the narrative drafting was contained) took priority over the appendix – the Court took the view that the worked examples provided a more detailed interpretation of the narrative clauses;
- the worked examples producing a result which was generally accepted as being commercially unreasonable; and
- the contract containing various drafting errors and redundancies which cast doubt on how much weight should be placed on any one provision (including the worked examples).

Why is this important?

Recent case law (see *Chartbrook v Persimmon*) has highlighted the usefulness of including a worked example to minimise ambiguity as to how complex formulae are applied. However, this case shows that expensive and lengthy litigation can still follow if sufficient care is not taken to ensure that the clause and the worked examples align. As with all contractual interpretation cases, this decision turned closely on the drafting and it isn't out of the question that the alternative approach could have been preferred in another contract.

Any practical tips?

Check (and doublecheck!) formulae and worked examples. Do they properly reflect the commercial deal on pricing, adjustments, etc. Worked examples can be a great way to explain complex calculations, but make sure you always check the maths and consider the commercial implications. Consider also keeping the formulae and the worked examples in the same place (eg together in the same appendix), as the chances of inconsistency are reduced if they are read together.

Autumn 2020

Commercial

Good faith: relational contracts and the implied duty of good faith

Essex County Council v UBB Waste (Essex) Limited [2020] EWHC 1581 (TCC)

The question

When will the courts imply a duty of good faith into a contract and when can a contract be categorised as a "relational" one?

The key takeaway

Long-term contracts are likely to be described as relational contracts, which in the absence of any provisions to the contrary, may imply a duty of good faith between the parties. The 25-year PFI contract in issue in this case was considered "*a paradigm example of a relational contract in which the law implies a duty of good faith*".

The background

Essex County Council (the **Employer**) contracted with UBB (the **Contractor**) to design, build, finance and operate a biological waste treatment plant for treatment of Essex's 'black bag' household waste. The agreement was a 25-year £800m Private Finance Initiative contract.

Once the plant was built, the contract anticipated a commissioning period followed by "Acceptance Tests" designed to ensure the plant could meet performance requirements set out in the contract. Once the Contractor passed the Acceptance Tests, they would receive increases in remuneration.

However, the plant underperformed and did not pass the Acceptance Tests by the "Acceptance Longstop Date". The Employer blamed the plant's failure on design and construction flaws, which were allegedly a default by the Contractor. Consequently, the Employer was entitled to terminate in accordance with the contract terms.

The Contractor claimed that the Employer could not terminate as the Employer had breached the contract in several ways. The Contractor argued that the failings were due to the waste that the Employer was sending to the plant. Further, the contract was a "relational" contract, which implied a term requiring the parties to act in good faith. If the Employer had acted in good faith and agreed to changes in the contract, the facility would have been deemed to have passed the Acceptance Tests in July 2016.

As a consequence, the Contractor claimed that the Employer should pay damages reflecting the Contractor's lost payments to date (approx £100m).

The decision

Drawing on recent case law (eg *Yam Seng*; *Bates v Post Office*), Pepperall J agreed with the Contractor that this was a "relational" contract and that there was an implied duty to act in good faith - noting that a "relational" contract would typically be long-term in nature; require a high level of communication and co-operation between the parties; and otherwise show an intention that the parties perform their duties with integrity, trust and confidence.

However, despite concluding that there was an implied duty of good faith, the Judge did not find that the Employer was in breach of that duty. The failure to pass the Acceptance Tests was due to the Contractor's design errors and not because of the Employer's actions or omissions. The plant was severely undersized and was not fit for its intended purpose. Attempts to remedy the defects by the Contractor were implemented in a way that amounted to breach of contract.

The Employer could therefore validly terminate the contract as the Contractor had defaulted on its obligations and the right to terminate did not have to be exercised within a reasonable time.

Why is this important?

If the circumstances mentioned above apply to a long-term contract, it may be considered a "relational" contract and the parties are likely to be subject to an implied duty of good faith – unless such a duty is expressly excluded by the contract terms.

The judgment also rejected the notion of a general principle requiring contractual termination rights to be exercised within a reasonable time. Whilst the conduct of the parties and the contract terms could mean that such an implied term applies in certain circumstances, it was not implied into this contract.

Any practical tips?

If parties do want to exclude an implied duty of good faith – particularly when entering long-term contractual relationships – they must do so through explicit drafting. In any event, careful drafting of a party's obligations, how these may be affected by the performance of the other party, and change management provisions remains crucial.

Autumn 2020

Commercial

Contractual interpretation: rectification not possible purely for a tax benefit

MV Promotions Ltd and another v Telegraph Media Group Ltd and another [2020] EWHC 1357 (Ch)

The question

Will rectification of a contract be permitted where the only effect of rectification would be to secure a tax benefit?

The key takeaway

The court exercised its discretion not to rectify a contract where all issues between the parties had been resolved, and rectification was only sought to secure a tax benefit that was not contemplated by the parties at the time of the contract.

The background

In 2008, Michael Vaughan and Telegraph Media Group Ltd (**TMG**) entered into a contract for Mr Vaughan to write newspaper articles. This contract was later amended so that Mr Vaughan's services company, MV Promotion Ltd (**MVP**), was the named counterparty, allowing billing and invoicing under the contract to take place between MVP and TMG.

In 2011, the parties sought to extend their agreement but erroneously named Mr Vaughan as the counterparty, instead of MVP. As a result, HMRC increased the tax payable by Mr Vaughan in relation to the services provided.

In 2018, Mr Vaughan, MVP and TMG entered into a deed of rectification, whereby it was confirmed that the contract was supposed to be between MVP and TMG.

The decision

The Court found that a rectifiable mistake had been made as the parties had a common intention for the contract to exist between MVP and TMG, and the 2011 contract was not supposed to alter that aspect of the 2008 contract. However, the court did not exercise its discretion to rectify the contract.

The parties had already signed a rectification deed, which resolved the issue and gave effect to the common intention of the parties.

The rectification deed was not binding on HMRC and the parties request to rectify the 2011 contract to bind HMRC only served to achieve a tax benefit that had not originally been intended. The Court drew a clear distinction between cases where the parties specifically intended to use a tax-efficient structure when entering into a contract, and cases where such intention did not exist at the inception of the contract.

Why is this important?

This case demonstrates that taxpayers should not rely on rectification to obtain tax benefits that were not originally contemplated by the parties. Although parties can agree to rectify a bilateral contract to correct a mutual mistake through a rectification deed, such amendment may not have retrospective effect for tax purposes.

Any practical tips?

When drafting a contract, parties should fully consider the tax implications of the arrangements and ensure that the terms give effect to the parties' intentions. When preparing amendments and variations, always carefully review the original agreement. Evidence of the parties' common intention in respect of their agreements should also be preserved in case needed.

Autumn 2020

Commercial

Restrictive covenants: restraint of trade and bespoke contracts

Quantum Advisory Ltd v Quantum Actuarial LLP [2020] EWHC 1072 (Comm)

The question

Restrictive covenants are typically unenforceable unless they:

1. are to protect a legitimate business interest;
2. are no wider than reasonably necessary to protect that interest; and
3. are not contrary to the public interest.

But does the restraint of trade doctrine apply to all restrictive covenants?

The key takeaway

Not all restrictive covenants are subject to the restraint of trade doctrine – in this case, the doctrine did not apply to restrictive covenants in a bespoke services agreement. The context of the agreement and the covenants must be considered.

The facts

A business providing various professional services was formed by certain individuals and split between three different companies (the **Legacy Companies**) with the intention of merging the Legacy Companies into a single entity after three years. However, the business was forced to undergo a restructuring due to the diverging interests of the individuals involved.

The business was to be carried on by a new limited liability partnership (**LLP**), with the Legacy Companies' clients (the **Legacy Clients**) remaining with the Legacy Companies and the LLP providing services to the Legacy Clients on behalf of the Legacy Companies at a fixed cost.

This restructuring was documented in a Services Agreement (the **Agreement**) between the LLP and the Legacy Companies which restricted the LLP's ability to:

1. solicit or entice away or attempt to solicit or entice away any Legacy Clients;
2. obtain instructions for any services from the Legacy Clients or undertake any services for the Legacy Clients; or
3. undertake services in relation to certain new business or any work introduced by Introducers without referring such matters to the Legacy Companies first;

for the term of the Agreement and for 12 months after its termination or expiry (the **Restraints**).

The parties conducted business under the Services Agreement for a number of years. However, the LLP became dissatisfied with certain terms (in particular, income allocation) and alleged that the Restraints were an unreasonable restraint of trade as the drafting of the Agreement meant that they lasted for a total of 100 years unless the Agreement was terminated early. In response, the Legacy Companies sought a declaration that the Agreement was binding on the parties and an injunction to restrain the LLP from acting in breach.

The decision

The Court concluded that the doctrine of restraint of trade did not apply to the Restraints. The Court emphasised that the Agreement needed to be considered on its own terms and circumstances as an Agreement created to address the competing interests of the parties. It focused on the purpose of the Agreement, noting that:

1. the Agreement was brought into existence wholly for the purposes of the restructuring. The LLP had no previous business or being but for the Agreement, which demonstrated that the Agreement provided it with an opportunity to trade, rather than restraining its trade; and

2. the Restraints were put in place to establish the ownership boundaries of the Legacy Clients.

The Court went on to determine that, even if the restraint of trade doctrine had applied to the Restraints, they would have satisfied the reasonableness requirements as the parties were of equal bargaining power and the Restraints were placed in a "free agreement" made between "*experienced, intelligent, articulate and highly competent business people, who were properly able to look after their own interests and who expressly agreed that the restraints were reasonable*" and were necessary to protect the parties' interests.

The potential 100-year duration of the Restraints was reasonable when viewed in context as it was not imposed on the LLP, and neither the term of the Agreement nor the termination provisions were within the scope of the doctrine.

Why is this important?

The decision offers a valuable insight into the court's attitude towards restrictive covenants outside of the usual employment and sale scenarios where these types of clauses are typically found. There is no general rule that the restraint of trade doctrine will not apply to bespoke contracts, but it shows that commercial context is crucial

Any practical tips?

The general rules as to the scope of restrictive covenants should always be considered carefully Consider using recitals and acknowledgements to identify the legitimate business interest(s) being protected, and any commercial context that should be taken into account.

Autumn 2020

IP

Copyright: Online platform operators' liability for users illegally uploading copyright material

C-682/18 *Frank Peterson v Google LLC and others* and C-683/18 *Elsevier Inc. v Cyando AG* EU:C:2020:586 – A-G opinion

The question

Are online platform operators liable for users' uploading of material that infringes copyright?

The key takeaway

Online platform operators should not be directly liable for users illegally uploading material that infringes copyright works, according to the opinion of Advocate General Saugmandsgaard Øe.

However, he also indicated that rightsholders should be able to obtain injunctions against those operators (eg to remove infringing content) under EU law.

The background

The German Federal Court of Justice referred two sets of proceedings to the CJEU, namely:

- **YouTube** – a claim brought by music producer Frank Peterson against YouTube in relation to various Sarah Brightman songs uploaded to YouTube by users without permission; and
- **Cyando** – a claim brought by publishing group Elsevier against Cyando, the company behind cyberlocker "Uploaded", concerning various copyright works that had been uploaded to Uploaded by users without permission.

The German Federal Court of Justice asked the CJEU to decide whether online platform operators making user-uploaded content available to the public meant that the online platform operators themselves were performing an act of "communication to the public" and therefore infringing copyright.

The decision

The AG has advised the CJEU to rule that the online platform operators themselves do not carry out an act of "communication to the public" as the role of the platforms is that of an intermediary – they are simply providing the physical facilities that enable users to carry out a "communication to the public". The process of a user uploading content is automated and does not involve the platform determining or selecting the content that is ultimately published.

As such, the liability is borne by the users who upload the content.

Further, the hosting exemption under Article 14 of the e-Commercial Directive (Directive 2000/31/EC) would, in principle, be available to these online platform operators in any event, as long as they did not play an “active role” which would give them “knowledge of or control over” the information in question.

The AG also considered the impact on rightsholders, proposing that the CJEU rule that rightsholders can still obtain injunctions against the online platform operators that impose obligations on them, eg the requirement to remove content. The rightsholders should be able to obtain such injunctions by establishing that their rights were infringed, without the need to show improper conduct by the intermediary.

Why is this important?

Although the AG’s opinion is not binding and the CJEU may depart from it, this opinion seeks to balance the rights of the online platform operators and rightsholders. - suggesting that online platform operators should not be directly liable for users’ actions in uploading content.

Any practical tips?

The AG’s opinion will be welcome to online platform operators and they will hope that the CJEU will concur when it issues its decision in due course.

Nevertheless, the online operators still need to keep the EU Copyright Directive (2019/790) in mind. The Directive seeks to introduce an obligation on operators to obtain authorization from rightsholders for works uploaded by users.

This may not affect the position in the UK (the UK Government has said that it is not required to implement the Directive and does not plan to do so), but such provisions may be implemented across the EU.

Autumn 2020

Data protection

ICO publishes guidance on AI decision-making

The question

How can companies comply with data regulation when using AI to make decisions affecting individuals?

The key takeaway

Guidance has been issued by the ICO on how best to ensure your AI systems are compliant with the GDPR requirement that decisions made are explainable.

The background

The ICO recently published guidance – Explaining decisions made with AI – to assist organisations with their explanations of how they use AI. The guidance is not intended to be exhaustive, nor is it a binding authority, but it aims to be a useful tool for compliance teams, data protection officers, and senior management by providing practical advice on data protection compliance.

The guidance

The guidance is split into three sections.

The first section: This describes the basics of explaining AI. The ICO identifies four principles to guide organisations on making decisions explainable:

- be transparent
- be accountable
- consider the context you are operating in
- reflect on the impact of the AI system on the individuals affected, as well as wider society.

The guidance then goes on to identify six different ways of explaining AI decisions:

- **Rational explanation** – explain the reasons which led to the decision, delivered in an accessible and non-technical way
- **Responsibility explanation** – describe who is involved in the decision, who is accountable, and who to contact for a human review of the decision
- **Data explanation** – explain what data was used by the AI in coming to the decision; in some cases it may also be necessary to provide more details of the decision itself eg where an individual has been placed in a particular category and does not understand why

- **Fairness explanation** – describe the steps taken to ensure an AI system's decisions are fair. Be sure to include fairness considerations at all steps of the process, from the design of the AI to the selection of data used
- **Safety and performance explanation** – explain the steps taken to make the AI system perform as accurately, reliably, securely and robustly as possible
- **Impact explanation** – describe how the AI system monitors and accounts for all potential impacts its decisions could have.

The ICO goes on to explain the contextual factors that organisations should bear in mind when providing explanations: domain (ie setting or sector of the AI system), data, impact, urgency, and audience.

The second section: This goes through the practicalities of explaining AI decisions to individuals and is primarily aimed at the technical teams of organisations. It provides a list of tasks that, when followed, assist in creating an AI which will provide more easily explainable decisions. The ICO recommends that any approach should be informed by the importance of implementing the principles of transparency and accountability into the AI systems.

The third section: This is aimed primarily at senior management and outlines the roles and responsibilities of those involved in the explanation process. General guidance is provided on what sorts of policies should be in place, and loosely describes what those policies might look like. For example, a data collection policy would detail the need to consider how decisions could be explained at every stage of the development of an AI system. A list of recommended documentation is provided, which if followed will provide evidence to demonstrate the explainability of an organisation's AI systems, and form an 'audit trail' of explanations provided to individuals.

Why is this important?

The explainability of AI decisions is crucial to GDPR compliance, and the guidance is pretty much essential reading for anyone engaged in developing AI systems.

Any practical tips?

- Have your technical teams review the second section of the guidance and consider whether your current systems comply. Can they amend their processes to follow the list of suggested tasks provided by the ICO?
- Draft (or if already drafted amend) the policies and documentation listed in the third section of the guidance. This describes what the policies should be trying to achieve and includes useful templates eg for documenting processing activities.

Autumn 2020

Data protection

Damages for distress for failing to verify personal data

Petr Aven v Orbis Business Intelligence Ltd [2020] EWHC 523 (QB)

The question

Can damages be awarded as compensation for distress arising from a defendant's failure to take reasonable steps to ensure the accuracy of personal data processed in breach of Principle 4 of the Data Protection Act 1998 (the **DPA**)?

The key takeaway

Damages are not confined to material loss and can be awarded as compensation for stress arising as a result of a defendant's breach of Principle 4 of the Data Protection Act 1998.

The facts

Orbis Business Intelligence Ltd (**Orbis**) published the so-called "Steele Dossier" (the **Dossier**) following instructions to provide intelligence memoranda to Fusion GPS (**Fusion**) on potential links between Russia, Vladimir Putin and Donald Trump. Fusion's client was Washington based law firm, Perkins Coie, their client being the US Democratic Party. Memorandum 112 of the Dossier (**Memo 112**) asserted the closeness of the three claimants (influential Russian/Ukrainian businessmen) to President Putin. Memo 112 was published by Buzzfeed News and disclosed by Orbis to Fusion, the FBI and certain politicians and government officials. The claimants alleged that the use of their personal data in Memo 112 contravened principles under the Data Protection Act 1998 as the data was inaccurate (Principle 4) and processed in a way that was unfair, unlawful or non-compliant with the DPA (Principle 1).

The claimants identified the below propositions in Memo 112 as personal data:

1. the giving and receiving of political favours between Putin and the claimants
2. the provision of informal advice by the claimants to Putin
3. a meeting between the second claimant and Putin
4. the use of an intermediary by the first and second claimants to deliver large amounts of "illicit cash" to Putin in his role as Deputy Mayor of St Petersburg, and
5. the first and second claimants doing Putin's political bidding during his presidency.

The defendants contested whether proposition (1) constituted data and whether proposition (5) contained sensitive personal data.

The decision

The judge concluded that proposition (1) was personal data relating to the claimants as the use of their company name, the Alpha Group meant that the reader would not plausibly separate Alpha Group and the claimants. He also concluded that proposition (5) was sensitive personal data as the reference to large amounts of "illicit cash" led the reader to infer criminal activity; a specific criminal offence did not need to be specified.

The defendant sought to rely on the legal purposes exemption arguing that its disclosure to Fusion was necessary for the purpose of prospective legal proceedings. Although the judge found that the disclosure to Fusion was not made for the purpose of prospective legal proceedings, it was made for the purpose of obtaining legal advice as Perkins Coie's sole or dominant purpose in commissioning the Dossier was to obtain information to provide legal advice to its client, therefore the exemption applied. However, as data controller, Orbis was still obliged to fulfil its duty of accuracy under Principle 4 which it failed to do in relation to proposition (5), as the steps taken to verify the sensitive data fell short of what would have been reasonable. The defendant also sought to rely on the exemption for national security, arguing that Memo 112 required disclosure to the FBI in order to safeguard national security. The judge accepted that national security defences could be relied upon by data controllers who are not "organs of the state" to conclude that although the purpose of safeguarding national security did relieve Orbis of its notification obligations under Principle 1, it did not provide any further exemption from Principles 1 or 4. Finally, as the disclosures satisfied at least one of the relevant requirements in the DPA schedules, they met the fairness requirement under Principle 1.

Why is this important?

Although the claimants' primary focus was to "set the record straight" in relation to the propositions, the judge only deemed a limited order for rectification necessary since Orbis was not responsible for the publication of the Dossier by Buzzfeed. However, despite exemptions being made out, the judge still ordered £18,000 compensation to be paid to each of the first and second claimants for distress suffered, even though no material loss was sustained. Whilst the judge followed defamation principles when calculating this figure, this judgment has the potential to set a benchmark for assessing the quantum for damages for data breaches.

Any practical tips?

In this case Warby J interpreted personal data in a holistic manner, rejecting an "item by item" approach whereby the contents of a document are read as discrete and separate propositions and instead favoured a coherent narrative approach. As such, extra precautions should be taken if disclosing personal data - just because an individual is not named does not mean that the disclosure is not personal data.

Autumn 2020

Data protection

Schrems II – where next for data transfers?

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*

The question

What is the impact of the CJEU *Schrems II* decision on international data transfers?

The key takeaway

The CJEU has invalidated the EU-US Privacy Shield arrangement and put significant limitations on the use of Standard Contractual Clauses (**SCC**) as a lawful international data transfer mechanism.

The background

On 16 July, the CJEU handed down a long-anticipated decision concerning the EU-US Privacy Shield, which is a scheme that companies can sign up to in order to certify they will adhere to higher privacy standards to lawfully transfer data between the US and EU. It also concerned the use of SCCs, a standard set of contractual clauses issued by the European Commission which can be incorporated into data transfer agreements to ensure safeguards on data protection.

This follows the CJEU judgment of *Schrems I* which, in 2016, invalidated the Safe Harbour arrangement which governed data transfers between the EU and US, foreshadowing what has been observed as a suspected “privacy trade war”.

The guidance

The CJEU held that the EU-US Privacy Shield was invalid, primarily due to concerns about the how US government surveillance programmes may restrict the privacy rights of EU citizens. In particular, it was found that US law did not place sufficient limitations on the access and use of data belonging to EU citizens by US intelligence services, and did not provide adequate remedies to EU citizens in relation to use of their personal data by US public authorities.

Whilst the use of SCCs was not declared invalid, the CJEU placed the onus on data controllers to conduct an assessment of the privacy laws of the country to which data is being sent. It is questionable whether SCCs can still be used to transfer data to the US in light of the judgment.

The ICO echoed guidance from the European Data Protection Board recommending that businesses conduct risk assessments as to whether SSCs provide adequate protection within the local legal framework. It also stated that businesses should take stock of their international transfers and react promptly as guidance and advice becomes available.

Why is this important?

International data transfers are vital for the global economy to function and must be carried out lawfully. Businesses which rely on international data transfers must now actively assess the privacy protections provided by the recipient country before data can be sent. Whilst the focus has been on EU-US data transfers, the principles from the judgment still apply to transfers to other third countries. It must be remembered that on 1 January 2021, save for any treaty otherwise, the UK will become a third country which will lead to an ongoing assessment of whether the UK's GDPR will be considered adequate to receive data as it potentially diverges from the EU GDPR over time.

*** **Breaking news** - on 6 October, the UK's chances of obtaining a successful adequacy decision suffered a major setback. The EU Court of Justice ruled that UK surveillance laws for the "general and indiscriminate" bulk collection of data "exceed the limits of what is strictly necessary and cannot be considered to be justified within a democratic society." This is the case even though the Court found that mass collection of data may be necessary in limited circumstances when faced with a "serious threat to national security". ***

Any practical tips?

- Identify which data transfers rely on the Privacy Shield and may require an alternative lawful data transfer mechanism.
- Identify data transfers to the US under SCCs and assess which recipients of your data may be subject to US surveillance laws.
- Conduct an audit of your data flows to third countries and the lawful data transfer mechanisms relied on in order to assess foreign privacy laws, and their compliance with the GDPR.
- Make preparations for and generally get ready to adopt updated SCCs once the European Commission releases them.
- Consider expanding the existing data protection obligations in your processing contracts, such that you can force your processing partners to put in place additional control mechanisms should these become necessary.
- Above all, keep a look out for guidance from national regulators and the European Data Protection Board. In particular, maintain awareness of UK Government & ICO statements on Brexit, and the UK's adequacy status. The position on data transfers continues to develop and you may need to move quickly to ensure ongoing compliance.

Autumn 2020

Data protection

EU Commission looks to new SCCs by the end of 2020

The question

What is the EU Commission doing in relation to the use of the Standard Contractual Clauses (**SCCs**) post-*Schrems II*?

The key takeaway

Following the uncertainty as to how the SCCs will work in a post-*Schrems II* world, the European Commission aims to finalise updated rules on the use of the SCCs by the end of 2020 to help give clarity on how EU companies can lawfully transfer data internationally.

The background

The CJEU decision *Schrems II* invalidated the EU-US Privacy Shield scheme as a lawful data transfer mechanism. However, whilst it stopped short of invalidating the use of the SCCs, it did impose a significant caveat to their use. Namely, it put the onus on data controllers relying on the SCCs to ensure that data-recipient countries maintain adequate levels of protection before any transfer takes place. This creates a complex set of verification obligations for data transfers which are meant to ensure that EU citizens benefit from an equivalent level of data protection (as guaranteed under the GDPR) in other countries to which data is transferred.

The development

Justice Commissioner Didier Reynders has said that EU businesses relying on the SCCs to transfer data to countries outside the bloc will see those rules overhauled by the end of this year. More imminently, the adoption process for the new SCCs will potentially be launched in the coming month. The adoption process will require an opinion from the European Data Protection Board and a positive vote from the European Parliament and EU member states.

Why is this important?

Following the invalidation of the EU-US Privacy Shield, the EU has scrambled to protect some 5,000 businesses relying on it to lawfully carry our international data transfers. The modern global economy relies heavily on such data transfers, and *Schrems II* removed a low-friction data transfer mechanism available to EU businesses. This places more importance on the use of the SCCs.

Any practical tips?

Watch this space! Any EU company relying on international data transfers should pay close attention to European Commission announcements in the coming weeks and months relating to the SCCs. In the meantime, it makes sense to get to grips with your international data flows through an internal audit, so you are in the best possible position to respond to developments and thereby maintain data compliance.

Keep an eye also on the 1 January 2021 Brexit deadline. Save for any treaty otherwise, the UK will become a third country and will depend on an adequacy decision going its way in order to continue receiving data in line with the EU GDPR without other mechanisms in place (eg the SCCs). And an adequacy decision looks increasingly shaky given the EU Court of Justice's recent ruling (6 October) that UK surveillance laws for the "general and indiscriminate" bulk collection of data "exceed the limits of what is strictly necessary and cannot be considered to be justified within a democratic society".

Autumn 2020

Data protection

ICO publishes contact tracing guidance

The question

What data can businesses collect from customers for contact tracing purposes?

The key takeaway

Organisations should collect only the information needed, as set out in the government guidance (eg names and contact details). Organisations should be transparent with customers, and carefully store the data they collect. The personal information collected as part of the contact tracing scheme should not be used for other purposes, and should be kept for no longer than necessary.

The background

The ICO has published initial guidance for businesses collecting customers' personal data as part of the government's contact tracing scheme. In line with supporting government guidance, the ICO has also created an online "Data protection and coronavirus information" hub that seeks to help individuals and organisations with data protection queries during the coronavirus pandemic.

The guidance

The guidance is laid out in five steps, as follows:

1. **Ask for only what's needed**
   Only ask for the specific information set out in the government guidance (eg names and contact details). Identity verification should not be requested unless this is standard practice for the business.
2. **Be transparent with customers**
   Be clear, open and honest with people about what you are doing with their personal information. Tell them why you need it and what you'll do with it. You could display a notice in your premises or on your website, or simply tell people.
3. **Carefully store the data**
   Any personal information collected must be securely maintained – this applies to both electronically held and paper-based information.
4. **Don't use it for other purposes**
   Any personal information collected for contact tracing purposes should not be used for other purpose eg direct marketing, profiling or data analytics.

5. **Erase data in line with government guidance**
   Any personal data collected should not be kept longer than the government guidelines specify. Paper documents should be shredded, and electronic documents should be permanently deleted.

Why is this important?

Organisations should seek to ensure they follow the basic five steps laid out above to minimise the risk of breaching the GDPR rules. As part of the government's COVID-19 contact tracing scheme, the ICO has published more detailed guidance than the above to assist those with limited experience of collecting and retaining personal data for business purposes – this includes for example the lawful basis for collecting the data, and the retention periods for the personal data.

Any practical tips?

The guidance is essential reading for all those involved in contact tracing projects. Remember also other sources of reference, including the Government's NHS Test and Trace Guidance which place obligations on designated venues/businesses in certain sectors (eg hospitality) to collect customer, visitor and staff contact details for contact tracing purposes. Note that there is currently no such obligation on companies to trace employees.

If you have a confirmed positive case of COVID-19 in your workplace, then consult the NHS Workplace Guidance, and if there is more than one case, you should contact your local health protection team (**HPT**) to report the suspected outbreak. The HPT will undertake a risk assessment, provide public health advice and where necessary, establish a multi-agency incident management team to manage the outbreak

Autumn 2020

Data protection

EU social media targeting guidelines – call for feedback

The question

Who are the key actors in the targeting of social media users, and what can they learn from the EU's new social media targeting guidelines?

The key takeaway

The Social Media Targeting Guidelines (the **Guidelines**) offer guidance on the targeting of social media users - in particular, it seeks to clarify the roles and responsibilities of "targeters" (eg advertisers utilising social media) and social media providers under the EU's General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**). The Guidelines have been submitted for public consultation. Social media platforms and adtech businesses are amongst those who have been invited to submit views to the European Data Protection Board (**EDPB**), with the deadline for responses being 19 October 2020.

The background

As part of their business model, many social media providers offer targeting services. Targeting services make it possible for natural or legal persons (**targeters**) to communicate specific messages to the users of social media in order to advance commercial, political, or other interests. Targeters may use targeting criteria based on personal data which a social media user will have actively provided or shared. Alternatively, targeters may use targeting criteria based on personal data which has been observed or inferred, either by the social media provider or third parties. This personal data is often aggregated by the platform or by other actors (eg data brokers) to support ad-targeting options.

On 7 September 2020, the EDPB launched a public consultation on the Guidelines. Taking into account the case law of the CJEU (the judgments *Wirtschaftsakademie* and *Fashion ID*), as well as the provisions of the GDPR regarding joint controllers and accountability, the Guidelines offer guidance on targeting of social media users, in particular the responsibilities of targeters and social media providers. Where joint responsibility exists, the guidelines seek to clarify what the distribution of responsibilities might look like between targeters and social media providers on the basis of practical examples.

Key elements

The Guidelines aim to provide the following:

- to clarify the roles and responsibilities among the social media provider and the targeter (including the lawful basis on which they can rely to process users' data)
- to identify the potential risks for the rights and freedoms of individuals
- to identify the other main actors and their roles
- to clarify the application of key data protection requirements (such as lawfulness and transparency, DPIAs, etc), and
- to identify the key elements of arrangements between social media providers and the targeters.

Why is this important?

The mechanisms that can be used to target social media users, as well as the underlying processing activities that enable targeting, may pose significant risks to the freedom and rights of individuals. This is particularly the case given that the sophisticated processes involved in the delivery of targeted ads may not be within a user's reasonable expectations. The EDPB has sought to provide clarity on the roles and responsibilities of the different types of actors involved in the process of targeting social media users (accompanied with useful examples) and guidance around their compliance with some key tenets of GDPR. In particular, targeters and social media providers should be aware that:

1. **Joint Controllership**: Following on from the Fashion ID case, the EDPB are clear that targeters and social media providers will, in most cases, be joint controllers
2. **Enhanced transparency**: In line with the ICO's Draft Direct Marketing Code, the EDPB highlights the importance of clearly informing users how their activity is being monitored for the purpose of targeted advertising. Using the word "advertising" is not enough
3. **Lawful basis**: the EDPB stresses that: (i) when acting as joint controllers, both parties must be able to demonstrate a lawful basis for their processing; (ii) the most appropriate lawful bases are consent and legitimate interests; and (ii) consent is required for intrusive profiling and tracking for advertising purposes
4. **Special Category Data (SCD)**: the EDPB are clear that assumptions or inferences drawn from data (which isn't SCD on its own) can constitute SCD

Any practical tips?

The Guidelines are aimed at the four groups of actors involved in the targeting of social media users: social media providers; their users; targeters and other actors which may be involved in the targeting process.

If your company falls within one of the identified groups, you should review the Guidelines to determine your role and responsibilities – both generally and under the identified targeting mechanisms. This will be especially important if you are a social media provider or a targeter. In particular, it's likely that your organisation should consider whether:

- your targeting related data terms adequately capture Article 26 of the GDPR
- your privacy policy contains a sufficient level of detail regarding social media targeting activities, beyond just referencing “advertising purposes”
- you can continue to rely on the same lawful basis going forward for advertising related processing activities
- you are processing SCD in light of the guidance and, if so, which Article 9 condition you are able to establish.

Remember that any comments on the Social Media Targeting Guidelines must be submitted to the EDPB via an online form by 19 October 2020.

Autumn 2020

Data protection

DMA issues "Seven-Step Ad Tech Guide" in a bid to restore trust in online advertising

The question

What needs to be done by UK businesses actively engaged in the programmatic delivery of digital advertising to ensure they protect the rights of individuals?

The key takeaway

The ICO has highlighted a number of critical issues with real-time bidding (**RTB**) and this new Guide by the Data & Marketing Association (**DMA**) seeks to help advertisers comply with their data responsibilities. The key message is that advertisers should work closely with tech firms and their agencies to ensure that their ad tech practices are compliant with the relevant laws, namely the GDPR and the ePrivacy Directive.

The background

Programmatic advertising is the bringing together of buyers and sellers of digital ad space in an automated process where computers use data to decide which ads to buy and how much to pay for them. RTB is the buying and selling of online ad impressions through real-time auctions that occur in the time it takes a webpage to load. It has introduced an auction pricing mechanism which allows publishers to sell to the highest bidder in a matter of milliseconds and almost 90% of programmatic advertising now relies on RTB. The ICO has expressed data protection concerns about RTB and sought to conduct investigations into issues surrounding consent, transparency and controls in the RTB data supply chain. Although these investigations were paused due to the coronavirus pandemic, the DMA has released a "Seven-Step Ad Tech Guide" for advertisers (**the Guide**).

The Guide

The Guide pulls together old and new initiatives, highlights areas of risk and recommends best practices in the following seven steps:

1. **Education and understanding**
   Advertisers must understand the ad tech ecosystem and take an active role in implementing organisational and technical measures. Cookie scans and cookie audits are also encouraged to ensure compliance with rules around consent.
2. **Special category data**
   Programmatic advertising will often process special categories of personal data, which is data that can be inferred from other information (for example it could be inferred that

somebody who is interested in baby products has a baby on the way). This data cannot be drawn with the intention to use it in digital advertising within explicit consent. Further, if the processing of this type of data is necessary, it will be mandatory to conduct a data protection impact assessment (**DPIA**).

3. **Understanding the data journey**
   A record of processing activities (**ROPA**) must be developed and there are a number of ICO templates that should be used.
4. **Conduct a DPIA**
   The DMA recommends conducting a DPIA in any situation where ad tech solutions are deployed. In addition, change control procedures implemented by advertisers should include a provision for reviewing DPIAs in case of relevant changes.
5. **Audit the supply chain**
   Due diligence must be carried out when data sharing or engaging processors and contractual warranties should not be relied upon without keeping sight of actual processing activities. The guidance has useful advice on what the ad tech contract should include and states that audits should be carried out on a periodic basis rotating between suppliers based on a risk assessment.
6. **Measure advertising effectiveness**
   Controllers must not use excessive personal data. The use of personal data should be proportionate to achieving advertising goals. The Guide also recommends a move away from tracking-based modelling to other forms of effectiveness monitoring.
7. **Alternatives to third party cookies (behavioural advertising)**
   This step recommends a shift towards contextual advertising which is considered less intrusive and does not rely on targeting segments.

Why is this important?

The Guide highlights a number of critical issues with RTB and offers useful practical tips for advertisers on how to minimise the risk of breaching GDPR rules. It is a collation of various credible industry initiatives and is approved by the ICO.

Any practical tips?

The Guide highlights the importance of understanding the basics and working closely with agencies and ad tech vendors on compliance matters. Advertisers should carefully review their ad tech practices and processes to ensure that they are GDPR and ePrivacy Directive compliant. In addition, media agencies should familiarise themselves with and prepare ROPAs, as well as conducting comprehensive ad tech vendor due diligence. Data protection training should also be provided to staff where appropriate.

Autumn 2020

Data protection

The EECC, the ePD and the GDPR – a complex interplay creating a breach notification nightmare for providers of communications services

The question

What impact will the implementation of the new Directive establishing the European Electronic Communications Code (2018/1972) (**EECC**) have on the scope and application of the ePrivacy Directive (2002/58/EC) (**ePD**) for providers of electronic communication services?

The key takeaway

The EECC, which amends the current definition of 'electronic communications service', will come into force on (or before) 21 December 2020. Once implemented, it will mean that the ePD shall apply to all over-the-top (OTT) services (ie Google Duo, WhatsApp and Facebook Messenger) catching a far broader range of providers within its scope. The implications are significant, not least the incredibly burdensome notification requirements placed on these providers in breach scenarios under both the ePD and the EECC – including, in the case of the ePD, local language notifications in (potentially) each of 27 EU member states within a 24 hour period.

The EECC, the ePD and the GDPR

The ePD was introduced in 2002 and focuses on protecting the privacy and security of personal data in electronic communications. It requires providers to ensure they take "appropriate technical and organisational measures to safeguard security of its services" (Article 4.1).

In 2009, the ePD was amended by the Citizens' Rights Directive (2009/136/EC) and introduced several new measures, including the requirement on providers to report personal data breaches and obtain consent (unless necessary for legitimate purposes) from its users to process their web cookies. As a result, the ePD has since been dubbed 'The Cookie Law'.

Following a public consultation by the European Commission in July 2016, the ePD was due to be replaced by the ePrivacy Regulation (**ePR**) in May 2018, alongside the General Data Protection Regulation (**GDPR**). To date, EU member states have been unable to agree on the new ePR and it remains in draft. Estimates vary, but some commentators do not expect the ePR to be agreed until 2023. A transitional period of 24 months would mean that the ePR would not come into effect before 2025. Once introduced, the ePR will essentially carry

forward the ePD but with stricter rules for securing electronic communications – ie requiring messages to be erased or anonymized after they have been received.

In the meantime, the EECC has been formally adopted (December 2018) and is due for implementation in each EU member state by 21 December 2020. Its aim is to drive investment in new high-capacity networks (think 5G, new fibre networks etc) and level the playing field between telecommunications companies and OTT providers. The Directive catches both internet access services and interpersonal communications services, sub-dividing these into 'number-dependent' (standard telephony) and 'number-independent' services (WhatsApp, Skype etc).

The notification nightmare

One of the practical impacts of the EECC is that all these providers must notify the competent authorities 'without undue delay' of a breach of security that has had a significant impact on the operation of the networks or services (eg number of users affected, duration of the breach, geographical area affected by the breach, the extent of disruption and the impact on economic and societal activities) – think issues such as outages, service disruption or unavailability.

This is in addition to notification obligations under the ePD, which provides that all in-scope personal data breaches must be reported within 24 hours to the relevant national regulator(s) for each respective country that the breach has impacted. Unlike in the GDPR, there is no "rights and freedoms" test in the ePD and therefore the obligation to notify within 24 hours is a strict one, applying to all data breaches suffered by a provider.

It is worth bearing in mind that on top of the notifications to the relevant competent authorities, both the ePD and EECC include obligations relating to the notification of impacted individuals.

At the time of writing, there is no pan-European 'one stop shop' for notifying data breaches under the EECC or the ePD, meaning an EU-wide breach must be reported to each competent authority of the 27 member states. It is also worth noting that there are substantive differences in the way notifications must be made under each piece of legislation – from the way questions are phrased to the detail required of each response and how that information is received by the relevant national regulator.

To complicate further, it is entirely possible for a breach to fall under the remit of both the ePD and EECC (imagine an incident hitting an OTT service and involving both a leak of personal data and a service outage at the same time) – meaning up to 54 notifications.

And, on top of all this, don't forget that the provider may also have an obligation to notify under the GDPR where there is a personal data breach which affects not only processing falling within the scope of the ePD (eg the accessing of a user's terminal data) but also other data

processing falling exclusively within the scope of the GDPR (eg the onward processing of that terminal data). In other words, while the ePD is a 'lex specialis' (so its specific rules override the more general breach notification principles under the GDPR), there may still be occasions where a separate GDPR notification is also required.

A highly complicated interplay of overlapping regulations which create a breach notification nightmare? Absolutely.

Why is this important?

In the UK, the Information Commissioner's Office is responsible for the enforcement of the ePD. Providers found to be in breach of the ePD could receive a fine of up to £500,000. Repeated across other member states and the figures would quickly begin to add up. In relation to the EECC, each individual member state is responsible for outlining penalties under its implementing legislation (very few of which have actually been put in place as at the date of writing).

The fact that there is no uniform way of notifying the regulators of data breaches under the ePD and EECC means that providers who offer OTT services across Europe should familiarize themselves with the notification procedures in each of the 27 member states. Preparatory work in setting up a process for meeting the requirements under each notification procedure (which differ between member states) is particularly crucial given the strict ePD obligation to notify within 24 hours.

Any practical tips?

While all eyes have been on the ePR, you would be forgiven for missing the extended application of the ePD by virtue of the EECC. But if you are a provider of OTT services and are about to be brought 'in scope', you better get familiar with the ePD – and quickly!

Reporting breaches under the EECC and the ePD, in particular setting up processes for making notifications in potentially 27 different member states within 24 hours with different language requirements, will take some planning – and that 21 December deadline is fast approaching.

If you need help in thinking this all through, including the practicalities of meeting international data breach notifications under tight timelines, RPC's award-winning 24/7 breach service – ReSecure – is here to help.

Autumn 2020

Data protection

Progress report on the ePrivacy Regulation – processing of metadata and use of cookies for "legitimate interests"

The question

Can you rely on the "legitimate interest" basis to process electronic communications' metadata and place cookies or similar technologies on end-users' terminals?

The key takeaway

On 29 May 2020, the Presidency of the Council of the European Union published its "progress report" on the controversial ePrivacy Regulation confirming what we already know; that there is still a long way to go before the European Commission's proposal for a Regulation which delivers a clearer, more workable ePrivacy regime aligned with the GDPR is finally adopted by the EU legislature. With Member States failing to reach an agreed approach on the proposed compromise text last year, further modifications to the draft have been made "*to simplify the text of some of the core provisions and to further align them with the GDPR*". Most notably, the focus has turned to the processing of metadata and use of cookies for "*legitimate interests*".

The background

In January 2017, the European Commission proposed a new Regulation on Privacy and Electronic Communications (**ePR**) to replace the current e-Privacy Directive (2002/58/EC). The Commission's aim was to update the e-Privacy regime by increasing its scope to all electronic communications providers whilst ensuring those rules were paralleled with the GDPR. While the intention was for the new Regulation to come into effect alongside the GDPR, there has been much controversy with Member States failing to reach agreement on several important areas, including cookie consents and the processing of electronic communications metadata.

Legitimate interests

The most important modification introduced by the Croatian Presidency is the possibility to process electronic communications metadata (Article 6(B)) and to use processing and storage capabilities of, and the collection information from end-users' devices (Article 8) when it is necessary for the purpose of legitimate interests, provided that specific safeguards are In place. For example, a prohibition on sharing the metadata or the collected information with third parties. Furthermore, the legitimate interests justification cannot be used when the legitimate interests pursued by providers are overridden by interests or fundamental rights and

freedoms of the end-users. This would be the case, for example, where the data is used to determine the nature or characteristics of the end-user or to build an individual profile of the end user.

Why is this important?

The uncertainty over the ePR continues to cast a shadow over the advertising industry, with companies hesitant to commit to new technologies and business models under the current e-Privacy regime. Additionally, the ePR will be a post-Brexit measure and the UK might have its own thoughts on how best to regulate electronic communications data, although EU rules will still apply to UK service providers targeting EU customers.

Any practical tips?

The progress report highlights the mixed reactions of the Member States to the introduction of, among other modifications, the legitimate interests ground. Subsequent deliberations on the draft e-Privacy Regulation were cancelled due to COVID-19.

Some say the Croatians were forcing a last throw of the dice to try and move through the ePR. The Germans take the presidency next, but how far they are willing to pick up where the Croatians left off – in particular the legitimate interest argument – remains to be seen.

Autumn 2020

Data protection

H&M hit with €35.3m fine for GDPR employee breach

The question

How did H&M's internal data collection processes land it with the second largest fine in data breach history?

The key takeaway

Despite the catastrophic financial impact of COVID-19, the Hamburg State Commissioner for Data Protection and Freedom of Information (**HmbBfDI**) showed no signs of leniency in issuing H&M with the second largest fine ever to be handed to a single company for breach of the GDPR.

The background

The HmbBfDI announced on 1 October 2020 that it had fined the German subsidiary of fashion retailer H&M €35.3 million for the unlawful monitoring of employees in its centrally operated service centre in Nuremberg. On the same day, H&M announced it was to close 250 of its stores globally.

The details

Having evaluated over 60GB of company data, the HmbBfDI found that H&M's service centre in Nuremberg had held extensive permanent records of personal information on the private lives of employees since at least 2014. The HmbBfDI noted that even after short absences of employees, team leaders conducted "Welcome Back Talks" in which holiday experiences and symptoms and diagnoses of diseases were recorded. Furthermore, the HmbBfDI found that supervisors acquired detailed knowledge about the private lives of their employees through informal corridor talks, which often revealed family issues and religious beliefs. It came to light that the recorded personal information was then used to measure employee performance and to create profiles which would then form a framework on which to base general employment decisions.

The issues came to light following a configuration error which allowed data stored on the network drive to be accessible company-wide for several hours in October 2019. In their assessment, the HmbBfDI evaluated how accessible the information was, how the information was recorded and stored as well as how detailed and organised the information was.

In response to the fine, H&M issued a statement assuring staff changes at management level in its Nuremberg service centre, and that managers would get additional training on data

protection and employment law. Furthermore, the company stated it would introduce new roles with specific proficiencies in assessing, investigating, and increasing privacy processes, improved data-retention and data-deletion processes, as well as implementing IT systems incorporating increased data protection measures. Finally, H&M announced that employees that are working or have been working at the Nuremberg service centre for at least one month since the GDPR entered into force will receive compensation.

Why is this important?

The size of the fine issued to H&M and accompanying detail emphasizes just how important an appreciation of the GDPR is at all levels of a business in order to avoid similar financial and reputational damage. However, those responsible for managing HR play a particularly important role in mitigating against these inherent risks. Whilst “Welcome Back Talks” with employees can be positive from an employee welfare perspective, HR must approach such talks with caution and avoid questions that may lead to responses including special category data, such as data concerning health or data revealing religious or philosophical beliefs. Additionally, HR should be trained on what data is recorded from the responses, what captured data is used for, how long that data stored and who has access to it. Managers should be cautious about the way in which they incorporate employee profiles into their assessment of employee performance and other decisions around employment. Particularly in light of the pandemic-induced shift to working from home, businesses should approach the use of employee monitoring tools with caution and with transparency at the heart of all personal data collection processes.

Any practical tips?

GDPR and the risks associated with the processing of personal data require that both a top-down and bottom-up approach is taken to managing those risks. In practice, management should be trained extensively and have a sufficient understanding of the issues in order to carefully navigate those risks. Employees should also have an understanding of just how sensitive what they say in formal or informal talks with supervisors might be. In this way, there exists a collective responsibility across the entire cross-section of a business to ensure overall GDPR compliance. As a response to the fine, H&M introduced a suite of new data protection measures including a newly appointed data protection coordinator, monthly data protection status updates, increasingly communicated whistleblower protection and a consistent concept for dealing with data subjects’ rights of access. It is crucial that all businesses learn from lessons arising out of this judgment and review their current data protection practices, implementing more robust processes where necessary. This is particularly critical given the impact COVID-19 is having on organisations having to furlough or lay off staff and the consequent potential rise in data subject access requests and general complaints received from those former employees.

Autumn 2020

Digital

Audiovisual Media Services Directive – European Commission adopts guidelines on video-sharing platforms and the promotion of European works

The question

What can be learned from the European Commission's new guidelines on the Audiovisual Media Services Directive (**AVMSD**)?

The key takeaway

The European Commission has provided two sets of guidelines to help Member States implement the revised AVMSD into national law. The guidelines focus on (1) European works and (2) video-sharing platforms.

The background

The European Commission has released guidelines on the interpretation of some aspects of the AVMSD, which are an interesting insight on how the European Commission evaluates the scope and application of the AVMS Directive. One of its core purposes is to regulate illegal and harmful online content and it extends these rules to cover certain social media platforms, if the provision of programmes and user-generated videos constitutes an "essential functionality" of these services. The guidelines provide a list of relevant indicators that can be used to assess the essential character of the audiovisual functionality of a platform.

The guidance

Guidelines on European works

The revised AVMSD has reinforced the obligations to promote European films and TV shows in on-demand services, which need to ensure at least a 30% share of European content in their catalogues and give prominence to such content. It also allows Member States, under certain conditions, to require media service providers that are established in another Member State, but target audiences in their territories, to contribute financially to the production of European works.

The guidelines also include a recommended methodology for the calculation of the 30% share of European content in each national catalogue, based on the titles of films and seasons of television series. They also clarify the definition of "low audience" and "low turnover", in view of exempting smaller providers from the obligations concerning the promotion of European works. So, neither undermining market development nor inhibiting the entry of new market players.

Guidelines on video sharing platforms

The revised AVMSD extends EU standards on illegal and harmful content to video-sharing platforms, including services like social media where the provision of audiovisual content is not the principal purpose of the service, but it still forms some of its essential functionality. As a result, online players will have to ensure, in a similar way to traditional media players, that users are protected against hate speech and that minors are protected from harmful content. Online platforms must take action against flagged content, which incites violence, hatred and terrorism, and ensure appropriate advertising and product placement in children's programmes.

In this context, the guidelines provide a toolkit for Member States to help them assess which online services should fall under the scope of the European media framework. They also identify a list of relevant indicators that Member States can use when evaluating whether audiovisual content is an essential, and not only a minor or ancillary, part of the online platform. Further, they take into consideration the dynamic nature of the online platform environment and therefore aim to ensure flexibility in this area.

Why is this important?

The guidelines aim to provide a practical tool to help ensure the promotion of European works in media content, thereby supporting cultural diversity and greater choice for European consumers. They also aim to help better protect users of video on-demand and video-sharing platforms, particularly minors, against hate speech and harmful content.

The guidelines are part of the Commission's broader work to define clearer responsibilities and accountability for social media and online platforms, and are complementary to the proposed Digital Services Act package, on which a public consultation is currently taking place.

Any practical tips?

The deadline for EU member states to transpose the revised AVMSD into national law was 19 September 2020. The guidelines are expected to contribute to its harmonised implementation and enforcement. They provide the Commission's views on how specific concepts should be applied to ensure a consistent implementation of the media rules across Member States. They are non-binding, so it remains to be seen to what extent the Member States will comply with them and how the European Commission will react on the Member States' respective practices.

Autumn 2020

Consumer

CMA publishes final report on online platforms and digital advertising

The question

What were the CMA's key findings in its final report on online platforms and digital advertising?

The key takeaway

The CMA outlined that key players have market powers in search, social media and digital advertising, such that rivals can no longer complete on equal terms. To tackle this, the CMA has laid out a blueprint for pro-competition in order to tackle this market power and increase competition, whilst still protecting consumers' data.

The background

UK expenditure on digital advertising was around £14bn in 2019, and the CMA estimates that around 80% of all expenditure on search and display advertising in the UK in 2019 went to Google or Facebook. The CMA therefore conducted a study which assessed whether problems such as market power, lack of transparency and conflicts of interest mean that competition in search, social media and digital advertising is working as well as it should.

The CMA released its final report on its Online Platforms and Digital Advertising whereby it called on the government to bring forward legislation to introduce a new regulatory regime aiming to tackle Google and Facebook's market power in search, social media and digital advertising markets. The CMA concluded that Google and Facebook have developed "*such unassailable market positions that rivals can no longer compete on equal terms*", and laid down a blueprint for a pro-competition regime to tackle market power and increase competition. The report addresses both consumer issues in the context of the use and control of consumers' data, as well as competition issues – principally whether platforms have market power in consumer facing markets and whether competition in digital advertising is distorted by a lack of transparency, conflicts of interest and market power.

The findings

Whilst digital advertising brings valuable services and content to consumers, including internet search and social media, the CMA finds that a lack of competition and limited choice in these markets can cause harm. The final report identified the following:

- **Impact on prices**
  Consumers are paying higher prices for goods and services reflecting that whilst search and social media appear to be free to those who use them, the cost of advertising revenues is included in the cost of goods and services. The final report found that together Google and Facebook receive over 80% of the digital advertising expenditure in the UK. If the £14bn spend on digital advertising in the UK is higher than it would otherwise be in a competitive market, consumers may be paying higher prices for products in industries that rely heavily on online advertising, such as hotels, flights and insurance. The Final Report found that Google's prices are around 30% – 40% higher than Bing's when comparing like-for-like search terms.
- **Consumers are receiving inadequate compensation**
  Consumers are receiving inadequate compensation for their attention and the use of their personal data and being less able to control how their personal data is used eg consumers may effectively be faced with a "take it or leave it" offer when it comes to signing up to a platform's terms and conditions.
- **Effect on the news industry**
  The CMA found that newspapers are reliant on Google and Facebook for almost 40% of all visits to their sites. This potentially squeezes their share of digital advertising revenues, undermining their ability to produce valuable content. This is potentially leading to wider social, political and cultural harm through the decline of authoritative and reliable news media and the potential for fake news.
- **Market specific barriers to innovation and new competition**
  The CMA identified that Google and Facebook have access to large amounts of user data, which allow them to improve their services and target advertisements at individual users. It was concerned that they may use GDPR as justification for restricting access to valuable data for third parties whilst retaining it for use within their own ecosystems. It also found that both companies use default settings to encourage consumers to use their services and operate a 'take-it-or-leave it' model, where consumers are unable to control their data. The CMA is concerned that almost all social media platforms make it a pre-condition of use that consumers must accept personalised advertising. It concluded that all these factors present potential barriers to new competition.

The proposed solution

The CMA notes that its existing powers are not sufficient to address the issues identified in its report, therefore a new regulatory regime is required. The CMA has called on the government to establish a pro-competition regulatory regime for online platforms by creating a Digital Markets Unit (**DMU**), whereby it will have powers to deal with concerns swiftly and before irrevocable harm to competition can occur.

The CMA has proposed that the DMU should have the ability to:

- enforce a code of conduct to ensure that platforms with a position of market power do not engage in exploitative or exclusionary practices, or practices likely to reduce trust and transparency, and to impose fines if necessary
- impose a range of pro-competitive interventions, including:
  - order Google to open up its click and query data to rival search engines to allow them to improve their algorithms so they can properly compete. This would be designed in a way that does not involve the transfer of personal data to avoid privacy concerns
  - order Facebook to increase its interoperability with competing social media platforms. Platforms would need to secure consumer consent for the use of any of their data
  - restrict Google's ability to secure its place as the default search engine on mobile devices and browsers in order to introduce more choice for users
  - order Facebook to give consumers a choice over whether to receive personalised advertising
  - introduce a "fairness-by-design" duty on the platforms to ensure that they are making it as easy as possible for consumers to make choices
  - order the separation of platforms where necessary to ensure healthy competition.

Working with the ICO to examine the impact of privacy regulations, the CMA is concerned that big platforms could be interpreting the GDPR in a way which favours their business models, instead of in a way which gives users control of their data. The CMA advocates a competitive-neutral approach to implementing privacy regulation to ensure that big platforms are not exploiting privacy regulations to their advantage, and will be working further with the ICO and Ofcom to address these issues through the Digital Regulation Cooperation Forum.

Why is this important?

The report illustrates the concerns relating to choice and giving consumers the information they need to make an informed choice between a paid-for subscription service and one that requires assigning personal data in lieu of payment. The CMA has proposed that the government takes forward legislative proposals and reforms, and proposes to assist in developing these through the DMU. This demonstrates the CMA's evolving thinking relating to digital issues. The CMA recommends that the DMU has the power to introduce greater consumer control and separation of platforms where necessary, in order to be pro-competitive and protect consumers data.

Any practical tips?

Any new regime will need to balance addressing potential competition harms identified without overpowering services that consumers typically regard as valuable and useful, and stifling the

disruptive innovation that made Google and Facebook the market leaders they now are. Keep an eye out for further guidance and commentary provided by the CMA and the ICO on online market practices.

Autumn 2020

ASA

The ASA's new UK Scam Alert System

The question

What is the latest tool in the ASA's technology toolbox to combat misleading advertising online?

The key takeaway

The ASA is continuing to build its technological capabilities, this time with its new UK Scam Alert System. This aims to identify and remove paid-for scam ads by working in collaboration with the leading digital advertising and social media platforms.

Background

As part of its five-year strategy, launched in November 2018, the Advertising Standards Authority (**ASA**) committed to escalate the regulation of online ads and to use new innovative technology such as artificial intelligence and machine learning to proactively seek out and take enforcement measures against advertisers whose ads may be in breach of the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (the **Code**). The strategy also aims to encourage industry collaboration and the use of online platforms in order to maintain advertising standards.

One area that has historically been a point of regulatory focus and contention is bogus ads that leave consumers out of pocket. In addition, specific concerns have recently been raised about online paid-for ads which link to fraudulent content, particularly with the increased popularity of cryptocurrency investment and advertising. The Financial Conduct Authority and Action Fraud have estimated that over £27m had been lost in 2018/19 by victims of cryptocurrency and forex related investment scams.

The update

In line with the ASA's recent emphasis on using technology to strictly regulate and monitor online advertising, it has now launched a UK Scam Alert System, in collaboration with the leading digital advertising and social media platforms (including Facebook and Google). This system will be used to identify and take down paid-for scam ads across various platforms.

How will this work?

The UK Scam Alert System works in three main phases:

- **Report** – consumers will now be able to report online scam ads on multiple platforms. This will include paid-for search engine ads, ads featuring on social media and those appearing on newspaper websites.
- **Notify** – in response, the ASA promises to promptly notify all participating platforms and publishers and provide them with key details of the offending ad.
- **Remove and block** – finally, partners will then seek to locate and remove the ads as well as suspend the advertiser's account. In some circumstances, partners will consider adding these accounts to cross-platform blocklists which could prevent them from appearing in the future.

Why is this important?

The launch of the UK Scam Alert System is the latest in a line of measures by the ASA aimed at using technology to strictly regulate and monitor online advertising. The ASA has previously used child avatars which simulate children's online behaviour to be able to identify ads that do not comply with rules on age restrictions in sectors such as alcohol, gambling and food.

As of January 2020, the ASA has also been using monitoring technology to find, identify and remove posts which promote botox to UK consumers on social media platforms. In similar fashion to the UK Scam Alert System, this technology has the ability to track issues in social media posts and recognise specific posts as being potentially non-compliant. These problematic posts may then be flagged for removal as part of a coordinated effort with Facebook. An enforcement notice was sent to more than 130,000 practitioners and, in the first quarter of monitoring, over 12,000 posts were removed.

These latest measures are a continuation of the ASA's policy of regulation through the use of technology and collaborations with online platforms. This strategy, as outlined in the ASA's 2019 Annual Report, is underpinned by contemporary social issues such as child protection, mental wellbeing and gender presentation. We are likely to see further use of artificial intelligence and machine learning in the regulation of advertising as the ASA attempts to strengthen its capabilities and ensure that the rules and regulations are properly adhered to.

Autumn 2020

ASA

P&G: verification requirements in comparative advertising campaigns

The question

How much detail do you need to include to meet the verification requirements under the CAP Code when making comparisons with identifiable competitors?

The key takeaway

Any ad which features a comparison with an identifiable competitor or competitors must be verifiable. This means that the ad needs to contain, or direct consumers to, sufficient information to allow them to understand the comparison and to check the accuracy of the claims. The ruling helps provide guidance on the level of detail required to meet the requisite sufficiency level.

The ad

Procter & Gamble (**P&G**) released an internet display ad for Fairy Dishwasher Platinum Plus Tablets on 12 June 2019 in a regional newspaper website. The ad featured large text which stated: "*BEST DISHWASHER TABLET ON TEST*". It also included a pack shot of Fairy Dishwasher Platinum Plus Tablets and a Which? Best Buy logo, which featured the text "*Which? Best Buy Dishwasher Tablets February 2019*".

The complaint

The ads were challenged by Reckitt Benckiser UK, who queried whether the claims "*Best Dishwasher Tablet on test*" and "*Which? Best Buy Dishwasher Tablets February 2019*" were substantiated and whether they were verifiable.

The response

P&G argued that the claims were verifiable as they would be understood to relate to awards provided by Which? (the independent consumer organisation) and that the information in respect of testing and products could be found on Which?'s website. P&G also noted that the ad provided a link to the information. Although the full results of the tests were only visible to website users who subscribed, they argued that it would be clear to consumers that the product awarded "Best on Test" would be the one that had the most points.

The decision

Was the "Best Dishwasher Tablet on test" claim substantiated?

The ASA agreed that the claim would be construed by consumers as referring to the testing performed by Which?, using its own testing criteria. It also agreed that the Fairy Dishwasher Platinum Plus Tablets had received the highest score of all the tested products. This was sufficient to satisfy the ASA that the "Best on test" claim was substantiated.

Did the "Best Dishwasher Tablet on test" claim require verification and, if so, was it verifiable?

The ASA took the view that consumers would interpret the claim to mean that the tablets had received the highest score of all the products in the dishwasher tablets category, which were tested by Which?. This is a comparative claim and, as such, there was a requirement that the claim must be verifiable.

Although the ASA acknowledged that the claim related to a score awarded by Which? for the relevant category, the ad did not contain any further information in respect of the basis of the comparison nor did it provide information about where such information could be found. The ASA therefore considered that the information required to verify the comparison was not clearly identifiable in the ad. The critical point is that, although the testing methodology information was available and accessible, the results of the tests (which would provide information on whether the product scored higher than other products) was only available to consumers who had paid for a Which? subscription. For this reason, the ASA concluded that the ad, and more specifically, the comparative component of the claim was not verifiable as the details of the comparison were not readily accessible to consumers. The "Best Dishwasher Tablet on test" claim had therefore breached CAP Code rule 3.35.

Was the "*Which? Best Buy Dishwasher Tablets February 2019*" claim substantiated, and was there a requirement for it to be verifiable?

Similarly, the ASA was satisfied that the "*Which? Best Buy Dishwasher Tablets February 2019*" claim did not breach the advertising rules as consumers were likely to understand from the Which? "Best Buy" logo and branding that the tablets had been independently tested and that they had met the criteria set for the Best Buy dishwasher tablet award. Crucially, the ASA considered that the claim would not be interpreted as a comparative claim against other products as the "Best Buy" criteria was simply that the product must receive an overall test score above a certain threshold (rather than be better than other products on any given criteria). Accordingly, multiple products could be awarded a Best Buy and there was no requirement for the claims to be verifiable.

Why is this important?

The ruling highlights the distinction between substantiation and verification. It also highlights the difference between claims which merely indicate that a particular threshold has been

reached and comparative claims. A comparative claim, such as “Best on test” is an assertion that the product has received a higher score than all competitors and it needs to be verifiable, in accordance with rule 3.35.

A claim which indicates that a specific standard has been met, such as “Best Buy” simply states that the applicable threshold has been met (in this case that it has achieved a certain overall test score). It will not be subject to rule 3.35 but will still need to be substantiated and must not mislead consumers.

Any practical tips?

When making comparative claims, ensure that the ad either:

- contains sufficient information to allow consumers to understand the comparison and to check the accuracy of the claims, or
- directs consumers to a page which contains sufficient information to allow them to understand the comparison and to check the accuracy of the claims.

Remember to include enough verification information. While this will depend on the nature of the claim, this ruling suggests that more, rather than less, detail is what is needed to meet the sufficiency standard.

Autumn 2020

ASA

BOXT: 'next day delivery' and comparative pricing claims

The question

How careful do you need to be with "next day delivery" claims? And is one product comparison enough when making a price comparison claim?

The key takeaway

Clear disclaimers containing cut off times are key for making next day delivery claims, as is the need to prove you can meet demand for next day deliveries. When making price comparisons with a competitor, sufficient information must be provided to substantiate the comparison claim – simply providing one example of the same appliance sold by two companies may well not be regarded as sufficient for the claim.

The ad

A video on YouTube and a TV ad for heating company BOXT Ltd (**BOXT**), seen in October and November 2019 featured a voiceover which stated, "*Listen up, if you're thinking of replacing your boiler with British Gas, you might want to come a bit closer. BOXT can install your boiler the next day and a boiler from BOXT costs on average … actually you may want to turn the sound up too … £1217 less than the same one from British Gas. BOXT are also rated Britain's number one heating company on Trustpilot. So don't buy a new boiler from anyone else until you've checked BOXT, you'd be a fool to yourselves. BOXT, faster, cheaper, trustier*".

The complaint

British Gas challenged whether the following claims in the ads were misleading and could be substantiated:

1. "BOXT can install your boiler the next day", and
2. "a boiler from BOXT costs on average… £1217 less than the same one from British Gas".

A member of the public challenged:

3. whether the claim "*BOXT are also rated Britain's number one heating company on Trustpilot*" misleadingly implied a comparison against British Gas, who they believed were categorised differently from BOXT on Trustpilot.

The response

Next day claim

BOXT said that they guaranteed next day installation if the purchase took place before the cut-off point of 3pm and showed a footer on the home page of their website which stated "*Buy online by 3pm and get it fitted the next day*". They also stated that customers were able to choose the installation date which suited them. BOXT stated if their website showed no availability for next day installation on a particular day, customers were provided with a telephone number to call them, as they had a number of engineers on standby to ensure customers received next day installation. BOXT said that if a customer wanted a specific date and they had capability in a different area, they may still fit on the date the customer wanted if they contacted them by telephone or live chat. They provided a spreadsheet which they said showed the number of customers who received next day installation between October 2019 and January 2020.

Clearcast supported this stating that the ad included a qualifying disclaimer which stated "*when you buy before 3pm*". They said that they also asked for evidence to show that British Gas did not offer next-day delivery and for BOXT to confirm that they would continue to monitor the situation. Should that change, Clearcast said the ad would be pulled from air.

£1,217 savings claim

BOXT provided a spreadsheet they believe demonstrated an average saving of £1,217.73 after commissioning a third party to carry out market research to compare pricing and customer experience regarding the replacement of a new like-for-like boiler including installation. The exercise was conducted on Worcester branded boilers because they were the leading boiler brand for both BOXT and British Gas and were therefore representative of those available. BOXT said both of the boilers shown on screen while the savings claim was being made were Worcester branded boilers and the claim stated "*BOXT £1217 LESS ON AVERAGE*". BOXT believed consumers would therefore understand the basis of the comparison was with Worcester boilers from British Gas and that they would save more on some models than others.

Clearcast said they were told that the base rates for all of the boilers compared were supplied for both BOXT and British Gas, and based on the information provided the average savings claim was approved.

Comparison claim with British Gas

BOXT said British Gas were not cited in the ad at the point at which the Trustpilot rating was mentioned. They said that there was a distinct pause and change in the creative after the comparative savings claim and that they believed consumers would see the statement as a fact and not a comparison. BOXT said the phrase "*so don't buy a new boiler from anyone else until you've checked BOXT*" was merely a call to action asking consumers to check with BOXT before

buying a new boiler and clearly stated "*anyone else*", not British Gas. BOXT said they were still rated as number one in the category "gas installation" which the two companies had in common on Trustpilot, and therefore felt the ad was not misleading. They said that consumers were directed to Trustpilot and were therefore capable of verifying the information themselves.

Clearcast said they did not believe the claim implied a comparison between BOXT and British Gas, and at no point did the ad compare the two companies' ratings on Trustpilot, and the use of the word "also" helped to separate the claim from the previous comparisons.

The decision

Next day claim

The ASA considered that consumers would understand from the claim "*BOXT can install your boiler the next day*", and the accompanying super-imposed text which stated "*when you buy before 3pm*", that if they purchased a new boiler before 3pm, they could choose to have the boiler installed on the next day. The ASA assessed the evidence by BOXT and understood that while next-day installation was subject to availability, the evidence demonstrated that BOXT had sufficient measures and personnel in place to ensure that those consumers who chose next day installation were given it. The ASA recognised that the next-day installation data over the period in question, October 2019 to January 2020, showed that few customers actually took up the offer of next-day installation. However, the price of installation generally decreased the further in advance it was booked, so understood the lower take up was not as a result of availability issues. The ASA therefore concluded that the claim "*BOXT can install your boiler the next day*" had been substantiated and was therefore not likely to mislead.

£1217 savings claim

The ASA considered that consumers would understand from the claim "*a boiler from BOXT costs on average … £1217 less than the same one from British Gas*" that based on BOXT's average boiler prices, customers could save around £1,217 on their chosen boiler in comparison to the price that British Gas sold that same boiler. The ad provided no additional information on the basis of the comparison, and the ASA therefore expected BOXT to hold evidence which demonstrated that such a level of saving could be achieved, taking account of the wide variety of boiler types and brands available on the market. The ASA assessed the information provided, which comprised a list of comparisons between quotes obtained from BOXT and British Gas for Worcester Bosch boilers. While the spreadsheet demonstrated that quotes were obtained for different types of Worcester Bosch boilers, the ASA understood that there were many other boiler brands on the market that had not been included in the comparison and which were available through British Gas. The ASA acknowledged that although BOXT's comment that Worcester Bosch were the leading brand on the market, the claim in the ad referred to those boilers available through British Gas, and the ASA therefore considered that the evidence was insufficient to support the claim. As such, the ASA considered that it had not been demonstrated that a boiler from BOXT was on average

£1,217.73 less than the same one from British Gas and therefore concluded that the claim was misleading.

Comparison claim with British Gas

The ASA noted the claim "*BOXT are also Britain's number one heating company on Trustpilot*" in the ad followed the comparisons with British Gas. However, there was no reference to British Gas by the voiceover or the visuals at the point the claim was made. Given the addition of the word "also", the ASA considered that consumers would understand the claim as separate to the comparative claims made against British Gas earlier in the ad, and would interpret it as a factual statement about BOXT's Trustpilot rating. As BOXT were the top-rated company under the category of "Heating service" on Trustpilot, the ASA concluded that the claim was not misleading.

Why is this important?

The ruling demonstrates the importance of holding substantive and supportive evidence in "comparison with identifiable competitors" claims. The ruling further demonstrates the fine-line between compliance and breach – by using the word "also", it can separate and differentiate different claims so that each is assessed individually.

Any practical tips?

Don't forget the importance of disclaimers and cut off times in "next day delivery" claims. Remember you also need sufficient evidence to show that you have measures in place to support your delivery claims. On comparative claims, be careful to ensure that you hold full substantiation for the breadth of any claim you are making.

Autumn 2020

ASA

Wish.com: sexually explicit in-app ads deemed offensive and inappropriately targeted

The question

Will an ad of a sexually graphic nature be deemed to be inappropriately targeting consumers and causing harm and offence if it appears on general audience platforms?

The key takeaway

Sexually explicit ads that appear on general audience platforms (which have a broad appeal to all ages) will breach advertising rules on harm and offence. Advertisers must ensure that sexually explicit ads do not appear where a consumer would not expect to see them as they will be deemed to be inappropriately targeting consumers. Particular care must be taken with apps of appeal to children.

The ad

The e-commerce platform, Wish.com, had four ads that appeared in various apps:

1. The first ad, seen in the BBC Good Food Guide app on 13 April 2020, featured images including that of a naked mannequin wearing a cape, a woman shown from the neck down wearing a corset that partially exposed her breasts and revealed nipple tassels, and an image of a reclining woman from the waist down wearing fishnet stockings and underwear.
2. The second ad, seen in the Google News app on 22 April 2020, featured images including a woman wearing a jacket that partially exposed her cleavage and midriff, and a woman shown from the neck down wearing a corset that partially exposed her breasts and revealed nipple tassels.
3. The third ad, seen in the Google News app on 1 May 2020, featured an image of a sex toy alongside text describing various sex toys.
4. The fourth ad, seen in a Solitaire game on Google Play on 1 May 2020, featured the same images as ad 3, and an image of a reclining woman from the waist down wearing fishnet stockings and underwear.

The complaint

Three complainants considered that the content of the ads was sexually graphic and objected that the ads were likely to cause serious or widespread offence. Two of the complainants also challenged whether ads 2, 3 and 4 had been responsibly targeted as they were likely to be seen by children.

The response

Context Logic Inc t/a Wish.com said that their ads were comprised of content from listings provided by third-party sellers on the Wish marketplace. The techniques used to identify and remove potentially objectionable content included filtering based on keywords and tags. Additionally, Wish.com stated that they had worked with an ad partner who had also imposed measures, including filtering, to prevent Wish ads from appearing in inappropriate forums.

In respect of the ads under investigation, Wish.com agreed that the keyword filters and image analysis used by Wish.com's ad partner had not sufficiently prevented the ads from being displayed in general audience forums. It had therefore taken action to halt UK campaigns with the ad partner in May 2020. They stated that they would not be advertising with the ad partner until they had more confidence in the ad partner's ability to be able to identify mature content and prevent it from being shown in general audience forums. Wish.com also agreed that the complained-of ads may not have been appropriate for all forums, such as those where the audience was largely comprised of minors. However, they did not agree that the ads were likely to cause serious or widespread offence.

With regards to ad 1, Immediate Media, the creators of the BBC Good Food app, said that the ad had been shown as a result of the programmatic advertising that was in place. Programmatic advertising allows advertisers to retarget users based on their visiting history and this had been used by Wish.com. Immediate Media detailed the preventative measures they have in place and stated that action had been taken to prevent offensive ads appearing on their websites and apps, which included blocking certain product categories and monitoring images. They did not consider the ad to be suitable to be presented to users of BBC Good Food.

The decision

The complaints were upheld. While the ASA was satisfied that the ads featured items that were available on Wish.com's website and the images were relevant to the products sold, it considered that the ads were overtly sexual and contained explicit nudity. Additionally, consumers using the apps for recipes, the news and online games would not expect to see such sexually explicit content. The ASA therefore concluded that in those contexts each of the ads were likely to cause both serious and widespread offence, in breach of CAP Code rule 4.1 (Harm and offence).

Regarding the complaint that the ads on the Google News and Google Play apps were not responsibly targeted, the ASA also upheld this complaint as, given the content of the apps, they were likely to have a broad appeal to all ages including children. Therefore, any ads that appeared within the apps should have been suitable for children and, given the sexually explicit nature of the ads, this was not the case. The ASA acknowledged that Wish.com and its ad partner had used measures such as keyword filters and image analysis to try to target the ads to a suitable audience. However, these measures had not prevented the ads being shown

in media where children were likely to be part of the audience. Due to the ads containing explicit sexual images and that they had been placed in apps that were likely to be used by children, the ASA concluded that the ads had been placed irresponsibly and breached CAP Code rule 1.3 (Social responsibility).

Why is this important?

The ruling highlights that the ASA has zero tolerance on sexually explicit content appearing in a context where a consumer would not normally expect to come across such material – especially if the ads are being shown in apps that were actually "likely to be used by children". If the ads reflected browsing history and the device being used was not a shared one, then perhaps the limitations or inefficacy of the measures undertaken by Wish.com and its ad partner may have been considered more favourably. However, as devices can be shared by multiple users, the measures employed by both Wish.com and its ad partner were deemed ineffectual.

Any practical tips?

The ASA's focus is on the type and appeal of the applicable platform itself. Advertisers and brands must ensure that ads with sexually explicit content must not be shown in, eg, an app which potentially could be used by children or where a consumer was not expecting to see such content. In short, ads need to be made appropriate for all audiences of the platform.

Autumn 2020

ASA

Sky UK: clarity over upfront costs and different fees charged to different groups

The question

Do you need to include additional upfront costs in the main body of your ad? And how clear do you need to be about different fees being charged to different groups of consumers (eg existing vs new customers)?

The key takeaway

Advertisers must make it sufficiently clear when there are additional upfront costs. If there is material information, then this must be stated in the main text of the ad so that consumers are aware of the full costs applicable, including difference prices for different groups.

The ad

A TV ad and a page on Sky's website:

- The TV ad, seen on 17 October 2019, included the voice-over, "Get both Sky and Netflix all in one place on Sky Q and open a world of unmissable entertainment … Sky and Netflix all in one place on Sky Q for one surprisingly low price, just £25 per month". Prominent on-screen text at the end of the ad included "Sky and Netflix £25 a month Existing and new customers". Smaller text superimposed at the bottom of the screen during the ad stated "Netflix part of Ultimate On Demand Pack. Upfront costs: £20: new customers; up to £219: existing", "Requires Sky Q box connected to broadband …", and "Prices may change during this period. Usually: £34pm. Kit loaned at no cost. Terms apply".
- The web page on www.sky.com, seen in November 2019, which was titled "*Sky Offers and Bundles*", featured three offers under the text "*Open up a world of unmissable entertainment from both Sky and Netflix with Sky Q …*". The first offer, titled "*Unmissable entertainment at superfast speeds*", included the text "*Sky TV & Netflix … £45 a month for 18 months Prices may change during this period Set-up cost: £39.95*". The second offer, titled "*Sky TV and Netflix, all in one place*", included the text *"… all on Sky Q £25 a month for 18 months Prices may change during this period Set-up cost: from £20*". The third offer was titled "*The TV you love plus exclusive premieres*" and included the text "*£35 a month for 18 months Prices may change during this period Set-up cost: from £20*". Underneath the information about the offers, small hyperlinked text positioned to the right of the web page stated "*Terms & conditions*". Below the offers, under the heading "*Here's the legal bit*", text stated "… *Sky TV & Netflix: £39pm outside 18-month minimum term. 'Sky's Best Price' based on lowest price for Sky Entertainment and Ultimate on Demand*

…Broadband: … Set up: £9.95 router deliver and £10 connection fee. Sky Talk: Compatible line required otherwise £20 connection charge may apply. Standard prices apply after 18 months …". A number of drop-down sections appeared underneath; the first was headed "*Offers*".

The complaint

The ASA received complaints that the ads were misleading because they did not make sufficiently clear that there was a set-up fee of £199 to take advantage of the offers.

The response

Sky UK Ltd (**Sky**) said that new customers and existing customers who had a Sky Q box would be charged a £20 set-up fee. Only existing customers who did not have a Sky Q box would be charged a £219 set-up fee. In relation to the TV ad, Sky explained that the upfront fee was explained in the on-screen text which stated, "*Upfront costs: £20: new customers; up to £219: existing*". Sky said that the text was sufficiently legible, and consumers would understand that upfront costs applied to those who wanted to take advantage of the offer. In relation to the web ad, Sky said that the full information on the associated upfront fees was presented in the "Offers" section at the bottom of the page, which contained information about the set-up fees. Sky said that text was also included in the terms and conditions which could be reached by clicking on the words "terms and conditions" in the body text of the ad.

Clearcast also responded, noting that in relation to the TV ad, the superimposed text was of sufficient size and legibility to be clearly read, and was held for long enough to meet requirements. Clearcast said the set-up fees involved in taking up Sky services varied according to a customer's particular status, such as whether they were a new or an existing Sky customer and what equipment they already had. Clearcast believed it was difficult for the advertiser to give specific information in the ad about those costs which would be meaningful to all viewers. However, Clearcast considered upfront set-up costs to be material information which needed to be included in the ad. Clearcast were content that the superimposed text "*Upfront costs: £20: new customers, up to £219: existing*" was sufficient to alert viewers that there were upfront costs which would have to be paid over and above the advertised monthly price. That wording gave some indication of what those costs were and made viewers aware that the costs would vary.

The decision

The ASA upheld the complaints. The ads related to a package which enabled consumers to obtain Sky and Netflix for £25 a month. Customers needed a Sky Q box in order to take advantage of the offer. New Sky customers and existing customers with a Sky Q box would have to pay an upfront cost of £20. Existing Sky customers who did not have a Sky Q box would have to pay an upfront cost of £219.

The TV ad: The ASA considered that viewers would understand from the presentation and claims that consumers would be able to obtain Sky and Netflix for £25 a month, when delivered via a Sky Q box. The voice-over in ad (a) stated "*Get both Sky and Netflix all in one place on Sky Q … for one surprisingly low price, just £25 per month*". The large on-screen text at the end of the ad which stated "*Sky and Netflix £25 a month Existing and new customers*" further emphasised the price claim and availability of that price to both new and existing customers. The ASA considered that the ad therefore made clear the monthly cost of subscribing to the service for all consumers. The ASA considered that in addition to the ongoing monthly cost, the set-up fees were also material information that viewers needed in order to make an informed decision about whether or not to take advantage of the offer. Given that the costs which applied to consumers differed depending on their status as a new or existing customer and whether they required a Sky Q box, the ASA held that this information needed to be clearly presented to viewers in order for them to understand the full costs that were applicable to them. Although the ad included superimposed text which stated "*Netflix part of Ultimate On Demand Pack. Upfront costs: £20: new customers; up to £219: existing*" and in a separate shot superimposed text stated "*Prices may change during this period. Usually: £34pm. Kit loaned at no cost. Terms apply*", the ASA considered that this presentation of the costs to new and existing customers was unclear and was likely to cause confusion to consumers. The wording used in the first piece of text to describe the costs which applied to each set of customers was unclear and was likely to be misinterpreted by many viewers.

The web ad: the main body of text described three different packages available via Sky Q, which included both Sky and Netflix. In relation to the £25 per month package, text stated "*Set-up costs: from £20*". Additional information about the set-up fees was not in the main text of the ad. The ASA considered that because the set-up fees constituted material information, they should have been stated in the main text of the ad so that consumers were clear as to the full costs which were applicable to their particular situation. As the full costs were stated only in a drop-down section or one click away, the ASA held they were not sufficiently prominent.

Why is this important?

Fees which are charged to different groups of consumers must be made sufficiently clear to avoid an advert being misleading. Material information such as set-up fees must be stated in the main text of ads, so consumers are clear as to the full applicable costs.

Any practical tips?

If there are additional costs, such as upfront costs or set-up fees, make this clear in the main text of the ad so that consumers are aware. If there are different fees for different consumers, and not everyone will benefit from the same offer, this also needs to be communicated clearly upfront.

Autumn 2020

ASA

Playrix: gameplay footage must be representative of the gaming experience

The question

When advertising a game, can you use gameplay footage which does not actually feature in the game, or only features to a limited degree?

The key takeaway

Any depiction of gameplay footage must be representative of what a consumer would experience when playing the game.

The complaint

Two paid for ads were shown on Facebook, one for Homescapes and one for Gardenscapes, both of which included video depictions of their respective games. The ASA received seven complaints from individuals who claimed that the ads were misleading on the basis that the content was not representative of the Homescapes or Gardenscapes games.

The response

PLR Worldwide Sales Ltd t/a Playrix said that the content that featured in in the ads was included in their games and that it represented part of the gameplay. The specific content in the ads was part of 'mini games' and available in some of the higher levels of each of the games. They explained that the two games contained thousands of levels and a number of elements, namely: an unfolding storyline which involved the renovation of a house or a garden; 'mini-games' (as featured in the ads); and 'match-three' style games. They explained that the 'mini games' generally featured once every 20 levels of the main games.

The decision

The ASA acknowledged that the ads included a disclaimer that "Not all images represent actual gameplay". They therefore accepted that consumers would understand that the exact gameplay featured in the ads may not necessarily be available when playing the game. However, the ASA said that consumers would nevertheless expect that the Homescapes and Gardenscapes games would consist of a similar problem-solving style to that featured in the ads. Given that users would need to play a significant amount of content which was of a different style in order to access the gameplay featured in the ads, the ASA considered that the ads were not representative of the games they were purported to feature and were consequently misleading.

Why is this important?

The adjudication is a helpful reminder of the care that needs to be taken when advertising games to ensure that the content/style of game depicted reflects what consumers would generally experience when playing.

Any practical tips?

Helpfully, the ASA seemed to accept that simulated gameplay footage or gameplay footage that does not actually feature as part of a game is acceptable, provided that the content shown is not substantially different to what a consumer can experience. However, given the reliance that the ASA placed on the use of the disclaimer, if any simulated footage is used advertisers should ensure that the ad features text confirming that “not all images represent actual gameplay” or similar.

Autumn 2020