RPC

Commercial law snapshots

Spring 2020

Spring 2020

Contents

Page

1. Commercial

Restrictive covenants and the tort of inducing a breach of contract 3

Good faith; contractual discretion 5

Acquisitions: clause in SPA construed as a covenant to pay, not an indemnity 7

Legal advice privilege: dominant purpose 10

Ministerial statement in response to Law Commission report on electronic execution of documents 12

2. Intellectual Property

Copyright: Works of artistic craftsmanship and Cofemel 14

Trade marks: Specifications and bad faith 17

3. Data protection

ICO consults on new direct marketing code of practice 19

Adtech and the data protection debate – where next? 21

ICO monetary penalty notice against DSG Retail Ltd for data breach 23

ICO issues monetary penalty notice against Cathay Pacific for data breach 26

Schrems II - Advocate General's Opinion 28

EPDB guidelines: Data Protection by Design and by Default 30

CJEU's CCTV ruling: guidance on legitimate interests processing 32

4. Digital

Online Harms White Paper: consultation response 35

European Commission proposal for new Digital Services Act 38

5. Consumer

New EU Consumer Protection Co-operation Regulation comes into force 40

6. Influencer marketing

Online Affiliate Marketing: New CAP advice note 42

New CAP/CMA Guidance: #Ad(vice) for Influencers 45

Influencer marketing and obvious brand references 47

Influencer marketing, alcohol and youthful looks 49

7. Gender stereotyping

Gender stereotyping and the use of one gender in an ad 52

Gender stereotyping and "that girl boss thing" 54

Commercial

Restrictive covenants and the tort of inducing a breach of contract

Allen t/a David Allen Chartered Accountants v Dodd & Co [2020] EWCA Civ 258

The question

What is the knowledge requirement for the tort of inducing a breach of contract? To what extent is this affected by the legal advice received?

The key takeaway

This case affirms the principle that a defendant must know that they are causing a breach of contract in order for the tort of inducing a breach of contract to be made out. It also shows that a business can rely on its legal advice for the purposes of demonstrating an honestly held belief that there would not be a breach.

The background

Mr Pollock was employed by an accountancy firm called David Allen Chartered Accountants (**David Allen**). His employment contract contained a restrictive covenant which included non-solicitation and non-dealing clauses, applicable for 12 months after the termination of his contract.

In July 2018 Mr Pollock resigned and started a new role at a Dodd & Co. Ltd (**Dodd**), a competitor of David Allen. Dodd's lawyers advised them that the restrictive covenants in Mr Pollock's contract were unlikely to be enforceable, as the 12 month limit on the non-solicitation and non-dealing clauses would probably be considered excessively lengthy for the purposes of protecting David Allen's legitimate business interests.

After starting at Dodd, Mr Pollock began to contact clients that he had worked with whilst at his previous employer. David Allen brought a claim against Dodd for inducing a breach of contract.

The decision

The Court of Appeal unanimously upheld the decision of the High Court. The Court applied the criteria set out in the House of Lords decision in OBG Ltd v Allan [2007]:

- there needs to be a binding underlying contract

- the defendant must know that they are inducing a breach of contract
- if a defendant deliberately turns a blind eye, this will not prevent them from having the requisite knowledge
- if the defendant honestly believes that they will not cause a breach of contract, it does not matter if their reasoning is illogical or mistaken in law.

The Court considered that people should be able to act on responsibly sought legal advice, even if it turns out to be wrong, and even if it was appreciated that there was a degree of risk attached to the advice. If definitive legal advice was required confirming that there would not be a breach of contract, it would have a chilling effect on legitimate commercial activity. Instead, legal advice that it is more probable than not that no breach will be committed would be sufficient. In this case, the requirement was satisfied.

Why is this important?

This case gives practical guidance as to how a party's knowledge is assessed when considering a claim for inducing a breach of contract and the relevance of the legal advice obtained at the relevant time.

Any practical tips?

Always bear in mind that, if you are involved in taking steps that may lead to the breach of a contract between two other parties, you may face allegations of procuring or inducing a breach of contract (especially if you are regarded as having the 'deeper pockets' for any claim).

If favourable legal advice is obtained (eg that it is likely that there would not be a breach), you can rely on that advice – but note that you may need to disclose such advice (and related instructions) if you wish to rely on it in the future.

Spring 2020

Commercial

Good faith; contractual discretion

Morley (t/a Morley Estates) v Royal Bank of Scotland Plc [2020] EWHC 88 (Ch)

The question

Was a loan agreement a "*relational*" contract and, if so, to what extent did that limit the lender's contractual discretion?

The key takeaway

The Court held that the loan agreement was not a "*relational*" contract. The lender's exercise of contractual discretions under that agreement were subject only to a duty to exercise them for a legitimate commercial aim, so as not to vex the borrower.

The background

There is no general requirement for good faith in English contract law, nor is a general duty to act in good faith usually implied in a commercial contract. However, as considered in *Bates v Post Office Ltd*[1], in certain cases a specific or general duty of good faith may be implied where the contract is a "*relational*" contract, eg a long-term commercial contract with a non-commercial aspect involving a high degree of communication, co-operation and performance based on mutual trust and confidence and expectations of loyalty or fidelity.

In this case, the borrower had entered into a three-year loan agreement with the bank in 2006, which was secured on a portfolio of properties. In early 2009, the bank obtained an updated valuation of these properties and found that the value had fallen, which demonstrated a breach of the loan to value covenant. The bank therefore started charging interest at an increased default rate and attempted to restructure the loan. Eventually, the parties reached an agreement enabling the borrower to salvage some of the portfolio, but the rest was transferred to the bank's subsidiary.

The borrower claimed rescission of those agreements, or damages in lieu of rescission, asserting the loan was a "*relational*" contract and that the bank had an implied duty to act in good faith, which it had breached by obtaining a new valuation of the portfolio and "*forcing*" a breach of the loan to value covenant.

[1] *Bates v Post Office Ltd* (No 3) [2019] EWHC 606 (QB)

The decision

The High Court held that the loan agreement was not a relational contract. It was an ordinary loan facility agreement and there was no implied duty of good faith.

The bank's exercise of its contractual discretions to obtain a revaluation of the mortgaged properties and charge default interest were valid, connected to the bank's commercial interests and not limited by a need to act in good faith. The bank's contractual discretions were subject only to a duty to exercise them for a legitimate commercial aim, so as not to vex the borrower.

Why is this important?

The decision confirms that the Court will not readily find a contract is "*relational*" and/or subject to an implied general duty of good faith. The exercise of contractual discretion is not therefore subject to additional restrictions in those circumstances.

Any practical tips

Parties should continue to review whether they wish to include express duties of good faith, whether for specific provisions or generally – or even whether they wish to expressly exclude any obligations of good faith – within their agreements.

Spring 2020

Commercial

Acquisitions: clause in SPA construed as a covenant to pay, not an indemnity

The question

When will a clause be considered a covenant to pay as opposed to an indemnity?

The key takeaway

In determining whether a payment obligation clause is expressed as a covenant to pay or an indemnity, the court will look at the proper construction and interpretation of the language of the clause against the factual matrix and the rest of the terms of the agreement.

The background

Pursuant to a share purchase agreement (**SPA**), AXA (indirectly) acquired from Genworth the entire share capital of two insurance businesses (together **F**) which were in the business of underwriting payment protection insurance (**PPI**) for store cards. The PPI was marketed and sold to customers on AXA's behalf by Santander under an agency agreement.

Unfortunately, there were extensive PPI mis-selling complaints by customers against F. Santander accepted liability for certain claims but there was a dispute as to whether it was liable for mis-selling complaints underwritten by F and arising prior to 14 January 2005. In negotiating the SPA, AXA and Genworth anticipated that F and Santander would enter into an agreement under which Santander would accept liability for all complaints, causing Genworth's liability to cease. On this basis, clause 10.8 of the SPA provided as follows:

"The Sellers hereby covenant to the Purchaser and each Target Group Company that they will pay to the Purchaser or such Target Group Company on demand an amount equal to:

a) *ninety percent (90%) of all Relevant Distributor Mis-selling Losses; and*

b) *ninety percent (90%) of the amount of all costs, claims, damages, expenses or any other losses incurred by the Purchaser or a Target Group Company after Completion resulting from the Relevant Distributor Dispute or settlement thereof including any such losses incurred pursuant to any Action which arises from such Relevant Distributor Dispute, but excluding, after the First Termination Date, the amount of all such losses resulting from a dispute described in clause (a) of the definition of "Relevant Distributor Dispute"…*

… Within thirty (30) Business Days of each of the First Termination Date and the Second Termination Date the Purchaser will issue a final demand in respect of all accrued and unpaid obligations of the Sellers under clause 10. 8(a) or, as applicable, (b) and upon payment of such demand the Sellers shall be released from their obligations under this clause 10. 8…"

However, after execution of the SPA, Santander refused to enter into a settlement agreement and pre-2005 complaints were directed solely at F, which was left facing significant liabilities.

AXA therefore issued a demand payment of approximately £28.5 million under clause 10.8 of the SPA and, when payment was not made, issued proceedings to recover the amount demanded.

Genworth argued that the payment obligation contained in clause 10.8 was an indemnity, not a performance bond, and therefore Genworth was not under an obligation to pay until F had asserted all defences reasonably available to it in respect of the liabilities. AXA countered that clause 10.8 was a bespoke provision pursuant to which Genworth had covenanted to pay identified losses on demand and there was no requirement for F to advance all reasonably available defences.

The decision

The Court accepted that its task was to construe the contractual language of the clause against the factual matrix to the SPA and the other terms of the SPA as a whole, using well established contractual construction principles.

The Court found that Clause 10.8 was a bespoke provision agreed between the parties that need not be classified either as an indemnity or a performance bond. The language used was a promise or "*covenant*" to pay which was triggered by the demand and not an agreement to indemnify. Had the parties intended the converse, they would have stated so.

As such, the Court found that on the ordinary and natural meaning of the language of clause 10.8, Genworth was obliged to pay the demand and it was neither an express or implied requirement of the SPA that AXA prove that all reasonably available defences had been advanced.

Why is this important?

It is common for agreements governing significant transactions to include bespoke provisions that set out how a particular risk or liability and any associated payment obligations will be dealt with post completion. The usual principles of contractual construction are more important than categorisation of terms.

Any practical tips?

When seeking to allocate risk/liability between the parties (eg through covenants to pay/indemnities), the relevant provisions should clearly set out:

- the trigger event(s) that gives rise to the liability
- the loss/liability covered
- the timing of any payment and how the loss/liability will be calculated/determined
- any conditions or limitations on recovery (eg obligations to mitigate, conduct of claims, etc).

Spring 2020

Commercial

Legal advice privilege: dominant purpose

Court of Appeal (Civil Aviation Authority v R Jet2. Com Ltd [2020] EWCA Civ 35)

The question

When do documents or emails have the benefit of legal advice privilege?

The key takeaway

In order to attract legal advice privilege, it must be demonstrated that the relevant document or communication was created or sent for the dominant purpose of obtaining legal advice.

The background

In April 2018, the Civil Aviation Authority (the **CAA**) published a press release in which it criticised Jet2.com for rejecting the opportunity to participate in its new ADR scheme for handling passenger complaints. Jet2.com wrote to the CAA, complaining of the fact that it had been named in the press release and setting out its reasons for not joining the scheme. In February 2018, the CAA responded by way of a letter (the **February Letter**), which was subsequently published by the Daily Mail.

Jet2.com commenced judicial review proceedings against the CAA.

During the proceedings, the CAA disclosed an initial draft of the February Letter alongside a covering email, which demonstrated that there had been several drafts of the February Letter in circulation between various employees at the CAA, including an in-house lawyer. Jet2.com made an application for specific disclosure of all drafts of the February Letter. The CAA claimed legal advice privilege.

The decision

The Court of Appeal held that a claim for legal advice privilege requires the party claiming privilege to show that the relevant document or communication was created or sent for the dominant purpose of obtaining legal advice.

The Court of Appeal also considered whether single, multi-addressee emails would be covered by legal advice privilege, where they were sent simultaneously to various individuals for their advice or comments, including a lawyer for the lawyer's input.

Taking into account the concept of a “continuum of communication”, the Court held that, if the dominant purpose of the document or communication is to settle the instructions to the lawyer, then that communication will be covered by legal advice privilege. That will be the case even if the communication is sent to the lawyer himself or herself, by way of information or if it is part of a rolling series of communications with the dominant purpose of instructing the lawyer.

However, if the dominant purpose is to obtain the commercial views of the non-lawyer addressees, it will not be privileged, even if there is a simultaneous subsidiary purpose to obtain legal advice from the lawyer addressee(s).

Why is this important?

The Court of Appeal has provided important guidance on the application of legal advice privilege, confirming that, for a communication or document to attract privilege, its dominant purpose must be the giving or obtaining of legal advice. The guidance on the circumstances in which an email addressed to multiple individuals would satisfy the test for privilege is also helpful.

Any practical tips

Clients should ensure that only those employees specifically tasked with giving or obtaining legal advice should communicate with the legal team.

Privileged communications should not be circulated internally without the approval of the legal team. Discussion of advice will not qualify as privileged where the purpose was to obtain commercial views, even if a lawyer is copied into the email.

Where possible, clients should keep communications with the legal team and the business teams separate, as this will help avoid ambiguity as to the (dominant) purpose of the communication.

Spring 2020

Commercial

Ministerial statement in response to Law Commission report on electronic execution of documents

The question

How has the government responded to the Law Commission report on electronic execution of documents?

The key takeaway

The government has confirmed that its views are aligned with several findings from the Law Commission's 2019 report on electronic execution of documents.

The use of electronic signatures is legitimate within both commercial and consumer contracts, although it is recognised that vulnerable individuals may need additional protection.

Whilst deeds require a witness to be physically present, the use of video to witness electronic signatures is being considered as a solution.

The background

In September 2019 the Law Commission published a report on the electronic execution of documents, to make the legal position on electronic signatures clearer and more accessible.

The basic legal position is that electronic signatures can be used to execute documents, (including deeds) provided that the party executing the document electronically intends for this to be the case.

In order for deeds to be signed electronically, a witness still needs to be physically present. However, the Law Commission has suggested that video-witnessing could be one of several solutions considered by a government-launched Industry Working Group of experts.

Reasonable electronic versions of existing execution methods are likely be accepted by the courts. Recent case law has shown that an electronic signature can be demonstrated by a name typed at the bottom of an email or by ticking a box on a website confirming acceptance of terms.

The development

On 3 March 2020 the Lord Chancellor and the Secretary of State for Justice issued a written response to the Law Commission's report. The key points were that:

- ministers agree that there is no need to bring forward primary legislation in order to support the validity of electronic signatures
- the government approve of the draft legislative proposal put forward by the Law Commission - it aligns with their views on the legal position
- electronic signatures can be used in commercial and consumer documents against a background of legal certainty
- vulnerable individuals need to be protected from the changes that electronic execution could bring about in other areas of law
- the government will adopt the Law Commission's recommendation and establish an Industry Working Group to consider security and technology issues and the use of video to witness electronic signatures
- the government will also ask the Law Commission to carry out a wider review of the law around deeds, although the timing of this will depend on the urgency of other reviews to be undertaken by the Law Commission.

Why is this important?

With many UK businesses currently operating work from home policies as a result of the COVID-19 pandemic, the electronic execution of documents is likely to become more prevalent than ever before.

In affirming the Law Commission's report, the government's response provides greater certainty to businesses on the use of electronic signatures and how they are likely to be dealt with by the courts.

Any practical tips?

Electronic execution of agreements is acceptable and effective.

If deeds are being executed electronically, note that the issue of witnesses needs to be considered.

Spring 2020

Intellectual Property

Copyright: Works of artistic craftsmanship and Cofemel

Response Clothing Limited v The Edinburgh Woollen Mill Limited

The question

What is the impact of the CJEU's decision in *Cofemel* on UK copyright law relating to "*works of artistic craftmanship*"?

The key takeaway

This is the UK's first decision following the CJEU's decision in *Cofemel*. It appears to recognise that UK copyright law is inconsistent with EU law, at least in respect of any requirement for a work of artistic craftsmanship to have aesthetic appeal.

The background

There has been much debate in the UK around whether certain elements of the Copyright, Designs and Patents Act 1998 (the **CDPA**) remain compatible with EU law following the CJEU's recent decision in *Cofemel*, which suggests that there is a harmonised EU-wide definition of "*work*" for copyright purposes, which is not restricted by any pre-specified categories and should not take into account any aesthetic considerations/limitations.

By contrast law, the UK approach has been:

- the "*closed-list*" of categories of works which can benefit from copyright protection under the CDPA
- the concepts of "*sculptures*" and "*works of artistic craftmanship*" as found in section 4 of the CDPA and developed over time by the English courts
- under section 51 of the CDPA, "*it is not an infringement of any copyright in a design document or model recording or embodying a design for anything other than an artistic work or a typeface to make an article to the design or to copy an article made to the design.*"

This IPEC case is the first judgment of a UK court following Cofemel to consider this question. The dispute concerned the supply from 2009 to 2012, by Response Clothing (**Response**) to Edinburgh Woollen Mill (**EWM**), of certain ladies' tops made of a jacquard fabric of a design

referred to as a "*wave arrangement*", consisting of multiple lines woven into the fabric in a wave pattern.

In 2012, following an attempt by Response to increase its prices, EWM supplied a sample of Response's top to other garment suppliers with an invitation to supply tops made from a similar fabric.

Response brought a claim of copyright infringement against EWM, alleging that copyright subsisted in its wave arrangement design, including on the basis that it was a work of artistic craftsmanship.

The decision

The judge referred to the New Zealand High Court's decision in *Bonz Group (Pty) Ltd v Cooke* (itself referred to by Mann J in the first instance decision in *Lucasfilm Ltd v Ainsworth* (the "*stormtrooper helmet*" case)) which established that for a work to be one of "*artistic craftsmanship*": (1) its creation required skilful workmanship; and (2) be artistic, such that there was creative ability that resulted in "*aesthetic appeal*".

The judge found that, in his view, the wave fabric could be a work of artistic craftsmanship following *Bonz*, despite being made with a machine rather than by hand, as the employee who designed the fabric would have been a craftsman working in a skilful way, and the primary goal was presumably to make something aesthetically pleasing to customers.

Turning to EU law, the judge was also satisfied that the wave fabric was original in that "its design was its author's own intellectual creation" and if "*no sufficiently similar design existed before it was created, it must have been the expression of the author's free and creative choices.*"

Pursuant to the *Marleasing* principle, the judge was required to interpret the CDPA in line with the Information Society Directive (2001/29/EC) so far as possible and therefore "*in conformity with the way in which that Directive has been interpreted by the CJEU*". In doing so, the judge noted (at paragraph 63 of the Judgment):

"*The issue I have to resolve is not whether Directive 2001/29 has the effect of removing all the gaps there may be in copyright protection available from a court at first instance for 'works' within the meaning of art. 2 of the Directive, but whether it is possible to interpret s. 4(1)(c) of the 1988 Act in conformity with art. 2 of Directive 2001/29 such that the Wave Fabric qualifies as a work of artistic craftsmanship and thereby its design becomes entitled to copyright protection. In my view it is, up to a point.* ***Complete conformity with art. 2****, in particular as interpreted by the CJEU in Cofemel, would* ***exclude any requirement that the Wave Fabric has aesthetic appeal*** *and thus would be inconsistent with the definition of work of artistic*

craftsmanship stated in Bonz Group. I need not go that far since I have found on the facts that the Wave Fabric does have aesthetic appeal. "

Why is this important?

Although the decision was not reached on this basis, the judge appears to accept that the consequence of the *Cofemel* decision is that UK copyright law is inconsistent with EU law, at least in respect of any requirement for a work of artistic craftsmanship to have aesthetic appeal.

Practical tips

The future development of UK copyright law is uncertain – in particular whether functional items, lacking aesthetic appeal, may nevertheless have copyright protection. Following Brexit, any inconsistencies between UK and EU law remain (and further divergence is possible).

In the meantime, carefully consider whether works (in the broadest EU sense) might attract copyright protection, rather than applying a traditional, narrower UK analysis of copyright subsistence for particular categories of work.

Spring 2020

Intellectual property

Trade marks: Specifications and bad faith

Sky Plc & Ors v SkyKick UK Ltd & Anr

The question

Is an EU trade mark invalid on the basis of an overly broad specification of goods/services?

The key takeaway

An EU trade mark will not be declared invalid on the ground of lack of clarity and precision of its specifications. Further, a lack of intention to use an EU trade mark is not in itself a ground for bad faith.

The background

Sky Plc (**Sky**), the large media and telecommunications company, brought trade mark infringement and passing off claims against SkyKick UK Limited (**SkyKick**), a business that provides software solutions to SMEs.

Initially, it was determined that SkyKick had infringed some of Sky's UK and EU trade marks as SkyKick were using marks that were similar to Sky's trade marks in the same goods and services categories and some customers would confuse the two brands.

The relevant issues arose on SkyKick's counterclaim where they argued that Sky should not be able to assert their rights over industries where they do not act, eg cloud computing software tools. As Sky technically had protected marks in respect of computer software and data storage, SkyKick argued that Sky's marks (i) should be invalid as their trade mark specifications lacked clarity and precision and (ii) were registered in bad faith as Sky lacked intention to use them in relation to the specified goods or services.

The High Court referred these questions to the CJEU.

The decision

Departing from the Advocate General's Opinion on the matter, the CJEU ruled that:

- an EU trade mark cannot be deemed wholly or partially invalid after registration on the ground that the specification lacks clarity or precision. Using broad terms such as "*computer software*" (which Sky had used to assert their rights), were not contrary to

public policy and did not "*confer on the proprietor a monopoly of immense breadth which cannot be justified by a commercial interest*".

- a lack of intention to use an EU trade mark is not in itself a ground for bad faith. The CJEU did however set out a test for finding bad faith, noting that a trade mark application will only be found to have been made in bad faith if the trade mark applicant had the intention of:

  – undermining the interests of third parties in a manner inconsistent with honest practices
  – obtaining, without even targeting a specific third party, an exclusive right for purposes other than those falling within the functions of a trade mark.

The CJEU also confirmed that, where bad faith was established in respect of certain categories applied for, then only that part of the trade mark will be invalidated.

Why is this important?

There could have been significant implications for trade mark owners if the CJEU had decided that a finding of bad faith against part of a trade mark registration would result in the whole of that registration being invalidated – leaving those holding wide registrations vulnerable to wholesale strike out of their trade mark rights as a result of invalidity challenges.

This decision should therefore be a welcome relief for brand owners seeking to maintain broader protection (albeit less so for companies seeking to clear new brands, as this decision will do little to "*de-clutter*" the trade mark register of overly broad registrations).

Practical tips

When considering making trade mark applications with wide specifications, it remains prudent to balance the scope of possible protection (and opportunity for further growth) against seeking to cover industries where you do not plan to operate.

Despite the CJEU's decision, trade mark applicants should remember that the bad faith test will still apply (and the UK does require an intention to use). In addition, whilst trade mark applicants will not be unduly restricted in applying for trade marks with wider specifications, that does not remove the benefit of appropriate specifications to reduce the risk of objections from third parties at the application stage and avoid possible disputes.

Spring 2020

Data protection

ICO consults on new direct marketing code of practice

The question

What is new about the ICO's proposed new Direct Marketing Code of Practice (the **New Code**)?

The key takeaway

The ICO states that it intends the New Code to apply to all processing of data for "*direct marketing purposes*". This includes all processing activities that lead up to, enable or support the sending of direct marketing by an organisation or a third party. If the intention of the processing is direct marketing, it will be caught! Examples the ICO has selected include: (i) collecting personal data to build a profile of an individual with the intention to target advertising at them; (ii) list brokering; (iii) data enrichment; and (iv) audience segmenting.

The background

As required by the Data Protection Act 2018, the New Code will supersede the ICO's existing Direct Marketing Guidance. The public consultation on the New Code was launched on 8 January and ended on 4 March. The aim of the New Code is to provide practical guidance and promote good practice in respect of processing for direct marketing purposes in compliance with data protection and e-privacy rules.

The development

Whilst we await the final version, here are a few of the key takeaways from the current draft:

Sending direct marketing messages

The New Code reiterates that no matter which method is used for sending direct marketing messages, the GDPR will apply when personal data is processed. The New Code advises businesses to keep a "*do not email or text*" list (also known as a suppression list) of those who object or opt out of direct marketing.

Social media platforms

When using social media presence to target direct marketing at individuals or using the platform's advertising services and technologies, the New Code stresses the need to be clear about what data is being used and why.

Tracking

The use of location-based marketing techniques must be transparent. People should also be told about the type of tracking. The New Code states that it will be difficult to demonstrate the legitimate interests requirement when using location-based marketing, as it is unlikely to be in people's reasonable expectations that their location will be tracked in order to send them ads.

Service messages

Consent is not required where a company sends a service message to an individual (such as a telecommunications company texting an alert of 90% of monthly data usage). In determining what a service message is, factors such as tone and phraseology will be key.

Viral marketing "*tell a friend campaigns*"

The New Code states that viral marketing "*tell a friend campaigns*" are likely to breach the Privacy and Electronic Communications Regulations 2003 (**PECR**) as it is almost impossible to obtain valid consent, particularly as the instigating organisation: (a) has no direct contact with the ultimate recipients; (b) will not know what the referring individual has told their friends about the processing; and (c) will not be able to verify whether the friend provided GDPR standard consent.

Providing notice for indirectly collected data

The ICO clarifies that where an organisation buys in data from a third party it can send out the privacy information alongside the marketing materials provided that: if applicable (a) valid consent has been obtained under PECR; and (b) the privacy information (required under Article 14, GDPR) is sent within one month of obtaining the data.

Publicly available information

An individual posting their details on social media is not an agreement to his/her content being analysed and for them to be profiled for direct marketing purposes. If an organisation collects publicly available personal data, as a controller it must still comply with the GDPR and PECR.

Why is this important?

Once adopted, the ICO says it will monitor compliance with the New Code through proactive audits. It has also said that direct marketers who do not follow the New Code will find it difficult to demonstrate that their processing complies with the GDPR or PECR.

Any practical tips?

Remember that all processing activities that lead up to, enable or support the sending of direct marketing will be caught by the New Code. Basically, if you're thinking of collecting or using any data for any direct marketing activities, you are likely to need to follow the new guidance.

Spring 2020

Data protection

Adtech and the data protection debate – where next?

The question

How has the discussion surrounding the regulation of real-time bidding (**RTB**) evolved since the publishing of the ICO's Adtech Update Report last June?

The key takeaway

The ICO considers the lawfulness of the processing of special category data in the industry, the lack of explicit consent for that processing, and the use of contractual clauses to justify compliance with data law as areas of concern in RTB. If industry participants do not engage with reform, the ICO has indicated it may take formal regulatory action.

The background

The ICO issued its Adtech Update Report on RTB back in June 2019. This concluded that the adtech industry appeared to be immature in its understanding of data protection requirements under GDPR for RTB. As a result, the ICO embarked on a 6-month fact-finding mission to further enhance its understanding of industry practices by consulting with industry participants. Upon the conclusion of this 6-month process, the ICO delivered an update on its findings, noting that the discussion has progressed to recognition that real change is needed.

The guidance

Whilst there are encouraging signs from the industry, some of the activity the ICO observed was considered unlawful, indicating that there is significant work to be done. The ICO considers there are 3 main areas that the industry should address:

- the lawfulness of processing special category data
- the lack of explicit consent by users for the processing of their special category data
- the reliance on contractual clauses to justify onward data sharing to achieve compliance with the law in the absence of supporting case studies.

Why is this important?

The ICO was struck by number of insufficient justifications for the use of legitimate interests as the lawful basis for the processing of personal data in RTB. As Simon McDougall (Executive Director for Technology and Innovation at the ICO) says, some organisations appear to "*have their heads firmly in the sand*" and the Data Protection Impact Assessments (**DPIAs**) the ICO has seen "*have been generally immature, lack appropriate detail, and do not follow the ICO's recommended steps to assess the risk to the rights and freedoms of the individual*". Basic data

protection controls around security, data retention and data sharing are also often seen to be insufficient. As Mr McDougall says, "*those who have ignored the window of opportunity to engage and transform must now prepare for the ICO to utilise its wider powers*".

Any practical tips?

This all points towards a hardening of the ICO's line, and regulatory action seems increasingly inevitable. If you have not done so already, you should consider:

- ensuring that senior management understand that industry practices are changing and encouraging them to review their current approach
- carrying out (deep-reaching) DPIAs of your RTB activities
- employing a privacy by design approach to your use of RTB
- keeping engaged with your industry trade associations, both to make sure your voice is heard in the ongoing discussions and to track their best practice recommendations, in particular those of the Internet Advertising Bureau.

Spring 2020

Data protection

ICO monetary penalty notice against DSG Retail Ltd for data breach

The question

What factors did the ICO take into account when issuing the maximum £500,000 penalty (under the old Data Protection Act) against DSG for a data security breach relating to its Point of Sale (**POS**) payment terminals?

The key takeaway

The ICO confirmed what many already know about acceptable security standards, namely that the key elements include: the type and volume of the data concerned; the nature, size and resources of the business; the prior knowledge of and timely response to known vulnerabilities; and compliance with industry standards.

The background

In May 2017 DSG, better known as Curry's PC World and Dixons Travel, commissioned IT consultants to assess its POS payment terminals across its stores to determine compliance with PCI DSS standards (operational security standards for organisations handling payment cards). Although the result of the assessment was that the system was not PCI DSS compliant due to various vulnerabilities, DSG was slow off the mark to remedy the issues and ensure that its systems were of the necessary security standards.

By April 2018 (notably just before GDPR took effect in May 2018), DSG became aware that its in-store POS payment terminals had been compromised. It was found that, for a period of nine months (July 2017 to April 2018), a cyber-attacker had taken control of numerous domain administrator accounts to install malware onto DSG's POS systems which accessed the payment card details of 5.6 million customers (although it was found that only 85 cards had been subjected to potentially fraudulent use) and gathered the non-financial personal data of approximately 14 million customers (including full names, postcodes, telephone numbers, email addresses and failed credit checks) from DSG's servers.

DSG received almost 3,300 customer complaints in respect of the breach, whilst the ICO recorded 158 complaints.

The decision

According to the ICO, DSG's data security processes fell below the basic minimum standards expected by the ICO as a result of various wide-ranging systemic failures, including:

- insufficient network segregation to contain the attack
- lack of local firewalls on the POS terminals to avert an attack
- systemically inadequate software patching
- irregular performance of vulnerability scanning
- inadequate incident response systems
- outdated and mismanaged software, including systems which do not support Point-to-Point encryption
- mismanagement of application white-listing across POS terminals
- mismanagement of the security of its domain administrator accounts
- failure to adhere to industry standard hardening guidance.

The ICO saw each of the inadequacies above as significant enough in their own right to be a contravention of the requirement to have appropriate data security. However, on a cumulative basis, the ICO considered the breach to have been a serious multifaceted contravention of the seventh data security principle in the Data Protection Act 1998 (**DPA 1998**) (its equivalent in the GDPR is Article 32), namely the requirement to keep data secure.

The ICO issued the maximum penalty under the DPA 1998; a £500,000 fine. In deciding to impose the maximum monetary penalty against DSG, the ICO pointed to several aggravating factors, including:

- the nine month delay in identifying the security breach
- the fact that DSG was aware of certain vulnerabilities due to the earlier PCI DSS assessment but did not adequately expedite its reaction to the issues identified (ie by ensuring that PCI DSS industry standard procedures and technologies were subsequently implemented and maintained (regardless of the cost))
- that as a large high-profile retailer controlling vast sums of financial and non-financial personal data, DSG would be expected by the public to lead by example in respect of data security
- the nature of the breach and the substantial distress caused to the individuals affected (supported by the fact that DSG had issued a press release recognising the 'upset' caused)
- that the ICO had previously fined Carphone Warehouse, a company belonging to the same group as DSG, £400,000 at the beginning of 2018 for similar security failings.

The ICO did consider some mitigating factors in DSG's favour such as the fact that DSG had taken steps to notify potentially affected customers, cooperated fully with the ICO investigation and invested significantly in its data security to avoid future breaches. Nonetheless, the ICO considered the maximum penalty to be appropriate in the circumstances. DSG is reportedly appealing the fine.

Why is this important?

A decision by the ICO to impose the maximum penalty under the DPA 1998, and its comment that "*the fine would inevitably have been much higher under the GDPR*" serves as a further reminder just how seriously the ICO takes data security breaches. As such, this decision is helpful in determining which factors the ICO will take into account when determining whether a business' security standards will fall below those expected by the ICO, including the nature, size and resources of that business, the type and volume of data, prior knowledge of and timely response to any known vulnerabilities and compliance with industry standards.

Additionally, given the number of complaints already received, it is still possible that DGS may be subject to potential civil action brought by those customers affected by the breach. If such a claim is forthcoming, this would provide welcome insight into how the civil courts intend to deal with such damages claims post the recent *Lloyd v Google* ruling.

Any practical tips?

Businesses should ensure that they proactively maintain proper security systems and processes, in accordance with both the ICO's expectations and also industry standards and guidelines. If testing of systems is carried out (such as happened with DSG's POS payment systems), then senior management should be warned on the way into those tests that they may need to spend time and money (quickly) fixing any deficiencies which are unearthed, particularly if they relate to data security.

Spring 2020

Data protection

ICO issues monetary penalty notice against Cathay Pacific for data breach

The question

When is the ICO likely to impose its maximum fine for a data breach?

The key takeaway

The costs of getting IT systems right can appear relatively light when compared to the fines, claims and reputational damage that a business can be exposed to from a data breach.

The background

Cathay Pacific (**Cathay**) is an airline headquartered in Hong Kong. Cathay conducted its UK operations out of an office in Hammersmith. The servers used by the office held customer data including names, dates of birth, passport numbers, nationalities and loyalty programme data. In October 2014 Cathay's systems were accessed by an unauthorised third party in the start of a 3.5 year cyber-attack. The data of more than 9.4 million data subjects was affected. Cathay self-reported the attack to the ICO on 25 October 2018. More than 12,000 customers have since submitted complaints to Cathay.

Cathay's London office qualifies as an establishment and brings it within the scope of the Data Protection Act 1998 (**DPA 1998**). Under the DPA 1998, data controllers are required to comply with a number of data protection principles. Data Protection Principle 7 (**DPP7**) requires that the data controller takes appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to personal data.

The development

The ICO found that Cathay Pacific was in breach of DPP7 based on the following:

- **databases were not encrypted**: Cathay had failed to comply with its own policies
- **the internet-facing server was potentially accessed via a publicly available vulnerability**: Cathay's systems had not picked this up despite the vulnerabilities having been published on the Common Vulnerabilities and Exposures system in 2007
- **the administrator console was publicly accessible via the Internet**: the console should only have been accessible to Cathay employees and authorised third parties
- **Server A was hosted on an operating system that was no longer supported**: as a result, security updates were no longer available

- **Cathay could not provide evidence of server hardening**: unnecessary applications and services had not been removed in accordance with Cathay policy
- **network users were permitted to authenticate without multi-factor authentication**: a simple authentication process made access easier for unauthorised third parties
- **the anti-virus protection was inadequate**: there was no anti-virus software installed on some of the servers
- **patch management was not carried out regularly**: the logs showed periods of time where security updates and patching were not completed
- **forensic evidence was not preserved for the ICO's further review**
- **accounts were given inappropriate privileges**: several of the compromised accounts unnecessarily had full administrator rights
- **penetration testing was inadequate**: some servers had not been penetration tested for three years
- **retention periods were too long**: for example, the loyalty scheme data was held indefinitely and was only deleted after seven years of inactivity.

The ICO found that the breaches on the part of Cathay were particularly serious because of the large number of individuals affected and the long period over which they had taken place, as well as the potential for fraud to be carried out using the data obtained. The breaches were likely to have caused substantial distress or harm to data subjects. The ICO also found that Cathay had been negligent in its actions by failing to follow its own procedures and to remedy ongoing issues. Whilst Cathay had acted to improve its systems and help the ICO once the inadequacies had been identified, this was to be expected of an organisation of its size. The ICO issued the maximum Monetary Penalty Notice available under the DPA 1998 (£500,000).

Why is this important?

The ICO can issue fines under DPA 1998 or the GDPR (depending on the timing of the breach) whether or not a business is headquartered in the UK. Those with a presence in the UK or an EU member state have no option but to invest properly in data protection compliance if their senior management want to sleep soundly at night, particularly given the scale of fines now available to the ICO and other European regulators under the GDPR.

Any practical tips?

Share this snapshot with your IT Director! Understanding where others have failed in data security processes help focus the collective mind and, could trigger an internal investigation which (under the GDPR's increased fining regime) could literally save your business millions.

Spring 2020

Data protection

Schrems II - Advocate General's Opinion

Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd

The question

Are the standard contractual clauses (**SCCs**) compatible with the requirements of data protection legislation, irrespective of the level of protection in the country of transfer?

The key takeaway

The Advocate General recommended that the CJEU upholds the validity of the SCCs, on the basis that they provide a valid mechanism of transfer regardless of the level of protection in the country of transfer.

The background

The SCCs are clauses issued by the European Commission that offer safeguards on data protection for the international transfer of data. A complaint was made to the Irish Data Protection Commissioner (**DPC**) by the privacy activist, Max Schrems. Mr Schrems complained about Facebook Ireland transferring his data outside the EU to Facebook Inc in the USA. The US data processing was authorised based on the SCCs, however Mr Schrems argued that the US regime did not provide the data protection safeguards he was entitled to under EU law.

The DPC had concerns that there was no sufficient US remedy for an EU citizen, whose personal data may be at risk of being accessed by US state agencies for national security purposes, in a way that was incompatible with the EU Charter of Fundamental Rights. The DPC sought a ruling on the validity of the SCCs.

The decision

The Advocate General noted that, if the European Commission has not decided that the level of protection in a third country is adequate, the data controller can proceed with the data transfer if sufficient safeguards are in place; the SCCs can be one of these safeguards.

The Opinion discusses two methods of ensuring GDPR protections on data transferred to third countries are met. One is an adequacy decision – the third country's law and practices awards protection equivalent to the GDPR, read in the context of the EU Charter. The second is the

use of the SCCs, which contractually ensure the required level of protection regardless of the level of protection guaranteed in the third country.

However, there must be a method of ensuring that SCC-based transfers can be suspended or prohibited where those clauses are breached or impossible to honour.

Why is this important?

An obligation appears to be imposed on companies and foreign authorities to suspend or prohibit data transfers where there is a conflict between the SCCs and the third country's laws. Hence data importers should review their transfers and inform the exporter should compliance with the SCCs be impossible due to national security laws in the importers' jurisdiction.

Companies are expected to review the national security laws of the data importer to ascertain compliance and examine all transfers made under SCCs carefully.

Although the Advocate General's opinion is not binding, it provides a useful perspective to the CJEU when it makes its final decision.

Any practical tips?

Don't relax quite yet. We await the CJEU's final decision, and it does not necessarily always follow the Advocate General's lead. Also, the Advocate General expressed doubts as to the validity of EU-US Privacy Shield. With the death of the Safe Harbour regime still in recent memory (Schrems I), it feels like there could be yet further change in the shifting sands of international data transfers. For now, the SCCs remain your best bet.

Spring 2020

Data protection

EPDB guidelines: Data Protection by Design and by Default

The question

How familiar are you with the obligations in the GDPR to protect personal data by design and default (**DPbDD**)? And what practical measures can you take to help ensure compliance?

The key takeaway

Data protection by design needs to be implemented both at the time of determining the means of the processing and at the time of processing itself. The latter means that an assessment of the effectiveness of the chosen measures and safeguards must take place on an ongoing basis. Implementing technical and organisational measures by default means only processing personal data which is necessary for each specific purpose.

The background

Article 25 GDPR specifies that data controllers must:

- **Art 25(1)**: "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing…both at the time of the determination of the means of the processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement the data protection principles, such as data minimisation*.."
- **Art 25(2)**: "*implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed*."

In November 2019, the EPDB published detailed guidance on how organisations can comply with Article 25 GDPR and the associated data protection principles. The guidance includes examples of best practice, which help add meaning to the concepts set out in Article 25.

The guidance

Data protection by design

According to the EPDB guidelines, data controllers should use measures designed to implement data protection principles:

- at the time when the data processing is being planned – by considering the concrete elements of the design including architectures, procedures, protocols and layouts
- when the data is actually being processed – by implementing appropriate safeguards
- on an ongoing basis – by continuing to re-assess and consider the safeguards in place.

The EDPB reminds controllers of their accountability for any third-party technology they use and recommends that they:

- include in their contracts with technology providers a requirement to notify the controller of any changes to the 'state of the art' which may impact the effectiveness of the measures being currently deployed
- require their providers to demonstrate accountability on how they are complying with DPbDD (eg through key performance indicators) and to push for transparency (eg through certification or via guarantees that they are DPbDD compliant)
- consider the costs in terms of money and economic advantage, plus time and human resources – and weigh up the potential cost of fines as a result of non-compliance
- mitigate risk when observing data protection by design, by carrying out Data Protection Risk Assessments (**DPIAs**).

Data protection by default

The EPDB guidance explains that data controllers must implement appropriate technical and organisational measures by default and that this means taking the principle of data minimisation into account when configuring systems and processes. Default settings should process as little data as possible to achieve the purpose. This may mean turning off parts of an off-the-shelf software product if certain functionalities are not necessary to achieve the purpose. Equally, it may mean that data is anonymised or deleted if it is not needed after it has been processed. Access should also only be granted to those who need it when necessary.

Why is this important?

The EPDB stresses the "*crucial part*" DPbDD plays in protecting privacy and stresses the use of effective compliant technologies.

Any practical tips?

Review your processes and systems in line with the EPDB's new guidance and consider what you can do to reinforce your policies and procedures to bring them in line with DPbDD. Also, review your contracts with existing third-party service providers (noting any terms that might need updating on renegotiation). Finally, don't forget the importance of DPIAs!

Spring 2020

Data protection

CJEU's CCTV ruling: guidance on legitimate interests processing

Case C-708/18 TK v Asociaţia de Proprietari bloc M5A-ScaraA EU:C:2019:1064

The question

When can you rely on the legitimate interests basis for processing personal data?

The key takeaway

Remember to carry out the three-stage test, namely the "*purpose test*", the "*necessity test*" and the "*balancing test*", when weighing up the processing of personal data on the legitimate interests basis. Also, don't forget to assess whether alternative means are available to meet the same objective of the processing and to apply the condition only in so far as is strictly necessary,

The background

The co-owners of a Romanian apartment block installed CCTV cameras in the common parts of the building. TK, who owned an apartment in the building, objected and brought an action seeking the removal of the cameras on the grounds that the cameras amounted to an infringement of the right to respect for private life.

The Romanian court decided to refer the case to the CJEU for guidance on whether Articles 6(1)(c) and 7(f) of the Data Protection Directive (95/46/EC), read in light of Articles 7 and 8 of the EU Charter of Fundamental Rights, precluded national law from allowing installation of a system of video surveillance in the common parts of a residential building, for the purposes of pursuing legitimate interests in ensuring the safety and protection of individuals and property, without the data subjects' consent.

The considerations

The CJEU observed that surveillance in the form of a video recording of persons, which is stored in a continuous recording device (ie the hard disk drive) constituted automatic processing for the purposes of Article 3(1) of the Directive. Such processing must comply, first with the principles relating to data quality (set out in Article 6) and also with one of the criteria for making processing legitimate (listed in Article 7).

The relevant criterion here was the legitimate interest basis for processing personal data. The court identified three cumulative conditions needed for processing of personal data to be lawful under the provision:

- The pursuit of a **legitimate interest** by the data controller or by a third party or parties to whom the data is disclosed
- The **need** to process personal data for the purposes of the legitimate interest pursued, and
- A **balancing exercise**, namely the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued.

To satisfy the **legitimate interests** condition, the interest must be proven to be present and effective at the time of processing. According to the CJEU, the requirement of present and effective interest was satisfied given the instances of theft and vandalism at the building prior to the installation of the CCTV cameras.

The CJEU re-emphasised that the legitimate interests condition requires processing to apply only so far as "**strictly necessary**". This means the objective "*cannot reasonably be as effectively achieved by other means less restrictive of the fundamental freedoms*." The CJEU turned to the data minimisation principle (under Article 6(1)(c)). Here, alternative measures were initially put in place but proved insufficient. For example, the installation of an intercom/magnetic card entry system had failed to prevent damage being caused to the apartment block. Additionally, the video surveillance device was limited only to the common parts of the building and the approach to it. The CJEU further considered whether it was necessary for the CCTV system to run constantly, or only at certain times of the day and night.

In carrying out the fact specific **balancing exercise**, the CJEU stated that factors such as the nature of the personal data at issue, the specific methods of processing involved, the number of persons having access to the data and the methods of accessing the data need to be considered. Additionally, the data subject's reasonable expectations of their data being further processed needs to be balanced against the legitimate interests of the building owners in protecting the property, health and lives of the building's occupants.

The decision

The CJEU concluded that the Directive, read in the light of the Charter, did not preclude national law authorising the installation of a video surveillance system, for the purposes of pursuing legitimate interests in ensuring the safety and protection of individuals and property, without the consent of the data subjects. The processing of this data satisfied the conditions in Article 7(F).

Why is this important?

The case provides a rare analysis of legitimate interest processing, and re-states the three test rule formed in Case C-13/16 *Rigas satiskme* EU:C:2017:336, namely the "*purpose test*", the "*necessity test*" and the "*balancing test*".

Any practical tips?

Consider whether there are alternative ways of meeting the same objective of the processing. Here the fact that the co-owners of the apartment building had tried other means to combat the damage to their property (eg the previous, failed installation of intercom/magnetic card entry) was of particular importance to the court. And remember to apply the condition in so far as is strictly necessary (eg with CCTV, consider whether all of a building needs to be recorded, or whether there are specific times that need to be recorded only). Ensure also that the data is only accessible to those necessary to satisfy the legitimate interests conditions.

Spring 2020

Digital

Online Harms White Paper: consultation response

The question

What has been the Government's response to the initial consultation on the Online Harms White Paper (**White Paper**)?

The key takeaway

Due to its organisational experience and robustness, Ofcom will be the new online harms regulator. Ofcom's responsibilities will include ensuring that online companies have processes and systems in place to fulfil their duty of care to keep people using their platforms in a safe manner.

The background

In April 2019, the White Paper was released. This set out the Government's intention to improve protections for users online through imposing a duty of care on online services to moderate a wide spectrum of harmful content and activity on their services, including child sexual abuse material, terrorist content, hate crimes and harassment. Following the release of the White Paper, a consultation was run from 8 April 2019 to 1 July 2019, which received over 2,400 responses from companies in the technology industry, including think tanks, rights groups, governmental organisations, individuals and large tech giants. On 21 February 2020, the UK Home Office and Department for Digital, Culture, Media & Sport published the Government's Initial Consultation Response to feedback received through a public consultation on its White Paper.

The guidance

Scope of regulation

The White Paper introduced a new duty of care that would apply to any online service that either (1) facilitates the hosting, sharing, or discovery of user-generated content; or (2) facilitates online interactions between users. Business to business services would fall outside the scope of this regulation. The duty of care will only apply to companies that facilitate the sharing of user generated content, such as through comments or video sharing. According to the UK government, only a very small proportion of UK businesses (less than 5%) will fit within the definition of who the duty of care applies to.

Scope of the duty of care

The White Paper introduced a new duty of care on companies to ensure that all companies have appropriate systems and processes in place to react to concerns over harmful content

and improve the safety of their users. These include compliant mechanisms (that are effective!) and transparent decision-making over actions taken in response to reports of harm. The Government indicated that it will take a different approach to content and activity that is illegal (such as hate crimes) as opposed to harmful but legal content (such as cyberbullying). While the duty of care will require companies to expeditiously remove illegal content from their services, they will not have a similar obligation to remove legal content. Instead, companies will have to state publicly what content and behaviours are unacceptable on the service (for instance in their terms of service), and to have systems in place to enforce these statements consistently and transparently.

Freedom of expression

The UK government has explained that it recognises the importance of free speech. Companies will now be required, where relevant, to state what content and behaviour they deem to be acceptable on their sites and enforce this consistently. A higher level of protection is required for children, and services in scope will need to ensure that illegal content is removed expeditiously.

The regulator

Ofcom will be the independent regulator as it has a proven track record of experience, expertise and credibility. It will be equipped with the powers, resources and expertise it needs to effectively carry out its new role. Ofcom's focus on the communications sector means it already has relationships with many of the major players in the online arena. The Response does not define the sanctioning powers that will be available to Ofcom, but it suggests that these may include the power to issue fines, impose liability on senior managers and, in certain circumstances, require companies to improve systems or even engage in measures like ISP blocking.

Age verification and transparency requirements

In-scope service providers will need to implement appropriate age verification technologies to prevent children from being exposed to inappropriate content. They will also need to adopt certain transparency measures depending on the type of service and risk factors involved. As such, the regulator will be able to require companies to submit annual reports explaining the types of harmful content on their services, as well as information on the effectiveness of the company's enforcement procedures.

Why is this important?

Companies within scope will be required to have appropriate processes and mechanisms in place, if not there already. Terms and conditions will also need to be amended to comply with the duty of care and codes of practice will need to be clear and accessible to all (including children). Ensuring compliance will be important as Ofcom is likely to have the power to

impose fines, disrupt business activities, block services and impose liability on individual members of senior management for non-compliant organisations.

Any practical tips?

While many platforms are already ramping up their efforts to combat harmful content, the impact of the new duty of care needs to be considered very seriously, not least as the Government stated in its response that "*online harms is a key legislative priority*". To underline this, the Government also said that it will start working on interim codes of practice with law enforcement and industry bodies to tackle terrorism and child exploitation in the meantime (ie while it waits for Ofcom to step into its new role).

Spring 2020

Digital

European Commission proposal for new Digital Services Act

The question

What's in the European Commission's proposal for a new Digital Services Act (**DSA**)?

The key takeaway

The European Commission is preparing a proposal for a DSA which is expected to recalibrate the way in which online platforms are responsible for the content on their services.

The background

Newly elected president Ursula von der Leyen of the European Commission has announced a sweeping digital strategy for member states for 2019-2024. The strategy focuses on three pillars: digital enablement and protection for individuals (including AI regulation and broadband availability), fair competition and sustainability. As Ms von der Leyen states: a DSA "*will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Mark*et." The DSA would serve as a basis for an upgrade of the E-Commerce Directive, which was adopted in 2000 and new rules on platforms.

The development

The European Commission has indicated that a public consultation will be held in the first quarter of 2020 and more legislative proposals will be published at the end of 2020. No wording has been put to paper yet, however the following issues are likely to feature in the Commission's plans for the DSA:

- **liability**: The DSA is expected to upgrade liability and safety rules for digital platforms, services and products to incentivise companies to remove unlawful and harmful content. Under the DSA, platforms may be subject to further obligations in the form of "*notice and take down*" orders
- **the question of anonymity online**: The ability to provide anonymous content online is important for several reasons. However, one of the many issues with harmful and unlawful content on online platforms is that the content provider is very difficult to identify and usually resides outside of the jurisdiction of EU Member State courts. It is seen as a great benefit if platforms were able to identify those content providers who are providing the harmful and unlawful content

- **enforcement**: The E-Commerce Directive does not provide an enforcement mechanism, therefore it is likely that the DSA will introduce this to both strengthen the internal market and ensure coherent enforcement across the EU
- **good samaritan protection for platforms**: This notion protects platforms when they take voluntary measures to restrict access to or availability of certain content, but also protects them when they miss such content. The rationale for this protection is to encourage platforms to take voluntary proactive measures to address unlawful and harmful content made on their services.

Why is this important?

This pan-EU initiative seeks to regulate social media platforms, search engines, video gaming platforms, and online marketplaces. This has gained enormous public and media attention as platforms have been pressed to act on their own accord to remove and monitor unlawful and harmful content. The proposals drawn up in the DSA will affect not only the entire technology sector, but potentially any service relying on user-generated content to any extent.

Any practical tips?

Act now! Businesses need to engage now to ensure that the new Commission understands the wide range of services that they are proposing to regulate. Businesses should also assess their platforms and implement plans and procedures to tackle unlawful and harmful content displayed across their services.

Spring 2020

Consumer

New EU Consumer Protection Co-operation Regulation comes into force

The question

What does the revised EU Consumer Protection Cooperation Regulation (**CPC**) mean for traders and consumers?

The key takeaway

The CPC was introduced by the European Commission to ensure compliance with consumer legislation across the EU and increase legal certainty, especially for traders and consumers engaged in cross-border activities. It strengthens the powers of national authorities to detect irregularities and take speedy action against traders operating in the e-commerce environment. Authorities should now be able to act faster, save costs and operate via a single coordinated procedure.

The background

The CPC came into force on 17 January 2020. It is intended to address wide-scale problems such as the fact that almost 70% of cross-border consumer complaints relate to e-commerce transactions. The CPC improves the previous EU-wide cooperation framework which enabled national authorities to work together to address breaches of consumer protection law in cases where the trader and the consumer are in different EU countries.

The development

The CPC introduces the following solutions, to ensure that cross-border infringements of EU Consumer law are detected and dealt with:

- it connects the European national authorities responsible for enforcing consumer protection laws to form the 'CPC Network'. The CPC Network enables authorities to share best practices and provides a mutual assistance mechanism (as introduced by the previous Regulation EC 2006/2004 and adopted in the CPC)
- all national authorities gain a minimum level of investigation and enforcement powers to enforce EU consumer laws. National authorities are now allowed to order the takedown of websites, order the restitution of profits or damages to consumers, and request information from domain registrars, internet service providers and banks to identify the infringing trader

- it provides for the right to take action against previous infringements, subject to a limitation period of five years and introduces the following two categories of infringements to allow for a more effective response from national authorities:
  - **widespread infringements**: Member States will be required to launch coordinated action in cases of infringements of EU consumer law affecting at least two Member States
  - **widespread infringements with a EU-wide dimension**: the Commission will coordinate any necessary actions itself and liaise with the relevant national authorities in cases of infringements which affect at least two-thirds of Member States and two-thirds of the EU population
- national authorities are required to alert the Commission and other national authorities if they suspect an infringement in their territory that may affect other Member States. Consumer and trader organisations will also be given the opportunity to alert the competent authorities and the Commission.

Why is this important?

National consumer authorities' investigation and enforcement powers are now broad, including financial penalties for infringements covered by the CPC, which can be up to at least 4% of the trader's annual turnover in the respective Member State or based on the trader's worldwide turnover. However, the CPC does not stipulate an EU-wide penalty regime and therefore the same domestic penalty regimes will apply. National authorities also have powers to order websites or social media accounts containing scams to be corrected, obscured or removed. It can also request information from domain registrars, internet service providers and banks to track financial flows and find out the identity of those behind bad practices. However, such powers will be limited by a strict proportionality test. This means that the use of powers must be necessary to avoid the risk of serious damage to the collective interests of consumers and may only be used if no other effective means are available.

Any practical tips?

It's not just the GDPR which contains the potential for huge fines by national authorities. The CPC may prove to be a highly effective weapon in forcing traders to curb wrongful trading which occurs on a cross-border basis. EU-wide traders should pay close attention and check that their web-based activities don't land them in (very) hot water.

Spring 2020

Influencer marketing

Online Affiliate Marketing: New CAP advice note

The question

What should brands do to ensure that their affiliate marketing complies with the CAP Code?

The key takeaways

Affiliate marketing must be obviously identifiable and must not mislead materially or cause serious or widespread offence.

The background

Affiliate marketing is a type of performance-based marketing where an affiliate is rewarded by a business for each new customer attracted by their marketing efforts, usually with a pre-agreed percentage of each sale.

The CAP Code applies to affiliate marketing within the categories of communication outlined in the scope of the Code. Content on an affiliate's own website and social media is therefore caught if it's directly connected to the supply or transfer of goods, services, opportunities and gifts. This connection is usually by virtue of the inclusion of a hyperlink, a promotional code or other means by which a new customer or sale can be attributed to a specific affiliate.

Rule 2.1 of the CAP Code requires that marketing communications are obviously identifiable as such. The Code also states that marketing communications must not falsely claim or imply that the marketer is acting as a consumer or for purposes outside its trade, business, craft or profession and that marketing communications must make clear their commercial intent, if that is not obvious from the context (rule 2.3). Accordingly, the CAP Code requires that:

- marketing communications (such as Instagram posts) are obviously identifiable as such
- marketing communications must not falsely state or imply that the author is acting as a consumer
- the author of the communication must make it clear that it has a commercial relationship with the product being marketed, unless it is evident from the context.

The note focuses on affiliate marketing mediums that are not easily recognisable as ads, such as social media, blogs, vlogs, news sites and voucher sites. The note provides practical guidelines on how to make it clear that there is a commercial relationship between the author and the product.

The guidance

Blogs and news sites

The easiest way to ensure that the commercial relationship between the author and the product is clear is to include an identifier, such as "*Ad*", in the title of the article or blog. This should be clear to those reading the title before they click and open the content, as well as to those reading the article or blog. Although not required by the CAP Code, the note also recommends explaining the nature of the relationship between the affiliate marketer and the seller of the product. This could take the form of a short sentence stating that that the marketer receives a share of sales.

Vlogs

As with blogs and news site, vloggers must identify their advertising content in a manner that is obvious to the consumer prior to engagement. CAP proposes that this can be done using on-screen text/signs making clear that this is an "*Ad*" or by simply explaining verbally which elements of the content are "*advertising*". It is important that this is done before the affiliated products are introduced to the consumer. The description should also be similarly forthcoming and transparent.

Social media posts

The underlying principle is that social media posts which include affiliate links should be obviously identifiable as advertising *before* consumer engagement. In terms of practicals:

- if only an image is visible, such as on Instagram, an identifier should be included on the image itself
- on Facebook, where there is no character limit, a post should include an identifier at the beginning
- on Twitter and Pinterest, where there is a character limit, the label should contain "*Ad*" or an equally clear identifier in order to ensure that the rules are complied with.

Voucher sites

Promotional offers on "*voucher*", "*free goods*" and "*deals*" websites should be easily recognisable as advertising if they include affiliate links. Care should also be taken not to mislead the consumer by implying that the website is "*independent*" or that there is no financial incentive behind the content.

Why is this important?

While the headlines tend to focus on celebrity influencers, the advice note reminds us that all forms of affiliate marketing are caught by the disclosure rules and that everyone in the chain needs to understand their obligations around appropriate labelling and the targeting of marketing communications.

Any practical tips?

Don't think that allowing your affiliates to have free rein over the content of your ads relieves you from the responsibility of ensuring that the advertising is compliant with the CAP Code. The ASA 's approach is that both the business and the affiliate marketer are responsible under the Code, notwithstanding the fact that the ads may have been created solely by the affiliate rather than by the business themselves. Similarly, as primary responsibility for observing the Code falls on marketers, promotions run by affiliates that do not adhere to the Code will be equally problematic.

Spring 2020

Influencer marketing

New CAP/CMA Guidance: #Ad(vice) for Influencers

The question

What should influencers do to avoid falling foul of the Committee of Advertising Practice's (**CAP's**) standards on labelling ads?

The key takeaway

The guidance puts it very simply: "Consumers should be able to recognise that something is an ad, without having to click or otherwise interact with it. Since it needs to be clear/obvious, consumers shouldn't have to work to figure it out".

The background

On 6 February 2020, CAP and the CMA published an updated version of the guidance: "*Influencers' guide to making clear that ads are ads*". The new edition takes on board feedback on the original version of the guidance (which was published on 28 September 2018) and further ASA research on ad labelling.

The original guidance attempted to bring together all the advisory information influencers need to ensure they do not breach advertising rules and provisions in consumer protection legislation. In its updated form, the guidance sets out what the relevant rules are, how to make clear ads are ads and who enforces what.

In addition to the updated guidance, CAP has also issued two new advice notes for influencers, namely "*#Ad(vice) – Making clear that an ad is an ad*" and "*Influencing responsibly – the ASA's Jurisdiction*", as well as some general guidance to help ensure that influencer marketing is "*obviously identifiable*". In addition, the ASA published a blog on influencing responsibly called "*Musings beyond the code*". The blog sheds light on some brand and influencer practices which have been observed in light of and despite the rules.

The guidance and advice notes

Some of the most relevant points in the guidance and the two advice notes are as follows:

- when brands have paid influencers, any of the influencer's posts promoting/endorsing the brand or its products/services becomes subject to consumer protection law
- in terms of what counts as "*payment*", the guidance points out that this includes any kind of monetary payment, including a free product/service, whether requested or not, (or loan of the same), commission or any other incentive

- turning to when disclosure of such "*payments*" is necessary, the guidance highlights that this includes situations where influencers refer to or feature a brand/product/service in any way, where the content is controlled by the relevant brand, or in cases of affiliate marketing (eg the influencer posts hyperlinks or discount codes)
- it should be clear when ads are ads and consumers should not have to work to figure this out. It may be more difficult where ads appear alongside organic/editorial content in a similar style and all parties involved in creating or publishing the content are responsible for making sure it is clear that it is an advert or has a commercial message. The guidance recognises that when individuals promote their own products/services on their channels, consumers are more likely to be able to recognise that the content is an ad, whereas influencer marketing or affiliate marketing is less likely to be clear
- ads which are similar in tone to other editorial content are very likely to need a label. Labels should be prominent, up front and capable of making the commercial message "*obviously identifiable*". The label should appear *before* the consumer interacts with the ad (either before viewing it, clicking on it, or otherwise engaging with it). Both the guidance and the #Ad(vice) give examples of labels which are clear (eg "*Advertisement Feature*") and those which are risky (eg "*Sponsored*")
- the #Ad(vice) also highlights that, when targeting under-12s, the fact that an ad is an ad should be made much clearer and gives guidance on how it expects influencers to do this. For example, the #Ad(vice) suggests the label should be prominent (eg in a bright colour), timely (presented at/before the ad is 'activated' or viewed) and the identity of the marketer should be clear
- the advice note "#*Influencing responsibly – The ASA's Jurisdiction*" provides an indicative (rather than exhaustive) guide to what online content falls within the remit of the ASA's jurisdiction. Broadly, the advice note identifies three kinds of ad which the ASA regulates: paid-for space (eg banner ads and pop-ups), advertorials and "*directly connected*" ads (eg non-paid for spaces which are within the control of the brand, such as a brand's own website).

Why is this important?

Influencer marketing remains the go to marketing technique of our times, and the updated guidance and new advice notes should be welcomed as they help reinforce those practices which CAP expects influencers to be implementing.

Any practical tips?

Shape your branding policies to match the guidance and advice notes. And don't forget to set up systems (eg one of your marketing team) to track influencers acting on your behalf – that way you can catch bad behaviours quickly (ie if they fail to disclose correctly) - and before the regulators do!

Spring 2020

Influencer marketing

Influencer marketing and obvious brand references

ASA ruling on idesigngold.com

The question

What if an influencer's post prominently features the brand within the content and caption (ie so it's arguably easily identifiable as an ad)? Do you still need "*#ad*"?

The key takeaway

Featuring a brand within the content (for example, the logo) and the brand's Instagram handle within the caption is not enough to identify a post as an ad. You still need a clear, prominent identifier such as "*#ad*".

The ad

On 28 June 2019, a post on Katie Price's Instagram account featured a video of her receiving a rose gold iPhone from idesigngold.com. In various shots throughout the video idesigngold's branding could be seen on screen and on the product. The caption beneath the video stated, "*Absolutely love my new @idesigngold phone I seem to be the only girl so far to have one check out the site x*."

The complaint

One complainant challenged whether the ad was obviously identifiable as a marketing communication.

The response

idesigngold did not respond to the ASA's enquiries. Katie Price did respond and stated that idesigngold produced the video but that there was no written agreement between them - the product was a gift and idesigngold did not approve the content of the post.

The decision

The CAP Code states that marketing communications must be obviously identifiable as such, and marketers and publishers must make clear that advertorials were marketing communications. The Code defines an advertorial as an advertisement feature, where the content is controlled by the marketer, and is disseminated in exchange for payment or other reciprocal relationship.

The ASA first assessed whether the post was an advertorial, and accordingly within the remit of the CAP Code. The ASA considered that because idesigngold provided the gifted item to Katie Price and had created the video, they had sufficient control over the content for the post to be considered a marketing communication within the remit of the Code.

The ASA then considered whether the advertorial was obviously identifiable as a marketing communication. The caption of the post included the handle @idesigngold and a call to "*check out their site*", as well as the logo for idesigngold.com which appeared in the first few seconds of the video. The ASA found that those elements did not indicate to users that the post was a marketing communication before users engaged with its content. In the absence of a clear and prominent identifier at the beginning of the post, such as "*#ad*", the ASA concluded that the post was not obviously identifiable as a marketing communication.

The ad breached CAP Code (Edition 12) rule 2.1 and 2.4 (Recognition of marketing communications).

Why is this important?

Ads must be obviously identifiable as marketing communications, for example by including a clear and prominent identifier such as #ad. Additionally, this ruling serves as a reminder that brands have a responsibility to provide a response to the ASA's enquiries.

Any practical tips?

Do not assume that because the content features your brand heavily (the brand logo, tagging the brand's Instagram handle in the caption etc) that this sufficiently indicates to a user that an advertorial is a marketing communication. It must also include *"#ad*" or similar and this must be placed prominently within the caption (prominently being upfront rather than in a bio or a click away caption)

Spring 2020

Influencer marketing

Influencer marketing, alcohol and youthful looks

ASA ruling on Sazerac UK Ltd t/a Southern Comfort

The question

What if your influencer appears younger than they are when it comes to posts promoting alcohol?

The key takeaway

Tread carefully when mixing alcohol and influencers. Advertisers must ensure that those drinking alcohol or playing a significant role in their advertising neither are, nor crucially seem to be, under 25 years of age.

The ad

The case concerned two Instagram posts promoting Southern Comfort:

(A) A post on Francesca Perks' Instagram page on 29 October 2019 included the caption "*AD. I can put my hand up and say I'm not a cocktail aficionado by any means, but boy do I love a slushie, so when @southerncomfortuk asked me to put a spin on a shark bite, I knew an adult slushie was the only route to take this down, so that my friends is what I present you with! Head over to my stories to how I conjured up this frozen beauty!*". The post included two images, one showed Francesca holding a cocktail, the other showed the cocktail on a table with a bottle of Southern Comfort in the background.

(B) A post on Jack Remmington's Instagram page on 29 October 2019 included the caption *"#AD So my bezzie mate's fave drink in the world is Southern Comfort and we got creative with this Halloween inspired treat! Obvy cos it's me I wanted to jazz it up and be extra, so have a gander over on my stories to see what we came up with. Let me know what you'd have added to the cocktail to make it extra special! Thank you @southerncomfortuk and @twisted for letting our imagination run wild (and for the beaut bev!)*". The post included two images, one showed Jack and a woman drinking a cocktail, the other showed the cocktail next to a bottle of Southern Comfort.

The complaint

The complainant challenged whether ad (A) breached the CAP Code because it featured someone who seemed to be, or who was, under 25 years of age. The ASA challenged ad (B) on the same basis.

The response

Sazerac UK Ltd t/a Southern Comfort responded that the ads were designed to promote a 'Shark Bite' drink served over the week of Halloween. They said that they engaged Francesca Perks and Jack Remmington to develop their version of the Shark Bite. They said that Ms Perks was 22 years old when the ad was posted. Upon receipt of the complaint, Southern Comfort requested Ms Perks remove the post from her feed to avoid further views. Ms Perks confirmed that she had removed the post upon being notified of the complaint by the ASA and confirmed that in future she would not engage in alcohol related marketing which would breach the Advertising Code. However, in Mr Remmington's post, both he and his friend featured in the ad were 25 years.

The decision

Both ads were found to have breached CAP Code (Edition 12) rule 18.16 (Alcohol). The CAP Code states that when advertisers show people drinking alcohol, or where they play a significant role in a marketing communication for alcohol, they must neither be, nor seem to be, under 25 years of age.

Here, both ads showed images which contained a bottle of Southern Comfort and a cocktail made using the drink. Ms Perks in ad (A) and Mr Remmington and his friend in ad (B) were the focus of the images and the ASA considered that they each played a significant role in their respective ads. Together with the text included in the posts, the ASA found it was clear from the ads' contexts that they were drinking alcoholic drinks.

In relation to ad (A), on the basis that Mrs Perks was 22 years old when the ad was posted, the ASA found that the ad had breached the CAP Code. Although Mr Remmington and his friend were both 25 years old when ad (B) was posted, the ASA also concluded that ad (B) had breached the CAP Code. The ASA found that both men appeared young in the image and that they seemed to be under 25 years old.

Why is this important?

The rulings highlight once again how careful drink brands need to be to ensure that any influencers shown drinking alcohol, or playing a significant role in the brand's advertising, neither are, nor crucially seem to be, under 25 years of age - an impression which may be compounded by the general nature of the images used.

Any practical tips?

When using an influencer to advertise alcohol, think not just about their age, but the impression they are presenting to their audience. Young-looking over 25s, especially those acting in an immature way, may quickly attract the attention of complainants and regulators.

Spring 2020

Gender stereotyping

Gender stereotyping and the use of one gender in an ad

ASA ruling against PC Specialist

The question

Can the use of only one gender in an ad breach the rules on gender stereotyping?

The key takeaway

According to ASA guidance, ads are not prohibited from featuring only one gender. However, an ad should not strongly imply that only one gender can excel in the specialisms and roles depicted in the ad.

The ad

A TV ad for PCSpecialist, seen on 17 September 2019, featured three men performing different activities on computers, including producing music and coding. The male voice-over stated, "*It's the beginning of the end. The end of following. It's the start of freedom, individuality, choice. It's an uprising. An insurgence. For the players, the gamers, the 'I'll sleep laters', the creators, the editors, the music makers. The techies, the coders, the illustrators. Bespoke, customised, like no other. From the specialists for the specialists. PCSpecialist.* "

The complaint

The complainants believed that the ad perpetuated harmful gender stereotypes by depicting men in roles that were stereotypically male and implying that it was only men who were interested in technology and computers. They challenged whether the ad breached the BCAP Code.

The response

PCSpecialist explained that their customer base was 87.5% male, aged between 15 and 35 years. Their product, branding and service had been developed for and aimed at that target audience and the characters in the ad therefore represented a cross-section of the PCSpecialist core customer base. PC Specialist also said it didn't believe the characters in the ad "*represented negative stereotypes*." They stressed there was no comparison between men and women in the ad and it did not imply that women were not interested in computers, and that the ad did not juxtapose men using computers with women not using computers, nor did the ad explicitly state that women did not use computers or that the service was unsuitable for them.

The decision

The ASA highlighted the ad began with a PC exploding and went on to state "*freedom, individuality and choice*" before referencing a number of specialist and creative roles in quick succession, encompassing leisure pursuits and professional positions, not just limited to information technology, but in the creative and artistic industries and entertainment, namely: players/gamers, creators, editors, music makers, techies, coders and illustrators.

The ASA considered that the voice-over and fast-paced series of scenes in the ad conveyed a sense of excitement and opportunity and implied that those depicted in the ad were innovative, highly skilled and achieving excellence in the roles and careers mentioned and that those watching should aspire to excel in them too. However, the ad repeatedly cut to images of only men, who were both prominent and central to the ad's message of opportunity and excellence across multiple desirable career paths. The ASA therefore considered that the ad implied that excellence in those roles and fields would be seen as the preserve of men. Because of that, the ASA considered that the ad went further than just featuring a cross-section of the advertiser's core customer base and implied that only men could excel in those roles.

The ASA upheld the complaints on the basis that the ad breached BCAP Code rule 4.14, which says "*Advertisements must not include gender stereotypes that are likely to cause harm, or serious or widespread offence*".

Why is this important?

While ASA guidance makes it clear that an ad can feature only one gender, they cannot strongly imply that only one gender can excel in the specialisms and roles depicted in the ad. The latter would present gender stereotypes in a way that is likely to cause harm, or serious or widespread offence, and therefore breach the BCAP Code.

Any practical tips?

Gender stereotypical characteristics include occupations or positions as well as attributes or behaviours usually associated with a specific gender. Ads should take care to avoid suggesting that stereotypical roles or characteristics are always uniquely associated with one gender and are the only options available to one gender; or were never carried out or displayed by another gender. One (simple) practical tip is to put the brakes on whenever you see a storyboard for an ad and try and view it through the (very) gender-aware spectacles now being worn by the ASA.

Spring 2020

Gender stereotyping

Gender stereotyping and "that girl boss thing"

ASA ruling against PeoplePerHour

The question

How careful do you need to be with language in an ad against the backdrop of the ASA's new rules on gender stereotyping?

The key takeaway

Screen every statement in your ad from a gender-stereotyping perspective, and don't think that light-hearted phraseology will somehow let you off the hook.

The background

In June 2019, the ASA introduced a new rule which states that ads "*must not include gender stereotypes that are likely to cause harm, or serious or widespread offence*". The *'likely to*' addition has significantly lowered the threshold for breach and led to a stream of ads being banned for gender stereotyping.

The ad

PeoplePerHour is an online platform that connects businesses and freelancers. They ran an ad on the London Underground which featured a picture of a red-haired woman next to text that stated "*YOU DO THE GIRL BOSS THING. WE'LL DO THE SEO THING*", (SEO standing for Search Engine Optimisation).

The response

19 complainants believed that the ad perpetuated harmful gender stereotypes by depicting a woman running a business in a patronising way and by implying that women were not technologically skilled. In response, PeoplePerHour said that the intention of the campaign was to celebrate entrepreneurs and business owners and that the term "*girl boss*" was a reference to a book and popular TV show.

PeoplePerHour acknowledged that the execution might unintentionally come across as sexist and demeaning to women and had therefore taken steps to rectify it by removing the word "*girl*" from the ad and issuing a public apology on their website.

The decision

The ASA upheld the complaints and banned the ad. It said that using the gendered term "*girl boss*", as opposed to just "*boss*", implied that the gender of the person depicted was relevant to their performance in a managerial or entrepreneurial role and that it was also likely to be interpreted that a female "*boss*" was an exception to the norm. Furthermore, the use of the word "*girl*" to refer to an adult woman reinforced the impression that a female "*boss*" was a novelty, playing at their role and somehow less serious than a man in the same position.

The ASA acknowledged that the term "*girl boss*" made reference to a book and TV show about a female entrepreneur and resulting use of that term more widely in popular culture. However, it considered that many people viewing the ad were unlikely to be familiar with that reference.

Why is this important?

This decision provides another example of the ASA's strict interpretation of its new rules on gender stereotyping in ads. Once again, the ASA has demonstrated that it is willing to find that harmful stereotypes are perpetuated even if the underlying intention of the ad was to achieve the opposite reaction, in this case, to celebrate female entrepreneurs, not undermine them.

Any practical tips?

Advertisers should take great care in ensuring that their ads do not suggest that stereotypical roles or characteristics are always associated with one gender. The text of an ad should be reviewed with the new rule in mind, as one word is enough to see an ad fall foul! Catching a potential problem early may save an otherwise clever (and no doubt expensive) campaign from being banned.

Spring 2020

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

38/F One Taikoo Place
979 King's Road
Quarry Bay, Hong Kong
T +852 2216 7000

12 Marina Boulevard
38/F MBFC Tower 3
Singapore 018982
T +65 6422 3000

RPC