RPC

Commercial law snapshots

Winter 2020

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Contents

Commercial

Material Adverse Change Clauses: Use of a MAC Clause during a Global Pandemic

Travelport Ltd v Wex Inc [2020] EWHC 2670 (Comm)

The question

Is it possible for a party to invoke a Material Adverse Change (**MAC**) clause because of the effects of the COVID-19 pandemic?

The key takeaway

Precision is key when drafting specific MAC clauses – clearly detail how a MAC should be measured and any relevant exceptions which alter the risk allocation between the parties.

The background

WEX Inc is a financial technology service provider which offers corporate payment solutions (the **Buyer**). The Buyer had agreed to purchase the parent companies of two business-to-business (**B2B**) payments companies specialising in the travel sector, eNett International (Jersey) Limited (**eNett**) and Optal Limited (**Optal**) from Travelport (the **Sellers**), pursuant to a Share Purchase Agreement (**SPA**) for a total of approximately USD1.7 billion.

Completion of the SPA was subject to a number of conditions, including that there had been no "*Material Adverse Effect, event, change, development, state of facts or effect that would reasonably be expected to have a Material Adverse Effect*" (the **MAC Condition**).

The unprecedented disruption to the travel industry as a result of the global COVID-19 pandemic resulted in a decrease in revenue for the eNett and Optal groups. As such, on 4 May 2020, the Buyer notified the Sellers that the MAC Condition had occurred and so the Buyer was not required to complete the transaction. The Sellers disagreed and issued proceedings to seek (i) a declaration that a MAC had not occurred within the meaning of the SPA, and (ii) specific performance of the Buyer's obligations to complete the transaction.

The definition of "*Material Adverse Effect*" (**MAE**) was central to the dispute, focusing on two express carve outs:

1. An exemption for the effects from causes including specifically "*conditions relating from… pandemics"* (**Pandemics Carve-Out**), and

2. an exception to the Pandemics Carve-Out providing that, even if an event otherwise falls within the Pandemics Carve-Out, an MAE may still exist if its impact had "*… a disproportionate effect on [the eNett or Optal Groups], taken as a whole, as compared to other participants in the industries in which [eNett], [Optal] or their respective Subsidiaries operate.*"(**Carve-Out Exemption**).

The key issue for the Court was the identity of the "*industries*" in which eNett and Optal operated in for the purpose of assessing the Carve-Out Exception. The Buyer argued that it was the general payments industry or the B2B payments industry, whereas the Sellers contended that it was the narrower travel payments industry.

The decision

The Court considered both a textual analysis of the MAE definition and interpretive considerations made in light of its commercial purpose.

A pure textual analysis favoured the Buyer's broader interpretation. The SPA referred to "*industries*" as opposed to "*markets*", "*sectors*" or an identified group of competitors which, in its natural and ordinary meaning, captured participants in a broad sphere of economic activity. That interpretation was also adopted elsewhere in the SPA.

When considering the commercial purpose of the MAE definition, the Court assessed the factual matrix against the objective intentions of the wording to decide whether it extended beyond "firm-specific" risks to eNett and Optal themselves and instead captured risks relating to the broader sector in which they operated. It found that, whilst the transaction related to the acquisition of a travel business, it also extended to a wider payments business. This was based on the Buyer's case that it saw future value in extending its reach into other sectors and markets. The commercial purpose did not therefore suggest that the Court needed to depart from an ordinary reading of the language used in the MAE definition.

The Court considered that the Sellers failed to establish the existence of a specific travel payments industry. eNett and Optal operated in the more general payments industry and B2B payments industry and so, in invoking the MAE Condition and, by extension the Carve-Out Exception, the Buyer had to demonstrate that Optal and eNett had been disproportionately affected by COVID-19 when compared to others in those wider industries.

Why is this important

Whether the pandemic has resulted in a MAE in these circumstances is still to be determined. However, the case provides useful guidance on the approach that the Courts will take when interpreting MAC clauses – construing an agreement on its wording, with reference to its commercial purpose, in order to appropriately allocate risk.

Any practical tips?

It is expected that similar disputes will emerge in the coming months which will provide further clarity. In the meantime, the scope and consequences of MAC clauses should be drafted clearly, and ambiguity and competing meanings avoided. If a market or industry comparator is being used, expressly identify it.

Winter 2020

Commercial

Exclusion Clauses: The Meaning of "Lost Goodwill"

Primus International Holding Co v Triumph Controls – UK Ltd [2020] EWCA Civ 1228

The question

What is the meaning of "goodwill" in the context of a contractual limitation of liability clause?

The key takeaway

"Goodwill" in contracts for the sale of a business should be given its ordinary legal meaning of "*a type of proprietary right* representing *the reputation,* good *name and connection of a business*".

The ordinary legal meaning of "goodwill" is not the same as the accounting definition (which considers "goodwill" in the context of share value). If a party intends to attribute an unusual or technical meaning to a particular term which differs from its ordinary legal meaning, that should be clearly spelt out in the terms of the agreement.

The background

In 2013, Primus and Triumph entered into a Share Purchase Agreement (**SPA**) for the sale to Triumph of two aerospace manufacturing companies owned by Primus for USD$76 million. At the time of sale, both companies were loss-making but financial forecasts provided to Triumph by Primus (and warranted in the SPA as being "*honestly and carefully prepared*") projected future profitability. However, following completion, Triumph discovered significant operational and business issues within the companies. They failed to achieve the earnings forecasted and Triumph had to invest USD$85 million to keep them afloat.

In August 2015 Triumph brought a damages claim against Primus alleging that the financial forecasts warranty had been breached. Primus sought to rely on an exclusion in the SPA that excluded liability "*to the extent that […] the matter to which the claim relates […] is in respect of lost goodwill*".

At first instance, the Court concluded that Primus was in breach of the warranty. There was no appeal of that decision. Triumph was awarded damages to reflect the USD$15 million difference between what Triumph actually paid for the companies and the lower purchase price they would have paid had the forecasts been properly prepared.

The Court also held that the loss arising from the breach was not "lost goodwill". The correct construction of "goodwill" was the ordinary legal meaning, not the accounting definition that Primus sought to rely on. The loss arising from the breach was for lost revenues and increased costs. Primus appealed that point.

The decision

The Court of Appeal unanimously dismissed Primus' appeal, agreeing that the correct construction of "loss of goodwill" in the exclusion clause related to loss of business reputation. The claim was not excluded as it was not "*a claim* for *loss of share value: it was a claim for overpayment as a result of the careless* [financial forecasts]. *The loss was the difference between the price actually paid, and the lower price which Triumph would have paid if they had known the true position*".

The Court of Appeal also set out several useful observations:

- The ordinary legal meaning of "*goodwill*" is not the same as the accounting definition – the ordinary legal meaning is not synonymous with "*value*".
- The use of "*goodwill*" in other parts of the SPA was consistent with its ordinary legal meaning (for example, the non-compete covenants which were intended to protect reputation).
- Previous case law "overwhelmingly" supported the conclusion that "*goodwill*" in contracts for the sale of a business refers to "*a type of proprietary right representing the reputation, good name and connections of a business*" rather than any other technical meaning.

Why is this important?

The English courts are generally reluctant to depart from the ordinary meaning of words used in contracts and will not ascribe an alternative definition (in this case, a technical accounting definition of "goodwill") unless there is good reason to do so.

Any practical tips?

This case reiterates the need for specific and clear language in contracts, particularly when attempting to limit or exclude liability. If parties wish to assign a meaning to a term which differs from its ordinary (legal) meaning, this must be spelt that out in the contract as clearly as possible (and used consistently within the contract).

Winter 2020

Commercial

Breach of Contract: The Privy Court Considers Remoteness of Damage

Attorney General of the Virgin Islands v Global Water Associates Ltd [2020] UKPC 18

The question

Will damages be awarded where a breach of contract resulted in an inability to earn profits under a separate agreement?

The key takeaway

Where contractual obligations under one contract impact on related contracts (eg maintenance contracts), clear provisions setting out the full extent of each party's liability in the event of termination of the contract and what losses are recoverable should be included.

The background

The Government of the British Virgin Islands (the **Government**) entered into two contracts with Global Water Associates Ltd (GWA). The first was a Design Build Agreement (**DBA**) related to the designing and building of a water treatment plant at Paraquita Bay, Tortola. The second contract, a Management, Operation and Maintenance Agreement (**MOMA**) for the water treatment plant for a period of 12 years.

The Government breached the DBA by failing to deliver a properly prepared project site on which the plant could be built. As a result of the breach, GWA gave the Government contractual notice to remedy its default. The Government failed to respond and GWA then terminated the DBA and claimed damages as GWA was unable to install the plant or subsequently, enter into the MOMA as there was no plant to manage, operate and maintain.

GWA initially referred the DBA damages claim to arbitration, claiming that there had also been a breach of an implied term of the MOMA, to the effect that the Government would perform its obligation to provide a prepared site as required under the DBA.

The arbitrator rejected GWA's claim, finding that although there had been a breach (i) the profits which would have been earned under the MOMA were too remote to recover, and (ii) the MOMA did not contain an implied term that the Government would deliver a prepared site. GWA took the case to the High Court and won on both points. The Government appealed.

The Court of Appeal reversed the High Court's decision and found in favour of the Government. That decision was then appealed to the Privy Council.

The decision

The Privy Council rejected the Court of Appeal's decision as GWA's lost profits under the MOMA were within the reasonable contemplation of the parties at the time both contracts were entered into. The Privy Council summarised the position concerning remoteness of damage as follows:

- Damages are intended to put the non-breaching party in the same position had its rights not been breached. However, a non-breaching party is only entitled to recover loss that was, at the time the parties entered into the contract, reasonably contemplated as a serious possibility in the event of a breach.
- Both contracts were entered into on the same day and incorporated the same DBA documents. Further, the parties had each intended that their performance of the DBA would lead seamlessly into the commencement of the MOMA.
- The fact that there were two separate contracts could not of itself support the view that the DBA contained an implicit contractual limitation of liability for breach. As the two contracts were so closely related, the loss of profit arising from an inability to enter the MOMA must have been reasonably contemplated as a "serious possibility" should the DBA fail.

Why is this important?

Many commercial arrangements which encompass distinct and separate phases (eg IT projects, affiliate programmes, construction/developments etc) often result in separate contracts between the same parties. This decision demonstrates that separate contracts are not enough in themselves to limit liability.

Any practical tips?

The relationship between contracts and the potential consequences if one or more is breached/not performed must be carefully considered. Cross-default termination provisions which automatically trigger default termination of related contracts may be appropriate, as well as including clearly defined heads of loss, compensation provisions, and exclusions of liability.

Winter 2020

Intellectual property

Confidentiality and Trade Secrets: Interim Injunction in Trade Secrets Claim

Shenzhen Senior Technology Material Co Ltd v Celgard LLC [2020] EWCA Civ 1293

The question

Were the English courts the appropriate forum for a US company to bring a claim against a Chinese company for misuse of trade secrets?

The key takeaway

This decision applied the Trade Secret Regulations[1] and granted an interim injunction under the Regulations to prevent the import of allegedly infringing goods into the UK pending trial.

The background

The dispute concerned the proposed importation of highly engineered "separators" for use in lithium ion batteries into the UK. Celgard (a US company based in North Carolina and the more established manufacturer of the two companies in the market) asserted that Shenzhen's battery separators had been developed using trade secrets and confidential information from an ex-Celgard employee who then left to work for Shenzhen.

Celgard brought an action for breach of confidence and sought an interim injunction in the UK only, both in equity and under Regulation 3(1) of the Trade Secrets Regulations, with the aim of preventing Shenzhen from supplying a sample of its separator products to a UK company that makes lithium-ion batteries for a well-known manufacturer of electric vehicles.

In the High Court, Trower J gave Celgard permission to serve outside the jurisdiction and granted an interim injunction preventing Shenzhen from importing or marketing battery separators in the UK. Shenzhen appealed, claiming that (i) Celgard had not established a serious issue to be tried, and, (ii) England was not the proper forum.

The decision

Arnold LJ (giving lead judgment in the Court of Appeal) dismissed Shenzhen's appeal. He noted that for permission to serve a claim form outside the jurisdiction, a claimant must show

[1] Trade Secrets (Enforcement, etc) Regulations 2018, which implemented the Trade Secrets Directive (2016/943/EU)

that there is: (i) a good arguable case; (ii) a serious issue to be tried; and (iii) that England is the proper place to bring the claim. To obtain an interim injunction, Celgard must have also proved that there was a serious issue to be tried.

Despite only being able to properly plead one its alleged claims of misuse of confidential information, Celgard's arguments were sufficient for the Court of Appeal to hold that there was a serious issue to be tried (both in equity and under the Trade Secrets Regulations).

Further, whilst the multi-jurisdictional history of the dispute (and ongoing parallel litigation in the US and China) meant that it was not a given that the High Court had jurisdiction to hear the dispute, England was the appropriate place for the claim to be heard. Celgard's claim focused on the loss that would be suffered if Shenzhen's products were supplied in the UK, not on the alleged theft of trade secrets in the US or alleged misuse of trade secrets in China. Celgard's claim concerned the interpretation of its rights (trade secrets) under the applicable law, which the judge had concluded was probably English law.

Why is this important?

Rightsholders will often be alert to the threat of infringing goods from outside the EU. This decision demonstrates that the English courts remain willing to grant interim injunctions in IP claims where the facts support it.

The Trade Secrets Directive provides an additional layer of defence in circumstances where competitors are suspected of trying to import products produced by the misuse of trade secrets.

Any practical tips?

Businesses looking to bring a claim for misuse of confidential information (whether in equity or under the Trade Secrets Regulations) should identify what claims for misuse of confidential information can be asserted in each key jurisdiction (eg where the defendant is based, manufacturing territories, key markets, etc). It may be possible, and desirable, to bring claims in more than one jurisdiction.

Winter 2020

Intellectual property

Breach of Confidence: Raceday Data is not confidential information

The Racing Partnership Ltd and others v Sports Information Services Ltd [2020] EWCA Civ 1300

The question

Can a duty of confidence be applied to live sports data between its creation and its broadcast when the information is available in real time?

The key takeaway

When assessing whether a duty of confidence could apply to the race data, the majority of the Court of Appeal held that no duty of confidence was imparted in these circumstances, given that the races were broadcast live and data known.

However, given the opposing views in the judgment and the decisions were reached on a majority basis, the issues may be considered by the Supreme Court.

In respect of the economic tort, a reasonable person would not consider that the circumstances gave rise to confidence obligations. The judgement also found (again by a majority) that knowledge by the parties was not required to prove unlawful means conspiracy.

The background

The Racing Partnership Ltd (**TRP**) supplied live betting and raceday data from racecourses (including weather conditions, withdrawal of horses or riders, start and finish times and the results) to off-course bookmakers. This data is important to off-course bookmakers to ensure that they have access to immediate, accurate data allowing them to take bets until the start of the race and to accurately reflect the prices offered by the on-course bookmakers.

Arena Leisure Ltd (**C2**), owned six courses and, in 2016, entered into a contract with TRP to c ollect data in respect of their racecourses from 2017. Sports Information Services (**SIS)** had previously held the right to collect and distribute the data from A2's racecourses prior to expiry of its contract on 31 December 2016. However, SIS continued to provide an unofficial feed of raceday data using data collected by the Tote (the pool betting services provided at racecourses).

TRP brought a claim alleging that SIS had supplied data to the Betfred Group and the Ladbrokes Coral Group and that the three companies (together with the Tote) had conspired

to cause injury to TRP by unlawful means. The High Court held that the information supplied by SIS was confidential to TRP and A2 – it had the necessary quality of confidence and was given in circumstances importing confidentiality obligations. SIS therefore acted in equitable breach of confidence by supplying the information to off-course bookmakers. However, TRP's unlawful conspiracy claim was rejected as TRP had failed to demonstrate knowledge between SIS and at least one other conspirator that the means was unlawful.

SIS appealed against the finding that it was liable for misuse of TRP's confidential information and TRP cross-appealed against the dismissal of its unlawful means conspiracy against SIS.

The decision

In majority decisions, the Court of Appeal allowed both the appeal and the cross-appeal, with each judge providing an alternative basis for their decision.

TRP's claim for misuse of confidential information by SIS was dismissed. Lewison LJ and Phillips LJ concluded that no duty of confidence was imparted in these circumstances given that the races were broadcast live, meaning data such as the finish, the winner and non-riders would be known in real-time. The question that had to be answered was whether a reasonable person would expect to understand whether SIS should have understood that the Tote was bound by confidence obligations. As SIS did not receive this information under an obligation of confidence, no equitable duty was owed.

Arnold LJ disagreed; he considered that there was misuse of confidential information, noting that the doctrine of misuse of confidential information is all about the control of information (ie accessibility, not secrecy) (referring to *Douglas v Hello!*) and that it is a species of unfair competition (referring to the Paris Convention, TRIPS and the Trade Secrets Directive).

SIS was however found liable for conspiracy to injure by unlawful means. An unlawful means conspiracy occurs where two or more parties acted together unlawfully with the intention of doing damage to a third party and doing so. On majority, the Court of Appeal found that knowledge of the unlawfulness of the means employed was not required. Arnold LJ concluded (and Phillips LJ agreed) that the High Court was incorrect to find that SIS's acts, taking pricing data from betting exchange websites, did not amount to unlawful means as some of the Tote's data came to SIS in breach of its confidence obligations to TRP, and some came from the betting exchanges, in breach of their terms and conditions.

On this issue, Lewison LJ dissented; he found that knowledge is an ingredient of the tort of intention to injure by unlawful means, and of conspiracy to commit that tort. He also concluded that SIS did not commit the tort as the breaches of the exchange terms were not the relevant unlawful means.

Why is this important?

First, a word of caution – given the various opposing views in the judgment and the fact that the decisions were reached on a majority basis, the dispute might well be considered by the Supreme Court, which could lead to a different outcome again.

In the meantime, it should be remembered that a contract is not the totality of the parties' relationships with one another. There are equitable rights (eg obligations of confidence) and tortious duties (eg economic torts) that may also be relevant, and the scope of those duties may change with differing circumstances.

Any practical tips?

Companies dealing with commercial data (eg financial/market data, advertising metrics, sports data, etc) should review and vet their data/information sources/feeds, ensure that their sources/suppliers have the necessary rights to supply the data (backed by appropriate warranties/indemnities), that usage is within the scope of licences/rights granted and that any onward licensing/commercial arrangements are "back to backed" and have suitable restrictions and protections in place.

Winter 2020

Data protection

ICO publishes new detailed Data Subject Access Request guidance

The question

How far does the new guidance assist with the some of the more challenging aspects of data subject access requests (**DSARs**)?

The key takeaway

In our connected world, the ICO sees it as vital that people have the right to be able to find out what's happening to their information. The new guidance helps businesses respond to these requests by explaining (amongst other clarification): (i) when the clock can be stopped for clarification; (ii) what constitutes a manifestly excessive request; and (iii) when a fee can be charged for excessive, unfounded or repeat requests.

The background

DSARs provide individuals with the right to access and receive a copy of their personal data, and other supplementary information. Given the vast amounts of data now stored as a result of the shift to digital working, compliance with such a request can place a large administrative and financial burden on all data controllers. The Information Commissioner's Office (**ICO**) has recently published its new "*right of access detailed guidance*" (**Guidance**), designed to provided clarity around some issues which data controllers frequently come up against.

The development

The Guidance helpfully indicates the approach that the ICO will take in assessing compliance with a DSAR and the key factors that should be considered by organisations when complying:

1. **Complexity**

   An organisation may extend the time for compliance with a DSAR by an additional two months where a request is particularly "complex". The Guidance specifies that complexity is fact-specific and will be judged on a case-by-case basis but aspects which the guidance indicates will be considered are:

   - the level of technical difficulty in retrieving the data
   - an especially large volume of data (although this in itself is not an indication of complexity)
   - where confidentiality considerations are at play

- where specialist legal advice must be sought (in circumstances where this is not a regular occurrence).

Where a request is non-GDPR related it is unlikely that it will justify an extension of time. Where an extension is justified, the data controller must inform the data subject why the extra time is required. A data controller should be cautious in exercising this right and can expect significantly higher levels of scrutiny from the DSAR requesting party and complaints to the ICO where they feel this has not been exercised properly.

2. **Stopping the clock**

This timeline for response can be paused and the clock "stopped" where: (i) the data controller legitimately requires clarification from the requesting individual; (ii) the data controller needs to verify the identity of the requester; or (iii) the data controller requires the payment of a fee (see below). The ICO makes it clear that these reasons must not be used as a delaying tactic; data controllers will be expected to contact the data subject promptly in order to clarify any points, keeping a record of any such discussions, and must be able to justify this course of action to the ICO is asked.

3. **Charging a fee**

The DPA 2018 permits data controllers to charge a "reasonable fee" to cover the administrative costs of complying with a request eg postage, copying, hardware and staff time under specific circumstances, for example, where a request is manifestly unfounded or excessive, or in cases where additional copies are requested. While there is no limit to the fees under the guidance, controllers who choose to charge should ensure that they have a clear and readily available set of criteria that explains the circumstances under which a fee will be charged, the level of fee, and how payment is taken. They should be prepared to share this with the ICO on request.

4. **Reasonable search**

Organisations are only expected to "*make reasonable efforts to find and retrieve the requested information*" when complying with a DSA. The ICO will take into account the circumstances of the request, the difficulty in finding the information requested, and the fundamental rights of the data subject to access.

While controllers should be thorough and must ensure that they have appropriate systems in place to enable them to conduct an efficient search for requested data, they are not required to leave no stone unturned in complying. The burden of proof remains with the data controller to justify that a search would be unreasonable or disproportionate.

5. **Refusal to comply with a request**

   Although the new guidance confirms that the right to make a DSAR is "purpose blind", refusal to comply with a request may be appropriate in circumstances where the request is manifestly unfounded or manifestly excessive. Where the data subject indicates no intention to exercise their rights of access, where the request is clearly malicious and designed as a means of harassment, or where an individual targets a particular employee, the guidance indicates that this would be manifestly unfounded. Regarding a request being manifestly excessive, the guidance indicates that this will be the case where a request is clearly obviously unreasonable eg the request is disproportionate when balanced against the cost of compliance.

Why is this important?

The above points are not exhaustive - the Guidance provides plenty of information and is designed to bring some much-needed clarity to the problematic field of DSAR requests, shedding light on the obligations of a data controller in receipt of a request, while also highlighting the rights of such an organisation to refuse to comply with a request or to charge a fee. Given the time and cost consequences of DSARs, the Guidance should become a key part of your DSAR response planning.

Any practical tips?

Where a data controller receives a DSAR that is likely to require a vast amount of data and manpower, requesting clarification of the request and, where appropriate, flagging that it is considered to be "manifestly unfounded" or "manifestly excessive" may be a good place to start. Beware that a data controller must be able and prepared to justify this position.

DSARs continue to prove a real challenge for most businesses whenever they land, not least given the relatively tight turnaround from receipt of a request to response. While the Guidance helps, of course it doesn't remove the underlying challenge, which is to ensure that your internal systems are streamlined enough to search and extract personal data as efficiently as possible in the first place. Time spent lining up your systems in advance is time well spent indeed, and will help ensure your compliance budgets aren't whittled away by DSARs in a reactive, rather than proactive, way.

Winter 2020

Data protection

British Airways slapped with biggest ever fine for data breach

The question

What does the BA fine tell us about the ICO's attitude towards calculating fines more generally?

The key takeaway

Mitigation of a breach will only get organisations so far. While BA were successful in reducing their original proposed fine of £183m, £20m is still the largest amount to be handed down by the ICO. This highlights the importance of having effective data governance protocols and systems in place.

The background

The ICO has fined British Airways £20m for a significant data incident that occurred over several months in 2018, resulting in the loss of personal data of over 400,000 staff and customers including banking/payment information, names and addresses. User traffic from the BA website was diverted to a fraudulent website which then harvested customers details including CVV and card numbers, as well as employee usernames and passwords. The fraudulent activity took place between 21 August to 5 September 2018 without interrupting the usual BA booking and payment procedure. The ICO found that BA were processing huge volumes of personal data with inadequate security measures in place to protect consumers and employees alike against the unauthorised or unlawful processing, accidental loss, destruction or damage of their personal data. The GDPR sets out two levels of fine. For less severe infringements, organisations can be fined up to €10m, or 2% of its total worldwide turnover of the preceding financial year, whichever is higher. The more severe infringements could result in a fine of up to €20m, or 4% of its total worldwide turnover of the preceding financial year, whichever is higher.

In June 2019, after their investigation was finalised, the ICO issued BA with a notice of intent to fine BA £183m (equivalent to 1.5% of BA's global turnover). However, upon review the ICO elected to reduce it to £20m (a 90% decrease but still the largest fine that the ICO has dealt out to date).

The development

When calculating the reduced fine, the ICO took into account BA's representations in response to the original fine notice, the supplementary information provided by BA, together with the factors listed in Article 83(2) of the GDPR, which include the nature, gravity and

duration of the infringement, the number of data subjects affected and the damage to them, and the steps taken to mitigate the impact of the incident. The ICO noted BA's mitigating factors including the immediate steps BA had taken to promptly inform the individuals affected, minimise any damage suffered and implement remedial measures. BA had notified the ICO once they became aware of the breach as well as actively cooperating with the ICO and other enforcement agencies. Interestingly, the ICO also considered that the media attention this breach received was likely to increase awareness of the risks posed by cyber incidents and mobilise other organisations to take preventative action, while also negatively impacting BA's brand and reputation. Finally, with the airline and travel industry being one of the most impacted sectors and demand decreasing by around 98%, the ICO took into account the impact of the pandemic on BA in its final assessment of the fine (although the overall reduction due to COVID-19 was only £4m out of the £163m reduction).

The Penalty Notice also sets out in some detail BA's legal challenges to the ICO's approach to calculating the fine, which include wide-ranging administrative law arguments and criticism of the ICO's apparent reliance on a Draft Internal Procedure (which the ICO stated it had not relied on in calculating the final penalty, in particular the turnover-based "bands" defined in the document). BA attempted to argue that relying on turnover in order to calculate fines was arbitrary because "*it bears no meaningful relationship to the wrong at issue*". However, the ICO remained steadfast that while turnover is not the sole factor, it remained a relevant factor in determining the most appropriate level of penalty and is unlikely to change this position.

Why is this important?

It must not be forgotten, that while BA received a reduction, it is still the largest fine that the ICO has handed down to date. The massive reduction here underscores the importance that effective representations and a committed mitigation policy can have.

Any practical tips?

The level of BA's fine only serves to highlight what we already know, namely that organisations must ensure that effective technical, organisation and administrative measures are in place to avoid being walloped by a massive fine for data compliance breaches. Ensuring that access to systems, applications, documents or data sets is centrally controlled and only given to those who need it to carry out their duties is critical, as is protecting log in details by multifactor authentication and regular staff training. Leaving the data door ajar is clearly one of the costliest errors a business can ever commit, and it remains incumbent on every employee (from legal to finance to IT to HR to marketing) to keep it firmly pushed shut.

Winter 2020

Data protection

ICO consults on its draft "Statutory guidance on our regulatory action"

The question

What can data controllers and processors learn about the ICO's approach to regulatory action from its proposed new guidance (the **Guidance**)?

The key takeaway

The Guidance, once finalised following the consultation, will provide some necessary clarity as to how the ICO will monitor and enforce compliance with data protection legislation. In the meantime, the draft Guidance gives organisations a sneak preview into what action could be taken against them and in what circumstances following a suspected breach. Organisations would do well to familiarise themselves with the ICO's suggested approach at this early stage.

The background

In October 2020, the ICO launched a public consultation on its draft Statutory guidance, which details how it will regulate and enforce data protection legislation in the UK in relation to information notices, assessment notices, enforcement notices and penalty notices; a step that it is required to take under the Data Protection Act 2018. The document aims to support the ICO's primary responsibility of ensuring compliance with data protection legislation and goes on to explain the ICO's powers in relation to the above notices, in which circumstances it will use these powers and how it calculates fines. The Guidance seeks to provide certain assurances to businesses that it will use its powers proportionately and consistently.

Notably, the document sets out its risk-based approach to taking regulatory action against organisations and individuals that have breached the provisions of data protection law. The ICO's primary focus is on the areas of highest risk where the most harm is likely to occur and the core principles it will apply when exercising its powers.

The development

The consultation sets out the current updated guidance in relation to the following notices:

Information notices

- An information notice requires that a data controller, processor or individual provides the ICO with information to help it with its investigations within a specified time.
- It is served at the ICO's discretion considering what is appropriate and proportionate (including the risk of harm to individuals or the level of intrusion into their privacy).

- Regarding time periods in which the information must be provided (or if an urgent information notice will be issued), the ICO will take into account the extent to which urgent investigation may prevent or limit the risk of serious harm or serious intrusion and, in particular, the extent to which it may prevent the alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing.
- If the recipient fails to respond within the allocated timeframe, the ICO can apply to the court for an order requiring compliance. Whether an application is made depends on the reasons for non-compliance, any commitments that may have been given, what evidence is to hand and whether the information can be obtained from another source and the public interest. Even considering this, the ICO can still consider issuing a penalty notice (see below).

Assessment notices

- An assessment notice requires that a data controller or processor allows the ICO to consider whether they are compliant with legal requirements or not. This can include requiring access to premises and/or specified documents and equipment.
- Such a notice may be issued where it is necessary to verify compliance with an enforcement notice (see below) or if the controller or processor has failed to comply with an information notice.
- The ICO states that it may require access to specific documents and/or information which indicate how companies have complied with the legislation and what governance measures they have put in place to monitor their compliance. The ICO may require access to documents covered by privilege, that are commercially very sensitive or exempt from the DPA in the interests of national security. However, they will only access the minimum amount of information needed to satisfy their assessment.
- The ICO will consider whether objectively the organisation has complied with the legal requirements, covering manually and electronically stored data, data stored locally and on mobile devices and media, as well as control information and physical and IT-related security measures, including how personal data is stored and disposed of.

Enforcement notices

- The ICO may issue an enforcement notice if a data processor or controller has breached one of the data protection principles. The notice will mandate that the organisation will have to take specific action in order to be compliant again. Failure to comply with such a notice may lead to further action, including penalty notices.
- These notices will usually be appropriate where the organisation has repeatedly failed to meet information rights obligations, if there are serious ongoing infringements to people's rights, or where the processing or the transfer of information to a third country fails to meet the requirements of the DPA and GDPR.

- The timeframe in which such notices may be sent will typically reflect the imminence of proposed action, the severity and scale of any breach or compliance failings and the feasibility of correcting measures or technology.

Penalty notices

- If data processors or controllers fail to comply with data protection legislation or ICO's notices, the ICO can issue a penalty notice indicating its intention to issue a fine.
- The Guidance notes that the ICO will reserve these powers for the most serious breaches, typically consisting of intentional or negligent acts or repeated breaches, which cause damage to individuals, or for non-compliance with the above notices. Penalty notices can also be issued if an organisation repeatedly fails to rectify identified problems or follow the ICO's recommendations.
- However, before the ICO issues a penalty notice they will first issue a Notice of Intent advising an organisation that they intend to serve them with a penalty notice. This gives the recipient 21 days to give a written response about the proposed penalty and its amount.
- The guidance also addresses the calculation of any penalties, which will depend on the type of breach and whether the "standard maximum amount" or "higher maximum amount" applies. It will also depend on factors such as the seriousness of the contravention, the degree of culpability, the ICO's determination about turnover, any aggravating or mitigating factors and the economic impact of the fine and the effectiveness, proportionality and dissuasiveness of any penalty.

Why is this important?

The Guidance will give organisations clarity on what type of action the ICO can take, in what timeframes those actions might be taken, and what the ultimate consequences will be for non-compliance of data protection law or ICO's notices.

While the consultation has already ended, the Guidance will change and evolve according to the feedback given by stakeholders, which will be hugely important to all organisations that process, or handle data once published.

Any practical tips?

Organisations that process personal data should keep careful tabs on their legal obligations and ensure to take proper action if any notices are issued against them to avoid steep financial penalties. They should make sure that all necessary mitigation steps are taken in the event of a breach in order to try to minimise the potential penalty. One preventative step that organisations should consider taking is to ensure that a core data response team is in place and fully trained, so that mitigation and response processes can be deployed as quickly as possible, thereby minimising disruption to management and wider business operations.

Winter 2020

Data protection

EDPB publishes guidance on the difference between controllers and processors under the GDPR

The question

How does the European Data Protection Board (**EDPB**) define the concept of data controller and data processor in a GDPR world?

The key takeaway

Parties to data processing activities must be clear on who is setting the purpose of the processing, as it will determine their status as a controller or processor, thereby defining their obligations under the GDPR.

The background

On 16 February 2010, the now dissolved Data Protection Working Party delivered an opinion on the concepts of controller and processor. As this predated the GDPR, its relevance to post 2018 data-compliance activities was considerably lessened. Following the coming into force of the GDPR, queries have arisen as to how the GDPR has impacted the concepts of controllers, joint controllers, and processors and their respective obligations and rights. The EDPB, as successor to the Data Working Party, recognised that further clarification on how these roles are to apply was required. This new guidance helps explain the concepts and responsibilities of controllers and processors, building on the 2010 opinion, but this time with a specific focus on how they operate within the GDPR framework.

The development

The EDPB guidance has confirmed that the identity of a controller or processor is determined in principle by its activities, rather than its formal designation as either one or the other; while contractual terms can assist in defining roles, they will not be decisive. Certain activities will naturally lend themselves to one role or another. For example, a controller is a body which decides key elements of the data processing process such as the purpose and the means of the processing. By contrast, a data processor may never determine the purpose of processing, although there is some scope for a processor to make decisions in relation to the more practical elements of implementation. Importantly, it would be possible for one entity to act as both controller and processor for different processing operations simultaneously.

Joint controllership is defined as where two or more controllers determine the purpose and means of the processing. It is important to note that the fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership.

Similarly, even though two or more data controllers may not have the same purpose for the processing, the fact that their purposes are similar or complementary may give rise to joint controllership. However, if a party that does not pursue any purpose of its own in relation to the processing, and is just being paid for services rendered, it is not a joint controller and is a processor.

Why is this important?

The EDPB's guidance clarifies that the starting point for assessing the status of an entity within a data transaction will be based on the factual circumstances of the transaction irrespective of how the parties are named or labelled. Purpose is considered the key indicator.

Data processors and controllers have different roles and responsibilities. Controllers must ensure that data subjects' rights are properly respected, and joint controllers must define who will be in charge of answering requests from data subjects and responding to which duties on controllers more generally. Processors must make relevant information available to controllers to allow controllers to comply with the GDPR and carry out other duties incumbent on them, such as notifying data breaches and assisting the controller in carrying out data protection impact assessments. In order to understand which duties apply, parties must take a view on whether they fulfil the definition of controller or processor and the EDPB's guidance assists in this determination.

Any practical tips?

The roles of controller and processor have been developed over the years and are well known. Organisations should nonetheless review the EDPB's guidance and consider whether any of their data processing agreements attempt to designate the roles of controller and processor in name rather than substance. Parties to any such agreements should look beyond just restating Article 28 of GDPR and consider providing details on exactly how processors will assist controllers to comply with their GDPR obligations, possibly in annexes to a data protection agreement.

Winter 2020

Data protection

ICO re-opens its "Regulatory Sandbox" for safer data innovation

The question

What does the re-opening of the Regulatory Sandbox mean for organisations who are engaged in more cutting-edge data development?

The key takeaway

Organisations should consider whether they would benefit from participating in the Regulatory Sandbox in the development of innovative products or services in the above industries, particularly where they are engaged in the two key areas of ICO focus, being children's privacy and data sharing. Experimenting with new data process within the safe boundaries of the Sandbox may be an ideal way to develop your new products, especially as one of the side benefits is a "comfort from enforcement" statement from the ICO.

The background

The Regulatory Sandbox is an ICO service that provides free support to organisations that use personal data as part of their development of products and services. The ICO has sought expressions of interest from companies that are involved in specific sectors; predominantly in the healthcare, financial services, higher education or law enforcement sectors. Participating organisations are able to use the Sandbox to engage with the ICO's team, to draw upon wider ICO expertise and advice in mitigating risks and embedding "data by design". The service will allow organisations to better ensure compliance with legal requirements, understanding data protection frameworks and how these affect their business directly through informal guidance and help throughout the development process.

The development

A beta phase was started in September 2019, but the ICO has indicated it has more capacity to take on new organisations that want to take part in the Regulatory Sandbox, with a focus on two themes: children's privacy and data sharing. In the light of this focus, the ICO is interested in hearing more from organisations concerned with the implementation of the "Age Appropriate Design Code".

What the ICO provides to organisations as a part of the Sandbox includes:

- phased or iterative informal steers during product development from the idea stage all the way to concepts and prototyping;
- informal supervision of product or service testing;

- processing design walkthroughs, which lead to informal advice; and
- informal review of your DP documentation including data protection impact assessments, privacy notices and data sharing agreements.

In addition to protection during participation in the Sandbox, the ICO can also issue a "statement of regulatory comfort" to all participants at their request once they leave the Sandbox. This will set out that, based on the information provided whilst in the Sandbox, the ICO did not encounter any indication that the organisation's operation of its developed product or service would infringe upon data protection legislation.

Why is this important?

The ICO hints that some of the products submitted to the Sandbox will be "*at the cutting edge of what is possible within specific fields and sectors*". The Sandbox can allow for organisations to develop these products with informal assistance from the ICO to better gauge compliance with data protection legislation in a more granular manner throughout the development process, especially where they operate in more challenging areas of data protection.

In some cases, the Sandbox may raise previously unthought of but fundamental questions which will have broader significance for data protection. It is anticipated that guidance and resources will be produced in response to the Sandbox assessments, that will in turn potentially feed into the development of codes of conduct.

Any practical tips?

Organisations should consider whether the Regulatory Sandbox would be of assistance in the development of their products and utilise this opportunity to receive direct guidance and avoid potential regulatory issues down the line. The Sandbox offers one way to potentially avoid obvious pitfalls and, in some cases, may assist with the quicker release of those products or services.

Winter 2020

Data protection

European Commission releases new draft Standard Contractual Clauses

The question

What changes can EU organisations expect from the new Standard Contractual Clauses (**SCCs**) and what steps should they be prepared to take to ensure compliance?

The key takeaway

Now is the time for EU organisations engaged in the transfer of personal data outside of the European Economic Area (**EEA**) to familiarise themselves with the newly drafted SCCs, and the obligations imposed on parties therein.

The background

The modern global economy relies heavily on the ability to transfer data between nations efficiently. When EU organisations transfer personal data internationally to a third country, they must ensure that certain standards of protection are adhered to; one way in which the parties can do this is by using the SCCs, a template set of contractual terms and conditions which parties to a data transfer sign up to and which are specifically designed to provide protections to personal data that is transferred outside of the EEA.

In July 2020, the Court of Justice of the European Union (**CJEU**) invalidated the EU-US Privacy Shield in the seminal case of Schrems II (covered in our Autumn 2020 Snapshot), finding it to be inadequate as a means of lawfully transferring the data of EU subjects between the EU and the US. In doing so, the CJEU removed a low-friction data transfer mechanism available to EU businesses, placing greater reliance on the use of the SCCs. In its decision, the CJEU also considered the adequacy of the SCCs as a means of safely transferring personal data in its decision. While the CJEU did not believe that the SCCs should be invalidated as a means of safely transferring data as the Privacy Shield had been, their use was to be heavily caveated with additional obligations placed on data controllers and processors to ensure that data-recipient countries maintain adequate levels of protection before any transfer takes place.

The development

On 12 November 2020, the European Commission published revised SCCs and a draft implementing decision. The new SCCs retain many of the principles that were considered positively in Schrems II and also bring the clauses more in line with the data protection

requirements under the GDPR, namely those that increase the safeguard requirements around data transfer, afford greater rights to data subjects, and increase transparency obligations.

Whereas previously there were two separate sets of SCCs depending on whether the transaction was between a data controller and processor (**C2P**), or just between controllers (**C2C**), the new SCCs are one holistic document that not only covers C2C and C2P data transfer, but also the additional categories of processor to processor and processor to controller data transfer, so as to reflect the full range of modern processing chains.

Some specific updates to the parties' obligations under the SCCs include:

- Governing law: under the new SCCs, the data subject has significantly increased rights as a resulting impact of GDPR compliance; while parties to the new SCCs may choose the law that will govern their contract, this law will only be permitted where it allows for third party beneficiary rights in respect of the data subject.
- Sub-processors: regarding the engagement of any sub-processor by the data importer, the SCCs now set out the procedure for general or specific authorisation from the data exporter as well as the requirement for a written contract with the sub-processor that ensures the same level of protection to personal data as under the SCCs.
- Assessment of third country data protection: in line with the CJEU decision in Schrems II, prior to agreeing any transfer of personal data, the parties must conduct an assessment of the specific circumstances of the transfer (such as the content and duration of the contract or the nature of the data transferred), the laws of the third country of destination in light of the transfer, and any additional safeguards (including technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination).
- Demonstrable compliance: the parties must be able to demonstrate their compliance with the SCCs. The data importer is required to keep appropriate documentation on its processing activities and make this available to the data exporter on request. The data exporter is permitted to audit the data importer to ensure compliance.
- Rights of termination: the data importer is obliged to notify the data exporter if, after having agreed to the SCCs, it is no longer able to comply with them. The data exporter is entitled to terminate the contract where (i) the transfer is suspended and compliance with the SCCs is not restored within one month, (ii) the data importer is in substantial or persistent breach of the Clauses, or (iii) the data importer fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under the Clauses.
- Public authority requests: the data importer is obliged to notify the data exporter and the data subject if it receives a legally binding request by a public authority for disclosure of personal data, or becomes aware of any direct access by public authorities to the personal data under the laws of the third country of destination. If, following a review of the legality

of such a request, the data importer concludes that there are grounds to challenge the request, it must challenge to the fullest extent.

Why is this important?

Following the invalidations of the EU-US Privacy Shield, the SCCs have taken on even more importance with regards to data transfer. In light of this overhaul, organisations will undoubtedly face greater administrative and financial burdens to ensure compliance under the new SCCs. Going forward, falling foul of the SCCs will in some cases be akin to breaching the GDPR, and potentially significant penalties

The new SCCs are out for consultation until 10 December 2020 and so it remains to be seen what additional changes may be made prior to finalising. There is expected to be a one-year grace period within which parties can continue to use the historic SCCs, provided that the contract remains unchanged (with the exception of changes required to ensure that data is adequately protected). If changes are made to contracts during this grace period, then parties will have to update their SCCs contemporaneously.

Any practical tips?

Get to grips with the new requirements under the draft SCCs sooner rather than later!

Organisations who intend to transfer data out of the EEA will need to be aware of their obligations under any new contracts, and also of any updates required under historic contracts going forward.

As highlighted in our Autumn Snapshots, make sure to keep an eye on the Brexit deadline. Without a deal in sight at the time of writing, it is looking likely that the UK will become a third country on 1 January 2021 and will depend on an adequacy decision going its way in order to continue receiving data in line with the EU GDPR without other mechanisms in place (eg the SCCs).

Winter 2020

Data protection

EDPB publishes its long-awaited guidance on Schrems II

The question

What key information should data handlers be aware of in the new guidance?

The key takeaway

Organisations who import data to third countries outside of the EU should review their existing means of transfer in light of the new EDPB recommendations, as these provide prescriptive guidance on the steps that now need to be taken.

The background

On 11 November, the European Data Protection Board (**EPDB**) published its long-awaited guidance on the Schrems II judgment. This is comprised of two sets of recommendations:

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the **Supplemental Measures Recommendations**), and
- Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures (the **EEG Recommendations**)

(together, the **Recommendations**).

The Recommendations are designed to provide details of measures which can be used to supplement transfer tools (such as the SCCs) to maintain the level of data protection required under EU legislation.

The development

Under the Supplemental Measures Recommendations, organisations should observe the following six-step process:

1. "*Know your transfers*": data exporters should identify all transactions whereby they transfer data to third countries, including any "onward transfers" of data. The exporter must be able confirm that the data transferred is GDPR compliant, namely limited to what is necessary for the purposes of transference, relevant, and adequate. While potentially time-consuming, the EDPB considers that this is a necessary step.

2. '*Verify the transfer tool your transfer relies on'*: where an adequacy decision exists with regard to the data transfer location, organisations do not need to take further steps other than ensuring the adequacy decision remains valid. Where no adequacy decision exists, organisations must rely on one of the transfer tools listed under Articles 46 and 49 GDPR.

3. Assess whether the third country law may reduce the effectiveness of your chosen transfer tool: this assessment should primarily focus on the third country's legislation that is relevant to the transfer and chosen tool. The EEG Recommendations provide details of the elements to be taken into account – for example, "*access, retention and further use of personal data by public authorities within the remit of surveillance measures must not exceed the limits of what is strictly necessary*". Organisations must make sure to document this assessment process thoroughly.

4. "*Identify and adopt supplementary measures*": this step is only necessary where, in compliance with (3) above, the organisation has identified that third country legislation impinges on the effectiveness of the transfer tool. As part of this step, organisations must identify and adopt any additional measures that might assist in bringing the data protection to an EU standard of essential equivalence. The EDPB provides a non-exhaustive list of potential measures at Annex 2 of the Supplementary Measures Recommendations including strong encryption of data and the splitting of data into unintelligible parts (amongst others).

5. Take any formal procedural steps required to put the supplementary measures in place.

6. Remain vigilant: accountability is an ongoing obligation so organisations must make sure to re-evaluate at appropriate intervals that the protection applied to the data in question remains effective, and consider whether there have been any developments that might impact this effectiveness.

Why is this important?

The Supplemental Measures Recommendations closed to public consultation from the end of November and then became immediately applicable. Importantly for UK based data handlers, from 1 January 2021 (Brexit), the Recommendations will apply to transfers from the EEA to the UK in the event that no adequacy decision is made.

The EDPB makes specific reference to US law in its Recommendations, finding that section 702 of the its Foreign Intelligence Surveillance Act (**FISA**) is not considered to provide the essentially equivalent protection necessary. Consequently, in relation to transfers under section 702, supplementary contractual or organisational measures will not be enough to satisfy the GDPR requirements. At Annex 2 of the Recommendations, the EDPB considers worked examples of data transfers and finds that, in its worked examples of (i) cloud service

providers that require access to data in the clear, and (ii) remote access to data for business purposes, the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

The UK will be classed as a third country from 1 January 2021. If the European Commission fails to give a positive adequacy decision in relation to data transfers between the EU and UK, then EU organisations who transfer data to the UK will need to comply with the six steps outlined in the Recommendations, including an assessment of UK surveillance laws.

Any practical tips?

Both EU and, for now, UK organisations should consider what organisational steps they will need to put in place to ensure that they are able to follow the EDPB's latest guidance. Appropriate staff training would be a first step in the right direction.

With regards to UK organisations that import personal data from the EEA, steps should be taken now to identify how UK surveillance laws might impact processing activities, what supplementary measures should be adopted in response, and whether these will be sufficient to allow the continual flow of data.

Winter 2020

Data protection

CJEU rules that the UK's "mass surveillance" regime is out of line with EU law

The question

Do national security concerns exclude EU member states from strict data protection law?

The key takeaway

Domestic national security legislation, including the UK's Investigatory Powers Act 2016 (**IPA**), must not require telecommunication service providers to indiscriminately retain traffic and location data for the purposes of national security. Any such provision would be out of line with the Privacy & Electronic Communications Regulations (**PECR**).

The background

In October this year, the Court of Justice of the European Union (**CJEU**) ruled in two separate cases that mass surveillance by national security agencies (in this case, French, Belgian and UK agencies) does not align with EU law, which allows for only specific data retention schemes with adequate safeguards.

The CJEU's decision relates to the case brought by Privacy International, a UK charity that claims to defend and promote the global right to privacy, which argued that the surveillance regimes in the UK, France and Belgium, contravened the PECR through their mass retention and collection of telecommunications data.

The cases were referred to the CJEU by the domestic courts to obtain a formal opinion on when EU law should be applied. The UK case concerned bulk data collection by the security agencies, while the French and Belgian cases concerned data retention schemes, whereby telecommunications providers are required to retain metadata on their customers' activities (eg who is calling who and when) in case it is required by government agencies.

The development

The CJEU confirmed that EU law precludes any national legislation which requires providers of electronic communications to retain traffic or location data for the purpose of preventing crime or for safeguarding national security.

Under EU law, member states are required to adhere to privacy safeguards in relation to the collection and retention of data by national governments. The courts have indicated that derogations – such as temporary bulk data collection and retention – may be permitted in the

face of a “serious threat to national security”, in which case the state may make an order for telecommunications providers to retain data. However, such emergency provisions must be limited in time, capped to what is “strictly necessary” and subject to review by an independent body. The CJEU found that, in the case before it, the three surveillance schemes complained of “*constitute serious interferences with the fundamental rights guaranteed by the Charter*”.

Why is this important?

The CJEU has made it clear that a Member State’s national security concerns will not exempt it from compliance with the EU legal requirements such as freedom of expression, right to privacy and proportionality. The cases will now return to each individual country’s courts for implementation of the judgment.

The UK’s IPA is incompatible with EU law as it gives government agencies the power to intercept and retain digital communications. This issue may therefore be a sticking point in the data protection sphere, as the UK and EU seek to negotiate their new relationship following the end of the Brexit transition period on 31 December 2020.

Any practical tips?

The CJEU’s judgments highlight the EU’s legal principles in relation to the collection and retention of personal data by national governments, but also serve as a timely reminder more generally about the EU’s strict approach to the collection and retention of data. Either way, these decisions coupled with the wider fallout from Schrems II have left the UK Government with a right proverbial data headache as we screech towards the end of the transition period without a UK adequacy decision yet in sight.

Winter 2020

Digital

The revised Audiovisual Media Services Directive – UK implements new online content rules

The question

What do audiovisual service providers need to consider following the UK's implementation of key aspects of the revised Audiovisual Media Services Directive (**AVMS**)?

The key takeaway

New rules apply to UK on-demand platform services (**ODPSs**) and video-sharing platforms (**VSPs**) that require concrete steps to be taken to proactively protect children and the general public from harmful online content.

The background

On 28 November 2018, the revised Directive (2018/1808/EU) amending the AVMS Directive (2010/13/EU) was published to better reflect the current media landscape and create a more level playing field between traditional television and on-demand and video-sharing services. The new Audiovisual Media Services Regulations 2020/1062 (the **Regulations**) implement the revised Directive and made the necessary amendments to the Broadcasting Acts of 1990 and 1996 and the Communications Act 2003. See our Autumn 2020 Snapshots for previous discussion on the guidelines issued in relation to implementation.

The development

The main changes to UK law introduced through the Regulations are to:

1. **Align the rules on protection from harm for ODPSs with that of linear TV**
   Content standards and advertising rules for on-demand program services are amended to bring them in line with those for broadcast television. Services are required to protect minors from harmful content using measures proportionate to the potential harm, including through selecting the time of the broadcast, age verification tools or other technical measures.

2. **Quota of 30% share of European works**
   The Regulations reinforce obligations to promote European films and TV shows in on-demand services by introducing a 30% quota for European works on services. European works are works originating from certain European countries, or from qualifying co-productions involving those states. Exemptions apply where the service has a low turnover

or a low audience or it is impracticable or unjustified for the requirements to apply because of the nature or theme of the service.

3. **Introduce new rules for Video-sharing platforms**
   The Regulations extend EU standards on illegal and harmful content to VSPs and requires providers to take "appropriate measures" to achieve specified protection purposes. These purposes are:

   - to protect minors from content and advertising that might impair their physical, mental or moral development;
   - to protect the general public from content and advertising that incites violence or hatred towards people with certain protected characteristics; and
   - to protect the general public from content and advertising that is a criminal offence under EU law to circulate (ie terrorist content, content containing child sexual exploitation and abuse, and racist/xenophobic content).

"*Appropriate measures*", for these purposes, include having in place and applying certain terms and conditions of service for users, establishing and operating flagging and reporting mechanisms, age verification systems, systems to rate the content and easy-to-access complaints procedures, and the provision of parental control systems. The Regulations introduce greater controls for content which is under the direct control of service providers, specifically commercial communications (ie advertising) that are marketed, sold or arranged by service providers.

Why is this important?

The House of Lords previously made statements on online content responsibility and accountability of platforms in relation to the spread of harms. The Regulations take a step in the direction of regulation that seeks to require organisations to demonstrate accountability for content on their platforms. The Regulations make provision for enforcement powers of Ofcom, including the power to give enforcement notices and to impose a financial penalty of up to 5% of "applicable qualifying revenue" or £250,000, whichever is the greater and the power to suspend or restrict a service. Ofcom can also charge a fee and demand relevant information from service providers, for example, to determine its jurisdiction over a particular service, whether a service has notified itself or in order to determine the appropriate fee.

Any practical tips?

Organisations within scope are encouraged to engage with Ofcom to clarify any uncertainties during their implementation journey so as to inform future guidance and to collaborate on what best practice will look like. VSPs in particular should ensure they complete the following:

- determine whether their online services are within the scope of the Regulations, which may involve consulting with Ofcom. The deadline by which to confirm to Ofcom whether the Regulations apply is 6 May 2021; and
- assess whether their existing compliance frameworks are sufficient to be deemed compliant under the Regulations and identify technical and organisational measures that may be required to ensure compliance.

Note that many of the rules introduced by the Regulations will be superseded by the proposed Online Harms Bill which will address a wider range of harmful content across a broader range of media and platforms. The implementation date of the Bill is still to be confirmed, which may well mean that Ofcom seeks to apply the Regulations more intensely, to fill what it has identified as a regulatory gap.

Winter 2020

Digital

UK faces major telecoms regulation overhaul courtesy of the European Electronic Communications Code

The question

What does the European Electronic Communications Code (EU) 2018/1972 (**EECC**) mean for the UK's communication services?

The key takeaway

The EECC (formally adopted in December 2018) is set to be implemented by each EU Member State by 21 December 2020. This will overhaul the current communications regulatory framework in order to further protect consumers and ensure that they are the priority for providers of communications services. New sets of obligations will be imposed on different categories of service provider (see flowchart below).

The background

Previously the Communications Act 2003 was the main source of regulation for communications providers in the UK. Communications provider encompasses fixed line owners and operators (such as BT and Virgin), mobile network operators (such as Vodafone and O2), Internet Service Providers (such as Sky), and VOIP operators (such as Skype) amongst others. The 2003 Directives which the Communications Act 2003 derived from have been updated and replaced by the EECC, which is designed to update and harmonise the existing framework regulating electronic communications services across the EEA.

The development

The EECC will result in a number of changes to existing communications regulation in the UK (including to the Communications Act 2003 and Ofcom's General Conditions). Ofcom and the Government have been in discussions in order to reach a collaborative approach towards implementation of the EECC. In July, the Department for Digital, Culture, Media & Sport (**DCMS**) published its responses to the consultation on implementing the EECC in the UK and will ensure the EECC is implemented (almost in full) by the transposition date. Examples of how the DCMS intends to implement the EECC include providing Ofcom with the ability to impose pro-investment regulations and promote competition in mobile markets including by the promotion of 5G and efficient use of the full radio spectrum.

All traditional Electronic Communications Networks and Services (**ECNs** and **ECSs**) including mobile, SMS, MMS, broadcasting transmission services, machine to machine communications and VoIP services will come within the requirements of the EECC. In addition, the EECC now

also extends the scope of the ECS to cover Interpersonal Communications Services (**ICSs**) for the first time, which includes over the top providers such as WhatsApp, Facebook Messenger and Skype, unless the ICSs are solely supplementary to a non-communications service. Over the top providers such as Google Duo will be subject to additional consumer protection measures such as (i) being more transparent, (ii) being required to disclose more information, and (iii) including certain additional provisions in contracts. Regulation requirements in respect of mobile and fixed line providers will tighten with respect of (i) bundle offers, (ii) sales of locked devices being prohibited and (iii) switching between services being made easier.

While ECSs and ICSs will be required to comply with additional measures under the EECC, information society services, e-commerce platforms and those who exercise editorial control over broadcasts and online content will not be covered by the EECC.

Ofcom has confirmed that the new customer protections will be implemented in full, proposing to prohibit "locked" devices being sold by mobile providers, make it easier to switch broadband providers, requiring communications providers to provide customers with more information and to extend the right to exit their contracts. New obligations to ensure disabled customers are provided with communications which meet their needs (eg braille) will also be implemented.

Why is this important

The EECC implementation date of 21 December 2020 falls within the Brexit transition period (ending on 31 December 2020). The UK therefore remains obliged to implement any UK directives into domestic law until that date. This means that those caught by the EECC need to get to grips quickly with what the new framework really means for them, including how they are going to implement any changes.

Any practical tips

Organisations seeking to update their compliance measures under the EECC should prioritise number-dependent over the top provider services (such as standard mobile services) as opposed to number-independent services (such as WhatsApp, Zoom and Skype) as it is likely that number-independent services will be de-prioritised and implemented at a later date. However, organisations should not ignore the latter entirely, as it is likely that from 21 December 2020 appropriate security measures will need to be in place and, if required, the number-independent services able to interoperate.

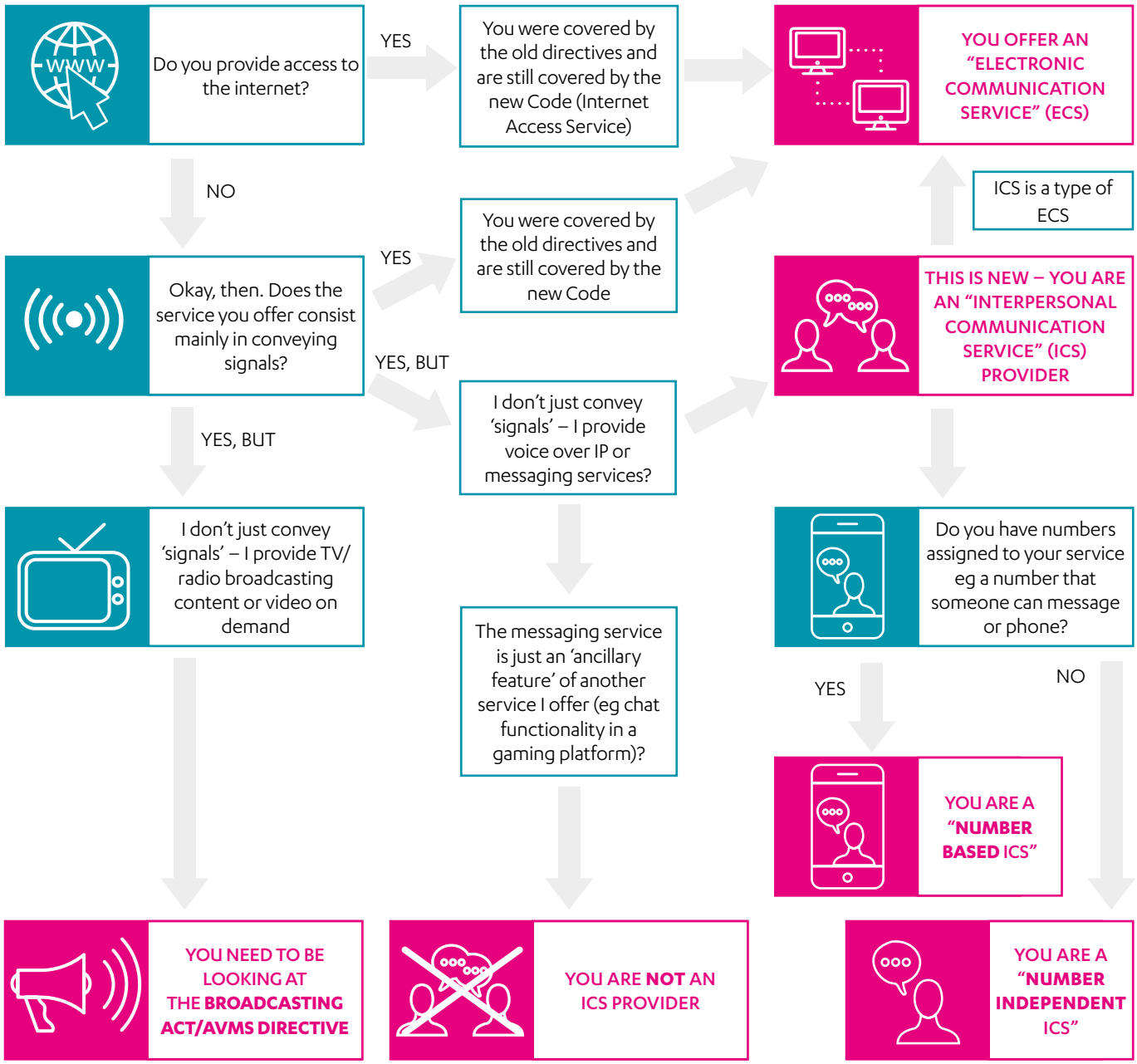
It would also be wise to get familiar with Ofcom's General Conditions of Entitlement, as all ECS providers and ICS providers will be required to comply with certain provisions. Ofcom have made this slightly less time pressured by allowing communications providers 12 months (from 7 May 2020) to implement any changes, regardless of the transposition date.

Finally, don't forget the breach notification obligations which the EECC brings into force, including by virtue of its extension of the ePrivacy Directive. See our Autumn 2020 Snapshot on the challenges of the potential breach notification nightmare brought into play by the EECC.

Winter 2020

RPC

Am I regulated by the new EU Electronic Communications Code?



Consumer

A holistic assessment of the fairness of penalty terms in consumer contracts

Case C-738/19 A v B EU:C:2020:687 (10 September 2020)

The question

What will the court take into account when assessing the fairness of penalty terms in a consumer contract?

The key takeaway

The European Court of Justice (**CJEU**) has clarified that, when assessing whether a specific term is unfair under the Unfair Contract Terms Directive, the courts are obliged to consider the cumulative effect of all the terms, and not simply the unfairness of the clauses relating to those which the consumer has challenged,.

The Background

In 2017 a social housing landlord (**L**) granted a lease to the tenant (**T**) in Amsterdam. The lease was subject to the "*General terms and conditions of social housing*" (the **T&Cs**), which included various penalty clauses that prohibited T from subletting the property and mandated that T must personally occupy the property and vacate on termination of the contract. Under clause 7.14 of the T&Cs, the tenant would be fined €5,000 if they were found to be subletting the property. The contract also included a general "residual" penalty clause that applied where the tenant breached any of its contractual obligations where there was no applicable special penalty clause.

Upon inspection, L discovered that T had been subletting the property to a subtenant (**ST**) for a higher rent price than under the original L-T lease. Consequently, L brought proceedings to:

- terminate the L-T contract and evict both T and ST;
- recoup overdue rent from T;
- recoup a €5,000 penalty for the breach of the no subletting rule; and
- recover the additional profit made by T.

The District Court of Amsterdam was unsure whether clause 7.14 was unfair in light of Article 3(1) of the Unfair Contract Terms Directive (93/13/EEC) (the **Directive**), so it referred the case to the CJEU for clarification on two specific points:

1. When assessing if a term is unfair under Article 3(1), does a national court need to take account of all the terms of the contract, or just certain terms?

2. When assessing if the €5,000 compensation is disproportionately high in relation to point 1(e) of the annex to the Directive, must an assessment concern only the terms that relate to the same breach?

The development

Under the Directive, every contract term that is not individually negotiated must be reviewable in order to determine if it is unfair. Where such a term causes a significant imbalance in rights and obligations on a consumer, then it will be deemed unfair. The Directive also requires domestic courts to take account of all the contract terms in the round when assessing whether the specific disputed term is unfair.

The CJEU recognised that, as L's action was not based on the "residual" penalty clause, despite its presence there could not be a cumulative penalty for a single breach. However, the CJEU was clear that where other terms of the contract are relied on by the supplier against a consumer in regards to the same breach, the cumulative effect of all the terms (even if they are not in themselves individually unfair) must be considered by the court when assessing whether the one contractual term that forms the basis of the dispute is unfair. The nature and context of the obligation and relationship, respectively, should be borne in mind. The national court would therefore be obliged to examine whether a consumer contract term is unfair by considering the interaction between the term at issue and all other relevant terms within the context of their respective scope. To determine whether a penalty amount is "disproportionately high" the court must place substantial weighting on terms that relate to the same breach.

Why is this important?

This ruling is consistent with the Competition and Markets Authority's (**CMA**) guidance on provisions relating to unfair terms in the Consumer Rights Act 2015 (which implements the Directive). This guidance states fairness must be considered in the context of the whole contract and the circumstances around the agreement. When assessing fairness, national courts will have regard to (i) the subject matter and nature of the contract, (ii) the factual matrix at the time of agreement, (iii) the other contractual terms, and (iv) where it depends on another contract, those terms also. The CMA guidance also makes clear that a finding on fairness does not require proof that a term has already caused harm.

It is therefore important to consider the cumulative effect of all the contractual terms as opposed to simply considering the unfairness of individual clauses relating to those that may be challenged by a consumer. A penalty that is according to law and appears fair may be

considered unfair by the courts when it and other relevant terms cumulatively expose a consumer to a disproportionate sanction for the same breach.

Any practical tips?

When drafting a consumer contract, consider consumer penalty and contract terms holistically and ensure that penalty terms: (i) relate to a genuine pre-estimate of loss; (ii) state that a consumer has to pay reasonable compensation; or (iii) state that the consumer has to pay compensation according to law.

Contracting parties would be wise to consider all of the following factors when agreeing to terms to ensure that a term can be considered fair:

- the nature and subject matter of the contract;
- all of the circumstances that exist when the term was agreed;
- all of the other contract terms; and
- all of the terms in any other contract that the current term relies on.

Winter 2020

Consumer

Law Commission consults on draft Bill to modernize the rules on ownership of goods under sales contracts

The question

What are the proposed changes to rules on transfer of ownership?

The key takeaway

The Law Commission's proposed changes are likely to improve consumers' odds of owning goods bought online in the event of retailer insolvency, even before they have left the retailer's possession.

The background

The current rules on transfer of ownership are woefully outdated, remaining substantially unchanged from the Sale of Goods Act 1893 (although they have been transposed into the Sale of Goods Act 1979). The gist of these rules in practice is that, under a sales contract, transfer of ownership only takes place once the goods are delivered to the consumer. However, the rules have been criticised for being unclear, overly complex, containing archaic language, and not fitting with consumers' reasonable expectations of the point at which they own the goods they purchase. Above all, the rules obviously fail to account for the nuances of online shopping.

In 2016 the Law Commission published a report recommending an update to rules on transfer of ownership. Among other small problems, the basic issue it sought to fix is as follows:

- a customer purchases goods online;
- before the goods leave the retailer's possession, the retailer becomes insolvent;
- due to the current rules on transfer of ownership, the insolvency practitioner must resolve that the goods remain property on insolvency;
- the customer is left as an unsecured creditor with little chance of claiming the goods they paid for.

The 2016 report laid out suggestions for criteria which, if met, would enable a transfer to the customer before they received the goods.

The development

The Law Commission has been asked by the Department for Business, Energy and Industrial Strategy to prepare draft legislation based on their 2016 report. After drafting the Bill, they recently consulted on a series of aspects of the Bill in a consultation period which ended on 31 October 2020, including:

- whether the draft Bill successfully implemented the recommendations of the 2016 report
- a call for evidence and views about sales contract formation (more on this below), and
- a request for information about the expected impact of the draft Bill in practice.

The draft Bill is intended to bring rules on transfer of ownership into the 21st century by clarifying language, simplifying the law, and taking into account new practices in retail such as online shopping.

The new rules

The Bill makes a distinction between goods which are identified and agreed on at the time the sales contract is made (for example, where the item is selected in a physical store, or it is an online purchase of a unique item), and goods which aren't identified and agreed on (for example, a standard online purchase, where the customer purchases an item according to a generic description).

Where goods are identified and agreed upon when the contract is made, ownership transfers at the point the contract is made. This is true even if the goods stay with the retailer, for example if they need to make alterations.

Where goods aren't identified and agreed upon when the contract is made, ownership will transfer where any of the following happen:

- goods are labelled with the consumer's name in a way that is intended by the trader to be permanent;
- goods are set aside for the consumer in a way that is intended by the trader to be permanent;
- alteration of the goods to a specification agreed between the trader and the consumer is completed;
- consumer is told by the trader that goods bearing a unique identifier will be used to fulfil the contract (especially for high-value goods, such as smartphones);
- manufacture is completed, if the goods are to be manufactured for the consumer to a specification agreed between the trader and the consumer;
- on examining the goods, the consumer agrees that they are to be used to fulfil the contract;
- goods are delivered to a carrier for delivery to the consumer;
- goods are delivered to the consumer; and/or

- goods that are to be used to fulfil the contract are identified by the trader in some other way, and the trader intends the identification to be permanent (this is a catch-all clause for analogous cases).

The Law Commission has noted that many of these criteria are heavily dependent on the practices of each individual retailer, and that in the case of insolvency, it will be up to the insolvency practitioner to determine if ownership of goods has transferred to the customer.

A particularly critical aspect of the Bill being consulted on relates to the formation of the contract. These proposed amendments all function on the basis of a sales contract existing from the point of payment onwards, but the Law Commission has noted that sometimes retailers will include terms and conditions which prevent formation of a sales contract until dispatch of the goods, rendering the proposed amendments ineffective. The Law Commission is therefore consulting closely on how widespread this practice is, and how it might be worked around. It naturally remains to be seen how the results of that consultation will affect the wording of the draft Bill.

Why is this important?

COVID has turbocharged trends in both online shopping and retailer insolvency. This draft Bill promises to alleviate one of the problems raised by the meeting of the two. It also signals a move in favour of consumer protection, since it seeks to broaden the circumstances in which consumers will own goods they have paid for, but not yet received. Since these rules will almost always function in insolvency situations, this broadening will be to the detriment of typical creditors.

Any practical tips?

Given the ongoing pressure the pandemic is bringing to the retail industry, retailers should already be clear on when ownership of goods passes to consumers. The new proposals under the Bill are a further incentive to do so. Understanding the point at which the contract is formed is key. Watch this space carefully to see how the consultation will affect the draft Bill.

Winter 2020

Consumer

UK Government eyes up new legislation for "smart" products

The question

What steps are being taken by the UK Government to upgrade security legislation for consumer Internet of Things (**IoT**) devices?

The key takeaway

The Government's new proposals will require manufacturers to comply with new security requirements for any products being distributed in the UK. Manufacturers and suppliers of IoT devices should get to grips now with these proposals to understand how they will impact the development of their products and support services (eg the need to provide minimum time periods for which a device will receive security software updates).

The background

The UK Government is attempting to establish a "*consistent, future-proofed cyber security baseline*" for smart devices, laptops, smartphones and PCs. They issued a legislative proposal and a call for industry views which closed in September 2020. The aim is to develop a baseline security standard that is technology "agnostic" such that it can withstand the changes of a market prone to swift innovation.

In October 2018, the UK Government introduced a Code of Practice for IoT security which aimed to provide manufacturers of IoT devices with a harmonised set of guidelines to ensure product security for consumers who often aren't aware of potential cybersecurity issues when using smart products. In May 2019, the Department for Digital, Culture, Media and Sport (**DCMS**) held a consultation on proposals for potential regulation in this area, considering that the self-regulating guidelines had not gone far enough to ensure consumer security. The response to this showed industry-wide support for the proposed legislation, and for making the following three security requirements mandatory:

- a means for users to report device vulnerabilities;
- information regarding the minimum length of time for which the device will continue to receive security software updates must be provided to consumers; and
- no default passwords on devices.

In July 2020, DCMS issued a call for views seeking further industry comments on proposals for legislation on these three measures. The call for views was aimed at addressing concerns

that legislative changes would merely add to the regulatory burden for manufacturers without addresses underlying concerns. The three core security requirements contained in the draft proposals align with the "*European Standard (EN) 303 645 v2.1.1 on IoT Cyber Security*" published this year after consultations between the UK and the European Telecommunications Standards Institute.

The development

The call for views closed on 6 September 2020. If DCMS's proposals are instituted, draft legislation can be expected to emerge in 2021. Once the proposals are formally implemented, the first requirement for a means to report vulnerabilities will be introduced after three months. After a further three months, the requirement regarding software updates will be introduced, and three months after that the requirement for no default passwords will come into force.

Why is this important?

The plan is to require full compliance with all three measures in 2021. It is also likely that the UK Government will propose further legislation on other measures contained in the European Standard on IoT Cyber Security in 2022 and 2023. This will affect both IoT device manufacturers and their resellers, as currently they will have only nine months from the date the legislation comes into force to comply with the requirements. UK-based parts of the supply chain will bear the regulatory burden for compliance, but manufacturers based overseas will need to amend their designs to avoid falling foul of new regulations.

The penalty for non-compliance could potentially be a fine up to 4% of annual worldwide turnover, or the product being suspended or recalled from the UK market. In cases of continued non-compliance, criminal sanctions may be applied.

Any practical tips?

As mentioned, it's expected that manufacturers will be given only nine months to ensure compliance, so producers of smart devices should start taking steps to meet not only the requirements contained in this first wave of legislation, but also the other measures in the European Standard which may soon become requirements in the UK.

Manufacturers and distributors should keep a close eye on the development of the legislation as it may significantly impact design and production processes. A failure to act in time before the enactment of the legislation could lead to disruption in supply chains where products are being sold by distributors in the UK.

Winter 2020

Advertising

The end of celebrity endorsements in gambling ads? CAP and BCAP consult on tougher rules for gambling advertising

The question

What will the CAP and BCAP's proposals for the introduction of tougher measures on gambling advertising mean for the industry?

The key takeaway

CAP and BCAP have launched a consultation into proposals aimed at updating their rules to further restrict the potential for gambling and lotteries ads to appeal to, and adversely impact, under-18s and vulnerable adults.

The background

The consultation was introduced in response to findings from research published in March 2020 commissioned by GambleAware, which looks at the effect of gambling marketing and advertising on children, young people and vulnerable adults. The research suggests that the use of lotteries and gambling advertisements which currently comply with the CAP Code could potentially adversely impact under-18s, more so than previously understood. The report found that 42% of people aged between 11 and 24 were "current gamblers", meaning that they had participated in gambling within the last month.

At present, gambling ads are prohibited from appealing "particularly" to under-18s. In practice, this means they are banned from appealing more to under-18s than to adults and, as such, child-oriented content (such as animated characters) is already banned. The proposals would strengthen the rules to prohibit creative content of gambling and lotteries ads from appealing "strongly" to under-18s. A "strong" appeal test identifies advertising content that has a strong level of appeal to under-18s regardless of how it is viewed by adults. Adopting the "strong" appeal test would decrease the potential for gambling ads to attract the attention of under-18s in an audience. CAP further proposes to update existing guidance to include prohibiting:

- presenting complex bets in a way that emphasises the skill or intelligence involved to suggest, inappropriately, a level of control over the bet which is unlikely to apply in practice;
- presenting gambling as a way to be part of a community based on skill;
- implying that money-back offers create security;

- humour or light-heartedness which is used specifically to play down the risks of gambling; and
- unrealistic portrayals of winners (for example, winning first time or easily).

Currently, gambling and betting ads are banned from any media where more than 25% of the audience is under 18. CAP however still deem this fit for purpose. CAP also state that there should not be an outright ban on gambling advertising, nor should a restriction be placed on the range of media where gambling advertisements are shown.

The consultation closes on 22 January 2021.

Why is this important

Whilst the broader shift to online has increased access to gambling and lotteries, recent research suggests that the overall trend in underage participation in any gambling activity has actually declined significantly since 2011 and adult problem gambling rates have remained stable. However, the recent consultation is perhaps better understood against the broader political pressure the gambling sector is being put under. For example, last summer, the gambling industry introduced the "whistle-to-whistle" blackout, a voluntary ban on betting adverts during sports programmes, under increased pressure to protect children from excessive exposure to gambling.

The proposals within the new consultation mean that gambling advertisers and the content they produce will be scrutinised to a stricter standard than at present. CAP have also recognised that this restriction could have "significant implications" on the use of prominent sports people, celebrities and social media influencers in future gambling ads. Given that at present the use of celebrities in gambling ads is rife, these proposals would have a huge impact on gambling ad content generally.

Any practical tips?

Whatever your interest in the gambling industry (be it advertiser, media owner or platform), you should seriously consider feeding into the consultation – and quickly. Remember that **the consultation period closes on 22 January 2021**.

In CAP and BCAP's words, the proposals are "*proportionate to the likelihood of harm identified by the evidence and are unlikely to result in disproportionate economic impacts on advertisers or media owners*". Now is the time to let them know whether you agree or not.

Winter 2020

Advertising

Foxy Games gambling ad deemed socially irresponsible

The question

How careful do you need to be with ad copy that presents gambling as a solution to financial concerns? And what about search terms which direct you to the ad?

The key takeaway

Ads which suggest that gambling can be used as a solution to financial concerns, an alternative to employment or a mechanism through which to achieve financial security will be in breach of the advertising rules and therefore deemed irresponsible. Care with the wording used is critical as is the context in which such ads appear.

The ad

A paid-for Google search ad for Foxy Games (placed by Electraworks Ltd t/a Foxy Games) was displayed in July 2020, appearing when the search term "make money online" was used. The ad used the text "*Earn Money Online – Foxy Games – Play Onl*ine".

The complaint and the response

The ASA received a complaint that the ad suggested that consumers could obtain financial security by playing the advertised slots and games and that this was irresponsible.

Electraworks' response was that the ad had been displayed as a result of human error and that it had consequently taken action to remove it.

The decision

The ASA unsurprisingly upheld the ruling against Electraworks, finding that the ad breached CAP Code rules 16.1 and 16.3.4 (Gambling). The CAP Code expressly states that advertisers must not suggest that gambling can be a solution to an individual's financial concerns, an alternative to employment or a way to achieve financial security. Electraworks' ad text "Earn Money Online" was considered by the ASA to suggest that Electraworks' Foxy Games could be used as a method of earning money and serve as a regular income stream. On the grounds that the ad suggested gambling was a way to achieve financial security, the ASA found it was socially irresponsible, in breach of the CAP Code, and must not appear again in the form complained of.

Why is this important?

This ruling highlights the ASA's willingness to ban ads that suggest that gambling can be used as a mechanism to achieve financial security. The ASA's primary concern was with the form in which the ad appeared; namely, the wording "Earn Money Online", which suggested that the gambling system offered could be used to earn money and therefore attain a regular source of income. In addition, the fact that it was displayed when the search term "make money online" was used, bolstered this message.

Any Practical Tips

Gambling advertisers must take care to ensure that the wording used in their ads makes no suggestion that the service offered can be used to provide a source of financial income. Advertisers must also ensure that paid-for Google search ads in relation to gambling are not shown in connection with searches linked to making money or otherwise improving personal financial security. Ultimately, gambling should never be presented as a solution to an individual's financial issues.

Winter 2020

Advertising

Self-reporting age is not enough to protect underage viewers from gambling ads: ASA bans Gala Spins ad

The question

When advertising an age-restricted product, what steps should advertisers take to ensure that they minimise exposure to underage viewers?

The key takeaway

It is not enough to rely on self-reported age as a means of targeting ads for age restricted products. Advertisers should make use of the wide range of tools available to them via online platforms to ensure that underage users are not able to view age restricted product ads. Beware also of the risks of shared devices and the consequences of liking, sharing and retweeting.

The ad

Gala Spins, an online slots website, produced a paid-for Facebook post shown in August 2020 for a game called "Fluffy Favourites" which included text that read "*IT'S A ROLLERCOASTER OF CUTENESS!*" and featured a video involving five stuffed-toy animals.

The complaint and the response

The ASA received a complaint that the gambling post was designed to be of particular appeal to children and was therefore inappropriate. Gala Spins responded highlighting that the ad had been posted via their Facebook page which was age-gated to under-18s. They claimed that this would therefore prevent the post from being viewed by underage users. Gala Spins did concede that they had posted the video featuring stuffed animals "in error" and that the video was out of date. The video had been designed as part of a multi-channel campaign targeting females in the UK aged between 18 and 65 with an interest in gambling and online gaming. Gala Spins provided analytics of the campaign which they claimed showed that the posts' viewers were over 18 and were all female. The ad was also taken down from all channels.

The decision

The ASA upheld the ruling that the ad breached CAP Code rules 16.1 and 16.3.12 (Gambling). It considered the steps taken by Gala Spins with regards to age-gating the audience for the post by targeting it only at those between 18 and 65 years of age. Importantly, however, the ASA noted that the targeting of the ad was based on an audience which had self-reported their age as over 18, and there were no other measures in place to check the age appropriateness of the audience. Any under-18s who falsely recorded their age

as being over 18 could be exposed to the ad, and the ASA therefore considered whether the ad complied with the Code's requirement that gambling ads must not be likely to be of particular appeal to children or young persons, especially by reflecting or being associated with youth culture. The ASA found that the ad was irresponsible and breached the Code as a result of its use of cartoon-like imagery, the chosen name "Fluffy Favourites", and the caption text used, strengthening its appeal to under-18s.

Why is this important?

The ASA has recently published its findings from the second of its online monitoring sweeps, designed to identify and tackle age-restricted ads appearing in children's media. Following on from the first report in a year-long project, the ASA carried out another "CCTV-style watch" in order to identify and tackle inappropriately placed online ads in relation to "*gambling, alcohol, e-cigarettes and tobacco, slimming and weight control products and food and soft drinks classified as high in fat, salt or sugar (HFSS products)*". Encouragingly, following this second sweep, the ASA found that the overall number of breaching ads has fallen since the last review; in relation to gambling ads, the ASA noted that while it identified seventy breaching ads as part of its first review, it found only five in the second.

Ads for gambling, alongside alcohol and e-cigarettes, carry an 18+ age restriction under the UK's advertising codes. As a reminder, the ASA states that where ads for age-restricted products cannot be individually targeted, they must not be placed in mediums where more than 25% of the audience is under 18 or under 16, as appropriate. Branded and business accounts are more likely to be able to individually target their audience by making use of the full suite of tools and data available to them via platforms such as Facebook, Instagram and Twitter. It's worth noting that the ASA is alive to the problem of households using shared devices. This means that the ASA may consider the age profile of online viewers to be a less relevant consideration as it will be linked to the ultimate Google account holder – in households with shared devices, under-18s can view content via a parent's log in and the given age may therefore not be indicative of the audience age. Problems can also arise when the mechanics of an ad include liking, sharing and retweeting – an advertiser can effectively lose control of their targeting by encouraging their viewers to like and share. Even if an advertiser can rely on more than 90% of people visiting page being over 18, as soon as those followers start reposting, this then delivers that material to their following, some of whom may be under 18.

Any tips?

The ASA Copy Advice Team strongly advise against the use of mechanics that involve ads being redistributed by members of the public. Advertisers should be conscious that the ASA will expect them to not simply rely on self-reported age data, which is heavily dependent on user honesty, but to make use of the wider platform tools available – for

example, actively deselecting any users whose interest profile coincides with a particular age profile and actively select those whose profile aligns with adult interests.

Winter 2020

Advertising

Skinny Clinic ads promoting weight loss products deemed irresponsible and at risk of endangering public health

The question

What are the boundaries on advertising weight loss products which promote prescription-only medicinal products? And what if the ad implies that such products could be used for people who are not overweight?

The key takeaway

Ads promoting weight loss will breach the advertising rules if they are found to be promoting prescription-only medicine and claiming precise amounts of weight loss within a stated period. Advertisers have a social responsibility to ensure that any ads promoting such weight loss products do not imply that consumers who are not overweight would benefit from weight loss treatment.

The ad

The ad consisted of three posts made to the Skinny Clinic's Instagram page as well as a featured product on the Skinny Clinic's website:

3. The bio on Skinny Clinic's Instagram page, seen in May 2020, featured the claim "*Lose 11-13 lbs in 3 weeks [surprised emoji]*".

4. The first Instagram post, seen in May 2020, was a screenshot of an Instagram story by glamour model Jemma Gilsenan which featured her in a mask alongside the text "@SKINNYCLINIC_", *"#skinnypen*", "*I'm gonna be coming out of lockdown half the size!!*" and "*Forgot to eat again [teary laughter emojis]*". The caption stated "*Keep posting and tagging @skinnyclinic_ please*".

5. The second Instagram post, seen in March 2020, featured an image of a slim woman in Jeans and a cropped top and the text "*Can't believe I've put on a size 8 pair of jeans today! I am so happy … can't wait for my next pen to come, it's a new way of life for me [smile emoji]*". The caption stated, "*We love your feedback @skinnyclinic_ The Skinny Pen suppresses your appetite, you feel fuller faster and it burns calories DM for more Details*".

6. The website www.skinnyclinic.co.uk, seen in May 2020, featured a product listing for "*Weight loss product Saxenda Novo NorDisk*", and included the text "*Our weight loss product Saxenda Novo NorDisk is a brand new revolutionary weight loss aid. It's a self injected daily jab which kicks the hunger, burns calories and makes you feel fuller faste*r" and "*Our Weight Loss Product is Saxenda Novo NorDisk which is newly for weight loss. Saxenda active ingredient is Liraglutide which is MHRA and FDA approved. It is the only licensed injectable prescription only medicine in the UK*".

The complaint and the response

The ASA challenged whether:

1. the claim "*Lose 11-13 lbs in 3 weeks*" in ad (1) complied with the CAP Code in that marketing communications must not contain claims that people can lose precise amounts of weight within a stated period;

2. ads (2) and (3) were irresponsible because they implied that the product could be used by people who were not overweight; and

3. ad (4) breached the Code because it promoted a prescription-only medicine.

In relation to ad (1), Skinny Clinic stated that the claim "*Lose 11-13 lbs in 3 weeks*" was based on feedback that they had received from their clients. Additionally, clients were provided with exercise and nutritional information as well as 24-hour support if necessary. Skinny Clinic also stated that they had not been aware that specific weight loss claims within a stated period were prohibited by the CAP Code.

In respect of ads (2) and (3), Skinny Clinic said that they gave their clients advice based on reduced calorie diets and increased physical activity as Saxenda had to be given in conjunction with this advice. Skinny Clinic confirmed that they had now removed the ads and would ensure that future posts complied with CAP guidance.

With regards to ad (4), Skinny Clinic accepted that they should not have promoted prescription-only medicines on their website and that they had made the necessary changes. In order to be found suitable for Saxenda, a prescription had to be written by a nurse but only after clients had undergone a telephone consultation and completed an online form to assess the client's suitability for the product. During the consultation, verbal advice relating to a reduced calorie diet and increased exercise was provided. The client would then be sent written information relating to diet and exercise; this information was also available on Skinny Clinic's website.

Skinny Clinic stated that they were not registered with the Care Quality Commission because they did not treat clinically diagnosed obesity. Their service was an online and telephone business purely for cosmetic purposes and the nurse was an independent nurse regulated by the Nursing & Midwifery Council to prescribe Skinny Clinic's medicinal product.

The decision

All complaints were upheld.

The ASA considered that the claim featured in ad (1) would be interpreted by consumers to mean that they could lose between 11 and 13 pounds within the stated period of three weeks. Whilst the ASA welcomed the removal of the ad, it found that it breached CAP Code rule 3.9 (Weight control and slimming) because the ad contained claims that people could lose precise amounts of weight within a stated period.

In relation to ads (2) and (3), the CAP Code requires marketers to ensure advertising is prepared with a sense of responsibility to consumers and to society. The image featured a glamour model, who appeared slim. Text in the post stated, "*I'm gonna be coming out of lockdown half the size!!*" and in ad (2), "*Forgot to eat again*". The ASA considered that this implied that she wanted to lose a significant amount of weight and the injection would enable her to skip meals to achieve that; consumers, therefore, could also use the product for the same purpose. Similarly, the image of a slim woman alongside the claim "*It's a new way of life for me*" in ad (3) implied that Skinny Clinic's injections could be used for cravings in people who were not overweight to maintain their weight on an on-going basis.

The message that people who were not overweight would benefit from weight loss treatment was held to be irresponsible by the ASA. Additionally, whilst Saxenda was indicated as an adjunct to a reduced-calorie diet and increased physical activity for weight management in adult patients who were obese (according to the European Medicines Agency), the ads suggested uses fell outside the licenced indications listed in the Summary of Product Characteristics for this medicine.

The ad was found socially irresponsible and breached the CAP Code rule 1.3 (social responsibility).

The advertising of prescription-only medicines to the general public was prohibited by the Human Medicines Regulations 2012 (HMR) and this is reflected in CAP Code rule 12.12. Advertisements for weight-control or slimming products must not suggest or imply that to be underweight is acceptable or desirable. If they are used, testimonials or case histories must not refer to subjects who are or seem to be underweight. Underweight, for the purpose of this rule, means a Body Mass Index below 20. The ASA found that ad (4) breached rule 12.12.

Why is this important?

This is just one ruling of three where the ASA has upheld rulings against three separate brands promoting similar weight loss products and services on social media. The trio of rulings from the regulator follow a CAP ban on cosmetic surgery ads targeted towards teenagers, amid fears of the over promotion of unhealthy body images.

The rulings highlight that the ASA is taking a zero-tolerance stance on any ads that promote products or services that exploit insecurities surrounding body image – especially during the COVID-19 lockdown.

Any practical tips?

This ruling serves as a reminder as to how careful any advertiser of slimming products needs to be. Even if a brand has customer testimony, claims of specified weight-loss within a defined period will not pass the ASA's strict tests. Remember also that advertisers and brands must not advertise prescription-only medicines. And finally, even if your copy for your weight loss product is 'safe', don't use it alongside models who don't need to use it.

Winter 2020

Advertising

Influencer and brand under fire for failing to clearly identify marketing communication on TikTok (Jamella t/a GHD in association with Emily Canham)

The question

What pitfalls should brands look out for when using influencers for marketing communications?

The key takeaway

Advertisers are now generally aware that paid marketing communications must always be clearly identified as such, whatever the platform – but it remains the case that influencers have much less awareness. While this is the first ruling published by the ASA regarding a TikTok post, the main take-away here is the need for brands to provide their influencers with practical guidance and, where the relationship is an ongoing one, reminders on how to properly label their posts.

The ad

The ad in question was posted by influencer Emily Canham on popular video steaming site TikTok in June 2020. The TikTok clip showed Ms Canham using a set of branded GHD straighteners and hairdryer, with the caption "*hiii just a lil psa there's 20% off the GHD website TODAY ONLY with the code EMILY … #fyp #foryourpage*".

The complaint and the response

The ASA received a complaint that the ad was not obviously identifiable as a marketing communication and was therefore in breach of CAP Code rules 2.1 and 2.3 (Recognition of marketing communications).

Jamella Ltd, the company which trades as GHD, produced the contract between the brand and Ms Canham in response to the complaint. Under this contract, Ms Canham was obliged to produce a number of sponsored social media posts while at a music festival. As a result of the COVID-19 pandemic, the music festival was cancelled and so the contract was varied. Accordingly, Ms Canham was instead required to produce (i) a TikTok video on 26 May 2020, (ii) a YouTube video including a promotional discount code "Emily" and two sponsored Instagram posts across 13 and 14 June 2020. Jamella pointed to the fact that the TikTok post (dated 14 June 2020) was created without the brand's oversight or approval and did not form part of Ms Canham's contractual obligations to them. Jamella claimed that they had not

compensated Ms Canham for the video, which in any event was later deleted from Ms Canham's TikTok account.

The decision

The ASA upheld the ruling against the parties. In this case, the ASA understood that there had been a financial agreement between GHD and Ms Canham, under which she was paid to publish posts to her various social media channels and the ASA acknowledged that the TikTok post in question had been made outside the scope of this agreement. However, the ASA also noted that the post featured the same promotional code specified in the agreement to promote GHD. Regardless of whether Ms Canham had received commission for this specific post, because its use was linked to the original agreement, the ASA considered the post to be an ad for the purposes of the CAP Code. The fact that the post was clearly part of Ms Canham's efforts to encourage her audience to purchase GHD products meant that the commercial nature of the content should have been clearly identified prior to consumers using the code.

The ASA assessed the TikTok post as it would have appeared contemporaneously on the app and found that there was nothing in its content, such as "#ad" placed upfront, that made clear to viewers that it was a paid marketing communication. The ASA concluded that the post was not obviously identifiable as such and was therefore in breach of the Code.

Why is this important?

The CAP Code is crystal clear on marketing communications – they must be obviously identifiable as such and that they must make clear their commercial intent, if that was not obvious from the context. This should not come as "news" to influencers; last year the CMA conducted a well-publicised investigation into influencer advertising and secured formal commitments from sixteen well-known celebrities – including the likes of Alexa Chung, Rosie Huntington-Whiteley, Rita Ora and others – that going forward they would clearly identify when they have been paid or received any gifts or loans of products which they endorse. The industry regulator bodies have published guides[2], designed to prevent these mistakes from being made.

This ruling also serves as a timely reminder that brands have a responsibility to provide their influencers with the necessary information to ensure compliance with the CAP Code – it is not enough to assume that the rules are common knowledge. More and more influencers are rising to prominence, but often they are not formally represented and generally they have little experience with the rules. While having a written commercial agreement requiring an influencer to properly label their posts is highly recommended, further steps may be required to ensure compliance with the CAP Code. Brands may want to consider practical and user-

[2] The CMA's quick guide for social media influencers, marketing companies, agents and brands and CAP's "An Influencer's Guide to making clear that ads are ads".

friendly guidance to sit alongside influencer agreements to help to ensure compliance and avoid the headache of an adverse ruling.

Any practical tips?

Brands who elect to use influencers to promote their products should ensure that they provide sufficient information to their influencers to ensure compliance with the CAP Code. A written contract is the starting point, setting out each party's obligations clearly, including the obligation to mark advertised posts as such. Almost as importantly though, brands should take a proactive approach to ensuring that their influencers remain alert to their disclosure responsibilities and are provided with practical guidance.

Winter 2020

Advertising

"Loot boxes" and other in-game purchases: ASA launches consultation

The question

What might gaming service providers expect to see in the ASA's new guidance on advertising in-game purchases?

The key takeaway

The proposed guidance provides direction on the existing rules in relation to in-game purchases, rather than introducing any new rules. It would be prudent for those who offer in-game purchases to get ahead now, by reviewing the proposed clarificatory guidance now for the impact on their business. Responding to the consultation is clearly important, but so is being aware of what's coming down the line from a software design and development perspective (eg the inclusion of "countdown" clocks, which have the potential to pressure vulnerable people).

The background

The ASA has published a consultation on its proposal to introduce new formal guidance on advertising "loot boxes" and other in-game purchases.

It is a common feature within video games and apps to be able to make purchases within the game, either directly or via an external platform. In-game purchases can range from low value purchases (for example, performance boosting items or queue skipping abilities), to significant spends (for example, in-game currency or expansion packs).

The ASA states that it has been notified about in-game purchasing concerns by a wide range of sources, from members of the public, Government Select Committees and the press to campaign and research organisations. Not all of these concerns are within the remit of the ASA as the advertising regulator, but three key areas have been identified where the ASA intends to produce formal guidance so as to "*help to mitigate the potential harms identified*":

1. **Clarity of pricing information at point of purchase**
   The CAP and BCAP Codes mandate that marketing communications must not mislead consumers by omitting or obscuring material information. In relation to in-game purchases; material information will include the price of the item or the manner in which the price is calculated. The concern is that certain methods of presenting in-game purchase prices effectively obscure the item price. Some of the proposals under the draft guidance include

greater clarity around premium currency purchases including (i) the real-world cost of in-game purchases, (ii) odd-pricing, and (iii) savings claims on bundled items.

2. **The language and approaches used to advertise in-game purchases (and the games they appear in)**
   CAP and BCAP are concerned that the nature of in-game purchasing can be potentially harmful to vulnerable individuals, particularly where this takes place within immersive gameplay or mimics gambling characteristics. These concerns arise in particular where in-game purchases are time-pressured, an element which the ASA notes is unique to this form of advertising. The draft guidance advises that, in the case of immersive marketing messages, marketers should avoid the use of excessively short countdown timers, particularly where significant sums of money are involved. In relation to "random-item purchasing", the ASA advises that encouragements to "try one more time" or suggestions that the next purchase may result in a rare item are unlikely to be acceptable.

3. **The use of in-game purchased items in ads for games**
   CAP and BCAP are concerned that the presence of in-game purchased items in advertising may be a material factor in the decision of a consumer to purchase or download a game, particularly in relation to those with gambling-related vulnerabilities. The ASA advises that marketers should make clear that a game includes in-game and random-item purchasing, and that this warning should be "*easily accessible ... and straightforward to find*".

Why is this important?

This proposed guidance will apply to all forms of advertising for in-game products, covering in-game storefronts to advertisements that depict in-game purchases. The CAP Code itself covers in-game advertisements and certain aspects of the proposed guidance will apply to external advertisements for in-game purchasing (eg emails relating to new in-game items or TV ads). The impact is likely to be wide-ranging.

Any practical tips?

The ASA welcomes consultation responses from a wide range of stakeholders. Gaming providers are advised to read the draft guidance and consider its impact upon their services. Where gaming providers consider that there is cause for concern or that the new guidance is not fit for purpose, they should respond to the ASA's consultation accordingly. The draft guidance is currently available via the ASA website and **the consultation will close on 28 January 2021.**

Winter 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

33170267

RPC