RPC

COMMERCIAL LAW

Snapshots

SPRING 2021

KEY DEVELOPMENTS FOR TODAY'S COMMERCIAL LAWYER

UK publishes response to consultation on online harms

PLUS

Confidential information and the duty to make enquiries

European Council makes progress on the ePrivacy Regulation

UK authorities consider position of AI in preparation for a new "Golden Age of Tech"

Singapore Court of Appeal issues landmark decision in first cryptocurrency related trial

DCMS begins inquiry into influencer culture and the power of influencers in marketing

Welcome to the Spring 2021 edition of Snapshots

Our publication seeks to cover everything the commercial lawyer needs to know from the previous quarter (well, almost!). We hope it hits the spot, as we aim to address all the major changes affecting commercial law, from the key cases to data, digital, consumer and advertising developments. We would love to hear your feedback and please do contact David or me with this, or if you have any queries.
Best wishes
Olly and David

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

David Cran
Partner
+44 20 3060 6149
david.cran@rpc.co.uk

WITH THANKS TO OUR FANTASTIC CONTRIBUTORS

Matt Davies
Harpreet Kaur
Dan Richards
Elizabeth Zang
Kiran Dhoot
Sarah Herniman
Jani Ihalainen
Tom James
Nicole Clerk
Jess Pease
Andy Hodgson
Noonie Holmes
Sophie Parkinson
Harvey Briggs
Ela Broderick-Basar
Jess Kingsbury
Sakshi Buttoo
Sumyutha Sivamani

EDITORIAL

Sub-editors Eve Matthews and Jani Ihalainen

Asia coordinators Davina Turnbull and Jonathan Crompton

Design Sean Alberts and Lynda McCarthy

Contents

"Change in law" provisions | COVID-19 and leisure facilities

***Westminster City Council v Sport and Leisure Management Ltd* [2021] EWHC 98 (TCC)**

The question

Which party to a contract bears the losses flowing from a change of law as a result of the COVID-19 pandemic?

Key takeaway

The consequences of an event (eg a change in law) should be clearly specified to provide certainty as to the allocation of risk under the contract – even if the change is due to unprecedented circumstances.

The background

Sports and Leisure Management Limited (SLM) and Westminster City Council (Council) had entered into a contract for the management of leisure services (Contract), under which SLM paid a regular "Management Fee" to the Council for the concessions that SLM provided for customers at the leisure facilities.

The enforcement of COVID-19 lockdown closures and restrictions in England meant that the Contract became loss making to SLM. The parties agreed that the introduction of lockdown restrictions was both a "Specific Change[s] in Law" and a "Qualifying Change[s] in Law" under the Contract, resulting in changes to the financial arrangements. However, the parties interpreted the Contract – and the financial consequences – differently.

SLM argued that the Contract was a standard template used by numerous local authorities (including the Council) and so the "industry norm" was for the Council to bear all financial consequences arising from a Specific Change in Law. As such, they argued that the Council was obliged to pay a "reverse management fee" to reimburse SLM for the financial loss.

The Council disagreed and sought declaratory relief that, on the proper construction of the Contract, a Specific Change in Law:

- did not oblige the Council to indemnify SLM in respect of any losses in excess of the Management Fee
- did not oblige the Council to indemnify SLM against all losses.

The decision

Whilst Kerr J acknowledged that the drafting lacked precision in places, the Contract was to be interpreted on its own merits through careful examination of the wording for each clause. The "industry norm" argument was rejected – it was not on industry standard terms; the template was adjustable and provided a starting point for negotiations.

The High Court agreed with the Council that the management fee could not drop below zero and become payable to SLM. The fee was defined as a payment to, and not by, the Council and the contractual mechanism provided for one-way payment only. SLM's interpretation was also inconsistent with the nature of a concession agreement, where a contractor bears the risk of running the concession in return for retaining all or part of the revenue. However, it was recognised that the management fee could reduce to zero in the circumstances and that the Council might be required to pay a lump sum to SLM to meet, for example, its salary costs.

Why is this important?

Whilst the judgment turns on the interpretation of the specific wording of the Contract, it provides a useful indication of the courts' approach to numerous claims that are expected to follow as parties seek to protect themselves from the extensive and unexpected financial consequences arising from the COVID-19 pandemic.

The Court was clearly unwilling to interpret (or rewrite) the financial provisions to deal with unexpected circumstances – even if this meant the contractor would face financial hardship.

It is also a reminder that the English courts will look at the merits of each contract and consider the balance between "textualism" and "contextualism" when establishing the intent of the parties. Parties should also not assume that the *contra proferentem* rule (the interpretation of ambiguous words against the beneficiary) will be applied automatically – as Kerr J noted, it should be used only as a last resort.

Any practical tips?

Whilst the case does not introduce new law, it is a reminder that clarity of drafting is key when interpreting the meaning and effect of relevant provisions. The operational or financial consequences, and which party bears them, should be clearly specified. Also consider how unforeseen or unexpected consequences should be addressed – is there enough flexibility for these to fall within existing provisions, or should they be excluded and dealt with on a different basis?

Commercial Court uses its freezing injunction powers in the battle to identify crypto-fraudsters

***Ion Science Ltd v Persons Unknown* (Unreported, 21 December 2020)**

The question

Can a court grant an injunction against unknown persons involved in crypto fraud, and where should the claim be brought?

Key takeaway

This is the first initial coin offering (ICO) fraud case to be heard before the English Commercial Court. It shows that the Court is prepared to treat cryptoassets as property within the common law definition and that the *lex situs* (ie the law of the place where the property is) for cryptoassets is the location where the owner is domiciled.

The background

Over several months, Ion Science Limited and its owner Duncan Johns transferred approximately £250,000 to his Coinbase account (a digital currency exchange) to invest ICOs, on the advice of several "advisers" claiming to be from a specialist investment company called Neo Capital (Neo). Mr Johns was then advised that his successful investment had made a US$15m profit, which could be released on receipt of commission payments. On each occasion, Mr Johns gave the "advisors" access to his computer to transfer money from his personal account via his Coinbase account to Bitcoin. Approximately £250,000 was transferred in Bitcoin to settle the commission debts, but Mr Johns never received his alleged profits.

He subsequently discovered that his contacts at Neo had used aliases which could not be traced, and that Neo was in fact listed on the Swiss regulator's warning list and was not the registered entity that it had made itself out to be.

Further, a significant amount of Mr Johns' Bitcoin had been dissipated through two cryptocurrency exchanges (Binance and Kraken).

Ion Science and Mr Johns applied for a proprietary injunction and worldwide freezing order over the assets of the individuals connected to Neo to secure the Bitcoin (or proceeds) and to identify the advisor(s) that had appropriated the funds. Ion Science and Mr Johns also applied for an order for alternative service against the advisors.

The court's decision

The Court confirmed that cryptoassets, such as Bitcoin, counted as property for the purposes of a proprietary injunction and was satisfied that it had the jurisdiction to grant the proprietary injunction and worldwide freezing order against persons unknown, as the description of the fraudsters was considered sufficiently clear to establish who was and was not included within the relevant group.

To try to find the recipients of the stolen bitcoin, the Court also granted a third-party disclosure order (referred to as a *Bankers Trust* order (BTO)) against the cryptocurrency exchanges, Binance and Kraken. The claimants required the Court's permission to serve the BTO out of the jurisdiction and had to show that there were serious issues to be tried on the merits of the claims. The Court was satisfied that this was the case and, in granting permission, indicated that the *lex situs* of a cryptoasset is the place where its owner is domiciled.

The Court also considered that *AB Bank Ltd v Abu Dhabi Commercial Bank* (which had held that there was no gateway permitting service out of the jurisdiction against a third party for the purposes of a *Norwich Pharmacal* order) was distinguished as these were exceptional circumstances and this case involved a BTO as opposed to a *Norwich Pharmacal* order.

Why is this important?

This is the first ICO fraud case to come before the English Commercial Court and has been viewed as a possible blueprint for future claims, particularly given the increased prevalence of cryptocurrency fraud, alongside its increasing publicity and rapid rise in value

The Court has demonstrated that it is prepared to treat cryptoassets as property and to grant proprietary injunctions where those assets are misappropriated, as well as third party disclosure orders to determine the identity of the fraudster(s).

Any practical tips?

Companies and individuals should ensure that appropriate policies are in place requiring enhanced due diligence for cryptoasset transactions and that staff are trained to spot the warning signs of crypto fraud. In particular, you should ensure that the party is legitimate; query whether the transfer can be made by other (more easily traceable) means and, if required, ensure that you have adequate information from the recipient for the purposes of identification (or, failing that, information regarding the recipient and the currency exchange that they use). If court action is required, the English courts are likely to be an appropriate forum to seek legal redress.

Penalty clause regarding IP rights harsh but not unenforceable

Permavent Ltd and another v Makin **[2021] EWHC 467 (Ch)**

The question

Were terms included in a settlement agreement preventing future challenges against IP rights unenforceable penalty clauses?

Key takeaway

The settlement agreement clauses were valid as they served and protected the Claimants' legitimate business interests and the detriment to the Defendant, though harsh, was not disproportionate to make the clauses unenforceable as penalties.

The background

Steven Makin (Makin) and Timofei Yeremeyev (Yeremeyev) supplied products (mainly roofing) to the construction industry through a group of companies, including the Claimants, Permavent and Greenhill. Makin invented and patented roofing products under the name "Easy Roof System" and, in 2014, he granted a licence to Permavent to manufacture, use, sell and supply the Easy Roof System products.

In 2016, the relationship between Makin and Yeremeyev broke down and Makin left the business in 2017, purporting to terminate the patent licences and withdrawing permission for suppliers of certain Easy Roof System products to produce patented products.

Permavent brought a claim against Makin in July 2017 and sought (i) a declaration that Permavent owned the patents and patent applications (the IP Rights); and (ii) an injunction preventing Makin from transferring or licensing the IP Rights.

The parties subsequently entered into a settlement agreement under which Makin assigned the IP Rights to Greenhill. Additionally, in return for his agreement not to challenge the ownership/validity of or claim an entitlement to the IP Rights, Makin would be entitled to various payments (which would be forfeited/repayable in the event of a breach). Pursuant to those clauses, Permavent stopped making the payments when Makin sought to register an interest in the IP Rights.

Makin was found to be in breach by way of summary judgment so the issue before the Court was whether the clauses constituted an unenforceable penalty.

The decision

The Patents Court held that the relevant clauses were not unenforceable as penalties.

Referring to the Supreme Court decision in *Cavendish Square Holding BV v Talal El Makdessi* (Cavendish), the judge noted that whether an obligation amounted to a penalty depended on (i) whether legitimate business interests are served and protected, and (ii) whether the detriment imposed on Makin was extravagant, exorbitant, unconscionable or out of all proportion to that interest. The judge, Zacaroli J found in the Claimants' favour.

The IP Rights were of vital importance to the business and any challenge could affect profitability through loss of sales and lead to reputational damage as it would damage the business' ability to source, manufacture and sell products. Whilst the clauses were harsh on Makin, the detriment was not considered to be extravagant, exorbitant or unconscionable, nor was it disproportionate – a breach could cause significant harm to Permavent.

In reaching its decision, the Court also took into account other factors, in particular Makin's aggressive and hostile behaviour in the period leading up to the agreement which demonstrated that he was likely to challenge the IP Rights and would maximise costs and the fact that he had entered the settlement agreement with the benefit of legal advice.

Why is this important?

This decision provides helpful guidance on the application of the *Cavendish* test on penalty clauses in a different context.

This decision also highlights the importance of the factual matrix as at the date of the agreement when assessing proportionality, considering the potential consequences of a breach at that time, as opposed to assessing the harm caused by an actual breach.

Any practical tips?

Consider whether the relevant provisions can be drafted as primary obligations that apply on a particular event or trigger (rather than a breach), so that the penalty rule is not even engaged. If the consequences do follow a breach, identify the legitimate interest(s) in question and the potential consequences/harm that may be suffered by a breach, and ensure that detriment (eg payments, loss of benefits, etc) are proportionate to those potential consequences. Ensure that the counterparty has taken legal advice (or at least had the opportunity to do so).

The Technology & Construction Court considers when damages will be awarded for wrongful termination of a services agreement

CIS General Insurance Ltd v IBM United Kingdom Ltd **[2021] EWHC 347 (TCC)**

The question

What is the nature of the losses suffered as a result of a wrongful termination of a services agreement?

Key takeaway

The starting point for assessing losses is to identify the contractual benefit lost as a result of the other party's breach. Even if losses are framed as "wasted expenditure", this may only represent a different method for quantifying the "loss of the bargain" and will not change the characteristics of the losses.

The background

In June 2015 CIS General Insurance Ltd (CIS), a Co-operative Group insurance company, engaged IBM United Kingdom Ltd (IBM) to supply a new IT system to underpin CIS' insurance services and manage the system for a 10-year period. The Managed Services Agreement (MSA) between the parties provided for payment by CIS against certain milestones.

A dispute arose in early 2017 as to whether these milestones had been met. IBM submitted an invoice to CIS in the sum of c£3m on the basis that it considered the milestones to have been fulfilled. CIS refused to pay the invoice alleging that the milestones had not been met.

Following several setoff notices by CIS and final payment notices by IBM, IBM purported to terminate the MSA because of CIS' failure to pay the invoice. CIS claimed that this amounted to repudiatory breach and brought a claim against IBM seeking damages of £128m, the majority of which was for wasted costs – which, given the language of the exclusion clauses in the MSA, was characterised as expenditure incurred in relation to the alleged wrongful termination by IBM. CIS also alleged that IBM failed to adequately implement the MSA and argued that it would not have entered into the MSA if it had known that the IT platform was not a proven, off-the-shelf product that could meet its requirements. IBM counterclaimed for the unpaid January 2017 invoice (c£3m).

The decision

The Technology & Construction Court (TCC) found that, whilst IBM's invoice was payable, it had been disputed by CIS under the agreed contractual procedure. As such, IBM was not entitled to terminate the MSA for non-payment.

Whilst IBM had taken all reasonable steps to ascertain the risks associated with the project and had accurately represented the rewriting and development work required, IBM were also found to be responsible for critical delays to the project and for failing to report these delays to CIS. IBM had therefore failed to meet key milestones and was in breach of the MSA. The TCC awarded CIS almost £16m in respect of additional costs incurred as a result of IBM's delays in reaching the contractual milestones and set off IBM's unpaid £3m invoice against that figure.

However, CIS's wasted costs claim was rejected by the TCC. They agreed with IBM that, although the quantum of CIS' claimed losses related to expenditure, the actual loss was the revenue, profit and savings through which that expenditure would have been recouped if the breach had not occurred – and these were expressly excluded.

O'Farrell J said, "*The starting point is to identify the contractual benefit lost as a result of IBM's repudiatory breach of contract*". While CIS was entitled to characterise its claim as one for wasted costs, that simply represented "*a different method of quantifying the loss of the bargain; it does not change the characteristics of the losses for which compensation is sought*". The TCC concluded that CIS' claim was expressly excluded under the terms of the MSA.

Why is this important?

This decision from the TCC provides useful guidance on wasted costs and how damages arising out of termination of a contract are categorised. It also provides useful discussion of the case law relating to reasonable and best endeavours, as well as set off, and highlights the importance of following contractually agreed procedures for submitting and disputing invoices.

Any practical tips?

The comments concerning the categorisation of loss and damage should be considered when drafting or reviewing exclusions and limitations of liability. Consider how exclusions in respect of revenue, profits and/or anticipated savings may interact with recovery of expenditure or wasted costs. Consider specifically stating that certain categories of loss are intended to be recoverable (in any event/notwithstanding the exclusions).

Also ensure that contractual procedures for raising, submitting, challenging and paying invoices are workable and consistent with related provisions (eg as to set off).

Confidential information and the duty to make enquiries

***Travel Counsellors Ltd v Trailfinders Ltd* [2021] EWCA Civ 38**

The question

When are recipients of information obliged to make enquiries as to whether that information is confidential?

Key takeaway

An equitable duty of confidence will arise in relation to information if a reasonable person would make enquiries as to whether it is confidential, but the recipient abstains from doing so.

Key background

Both parties are travel agencies. When several employees moved from Trailfinders Ltd (Trailfinders) to Travel Counsellors Ltd (TCL), they took customers' details from Trailfinders' database and added those contacts to TCL's database.

Trailfinders brought a claim against TCL on the basis that the information their ex-employees had supplied to TCL was confidential and that TCL's use of that information constituted a breach of an equitable duty of confidentiality owed to Trailfinders. The High Court agreed with Trailfinders, finding that the ex-employees had breached their duties of confidence and that TCL were also in breach of the equitable duty of confidence that they owed to Trailfinders.

TCL appealed, arguing that the High Court judge had applied the wrong legal test when assessing whether TCL owed a duty of confidence to its rival as an equitable obligation of confidence would arise only if it knew or had notice that the information was confidential.

The decision

The Court of Appeal upheld the High Court's decision.

Referring to the limited authority on this point, including *Primary Group (UK) Ltd v Royal Bank of Scotland plc* and the recent Court of Appeal decision in *Racing Partnership Ltd v Done Brothers (Cash Betting) Ltd*, Arnold LJ stated that TCL should have known that the information was confidential as a "*reasonable person in the recipient's position*" would have reached the conclusion that a list of clients from a competitor's database would be confidential.

The Court of Appeal also clarified that a party did not necessarily need to have known the information was confidential or intentionally turned a blind eye to this fact. Although it would be context and fact dependent – both as to whether a reasonable person would make enquiries and, if so, what enquiries would be made – if the reasonable person would make enquiries (eg they were on notice that all or some of the information may be confidential), a failure to make enquiries may be enough to establish an equitable duty of confidence.

Why is this important?

This case demonstrates the broad nature of the duty of confidentiality and the circumstances in which it may arise. A recipient of information not only has a duty to treat information as confidential if they know or ought reasonably to know it was confidential, but also in circumstances where a reasonable person would make enquiries as to the information, but the recipient did not do so.

Any practical tips?

Businesses must be very careful when receiving potentially confidential information (from new employees) – and ignorance is not bliss! A person cannot deliberately ignore the position ("blind eye" knowledge) or even avoid asking reasonable questions about the nature or provenance of the information in question. If potentially confidential information is received without permission, it should be treated as strictly confidential, not shared further or used for any unauthorised purpose, and ideally secured and isolated (for example within the internal/external legal team).

Unfair Contract Terms Directive | Fairness of term containing possibility of creating a significant imbalance

***Dexia Nederland BV v XXX and Z* (Joined Cases C-229/19 and C-289/19)**

The question

When should the fairness of a term be assessed in a consumer contract?

Key takeaway

When considering whether a term is "unfair" for the purposes of Unfair Contract Terms Directive (Directive), the courts should ascertain whether, as at the date on which the contract was concluded, the contract terms gave rise to a significant imbalance in the parties' rights and obligations, to the detriment of the consumer. The fairness assessment cannot depend on subsequent events that are beyond the parties' control.

The background

The Directive, which was implemented in the UK by the Consumer Rights Act 2015, provides that, where a contractual term has not been individually negotiated, the court will consider it to be unfair if it is found to cause a significant imbalance in the parties' rights and/or obligations under the contract, to the detriment of the consumer, and contrary to good faith.

In this case, separate share leasing agreements were entered into between Dutch consumers XXX and Z (Consumers) and a bank (the predecessor in title of Dexia Nederland BV (Dexia)). Under the agreements, the Consumers were permitted to borrow a sum of money for a fixed period and the bank would use this sum to acquire shares on behalf of, and for the benefit of, the Consumers. The bank remained the owner of those shares until repayment of the sum borrowed, with any dividends paid to the Consumers.

The agreements included a mechanism to calculate the amounts payable by the Consumers if the bank terminated early for default. Depending on certain factors, including the termination date and interest rates, the bank potentially obtained significant benefit from early termination.

In 2005/2006, Dexia terminated the leasing agreements with XXX and Z for late payment and drew up final statements, using the contractual mechanism and accounting for delays to monthly payments. The Consumers refused to settle the balances.

The Court of Justice of the EU (CJEU) was asked to consider whether the contractual terms were compatible with the Directive, drawing attention to Dexia's significant advantage in the event of an early termination. In particular:

- should the Directive regard a term as unfair where it was a conceivable possibility, as opposed to a certainty, that it would cause a significant imbalance?
- can the user deriving the benefit of a now void unfair term claim legal compensation under supplementary national law as an alternative method of recovery?

The decision

On the first question, the CJEU found that such an imbalanced term in a risk-weighted consumer contract must be regarded as unfair, even where the imbalance only arose under a specific set of circumstances and where, in different circumstances, it operated to benefit the consumer. The fact that there was only a possibility of a significant imbalance did not alter that position.

The CJEU also noted that a contract should transparently set out (i) the specifics of the mechanism in question, and (ii) where appropriate, the relationship between the mechanism and other contractual term, to allow the consumer to evaluate, based on clear, intelligible criteria, the economic consequences of the contract on them.

On question two, the CJEU held that, if a term is void, it should not then revise the problematic term to give it new effect and allow for compensation where the contract is capable of surviving without the term. That would undermine the objective of the Directive.

Why is this important?

The **possibility** that a contractual term could cause significant imbalance in the parties' rights to the detriment of the consumer was enough for it to be considered "unfair" under the Directive – even where the term might benefit the customer in different circumstances.

Any practical tips?

Consider all of the potential consequences of terms in standard form, consumer facing agreements, and avoid those terms in the non-exhaustive list in the Annex to the Directive which may be regard as unfair (eg inappropriately limiting legal rights, disproportionate compensation, unilaterally altering/determining terms, etc).

Data Subject Access Requests | High Court declines to issue order compelling compliance with multiple DSARs when used abusively or for an alternative purpose

***Lees v Lloyds Bank Plc* [2020] EWHC 2249 (Ch)**

The question

Can the courts decline to order compliance with data subject access requests (DSARs) if they are used abusively or for a purpose other than acquiring personal data?

Key takeaway

If DSARs are used abusively, for example to obtain documents rather than personal information or there is a collateral purpose, the courts may exercise their discretion and decline to make an order to compel the production of data or documents in response to DSARs.

The background

Between 2010 and 2015 Lloyds Bank plc (Lloyds) granted the Claimant, Silas Lees, buy-to-let mortgages in respect of three separate properties. For each property, Lloyds was shown as the proprietor of the registered legal charges. Mr Lees believed that Lloyds had assigned the benefit of the legal charges over the properties as a part of the securitisation of a portfolio of loans, which meant that Lloyds would not be entitled to pursue possessions claims against him over the properties.

After possession claims were initiated by Lloyds in 2019, Mr Lees sent around 70 DSARs to Lloyds and other parties, specifically requesting details of their fiduciary capacity and whether Mr Lees' loans had been sold onward as a part of securitisation. Many were sent even after Lloyds had responded to Mr Lees' first DSAR confirming that the loans had not been sold onward. Lloyds also responded appropriately to each subsequent DSAR made by Mr Lees.

Mr Lees then issued Part 8 proceedings for, among other things, Lloyds' failure to provide data following his DSARs contrary to both the Data Protection Act 2018 and GDPR. At the time of the DSARs, the legislation in-force for data protection was in fact the Data Protection Act 1998 (DPA 1998), which gives individuals certain rights to access personal data pertaining to them and to enforce compliance with requests if data controllers failed to do so.

The decision

In his decision Chief Master Marsh held that Lloyds had provided adequate and appropriate responses to Mr Lees' DSARs and was not in breach of the DPA 1998.

But even if Mr Lees could have shown a failure to provide a proper response, the Court went on to consider the discretionary nature of the remedies sought, noting that, following the Court of Appeal decision in *Ittihadieh v 5–11 Cheyne Gardens RTM Co Ltd*, the discretion was not "general and untrammelled". The courts will take various factors into account when assessing whether to make an order to comply with a DSAR, which included in this case:

- the numerous and repetitive DSARs from Mr Lees, which was abusive
- the real purpose of the DSARs was to obtain documents rather than personal data
- the collateral purpose that lay behind the requests, namely that the documents sought would be used in another case involving Mr Lees and Lloyds. As noted in *Ittihadieh*, a collateral purpose of assisting in litigation is not an absolute answer to there being an obligation to answer a DSAR, but it is a relevant factor in the exercise of the court's discretion
- the data sought was of no benefit to Mr Lees, when an adequate defence could have been levied through case law, and
- the claims for possession had been the subject of final determinations in the County Court from which all available avenues of appeal have been exhausted.

Mr Lees' claim was dismissed as it was without merit.

Why is this important?

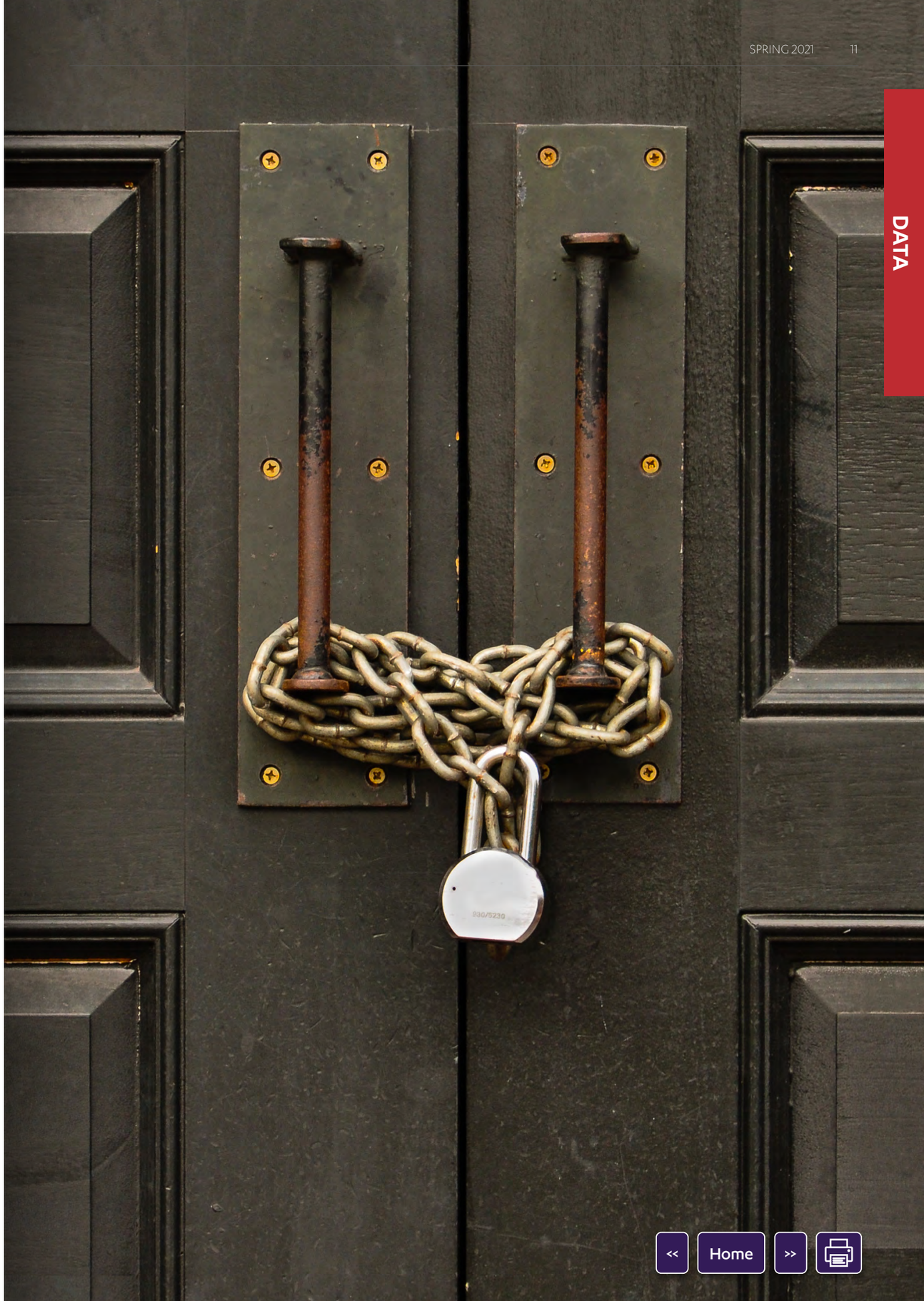
In a significant decision for those processing personal data, the courts have demonstrated that they are willing to take a robust approach in respect of the tactical deployment of DSARs. Whilst DSARs can be used to assist with litigation, they should not be used in an abusive fashion or where they would serve no purpose.

Any practical tips?

This decision provides a helpful authority on which to rely when resisting DSARs which are unfounded, abusive or used for an inappropriate ulterior purpose, demonstrating that the courts will not force compliance for the sake of it, but will consider the purpose and effect of the DSARs.

The mere fact that a DSAR is being used for litigation or for another purpose is not usually enough of itself to refuse to comply, but the context should be carefully reviewed. The ICO guidance also recognises that you can refuse to comply with a DSAR if it is manifestly unfounded or manifestly excessive.

DATA



European Commission awards draft adequacy decision to the UK

The question

How can data transfers between the UK and the EU be securely and legally executed following Brexit?

Key takeaway

Entities transferring data between the UK and EU, and who feared a new hard-line data transfer regime following Brexit, can begin to breathe easy again following a display of support from the European Commission in the form of its draft adequacy decision for the UK in February 2021.

The background

Under the General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED), the European Commission is empowered to assess whether a non-EU state provides a level of data protection that is essentially equivalent to that provided within the EU. Where such protections are deemed to be "adequate", any transfers of personal data between the EU and non-EU state can take place without being subject to any further conditions.

Following the UK's exit from the EU, the UK's data regime had to be reassessed to judge whether it was truly adequate under EU law and whether the EU could continue to permit the free flow of data that had been enjoyed between the UK and other Member States. The UK's data protection regime is governed by the UK GDPR and the Data Protection Act 2018 (DPA). Both are derived from the EU GDPR and the LED, providing similar rights to data subjects and placing similar obligations on controllers and processors, and this had created optimism as to the UK's position post-Brexit.

However, 2020 saw the unfurling of a series of unexpected events in the data sphere which cast uncertainty over what would come next for the UK, in particular:

- the CJEU's invalidation of the longstanding EU-US Privacy Shield as an accepted data transferral mechanism following the hearing of Schrems II in July 2020. Under this decision, the CJEU held that the Privacy Shield failed to comply with the level of protection required under EU law, causing massive disruption in the EU-US data transfer market
- the CJEU's rulings in two separate cases in October 2020 that mass surveillance by national security agencies in France, Belgium, and the UK did not align with EU law (see our Winter 2020 Snapshots). Following these judgments, questions were raised regarding the future data transferring relationship between the UK and the EU, with the Investigatory Powers Act 2016 appearing incompatible with EU law with respect to data processing.

If the EU had deemed the UK's data protection regime to be inadequate, the implications would have been huge, including from an administrative and cost perspective.

The development

Despite the fears around compatibility, on 19 February 2021 the European Commission concluded that the UK ensures "an essentially equivalent level of protection" to the one guaranteed under EU law. Following this assessment, the Commission launched the process towards the adoption of two adequacy decisions for transfers of personal data to the UK under the GDPR and LED.

One influencing factor in this decision is thought to be that the UK, despite leaving the EU, remains part of the European "privacy family" through its adherence to both the European Convention of Human Rights and to "Convention 108" of the Council of Europe, the only binding multilateral instrument on data protection. Compliance with such measures is a key factor for the Commission in judging whether a nation can provide appropriate levels of stability and durability.

Why is this important?

The UK government has warmly welcomed the draft decisions stating that "*seamless international data flows are essential in a hyper-connected world. They underpin the exchange of information and ideas supporting trade, innovation and investment, assist with law enforcement agencies tackling crime, and support the delivery of critical public services sharing personal data as well as facilitating health and scientific research*".

The announcement will be gratefully received by many UK and EU businesses, for whom uncertainty around the future status of data transfers has led to the postponement of significant data innovation projects and the setting aside of finance to account for potential additional compliance requirements had adequacy been denied. Although the Commission's decisions will need to be finalised and approved, this vote of confidence creates a strong and stable base for digital trade with the EU that will give businesses the confidence to invest and to advance their data-focused projects at a time where such innovation is critical to survival in an increasingly competitive market space.

Following the receipt of an opinion from the European Data Protection Board, the Commission will be able to proceed with obtaining approval from Member States through the comitology procedure (a process by which EU law is modified or adjusted via "comitology committees" chaired by the European Commission). This then enables the Commission to adopt the final adequacy decisions for the UK. Once adopted, the Commission's decisions will be valid for four years, following which it will be possible to renew. Until then, data flows between the EEA and the UK continue and remain safe under the EU-UK Trade and Cooperation Agreement. This interim period expires on 30 June 2021.

The UK's adequacy status going forward will remain dependent on the UK maintaining the existing standards of its data protection regime. The Commission Vice President has taken this opportunity to remind the UK that the Commission retains the power to withdraw adequacy in order to "*address any problematic development of the UK system*". At a time when the UK is seeking to forge new trade relationships outside of the EU, this serves as a timely reminder to the UK to be cautious in the face of any pressure from potential trade partners to relax its existing standards.

Any practical tips?

Breathe a deep sigh of relief! If the European Commission had gone the other way on its adequacy finding, life would have become very costly, and frankly very boring, putting all those Standard Contractual Clauses in place.

European Council makes progress on the ePrivacy Regulation

The question

Where have the negotiations on the ePrivacy Regulation got to and what comes next?

Key takeaway

The European Council has taken a significant step forward in the progression of the draft ePrivacy Regulation (the ePR) by agreeing a mandate to carry forward into trilogue negotiations.

Key background

The existing ePrivacy Directive (Privacy and Electronic Communications Directive, also known as the ePD) is an important legal instrument that works to protect privacy in the digital age, with a specific focus on maintaining the confidentiality of communications and providing rules on the tracking and monitoring of individuals. However, in the face of a rapidly changing environment, legislative updates are required in order to tackle new market developments (eg the increasing use of Voice Over IP, web-based email and messaging services etc).

The new ePR is intended to repeal the ePD and is designed to complement and expand on the provisions of the General Data Protection Regulation (GDPR). First proposed in January 2017 as part of the EU's Digital Single Market Strategy, the draft ePR has been working its way through various stages of negotiation. Given its significance, the consequent importance of getting it right, and the many stakeholders involved, the progression of the draft ePR has been slow to say the least. Progress was further hampered by the 2019 EU elections. With no trilogue negotiations – the lengthy inter-institutional negotiations that seek to forge compromises between the Council of Ministers, the European Commission and Parliament – getting underway since the proposal was first adopted in October 2017, concerns were raised over how progress could be expedited.

The development

On 10 February 2021, the European Council's Committee of Permanent Representatives, successfully moved the draft ePR on a stage by agreeing their negotiating mandate. With this mandate now in place, the Council can commence discussions with the European Parliament in order to agree the final text in trilogue negotiations. Once an informal trilogue agreement is in place, the draft ePR will undergo its first reading at plenary session before the European Parliament, followed by the Council.

Why is this important?

Progress regarding the draft ePR has been glacial. As the draft ePR can only become applicable 24 months from entry into force, the timeline for this legislative change remains distant. While the draft ePR text itself remains unpublished at the time of writing, a press release published provides some insight into the decisions made so far. Key updates include:

- communications data: "*as a main rule, electronic communications data will be confidential. Any interference, including listening to, monitoring and processing of data by anyone other than the end-user will be prohibited, except when permitted by the ePrivacy Regulation*"
- cookie consent: "*the end-user should have a genuine choice on whether to accept cookies or similar identifiers. Making access to a website dependent on consent to the use of cookies for additional purposes as an alternative to a paywall will be allowed if the user is able to choose between that offer and an equivalent offer by the same provider that does not involve consenting to cookies*"
- direct marketing: the press release has been fairly tight-lipped around this aspect. It is worth noting that in the previous Portuguese draft (published January 2021) online display advertising did not come within the proposed ePR direct marketing provisions, and the soft opt-in rules for email marketing were to be preserved
- metadata: "*may be processed for instance for billing, or for detecting or stopping fraudulent use. With the user's consent, service providers could, for example, use metadata to display traffic movements to help public authorities and transport operators to develop new infrastructure where it is most needed. Metadata may also be processed to protect users' vital interests, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters*".

Any practical tips?

Although trilogue negotiations remain ahead, the announcement of an agreed mandate over four years after the initial proposal in January 2017 is a huge step forward, particularly in the face of ongoing disagreements between Member States. When adopted, the ePR will be the most significant development in EU data protection law since the UK's exit from the block. While the ePR will not apply directly to the UK, eyes will undoubtedly be sharply focused on what steps the UK takes next and whether the government will introduce aligned domestic legislation or whether it will diverge from the EU approach. Irrespective of this, non-EU businesses that operate within EU member states will find themselves within the scope of the ePR eg where they provide electronic communication services or direct marketing to EU subject end-users.

The impact of the ePR is far-reaching and failure to prepare in advance of its implementation will inevitably prove costly.

ICO resumes investigation into real time bidding (RTB) and AdTech

The question

What will be the ultimate impact of the ICO's continuing investigations into RTB and AdTech?

Key takeaway

In May 2020 the ICO paused its investigation into RTB and the AdTech industry, since they prioritised activities responding to the COVID-19 pandemic. The ICO has now resumed the investigation into RTB and data processing. The ICO has said that the complex system of RTB uses people's sensitive personal data to serve ads requires explicit consent, which is currently not happening.

The background

Having started its review into RTB in February 2019, the ICO paused its investigation into the matter following the start of the pandemic. With things beginning to settle down, the ICO has now been able to resume its investigation.

In a statement in early 2020, the ICO highlighted a lack of transparency due to the nature of the supply chain and the role different actors play in RTB. Six months were given to the RTB industry to work on the points raised by the ICO, which ended in May 2020, when they paused the investigation. The key concerns at the time were, among others:

- the use of "legitimate interests" as the lawful basis for the processing of personal data in RTB being insufficient
- the lawfulness of processing of special category data and the processing of non-special category data without consent
- the reliance on contracts for data sharing across the supply chain
- the lack of transparency on what happens with users' data
- wider security and data sharing issues caused by this data supply chain.

The development

The ICO has announced that its investigation will continue with a series of audits focusing on data management platforms. They will also be issuing assessment notices to specific companies in the coming months where necessary. Naturally, the ICO will be publishing their final findings at the conclusion of the investigation.

Why is this important?

The sharing of data with potentially hundreds of companies, without properly assessing and addressing the risk of these counterparties, raises huge questions from a data compliance perspective, including around the security and retention of this data.

Since the ICO is committed to undertaking further investigations and assessments as to the processing of data for RTB, organisations should be reviewing their practices urgently with a view to avoiding any possible action by the ICO.

Any practical tips?

All organisations operating in the RTB space should assess how they use personal data as a matter of urgency. It's no easy task, but any review should focus on users' consent, legitimate interests, data protection by design and any data protection impact assessments, including through their supply chain. The ICO's guidance should be kept front of mind. Data compliance and RTB is an issue that is not going away.

European Data Protection Board (EDPB) issues draft guidelines for data breach notification

The question

What more could be done to aid data controllers in responding to personal data breaches and the practical considerations they face while operating under the General Data Protection Regulation (GDPR)?

Key takeaway

The EDPB "Guidelines 01/2021 on Examples regarding Data Breach Notification" (Draft Guidelines) are intended to be used by data controllers in conjunction with their pre-existing tool kit to effectively manage and prevent data protection breaches. These new Draft Guidelines are not intended to serve as a comprehensive list of recommended actions, as every incident requires its own assessment and appropriate actions.

The background

The EDPB accepted that the guidelines on personal data breach, produced by the former EDPB Article 29 Working Party, lacked adequate detail and provided little by way of practical considerations. In response, the EDPB has published its Draft Guidelines to provide data controllers new guidance on how to better handle prevent, understand and respond to data breaches.

The guidance

The Draft Guidelines outline six categories of data breaches with example cases as listed below. Many of these examples refer to "data exfiltration", which essentially means a form of security breach (often using malware) when an individual or company's data is copied, transferred or retrieved from a computer or server without authorisation.

1. **Ransomware**
   - Ransomware with proper backup and without exfiltration (Case No.01)
   - Ransomware without proper backup (Case No.02)
   - Ransomware with backup and without exfiltration in a hospital (Case No.03)
   - Ransomware without backup and with exfiltration (Case No.04)

2. **Data exfiltration attack**
   - Exfiltration of job application data from a website (Case No.05)
   - Exfiltration of hashed password from a website (Case No.06)
   - Credential stuffing attack on a banking website (Case No.07)

3. **Internal human risk**
   - Exfiltration of business data by a former employee (Case No.08)
   - Accidental transmission of data to a trusted third party (Case No.09)

4. **Lost or stolen devices or paper documents**
   - Stolen material storing encrypted personal data (Case No.10)
   - Stolen material storing non-encrypted personal data (Case No.11)
   - Stolen paper files with sensitive data (Case No.12)

5. **Mispostal**
   - Snail mail mistake – sending of incorrect packing bills with goods to customers (Case No.13)
   - Sensitive personal data sent by mail by mistake (Case No.14)
   - Personal data sent by mail by mistake (Case No.15)
   - Snail mail mistake – sending of two different insurance summaries to one recipient (Case No. 16)

6. **Social engineering**
   - Identity theft (Case No.17)
   - Email exfiltration (Case No.18)

The example cases within the categories highlight the practice-based focus of the Draft Guidelines and further serves to provide data controllers with a wide-ranging list of forms data breaches can take.

Each case in the Draft Guidelines is broken down into two sections:

A. **Prior measures and risk assessment** – this section looks at reducing the overall likelihood of data breaches occurring whilst providing guidance on how to assess the risks from a breach. It cites examples such as implementing proper patch management, the use of appropriate anti-malware detection systems, proper and separate backup systems and providing employee training (SETA program).

B. **Mitigation and obligations** – this section is concerned with mitigating the damage caused by the data breach and the resultant obligations on the data controller. It suggests carrying out an impact assessment, ensuring there is an incident response process, documenting all data breaches in accordance with Article 33(5) and knowing when an obligation to communicate with the data subject arises.

Why is this important?

The previous EDPB guidelines were more theoretical than practical, and the practice-based, example-driven approach of the new Draft Guidelines should be welcomed. They provide greater clarity and concrete guidance for both the prevention and mitigation of data breaches.

Any practical tips?

The UK is of course no longer a member of the EU, but the GDPR remains at the core of data protection law in the UK and, although the ICO has final authority on these issues, it is highly unlikely the ICO will deviate from the EDPB's Draft Guidelines. Either way, the categorisation and recommendations in the Draft Guidelines should certainly be welcomed by data controllers in the UK.

The Draft Guidelines emphasise good practice in lieu of strict legal obligations and aims to provide accountability to data controllers. Remember that the categories and examples provided are not intended to be used as an exhaustive list. It goes without saying that data protection is one of the fastest evolving areas and no single list can accurately depict all forms of data breaches.

DATA

DCMS publishes prototype trust framework on digital identity products and services

The question

What is the potential impact of the trust framework on the provision and use of digital identity services published by the Department for Digital, Culture, Media & Sport (DCMS)?

Key takeaway

The draft "alpha" framework sets out principles, policies, procedures and standards governing the use of digital identity to allow for the sharing of information to check people's identities or personal details. It also sets out the requirements that organisations will have to meet in order to be certified against the framework once, as is expected, it becomes law.

The draft framework

The publication of the draft framework follows off the back of the call of evidence on digital identify policy in July 2019. It sets out specific future standards and requirements for organisations which provide or use digital identity services, including:

- how organisations should handle and protect people's data (published through a data management policy)
- what security and encryption standards should be followed
- informing users of changes made to their digital identity and how their accounts are managed
- having account recovery processes and notifying users if organisations suspect a user's account has been fraudulently accessed
- following guidance on how to choose secure authenticators for their service.

Under the new framework organisations will also have to publish a yearly report explaining which demographics have been, or are likely to have been, excluded from their service and why. Additionally, the framework promotes "vouching" where trusted people within the community such as doctors or teachers "vouch for" or confirm a person's identity as an alternative to using traditional identification documents (eg passports and driving licences).

Why is this important?

All organisations providing or using digital identity services will need to meet the requirements in order to be certified against the trust framework. It is therefore important to start preparing ahead of the framework becoming law in the future in order to ensure compliance ahead of certification.

Any practical tips?

The deadline for any comments from organisations was 11 March 2021 through an electronic survey. Following comments, the DCMS will incorporate the feedback into the framework and intends to publish a second iteration in short order after March 2021 containing further details relating to the framework and certification.

The publication of the "alpha" framework allows organisations to start planning ahead of the implementation of the framework into law and the introduction of any new requirements. If you're providing digital identity products and services, now is the time to start studying how the framework may impact your business. Equally, if you rely on third party providers of these services, consider how to start integrating the requirements into your contracts.

ICO launches data analytics toolkit

The question

What's in the ICO's new data analytics toolkit, and how far down the privacy compliance road does it take you?

Key takeaway

The UK Information Commissioner's Office's (ICO) new toolkit provides organisations with key data protection points they need to consider for any project which involves data analytics and personal data.

The background

As part of its priority work on artificial intelligence (AI), the ICO has launched a new toolkit for organisations which are planning to use personal data for data analytics. The toolkit outlines important personal data protection considerations which organisations should consider at the beginning of any scheme involving personal data processing. It is part of the ICO's AI priority work and follows the ICO's recent publications "*Explaining decisions made with AI*" and "*Guidance on AI and data protection*". As the ICO notes, the toolkit will assist businesses in identifying some of the most significant risks for individuals' privacy rights and freedoms that can result from the use of personal data analytics. The ICO stresses that many data analytics risks are context specific, so the toolkit cannot guarantee complete compliance with data protection law. That said, it should be regarded as one of your main starting points on any data analytics project you are considering.

The toolkit

The toolkit is aimed at assisting organisations at the beginning of a data analytics project lifecycle. It focuses on helping recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics and is designed to be a basic introduction to some of the risks to individuals that data analytics may create or worsen.

Many of the risks that arise from the application of data analytics are context specific, therefore the ICO cannot include an exhaustive or definitive list of issues to consider. Naturally assessing the risk in the context of organisations processing activities form part of the organisation's responsibility as a controller. The toolkit therefore comes with the clear caveat that: "*you should not view this toolkit as a pathway to absolute compliance with data protection law, but as a starting point for what you will need to consider*".

The toolkit is designed for organisations and their data protection officers (DPOs) to consider risks, rights and freedoms in the context of data protection law. It is not a comprehensive analysis of every factor that needs to be considered when implementing a data analytics system. Although there are links between the fairness principle of data protection law to ethics and equality, organisations will need to consider these and other elements separately to ensure they are compliant with any additional obligations they may have.

Data analytics

The toolkit defines data analytics as "*the use of software to automatically discover patterns in data sets (where those data sets contain personal data) and use them to make predictions, classifications or risk scores*". Integral to data analytics as defined by the ICO are algorithms, and organisations are increasingly using a specific category of advanced algorithm, namely AI to complete tasks. The ICO defines AI as "*the theory and development of computer systems able to perform tasks normally requiring human intelligence*" and cross-refers to the ICO's earlier guidance on AI for an analysis of the risks that the use of AI can create for individuals. The ICO stresses that the toolkit can assist regardless of whether AI is used in connection with personal data analytics projects.

How does the toolkit work?

The toolkit starts by asking various questions to determine the legal regime the organisation will be processing under as well as questions relating to lawfulness, accountability and governance, the data protection principles, and data subject rights. Upon using the toolkit, a short, tailored report is created suggesting practical actions the organisation can take and provides links to additional guidance that will help the organisation improve its data protection compliance. The ICO notes that complying with these recommendations is not a guarantee that the toolkit will comply with data protection law, and it is crucial that organisations consider the advice the ICO gives in the context of processing and seek the advice of their DPO where needed.

The ICO further notes the toolkit is anonymous, and the answers provided are not visible to or retained by the ICO. It advises organisations to download a copy of the report generated and retain this for future reference.

Why is this important?

It is vital that data protection compliance is built in from the start whenever data analytics are being contemplated to process personal data. This is not only the law but a crucial step in gaining public trust and confidence.

The toolkit is a useful practical addition to the ICO's two pieces of guidance on AI referred to above, namely "*Explaining decisions made with AI*" and "*Guidance on AI and data protection*". Although none of these, either individually or combined is intended to provide a one-size fits all solution, they do provide a strong foundation for data protection compliance and their application will provide key evidence of accountability under the GDPR.

Any practical tips?

The toolkit is a welcome addition to compliance processes when commissioning, designing, and implementing data analytics. It's definitely a good place to start on any of these projects, but there's no substitute for doing a deeper dive with your DPO. After all, data compliance sits at the heart of any analytics programme and getting the privacy building blocks lined up correctly from the start is crucial.

Leads Works lands £250,000 fine for sending marketing messages without consent

The question

What level of fine are you looking at for sending mass marketing messages without consent?

Key takeaway

Take great care over who you partner with on data marketing campaigns. They may not be as strong on data compliance as they (and in turn you) think they are. Running some basic due diligence checks is a must if they claim to be relying on marketing consents obtained themselves or through other third parties.

The background

On 1 March 2021, West Sussex-based Leads Works Ltd (LWL) were issued with a £250,000 fine for sending 2,670,140 marketing text messages, between 16 May 2020 and 26 June 2020, to individuals without their consent in breach of Regulation 22 of the Privacy and Electronic Communications Regulations 2003 (PECR). The messages resulted in excess of 10,000 complaints over a period of 14 days.

LWL is a lead generation company which operates primarily in the "multi-level marketing" sector. It generates leads under the Avon cosmetics brand for the purpose of enlisting downstream recruits to sell Avon products. These leads are then passed directly to independent Avon sales representatives for further contact in terms of recruitment.

LWL first came to the attention of the ICO in connection with complaints about text messages seemingly sent by Avon Cosmetics. The investigation found that Avon did not send or instigate the texts. LWL were contacted, but not investigated at that time. LWL then came to the attention of the ICO again during the COVID-19 pandemic, when a significant number of complaints were received about the following text message: "*In lockdown and want to earn extra cash? Avon is now FULLY ONLINE, FREE to do and paid weekly. Reply with your name for info. 18+ only. Text STOP to opt out*". At this stage, complaints started to be received in significant numbers prompting the ICO to open an investigation in May 2020.

The ICO's investigation

LWL provided information relating to the purchasing of their data sets and the contractual structure of their working relationships with their partners, as well as evidence of their GDPR policies and purported evidence of consumers opting in. In respect of the latter, LWL explained that they had received most of their data sets from one provider's data capture website. This website consisted of a landing page to opt-in, a privacy notice and an option to unsubscribe. A link on the website presented individuals with a further list of 457 distinct organisations from whom individuals could expect to receive marketing communications. LWL was not included in this list. Furthermore, the ICO found the website to be vague and confusing and the consent statement lengthy and digressive. It also prevented individuals from submitting their details without checking "at least one" marketing channel. Unsurprisingly, the ICO concluded that the consent was not freely given, specific and informed.

In deciding to impose a substantial monetary penalty, the ICO took account of the seriousness of the contravention as well as other aggravating factors. For example, the ICO noted that the text messages misleadingly appeared to be sent by Avon Cosmetics Limited, when in fact they were not responsible for these. LWL subsequently accepted that it had deliberately failed to identify itself in the body of the texts as the sender. The ICO also highlighted that LWL had continued to run the marketing campaign both during and since the conclusion of the ICO's investigation, with no attempt to amend or review its practices – this was despite having received a Notice of Intent from the ICO that its practices were deemed non-compliant. This resulted in an additional 28,000 complaints being lodged using a SPAM reporting tool in place from August 2020. To add to the ICO's frustration, LWL repeatedly indicated that they were compliant with PECR and had a long-standing commitment to compliance, which was found to be blatantly untrue as a result of the investigation. The ICO stated, among other things, that LWL had not been completely open and transparent in relation to the enquiry and had failed to inform the ICO in its response to enquiries about marketing methods that it had also conducted email marketing. The ICO failed to find any mitigating factors.

Why is this important?

The ICO's investigation and the penalty imposed shows the importance of obtaining freely given, specific, informed and unambiguous consent before sending any marketing communications to consumers. It also highlights the dangers of relying on third parties to obtain consent and of failing to be completely transparent with the ICO with an investigation and acting quickly when compliance errors are identified.

Any practical tips?

Be careful who you partner with to run your data marketing campaigns! The case underlines the need to carry out due diligence into their marketing practices, rather than simply relying on contracts terms. This is especially the case where your partner is relying on marketing consents derived from a third party's database – always a compliance red flag! And remember it's the brand name, which is tarnished by aggravating marketing tactics, not the agency you partner with.

EDPB adopts guidelines on virtual voice assistants

The question

Virtual voice assistants (VVAs) are becoming mainstream. What are the data protection implications and how does the European Data Protection Board (EDPB) suggest you address them?

Key takeaway

The EDPB's recently adopted draft guidelines identify some of the most relevant compliance challenges with VVA's and include recommendations on how to address them. These focus on improved transparency, for example giving users better access to privacy policies and clearer information on how their data is being processed for e-commerce and telecommunication services. The guidelines also note that consent might not always be required for the processing of user data and set out the specific legal basis for the processing of VVA data.

The draft guidelines

The EDPB adopted its draft guidelines on 9 March 2021 and started a consultation on them on 12 March 2021, which closed on **23 April 2021**. The EDPB aims to publish a final version later this year once it has received the feedback.

As VVAs process users' personal data in their functionality, they must comply with the legal requirements under the General Data Protection Regulation (GDPR) and the e-Privacy Directive. Some of the key areas the new guidelines address are as follows:

- **briefer privacy policies and improved transparency** – VVA developers are encouraged to refrain from using lengthy and complex privacy policies and to better communicate them, either through a display (if the device has one) or through voice-based interfacesm
- **requirement for registration** – currently VVAs only require a single registration for the use of all of the VVAs' functionalities, but the EDPB now recommends that developers implement requirements for users to register separately for all the different services, thereby enabling data protection by design and by default.

The guidelines also address the possible legal basis for the processing of personal data by VVAs, specifically in relation to executing requests, improving the VVA machine learning model, biometric identification and profiling for personalised content or advertising. For the purposes of executing users' commands, VVAs do not have to have consent to process their data, but instead are exempt under Article 5(3) e-Privacy Directive. However, consent will still be required for the storing or gaining of access to information for any purpose other than executing users' requests.

According to the guidelines, VVA developers should also not retain users' data for longer than is necessary for the purposes for which the personal data are processed. Currently many retain it indefinitely until requested to be deleted, which is not in line with the storage limitation principle.

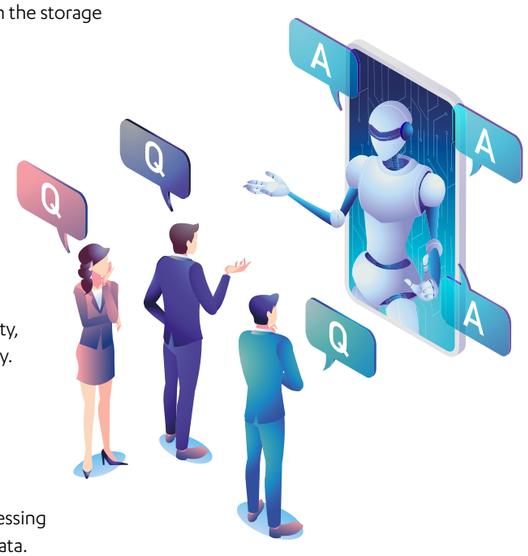
The guidelines also note that VVAs can process the data of multiple users (eg family members), so developers should implement access control mechanisms to ensure confidentiality, integrity and availability. As passwords are not suitable for VVAs, the guidelines set out options such as using biometric identification for processing special categories of data.

Why is this important?

The guidelines are an important, and timely, reminder of the importance of good data protection practice in the development of new technology, like VVAs, which have the power to hoover up vast amounts of data directly from within the home.

Any practical tips?

Clearly the guidelines are a "must read" for those closely involved in any VVA projects. On the practical side, and as recommended by the EDPB, remember also the need to carry out a full Data Protection Impact Assessment at an early stage.



UK publishes response to consultation on online harms

The question

What does the government's response to its consultation on the Online Harms White Paper mean for "Big Tech"?

Key takeaway

Companies are going to be obliged to ensure that their services and platforms provide safe spaces for users, as well as take steps to halt the proliferation of harmful misinformation.

The background

The government has published the response to its Online Harms White Paper, following the paper's first publication in April 2019. The White Paper sets out significant evidence of harmful content and activities taking place online, as well as the increasing public awareness and concern about online content that is not illegal but is potentially harmful. It covered *"online content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by reducing trust and undermining our shared rights, responsibilities and opportunities to foster integration"*. The types of content/activities range from cyber-bullying to misinformation. While the White Paper acknowledges that these activities may not be illegal, it does recognise they can have significantly damaging effects as well as having a detrimental impact on user's online experiences, particularly amongst children and young adults.

In order to address the harmful content and activities identified in the White Paper a new duty of care, aimed at making companies take responsibility for user safety, was proposed. Its aim is to improve the safety for users of online services and prevent people from being physically or psychologically harmed as a direct consequence of content and activity on those services, as well as holding content providers and/or facilitators accountable. The consultation gathered views on various aspects of the government's plans for regulation and tackling online harms, including:

- the online services in scope of the regulatory framework
- options for appointing an independent regulatory body to implement, oversee and enforce the new regulatory framework
- the enforcement powers of an independent regulatory body
- potential redress mechanisms for online users
- measures to ensure regulation is targeted and proportionate for industry.

The development

The government has committed to making the Online Safety Bill ready in 2021, which will give effect to the new regulatory framework outlined in the response. This follows criticism from the House of Lords regarding the urgency with which a new regime was needed, and the fact that the COVID-19 pandemic has meant that *"the risks posed by illegal and harmful content and activity online have also been thrown into sharp relief as digital services have played an increasingly central role in our lives"*. The incoming regulatory framework, to be overseen and enforced by Ofcom, will apply to companies whose services host user-generated content, or who facilitate public or private online interaction between users and search engines. This means that as well as applying to, for example, publicly shared content on social media platforms, it will also apply to online instant messaging services and private social media groups.

There are several exemptions provided, including for business-to-business services and services used internally by organisations. Additionally, the legislation will not impact journalistic content published by a newspaper or broadcaster on its website. It should also be noted that regardless of the country in which a company is based, if they provide services to users in the UK then they will be in scope of the new regulatory framework.

One question of importance to those companies likely caught by the incoming regulations is what exactly constitutes harmful content or a harmful activity and what steps need to be taken to ensure compliance with the rules? The response states that the legislation will provide a general definition and that it will include content or activities that give rise to a reasonably foreseeable risk of harm to individuals. The framework will also take a tiered approach that outlines the steps that need to be taken in relation to harmful activities or content.

Most services provided by companies will be Category 2 services, such as dating apps and private messaging services. Providers of Category 2 services will need to take proportionate steps to address illegal content and activity (in each case which meet the definition of harm) and to protect children from content that would be harmful to them, such as violent or pornographic content. There is then a small group of high-risk, high-reach services, that will be designated as Category 1 services, mainly consisting of large social media sites. Providers of these services will additionally be required to act in respect of content or activity on their services which is legal but harmful to adults. All companies in scope will also have several additional duties in addition to the core duty of care, including providing mechanisms to allow users to report harmful content or activity and to appeal the takedown of their content.

Additionally, the regulations aim to take on the recently spotlighted phenomenon of "fake news". The new duty of care will cover misinformation and disinformation and oblige companies to implement specific transparency requirements that are likely to be more stringent that the steps already being taken by social media organisations to curb the potential harm caused by fake news.

The government has also confirmed that Ofcom will have robust enforcement powers in order to ensure compliance with the regulatory regime. The current proposal is to give Ofcom the power to issue fines of up to £18m or 10% of global annual turnover, whichever is the higher, for non-compliance with the new regime.

Why is this important?

Continued accessibility to the internet as well as the increasingly central role that online services are playing in our day-to-day lives mean that there is more and more of a spotlight being shone on the content that is able circulate across platforms.

Organisations must ensure that effective technical, organisational and administrative measures are in place in order to ensure compliance with the new regulations as well as taking steps to increase both government and public confidence in the ability of organisations to properly police the services they provide.

Any practical tips?

Implementing and maintaining appropriate measures to ensure compliance with the regulations will be a cheaper alternative that getting stuck with an investigation and a potentially sizeable penalty from Ofcom.

It will be important to keep an eye on publications and any enforcements coming from Ofcom to understand how they will interpret and enforce the regulations. In the meantime, organisations should be starting to implement robust procedures to ensure that harmful content is not propagated through their platforms. Some measures could include:

- ensuring fast responses to reports of harmful content
- ensuring that effective monitoring procedures are in place in order to detect and remove harmful content
- updating codes of conduct for users, and
- considering bans for users found to be in breach.

Ofcom introduces new rules protecting the mental health of those participating in TV and radio programmes

The question

What measures will TV and radio broadcasters have to put in place to protect the mental health of participants?

Key takeaway

TV and radio broadcasters will have to take due care over the welfare of people who might be at risk of significant harm as a result of taking part in a programme they produce. The participants must also be informed about any potential welfare risks that might arise from their participation and any steps the broadcaster or programme-maker intends to take to mitigate these risks.

The background

In March 2021 Ofcom updated section seven (specifically 7.15) of the Broadcast Code to include a provision requiring broadcasters to take due care over the welfare of a participant who might be at risk of significant harm as a result of taking part in a programme, except where the subject matter is trivial or their participation minor.

The new rules apply to all programmes that began production on or after **5 April 2021**.

The development

Ofcom also specify that a participant might be regarded as being at a risk of significant harm as a result of taking part in a programme for reasons including:

- they are considered a vulnerable person
- they are not used to being in the public eye
- the programme involves being filmed in an artificial or constructed environment
- the programme is likely to attract a high level of press, media and social media interest
- key editorial elements of the programme include potential confrontation, conflict, emotionally challenging situations
- the programme requires them to discuss, reveal, or engage with sensitive, life changing or private aspects of their lives.

Broadcasters should, under the new rules, conduct a risk assessment to identify any risk of significant harm to a participant, unless it is justified in the public interest not to do so. However, the level of care required will be proportionate to the level of risk associated with their participation in the programme.

Why is this important?

The rule changes set a clear standard for the protection of participants' wellbeing, especially given the level of notoriety and criticism often faced by participants in, for example, reality shows such as *Love Island*. The Broadcast Rules therefore require that broadcasters take steps to help protect them from the onslaught of attention and undoubted impact thereof on their mental health.

The rules will apply to online broadcasters, such as YouTube, and can include original programming that might put participants at risk of damage to their welfare mentally.

Any practical tips?

According to Ofcom's guidance on the new rule, published in March 2021, there are some best practice considerations that broadcasters and programme-makers should be mindful of:

- having written guidelines and/or procedures in place setting out key considerations for working with participants in particular programmes, and production staff should be familiar with them and have access to them where needed
- making and retaining records, contemporaneous notes, and/or any other documentation, which can assist in demonstrating what information and support was offered and provided to a contributor during production
- seeking of independent expert advice from qualified specialists where needed at different stages of production, including in the participant selection phase to help with the selection process can assist in identifying, before production begins, people who may be vulnerable, or may become vulnerable. This early identification can then enable the assessment and management of any reasonably foreseen risks in advance
- participants should have access to specialists in certain circumstances without the need for intervention by production staff, and participants should be given a nominated single point of contact within the production team with whom they can liaise throughout the production process
- aftercare should also be given to participants and programme-makers should be flexible to the type of support a contributor might reasonably require or request and remain responsive to a contributor's needs for an appropriate period of time after the programme has been broadcast.

DIGITAL

"The rule changes set a clear standard for the protection of participants' wellbeing, especially given the level of notoriety and criticism often faced by participants in, for example, reality shows such as Love Island."

CMA publishes refreshed Digital Markets Strategy

The question

What has changed as part of the Competition and Markets Authority's (CMA) refresh of its Digital Markets Strategy?

Key takeaway

The CMA has announced that, as part of its refreshed Digital Markets Strategy, it has reoriented towards a new overarching ambition that focuses on developing the Digital Markets Unit into a "*proactive new pro-competition regulator for digital markets*".

The background

In 2019 the CMA published its Digital Markets Strategy, which acknowledged the significant changes taking place across the UK economy (and our society more broadly) as a result of the development of digital markets. Under this strategy, the CMA committed itself to a broad digital strategy and, in the 18 months since the unveiling of this plan, the CMA has announced that it has successfully achieved several of its goals, including:

- the publication of its final report on the market study into online platforms and digital advertising, assessment of the effectiveness of competition in the digital advertising space and making recommendations for a new regulatory framework
- the establishment of the Digital Regulation Co-Operation Forum (DRCF) alongside the Information Commissioner's Office (ICO) and Ofcom, designed to promote cooperation and coordination on online regulatory matters
- the increase of its data and behavioural science capabilities through the work of the DaTA unit, including launching an "Analysing Algorithms Programme", and
- the hosting of its "Understanding Digital Markets: Innovation, Investment and Competition" conference in March 2020.

The development

As a result of the CMA's achievements outlined above, and due also to significant developments in both the political and regulatory spheres during this time, the CMA has announced that its strategy has undergone a refresh. This marks a step-up across its digital work and a new focus on what it describes as its "overarching ambition" – building towards a proactive new pro-competition regulator for digital markets in the shape of the Digital Markets Unit (DMU). Under this new umbrella policy, the CMA has set out seven priority areas that will become its focus going forward.

1. **Establishing the pro-competition regulatory framework and function**: The CMA will look to build out and strengthen the DMU focusing on its funding, governance and decision-making structures. The CMA will continue to support the government as its consults on the CMA's advice around the design and implementation of a new pro-competition regulatory regime and its application to businesses designated with "Strategic Market Status".
2. **Using its existing tools**: The CMA will continue to use its existing powers to "maximum effect" to become an increasingly active enforcer, for example through its use of consumer protection law to guard against fake online reviews and unfair roll-over contracts in subscriptions for online gaming.
3. **The work of the Data Technology and Analytics (DaTA) unit**: The DaTA unit is an invaluable resource to the CMA, using the latest in data engineering, machine learning and AI techniques, it assists the CMA's understanding of how organisations use data, what algorithms they use and the consequences of this, and ultimately, what actions the CMA should take.
4. **Digital Regulation Co-Operation Forum**: The DRCF is due to publish an ambitious workplan shortly and the CMA has confirmed that, alongside Ofcom and the ICO, it will continue to work with the Government on projects of interest, for example, algorithms and how regulatory coherence can be ensured.
5. **International cooperation**: The CMA intends to continue to forge close relationships with other international regulatory authorities in the digital sphere – such as the Organisation for Economic Cooperation and Development, International Competition Network and the International Consumer Protection and Enforcement Network. By strengthening these relationships, the CMA hopes to form a strong foundation for the DMU to build on.
6. **Support Government on reform proposals of existing tools**: The CMA supplemented its reform proposals with its Taskforce advice, including proposals to: (i) strengthen the markets tool; (ii) to establish a distinct merger control regime for firms with Strategic Market Status, (iii) to address economically harmful online content; and (iv) to strengthen enforcement of the Platform to Business (P2B) Regulation. The CMA has committed to supporting the Government as necessary to ensure that its tools remain relevant in line with evolving digital markets.
7. **Updating existing CMA guidance**: Keep your eyes peeled for incoming guidance from the CMA which is expected to cover the Merger Assessment Guidelines.

Why is this important?

International regulatory authorities are increasingly beginning to action digital market policy proposals. While the government will ultimately dictate the direction of the CMA's strategy, it is unavoidable that this regulatory sphere is to undergo a significant shift over the coming years.

Any practical tips?

Organisations subject to the scrutiny of the CMA should familiarise themselves with the CMA's refreshed strategy and look to proactively monitor any updates or announcements that are published over the coming months. The CMA and the government are looking to encourage, not stifle, the digital development of the UK; however, as part of this the CMA will look to develop an in-depth knowledge of the workings of large tech organisations and the algorithms being employed. Transparent practices are therefore strongly encouraged in the face of what is anticipated to be an increasingly inquisitive regulator.

HM Treasury publishes consultation on the regulatory approach to cryptoassets

The question

What is the regulation of cryptocurrencies in the UK likely to look like?

Key takeaway

While still not totally mainstream, steps are being taken by the UK Treasury and the Financial Conduct Authority (FCA) to effectively regulate cryptocurrencies.

The background

A cryptoasset (also known as a "tokens" or "coins") is a digital representation of value or contractual rights that can be transferred, stored or traded electronically. At present a large proportion of cryptoassets fall outside, or are likely to fall outside, the regulatory perimeter. This means they may not be subject to the same consumer protections or safeguards found in other areas of financial services and payments. This may prevent benefits from being realised and exposes consumers to potential harms. Depending on prevalence and value transferred, they could also pose financial stability and consumer risks.

While there is currently no internationally agreed schedule of cryptoassets, the FCA essentially takes the view that it will regulate assets based on a system that emulates the "*if it walks like a duck and quacks like a duck*" test. Essentially, if a cryptoasset looks like e-money it will be regulated as e-money. Similarly, if a coin or a token meets the definition of a financial instrument (for example, a share, a bond or a derivative), then it will be regulated as such.

"Stablecoins" are an evolution of cryptoassets, which, as the name suggests, seek to minimise instability in value. This is achieved by backing the Stablecoin with collateral such as an asset, commodity or a fiat currency (government-issued money that is not pegged to or backed directly by any commodity, eg gold or silver). Stablecoins have gained traction as they are seen to offer the best of both worlds, offering users the instant processing and payment of security/privacy of cryptocurrencies, and the volatility-free stable valuations of fiat currencies. Currently Stablecoins, depending on their design/anchoring, can fall into one of several sub-categories of cryptocurrency and as such are largely unregulated. However, the proposals set out in the Treasury's consultation paper seek to change this.

The development

The Treasury's proposals set out in the consultation paper would maintain the FCA's classification of cryptoassets but add to this a new form of regulated cryptoasset, the "Stablecoin" or "Stabletoken", for use as a means of payment. In doing so it is seeking to improve certainty for Stablecoin users, and the market, and to address risks likely to arise on the developing market if such tokens remain outside the regulatory perimeter. Other forms of cryptocurrency, such as Bitcoin, will retain their position as being largely unregulated with regards to conduct and practical matters. Instead, the proposal is to bring these within the scope of the financial promotion's regime, so that they are subject to stricter regulation in respect of communications made about them to the public.

The proposals set out in the paper reflect the government's view that Stablecoins (as opposed to other forms of cryptocurrency) have the potential to play an important role in retail and cross-border payments. However, this is not without some inherent risks. In particular, the government highlights potential financial instability and damage to market integrity that could arise from system disruption or outages in addition to the well-known concerns about cyber-security and financial crime.

In order to subvert these risks, the government is proposing to bring Stablecoins used as a means of payment into the scope of regulation and subject them to minimum requirements and protections as part of a UK authorisation regime. The new regime would cover both firms issuing Stablecoins and firms providing services facilitating the use of Stablecoins, based upon a specified list of activities that the government considers should be regulated (including issuing, creating or destroying asset-linked and fiat-linked tokens, transmission of funds, and providing custody and administration of a Stablecoin for a third-party). Businesses likely to be caught by the regulations include issuers, system operators, cryptoasset exchanges and wallet providers.

The consultation paper also notes that the proposed regime will provide for exclusions, for example where the Stablecoin is used only within a limited network of service providers or for acquiring a very limited range of goods or services. However, outside of those exclusions, all Stablecoins will be subject to some form of regulation, though a lighter regime is being considered for smaller firms which have turnover which falls below a certain level. In determining its approach, the FCA will be considering how to align regulatory treatment with existing comparable frameworks. For example, the government is contemplating whether Stablecoins that are linked to a single fiat currency should be subject to the same requirements that apply to e-money tokens.

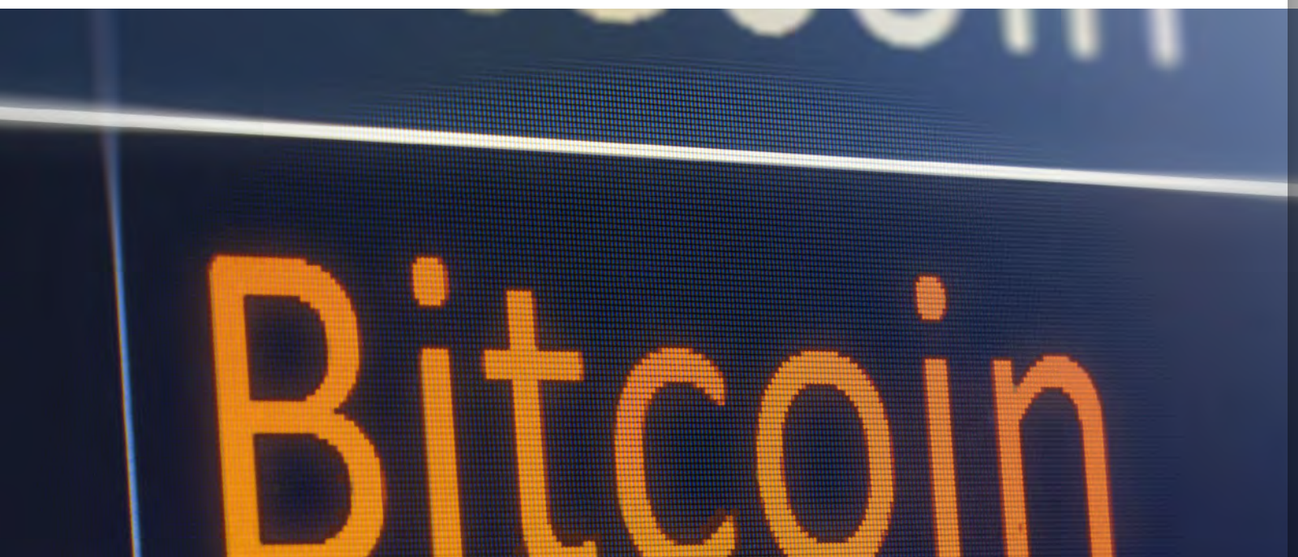
Why is this important?

Companies that fall within the scope of the regulatory framework will be subject to all the usual authorisation requirements and regulatory obligations regarding systems and controls, the maintenance and management of a reserve of assets, conduct rules, operational resilience and notification and reporting requirements.

Additionally, the proposed framework highlights greater government oversight of cryptoassets and could signal the start of things to come.

Any practical tips?

Keeping an eye on the developments from the FCA will assist companies in preparing for the regulations. However, in the meantime companies can look to existing regulatory regimes with regards to cryptocurrencies (such as the Electronic Money Regulations) which could give some basic indication as to the types of regulations that could be expected.



The EDPS publishes its opinion on the Digital Services Act and Digital Markets Act

The question

What recommendations has the European Data Protection Supervisor (EDPS) made in respect of the EU's proposed Digitals Services Act (DSA) and Digital Markets Act (DMA)?

Key takeaway

The EDPS has announced additional recommendations designed to give greater protection to individuals when it comes to content moderation, online targeted advertising and recommender systems used by online platforms under the DSA and DMA.

Key background

As part of the Europe's Digital Strategy "*Shaping Europe's Digital Future*", at the end of 2020 the European Commission published proposals centring around an ambitious reform of EU legislation and designed to safeguard consumers and businesses that make use of online platforms such as search engines, social networking sites and online marketplaces.

The proposed reforms will take effect through two directly applicable, full harmonisation Acts: the DSA and the DMA. The stated goals of both the DSA and the DMA are:

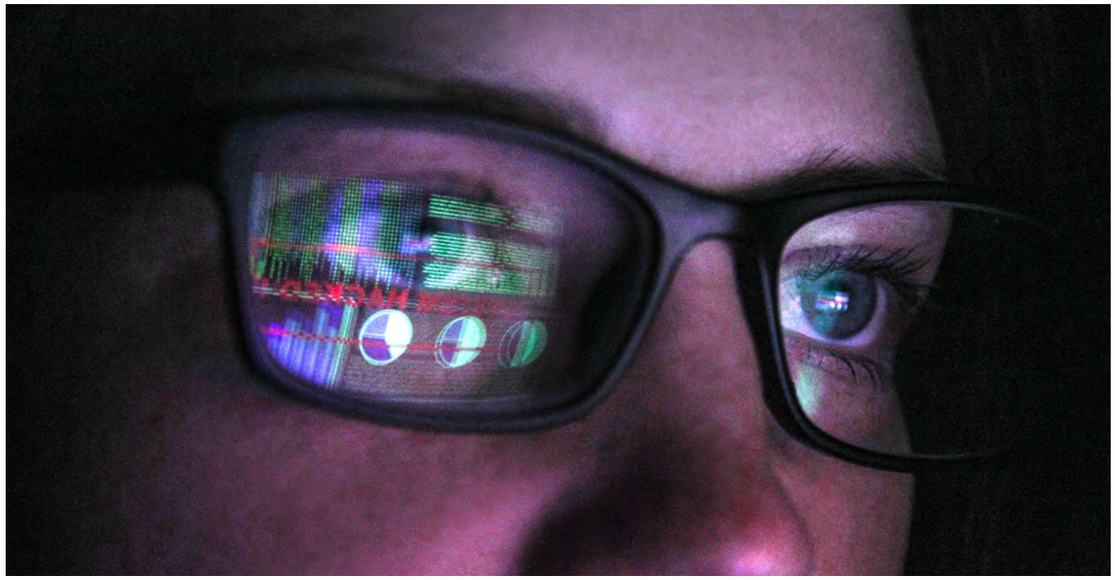
1. "*to create a safer digital space in which the fundamental rights of all users of digital services are protected; and*
2. *to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally*".

The development

In February 2021, the EDPS published its opinions in respect of the European Commission's legislative proposals.

These opinions are intended to influence and assist legislators to produce final form legislation which reflects the EU's fundamental values around individual data protection rights.

Through these opinions, the EDPS has signalled its approval of the DSA's stated intention to promote a transparent and safe online environment and noted that while the proposal "*does not impose a general monitoring obligation, it confirms reasonable liability exemptions and supplements them with a pan-European system of notice and action rules, so far missing*". In relation to the DMA, the EDPS has welcomed the Act's stated intention to "*promote fair and open digital markets and the fair processing of personal data through the regulation of large online platforms acting as gatekeepers*".



Digital Services Act

In relation to the DSA, the EDPS has made several recommendations designed to better protect individuals with regards to: (i) targeted advertising; (ii) the moderation of content; and (iii) recommended systems used by online platforms. The EDPS specifically recommends:

1. additional safeguards around the three areas specified above, eg providers who wish to profile their users for content moderation, should be able to demonstrate that such measures are strictly necessary to address the systemic risks identified by the DSA
2. the phasing-out, and eventual prohibition, of targeted advertising based on pervasive tracking
3. increased restrictions around which data categories can be processed for targeting purposes and which data categories may be disclosed to advertisers or third parties to enable targeted advertising
4. the introduction of minimum interoperability requirements for large online platforms with explicit obligations on very large online platforms to support interoperability, as well as obligations not to take measures that impede such interoperability
5. the development of technical standards around interoperability at European level, in line with the applicable EU legislation on standardisation.

Digital Markets Act

The EDPS highlights how the relationship between competition, consumer protection and data law are "*inextricably linked policy areas*" in the context of the online platform economy, and that this relationship should be one of complementarity. The EDPS elects to specifically highlight those provisions of the proposed Act which have the effect of mutually reinforcing the "*contestability*" of the market and which affect the control of individuals over their personal data. These include, for example, articles 5(f) and 6(1)(b) which prohibit mandatory subscription by end-users to other core platforms services offered by the gatekeeper and allow the end-user to uninstall pre-installed software applications on the core platform service, respectively.

As it did with the DSA above, the EDPS also makes some specific recommendations for improvements to the DMA:

1. that gatekeepers are to provide end-users with a solution of easy and prompt accessibility for consent management
2. increased clarity around the scope of the data portability
3. where necessary (eg see Article 6(1)(i)) rewording provisions of the Proposal to ensure full consistency with the GDPR
4. highlighting the need for effective anonymisation and re-identification tests when sharing query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper.

As part of its recommendation, the EDPS recommends that the DMA Committee should include representatives from the EDPS, and also calls for structured cooperation between the relevant oversight authorities in order to ensure the uninhibited exchange of information between them, allowing them to fulfil their complementary role.

As with the DSA above, the EDPS once again invites the co-legislators to consider introducing minimum interoperability requirements for gatekeepers and to promote the development of technical standards at European level, in line with EU legislation on standardisation.

Why is this important?

The EDPS' opinions, as detailed above, once again highlight the importance of its role in protecting the data rights of European subjects and specifically their rights under the Commission's new Digital Strategy. While they are non-binding, the EDPS' opinions give an indication of the direction that data protection, and its enforcement in Europe, is taking and highlights a clear intention to harmonise this approach across the authorities within the EU.

Any practical tips?

The opinions given by the EDPS are likely to shape both the final form legislative proposals and the national implementation of the DSA and DMA. Stakeholders would do well to keep their ear to the ground in relation to the effects of EDPS' recommendations and take note of how the DSA and DMA are amended as a result. There are likely to be direct knock-on effects for online service providers and their management of end-user data.

UK authorities consider position of AI in preparation for a new "Golden Age of Tech"

The question

What direction is the UK taking regarding policies on artificial intelligence (AI)?

Key takeaway

The AI Council and Office for AI have begun engaging with the AI ecosystem on the AI Council's Roadmap. This collaboration will continue with a view to shaping the National AI Strategy. Stakeholders are encouraged to engage in the development process to remain abreast of the Government's intended approach.

The background

At the end 2020, the House of Lords Liaison Committee published its follow-up report "AI in the UK: No Room for Complacency", which examined the progress made by the Government in relation to the recommendations set out in the Select Committee's 2018 report "AI in the UK: ready, willing and able?". The Committee concluded generally that ethical AI would be the only sustainable way forward and that the government would need to therefore better coordinate its AI policy and the use of data and technology at both a national and regional level. Other more specific recommendations made by the report included:

- the government to take active steps to explain to the general public the use of their personal data by AI
- the government to take immediate steps to appoint a Chief Data Officer
- the government to ensure that the digital skills of the UK are brought up to speed (reflecting the concern that around 10% of UK adults were non-internet literate in 2018), as well as ensuring that individuals are given the opportunity to reskill and retrain to operate within the evolving labour market caused by AI
- the AI Council to identify those industries most at risk of becoming redundant due to AI, and the skills gaps in those industries. The government should then look to implement a national training scheme, designed to support people to work alongside AI and automation, and to maximise its potential.

The AI Council published its AI Roadmap in January 2021, claiming that AI has the potential to deliver a 10% increase in UK GDP in 2030 and setting out sixteen recommendations designed to assist the government in developing a national AI strategy. There are two underlying messages that can be taken from the report, the first being that the UK needs to "double down" on the recent investments made in AI, and the second being that the UK must prepare for the future by being forward looking and prepared to adapt to disruption caused by AI. EU Member States have produced similar documents in the past with commentators noting that such programme announcements have been partnered by notable financial investments from national governments (eg France and Germany setting aside a combined approx. €4.5bn). The Roadmap has been criticised for failing to put real meat on what are bare bones recommendations (aside from positioning of The Alan Turing Institute at the centre of national AI activities), giving the government significant commitment flexibility, although this is perhaps unsurprising in the wake of the ongoing coronavirus pandemic.

The development

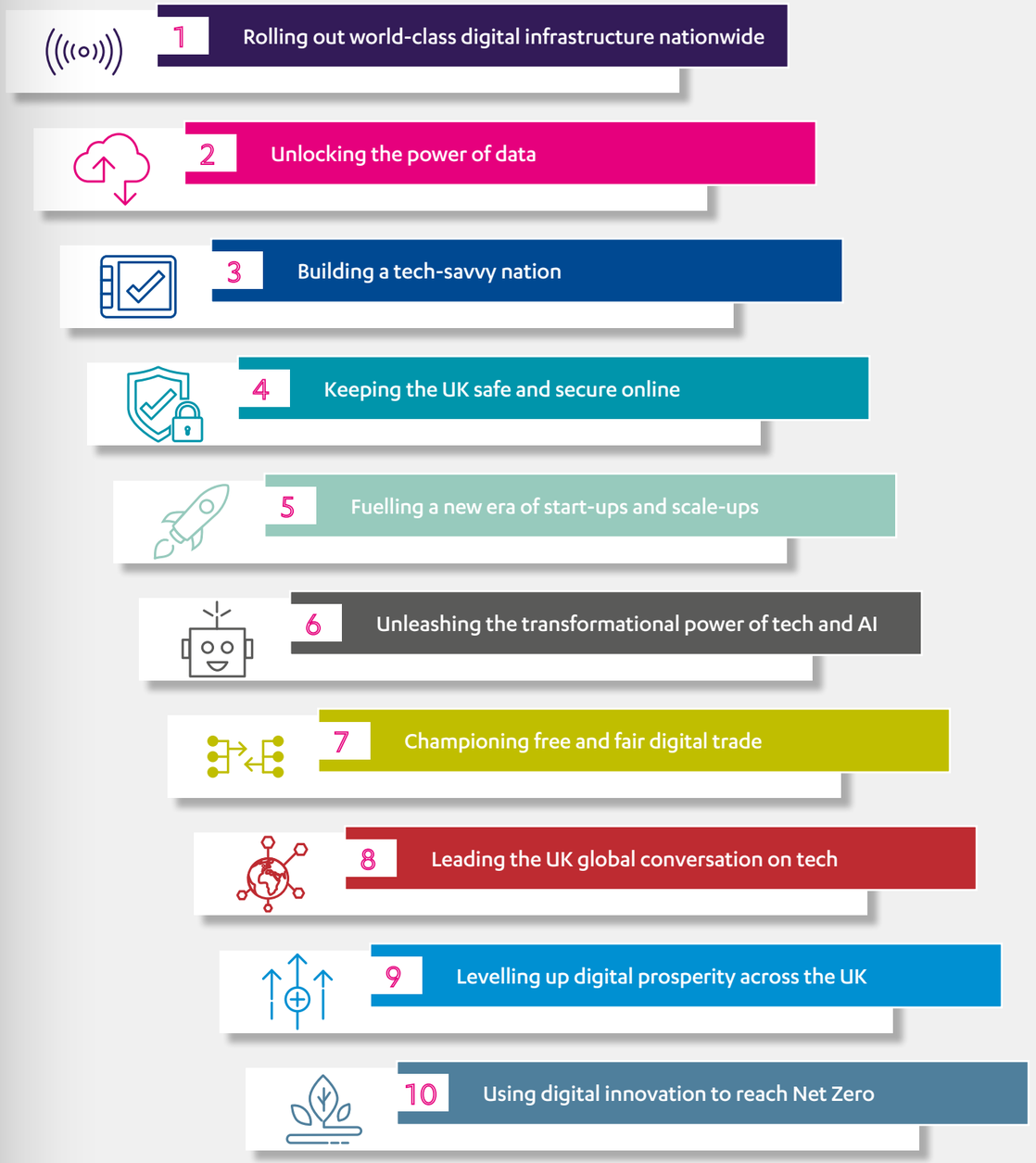
Last month, Digital Secretary Oliver Dowden announced that the government would be unveiling a new national strategy designed to "*unleash the transformational power of Artificial Intelligence*" and to make the UK a "*global centre for the development, commercialisation and adoption of responsible AI*". The outline of this strategy is set out in the Department for Digital, Culture, Media & Sport (DCMS)'s Ten Tech Priorities – see illustration opposite.

Why is this important?

The Ten Tech Priorities clearly identify the government's priorities going forward, namely that the strategy will focus on growth of the UK economy through widespread us of AI tech, an intention to develop AI in an ethical way and, finally, the need to exercise resilience in the face of inevitable disruption. The Priorities also appear to add some firm figures to what was previously a fairly high-level governmental strategy – eg by committing the government to £5bn worth of spending to ensure that homes and businesses nationwide benefit from gigabit broadband and an investment of £520m in a Help-to-Grow scheme designed to empower up to 100,000 businesses to adopt the latest tech.

Any practical tips?

The AI Council will be working together with the DCMS and Office of AI to arrange workshops during 2021 and shareholders are invited to engage on these topics and to assist in the development of an "*ambitious, multiyear AI Strategy*". Given the significance of the impact of this Strategy on tech companies operating within the UK and the potential opportunities that may spring from it, this is certainly a space worth watching and engaging with.



Catching up | data privacy laws in Asia are changing

The data privacy landscape in Asia is varied, complex and evolving. We are already seeing the wheels of change in motion as the data privacy laws of several Asian jurisdictions are being updated to reflect more closely the European data protection regime. This article summarises some of those changes.

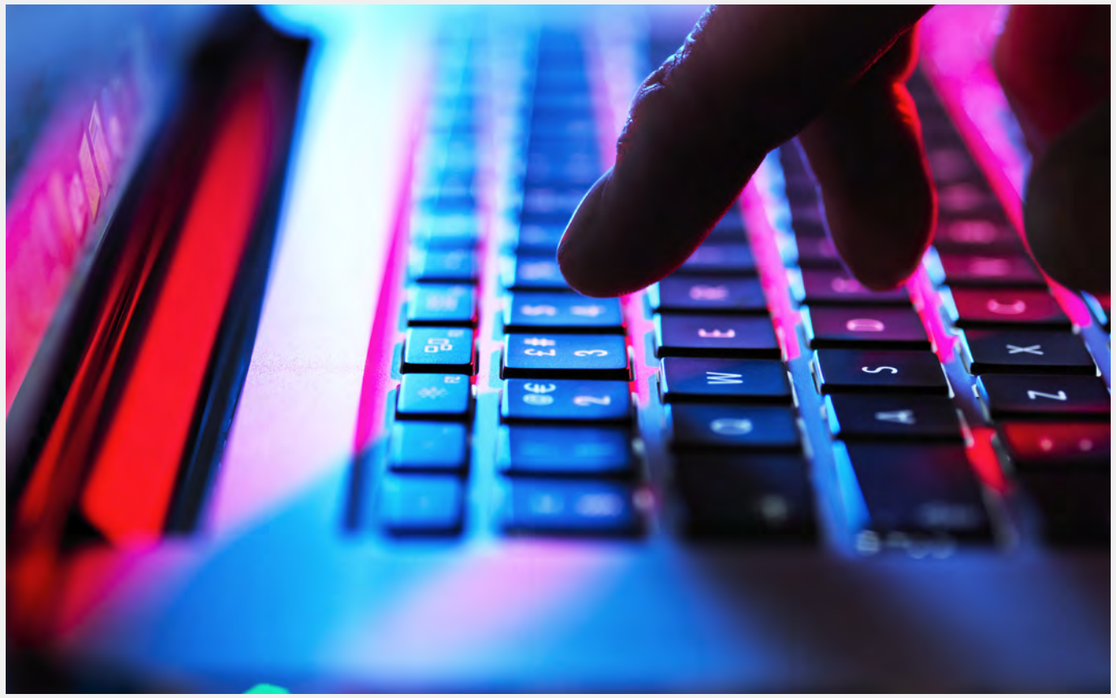
Introduction

In Asia, the data privacy landscape is varied, complex and evolving. Many, but not all, jurisdictions have some form of data protection regime, comprising of data protection and/or data security laws (or a combination of both).

To add to these differing approaches, many Asian jurisdictions are in the process of substantially updating their data protection regimes. For example, in 2019 Thailand introduced its Personal Data Protection Act which imposes data use restrictions, civil liability for misuse and sanctions. The Act was due to come into effect in May 2019, but full implementation has been postponed until June 2021.

The tables below provide a brief overview of some of the key changes which companies can expect to see coming into force in Hong Kong, Singapore, Japan and Taiwan in the near future.

Since these upcoming changes are increasing the level of protection afforded to data subjects, organisations operating in Asia markets will need to assess the impact of the changes on their business and take steps to ensure compliance. In the same way that data protection regulation is stringent in the EU market, the Asia market is fast becoming an environment in which data is protected with greater care, and mandatory breach notification obligations. Failure to follow the updated requirements could result in substantial penalties and reputational damage.



Hong Kong

Key amendments to the Personal Data (Privacy) Ordinance (PDPO)

ISSUE	CURRENT LAW (PDPO)	PROPOSAL	IN FORCE
Definition of personal data	◦ Information relating directly or indirectly to an "identified" living individual	◦ Information relating directly or indirectly to an "identifiable" living individual	TBC
Data retention policy	◦ No specific requirement (retention no longer than necessary)	◦ Mandatory requirement for a "clear" retention policy	TBC
Regulation of data processors	◦ No direct regulation	◦ Direct regulation of data processors or sub-contractors	TBC
Data breach notification (privacy regulator)	◦ No requirement (but recommended)	◦ Mandatory notification to PCPD within specific timeframe (timing TBC)	TBC
Data breach notification (data subjects)	◦ No requirement (but recommended)	◦ Mandatory notification within specific timeframe (timing TBC)	TBC
Sanctioning powers	◦ Fine/imprisonment only if breach of PDPO continues after enforcement notice	◦ PCPD power to impose direct administrative fines linked to annual turnover	TBC
'Doxxing' (non-consensual publication of personal data)	◦ Fines/imprisonment "on conviction"	◦ Wider powers for the PCPD, eg removal requests and investigation/prosecution	TBC

Hong Kong's PDPO originally came into force in 1996, and was amended in 2012, largely to introduce restrictions on direct marketing. It was designed in a previous era of data use.

In January 2020, the Hong Kong SAR Government has proposed to update the PDPO to adopt a harder regulatory approach. The Privacy Commissioner for Personal Data (PCPD) will obtain powers to impose direct sanctions. It is expected to take on more of an enforcement role, particularly in light of the PCPD's new MoU with the Information Commissioner's Office in the UK this year to collaborate on joint investigations and enforcement actions.

The proposed amendments to the PDPO, which are still being considered by the Legislative Council, would give the PCPD the power to impose direct administrative fines linked to annual turnover of the data user. It is not yet known how fines would be calculated but the Legislative Council papers refer both the current positions in Singapore (where a maximum fine of SGD1m can be imposed) and under the GDPR (a maximum fine of EUR 20m or 4% of a company's global annual turnover in the preceding year, whichever is higher).

The new rules would also impose mandatory breach notifications to both the PCPD and relevant data subjects within a specific timeframe when a data breach has occurred which presents a real risk of significant harm. The Legislative Council papers recommend that the timeframe for notifying should be as soon as practicable and, in any event, within five business days of becoming aware of the data breach. This amendment would not be as onerous as under the GDPR (which requires notification within 72 hours of knowledge) but steps up the obligations on data users that fall under the Ordinance.

Singapore

Key amendments to the Personal Data Protection Act (PDPA)

ISSUE	CURRENT LAW (PDPA)	PROPOSAL	IN FORCE
Data breach notification (privacy regulator)	◦ No general statutory requirement (but recommended, plus sector specific obligations)	◦ Mandatory notification to PDPC within 3 days from the date the data breach is assessed to be notifiable ◦ Breach notifiable if of a significant scale (affecting 500 individuals or more)	1 February 2021
Data breach notification (data subjects)	◦ No general statutory requirement (but recommended, plus sector specific obligations)	◦ Mandatory notification if breach likely to (or did) result in significant harm	1 February 2021
Sanctioning powers	◦ PDPC able to impose penalty for breach, up to SGD 1m	◦ Financial penalty increased to the higher of: – SGD 1m, or – 10% of annual gross turnover if such turnover exceeds SGD10m	Early 2022
Individual accountability for data breach	◦ No provision	◦ Individuals accountable for "egregious mishandling of personal data", incl. knowing or reckless unauthorised: – disclosure – use for a wrongful gain or causing wrongful loss – re-identification of anonymised data ◦ Fine ≤ SGD5,000/imprisonment up to two years/both	1 February 2021

In Singapore, the data protection regime continues to evolve and is becoming more robust. Recent amendments to the PDPA, which were passed by Parliament in November 2020 and are coming into effect in phases, mandate important recommendations from the Personal Data Protection Commission (PDPC) best practice guidelines.

Key amendments, including mandatory breach notification and individual accountability for data breaches, came into force on 1 February 2021. The PDPC guidelines were also updated to provide further clarity on these amendments. Therefore, businesses should already be taking steps to comply with the new rules.

If the breach is of a significant scale (ie a breach involving the personal data of 500 or more individuals), the amendments impose mandatory breach notifications to both the PDPC and relevant data subjects within 72 hours of the data user becoming aware that the breach is notifiable.

Organisations with global policies for data incidents should therefore localise a response plan for the requirements in Singapore. Having such a plan may also improve an organisation's chances of having a voluntary statutory undertaking being accepted by the PDPC in lieu of it carrying out an investigation into the organisation.

The PDPC guidelines indicate that increased penalties will take effect at a later date and no earlier than 1 February 2022. Financial penalties will increase to either SGD1m or 10% of a company's gross annual turnover in Singapore if such turnover exceeds SGD10m (whichever is higher). This change has major implications for larger organisations which operate in the Singapore market. Furthermore, given the tighter rules on telemarketing and spam control, businesses that engage in telemarketing or the bulk sending of marketing emails will need to comply with these updated requirements, or risk being subject to a financial penalty by the PDPC.

Japan

Key amendments to the Act on the Protection of Personal Information (APPI)

ISSUE	CURRENT LAW (APPI 2017)	PROPOSAL (APPI 2020)	IN FORCE
Expanding rights of data subjects	◦ Right to *request* access, correction, deletion and cessation of use of personal data that is/is intended to be retained for +6 months ◦ Opt-out: data transfers to 3rd parties allowed unless data subject opts out	◦ Right to *require* deletion or disclosure where there is a possibility of violating rights/legitimate interests (includes short term data) ◦ Restriction on opt-out: data transfers allowed on opt-out basis only to first level 3rd party recipients	2022
Pseudonymisation (processing personal data so it cannot be used to identify the individual)	◦ No specific provision	◦ Consent required to transfer pseudonymised data in certain circumstances	2022
Extra-territorial application	◦ Applies to foreign entities who obtain personal data of data subjects in Japan	◦ Commission has authority to supervise and sanction foreign entities (if provide goods/services in Japan, and handle personal data of data subjects in Japan)	2022
Data breach notification	◦ No requirement under most circumstances	◦ Mandatory notification to the PPC and relevant data subjects, if incident may cause violation of rights/interests ◦ Preliminary report ASAP (no timeline indicated)	2022
Sanctions	◦ Fines of up to ¥300,000-500,000 (approx. USD2,900-4,800)	◦ Fines increased up to ¥100M (approx USD950k) ◦ False submission of reports – fine up to ¥500k ◦ Potential fines for individuals	2022

Amendments to the Japanese APPI were passed in June 2020 and follow the trend of creating a more robust data protection regime with more authority for the regulatory body, the Personal Information Protection Commission (PPC). The amended APPI, which will mostly come into force within two years, will have a major impact on businesses that operate in Japan (as well as many global organisations that may be affected by its extra-territorial aspects).

The new rules will allow the PPC to order foreign companies, which either handle the personal data of data subjects in Japan or provide goods or services in Japan, to submit information on how that data is being managed. Further, the PPC will be able to publish the fact that an overseas company has not followed a PPC order. Penalties imposed by the PPC will also increase, up to ¥100m for companies. Individuals responsible for a breach may also be subject to individual penalties.

Breach notifications to both the PPC and relevant data subjects will be mandatory as soon as possible following a data breach, in the event of an incident which may cause the violation of individual rights and interests (similar to the notification threshold envisaged in Hong Kong). Businesses would need to provide a preliminary report to the PPC and data subjects as soon as possible, followed by a more detailed report regarding cause and remediation.

Taiwan

Key amendments to the Personal Data Protection Act (PDPA)/Cybersecurity Act (CSA)

ISSUE	CURRENT LAW (PDPA/CSA)	PROPOSAL	IN FORCE
Definition of personal data (PDPA)	◦ Information/data which may be used to identify a natural person ◦ Directly or indirectly	◦ Specification of which types of web-based data constitute personal information	TBC
Protections afforded to children under 13 (PDPA)	◦ No provisions	◦ Requiring a legal representative to approve collection and processing ◦ Prohibiting sale or other commercial use of data	TBC
Definition of 'critical infrastructure provider' (CSA)	◦ Those who maintain or provide critical infrastructure either in whole or in part ◦ To be designated by competent industry authority (and ratified)	◦ Clarification by specific examples: government offices, communication networks, national defense and military facilities, and businesses engaged in private energy, transportation, finance, health care, and food and water supply	TBC
Government agency obligations (CSA)	◦ Several cyber security management obligations	◦ Additional requirement to prepare information security budget	TBC

Taiwan adopts a 'split' data protection regime, with personal data protected by both the PDPA and the CSA. The PDPA, which primarily concerns data privacy, applies to businesses; whereas the CSA, which is aimed at data security (regardless of whether such data is 'personal data' as defined under the PDPA), applies only to those businesses which are deemed to be critical infrastructure providers, designated by the sectoral regulator and ratified by the Executive Yuan.

Both Acts are currently under review by the Legislative Yuan and the underlying intention to the amendments is to clarify the law, more than to effect substantial change. The PDPA aims to meet EU standards so that Taiwan may obtain an Adequacy Decision from the European Commission. For example, the proposed amendments to the PDPA include increased protections for children under the age of thirteen.

An Adequacy Decision would allow personal data to flow from the EU (and Norway, Liechtenstein and Iceland) to Taiwan without further safeguards, treating transfers to Taiwan as if they were intra-EU transmissions of data, ie the same guarantees as those under EU law will continue to apply. In Asia, only Japan has so far obtained an Adequacy Decision.

Conclusion

Data protection regimes in Asian jurisdictions are catching up to the GDPR (hailed as a world-leading data protection regime for its extra-territorial application and significant sanctions). International businesses across Asia, often aware of the key requirements of GDPR, will now need to be aware of more stringent rules and regulations applicable in several Asian jurisdictions.

This article has provided just a snapshot of a handful of jurisdictions in Asia. Other jurisdictions' laws (beyond the reach of this short summary) should also be considered carefully, eg the upcoming and expansive changes to the data protection regime in Mainland China.

In summary, any business that is established or operates in locations across Asia (or is looking to set up a presence in Asia) should keep a close eye on the changing legal landscape across the region and the data that the business controls or processes in such a large and diverse market. Thoroughly researching the regulatory regime in each Asian jurisdiction and implementing a robust and compliant data protection policy, data map and data breach plan will be key to navigating the evolving Asian data protection landscape.

RPC frequently advises its clients on all aspects of data privacy and cyber security matters – please do get in touch with us if you would like to discuss how we can help.

Data privacy in China | Measures for the Supervision and Administration of Online Transactions

On 15 March 2021, the State Administration for Market Regulation in Mainland China officially approved the Measures for the Supervision and Administration of Online Transactions (the "Measures"), which came into force on 1 May 2021. The Measures provide detailed guidance on e-commerce, consumer protection and cybersecurity law. Given the growth of online transactions such as social e-commerce and live-streamed shopping in China, the new and more stringent rules aim to better protect the rights of consumers.

When customers' personal details are collected and used, online transaction operators will have to state the purpose, method and scope of personal information being collected and obtain consent from customers. In addition, when collecting and using sensitive information such as biometric data, health data, financial account data and personal tracking data, customers' consent must be obtained for each item of data. Once collected, customers' personal information must be kept strictly confidential.

The new rules cover further areas such as the retention of information and the regulation of competition between online transaction operators. Importantly for such operators, all product or service information will have to be disclosed comprehensively, truthfully, accurately and in a timely manner. Furthermore, they will not be allowed to send commercial information to consumers without their consent or request.

Failure to comply with the Measures may result in criminal liabilities, such as rectification orders and fines.

"The new rules cover further areas such as the retention of information and the regulation of competition between online transaction operators."

Singapore Court of Appeal issues landmark decision in first cryptocurrency related trial

***Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 02**

The Singapore Court of Appeal (SGCA) has issued a landmark ruling in *Quoine Pte Ltd v B2C2 Ltd*, a breach of contract case involving the autonomous algorithmic trading of digital tokens. The SGCA affirmed in part the decision of the Singapore International Commercial Court (SICC) that Quoine, a digital token exchange operator, breached its contract with B2C2, a trader on Quoine's exchange, for unilaterally reversing completed trades in digital currency, notwithstanding a catastrophic error in logic in Quoine's platform software that led to a windfall profit for B2C2.

The central issue was how the doctrine of unilateral mistake ought to apply to contracts involving autonomous computerised processes. The majority was of the view that traditional principles governing unilateral mistake are capable of dealing with such novel circumstances and rejected Quoine's defence of unilateral mistake. The SGCA was of the view that a programmer's state of knowledge when programming was relevant as algorithms are bound by parameters set by the programmer and generally will only do what it was programmed to do. Any assessment of knowledge attributed to the parties at the time of contracting would thus differ in contracts made by way of deterministic algorithms.

While the SGCA did not decide on whether cryptocurrencies are capable of assimilation into general property concepts, such as being held on trust, the technology community should bear in mind the lessons from the earlier SICC decision and be mindful of pitfalls in modern contracts.

Recent investments made in AI, and the second being that the UK must prepare for the future by being forward looking and prepared to adapt to disruption caused by AI. EU Member States have produced similar documents in the past with commentators noting that such programme announcements have been partnered by notable financial investments from national governments (eg France and Germany setting aside a combined approx. €4.5bn). The Roadmap has been criticised for failing to put real meat on what are bare bones recommendations (aside from positioning of The Alan Turing Institute at the centre of national AI activities), giving the government significant commitment flexibility, although this is perhaps unsurprising in the wake of the ongoing coronavirus pandemic.

Hong Kong crypto regulation | Proposed mandatory licensing and supervisory regime for Virtual Asset Service Providers (VASPs)

In November 2020, the Financial Services and Treasury Bureau (FSTB) issued a public consultation paper proposing a new mandatory licensing and supervisory regime for all VASPs under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO).

The new regime would require the licensing of virtual asset exchanges that are not required to be licensed under the Securities and Futures Ordinance because they trade virtual assets (such as Bitcoin and Ether) which are not within the statutory definitions of "securities" or "futures contracts". The new regime would be administered and enforced by Hong Kong's Securities and Futures Commission which will be given the necessary powers under the AMLO.

The new licensing conditions, including know-your-client and due diligence requirements, would be comparable to those currently applicable to licensed securities brokers and automated trading venues. The proposed regime would help to tighten cryptocurrency regulation in Hong Kong (which is currently a voluntary opt-in regime) to mitigate money laundering and terrorist financing risks and ensure compliance with international obligations.

Looking ahead, market participants are advised to keep abreast of developments in this area since the FSTB is contemplating an expansion of the mandatory licensing regime to cover more forms of virtual asset activities where the need arises in the future.

Government to review the Gambling Act

The question

What legislative changes are being considered to address the risks associated with modern gambling?

Key takeaway

Significant reform of UK gambling legislation is likely to be on its way. Key areas affected are likely to be control of online gambling accounts (including deposits, losses and spending limits), children's access to gambling products and the role of gambling advertising in particular in sport. The review will also consider how to "future proof" legislation to provide flexibility for regulators responding to rapid technological change.

The background

The landscape of the gambling industry has changed significantly since the Gambling Act 2005 came into force. The internet has fundamentally altered the way people access gambling services, and there is a growing concern about the ease with which vulnerable groups and children can access gambling, the addictive nature of online gambling, and the prevalence of gambling marketing both online and in live televised sport. There has been pressure on the government to review gambling laws for some time, and in 2019 the maximum stake on B2 gaming machines (so called "fixed odds" betting terminals) was cut from £100 to £2. The same year a collective of prominent gambling companies instituted a voluntary ban on advertising during live sport before the watershed.

In December 2020, the government announced a comprehensive review of UK gambling legislation, the aim of which is to reform current regulations to reflect the industry as it is now and will be in years to come.

The development

The Government has launched a call for evidence from the industry to aid the review, which ran until 31 March 2021. The following areas are being considered:

- the effectiveness of current measures to prevent underage and youth gambling
- the impact of greater controls at a product level, such as stake and prize limits
- the benefits and harms of gambling sponsorship arrangements in sport
- the role and powers of the Gambling Commission.

A white paper containing the findings will be published later in 2021. A good indication of the areas of reform likely to be pursued comes from the government's response to a recent House of Lord's paper on the subject, which was published alongside the call for evidence. This suggests that the review will seek to balance the need for reform with consumer freedoms and commercial interest. For example, in the case of sport and advertising, the government has shown an awareness of the financial reliance many sporting organisations have on gambling sponsorship.

Why is this important?

This review is likely to bring about the most sweeping changes to gambling law since the Gambling Act was introduced in 2005. The government has endorsed the idea of imposing stricter requirements on gambling operators including more affordability checks on consumers, maximum stakes and prize limits, and controls on how gambling interfaces appear online. Some betting platforms will need to change their formats to comply.

Any reform to gambling sponsorship and advertising rules could also mean changes in the sports industry, which is heavily reliant on betting companies for funding. Any sponsorship rule changes could contribute further to the financial difficulty some teams are already facing as a result of the pandemic and a year of empty stadiums.

Any practical tips?

Watch this space, as reform is likely to come in the next twelve months. The government's objectives include changes to gambling advertising and online products, and any future legislation will have a significant impact on the relationship between gambling and advertising. If your company is involved in either of these industries, you should keep an eye out for announcements.

In the meantime, other changes to betting regulation continue, for example new rule changes for online slot games will come into force on 31 October 2021 and must be fully implemented before then. These are aimed at decreasing the "intensity" of online play.

Making online games safer by design

The question

How does the UK Gambling Commission's new rules modify online game design?

Key takeaway

Consumer protection on online gambling platforms is a growing area of focus. From 31 October 2021 new rules will ban features that increase gameplay speed, celebrate losses as wins or enable customers to cancel withdrawal requests.

The background

The Gambling Commission has been steadily increasing protections for consumers of online gambling platforms. In April 2020 the Commission strengthened protections relating to online age and ID verification, banned gambling on credit cards and improved customer interaction practices. Since then, the Commission has been keen to develop these protections further, particularly for online slots players. "Slots" are widely defined under the Commission's new rules to cover reel-type games and casino games with non-traditional reels.

The Commission has found that slots game players have the highest average losses per player of any online gambling product. Slots are one of the largest online gambling products in terms of "Gross Gambling Yield" (ie they are played by few but recoup a high average spend per person). As a result, the Commission is keen to implement changes to slots rules to protect consumers. The Commission found that features that increase the intensity of play such as those that increase the speed of play and frequency of gambling opportunities increase the risk of addiction and harm.

The Commission aims to rigorously enforce the new changes from October 2021.

The development

The Commission is clearly moving towards a more consumer-protective stance. The new rules are intended to give players more control over their gameplay, which include:

- no auto-play features – all games must be started with a "start button" and there must be at least 2.5 seconds between each game cycle
- all gaming sessions must display the customer's net position and elapsed game time since the start of the session
- players cannot engage in multiple slot games at once
- games can no longer celebrate losses as wins (or returns that are equal to the total stake gambled). Previously equal returns could be celebrated, but from 31 October 2021, only those wins that are greater than the total stake gambled can be celebrated (eg with fanfares).

Additionally, customers will not be able to cancel withdrawal requests (reverse withdrawals) on any online gambling platform. This means that once a withdrawal request has been made, the customer will not be able to override the request to gamble with the money instead.

Why is this important?

These developments will require remote operators to review and update online slots games and any other online gambling products that currently allow reverse withdrawals to ensure compliance by 31 October 2021. Slots games specifically will have to comply with the additional regulations and the Commission expects online operators to show a "greater commitment to... consumer protection".

Online operators now only have nine months to implement the new rules ahead of the deadline.

Any practical tips?

Online gaming operators need to review how aspects of their platforms are impacted by the new rule, in particular their slots games and reverse withdrawal processes. For example, they should ensure ahead of the deadline that:

- any celebration settings are not triggered if the customer receives the same amount back as was gambled. Sounds and imagery that give the illusion of a win in an equal stake return scenario must be removed
- all games will need to be updated to check how reverse withdrawal policies are applied
- consider reviewing and disabling any slots game features that enable auto play or those that give an illusion of control over the outcome.

On a wider level, it is clear that the roll is on towards greater consumer protection measures on gaming platforms. If operators are aware of features on their sites which run contrary in spirit to this approach, now would be the time to start looking at them – before the regulators do. The government's review of UK gambling legislation announced in December 2020 is further evidence of the way the regulatory wind is blowing.

New "right to repair" regulations due Summer 2021

The question

What requirements will manufacturers and importers of consumer goods, particularly electronic displays, need to meet under new "right to repair" rules?

Key takeaway

Manufacturers and importers of electronic displays will have to provide information and spare parts to consumers and professional repairers in order to better facilitate the circular economy. The new regulations are likely to come into force in **Summer 2021**.

The background

Following a consultation that ended in November 2020, the Department for Business, Energy and Industrial Strategy (BEIS) has published its response to the eco-design and energy consumer information requirements for electrical goods (10 March 2021). Specifically, the consultation sought views on, amongst other things, energy labelling, resource efficiency, circular economy and professional repairer registers. BEIS has proposed eco-design requirements for consumer electrical goods, set to come into force in England, Scotland and Wales in Summer 2021.

BEIS intends to provide draft regulations to Parliament during Spring 2021, with a view for the new regulations to apply to the products discussed in the consultation from Summer 2021.

The development

Amongst many new eco-design requirements for consumer electrical goods, including higher minimum energy performance standards and new material efficiency and information requirements, the proposals seek to improve access to spare parts for certain electronics and maintenance information to enable repairs by consumers.

Essentially, BEIS is highlighting the need for companies to better facilitate the circular economy. While white goods are the focus of the consultation, it also includes electronic displays, which are prominently used in TVs, smart phones and other Internet of Things devices. All will have to comply with the proposed regulations.

The draft regulations include, amongst others, the following requirements for electronic displays:

- any electronic displays will have to conform to specific eco-design requirements (discussed further below)
- the energy consumption of electronic displays must not deteriorate after a software or firmware update without consent from the user
- the performance of an electronic display must not deteriorate without the user's consent.

The eco-design requirements for electronic displays include:

- ensuring that all displays are fastened to any device in a way that does not prevent its removal using commonly available tools
- making available, on a publicly accessible website and without charge, the dismantling information needed to access any of the products' components, including specific steps and required tools
- the manufacturer or importer must provide access to the appliance repair and maintenance information to professional repairers no later than two years after the first time a display is put on the market
- ensuring delivery of spare parts for electronic displays within 15 working days of receiving an order
- making available the latest available version of the firmware for a minimum period of eight years after the after placing the last unit of the model on the market.

Why is this important?

The new regulations will create an improved ecosystem for the repair of goods, including requirements on provision of information and spare parts. Electronic items with displays are not cheap, and BEIS's proposals signal a push to give consumers greater protection over their investments.

Any practical tips?

Manufacturers and importers of these consumer electronics with electronic displays need to quickly get to grips with the new regulations. It is a big development for manufacturers and importers of consumer goods with electronic displays and one that will need significant planning in advance, including from a design perspective.

Committee of Advertising Practice publishes guidance for marketing on TikTok

The question

What does the Committee of Advertising Practice's (CAP) new guidance note on marketing on TikTok tell us about making compliant ads for the platform?

Key takeaway

CAP reminds us that the rules in the CAP Code are largely media neutral and so the same principles that apply in other media are equally applicable to advertising on TikTok, or indeed any new and innovative service. CAP's headline for the guidance quips that following these principles can make ads on TikTok "run like clockwork".

The background

TikTok is a social media, video-sharing app, with in-built video editing tools that allows users to create and share 15-60 second videos on any topic (such as challenges, dancing, singing and humorous videos). In addition, the app has an algorithm which allows relevant content to circulate to specific users. Launched in the UK in August 2018, it is currently the seventh most popular (and fourth most famous) social media platform, according to YouGov. Due to the platform's meteoric rise in popularity and the vast and innovative ways in which brands can advertise on the platform, TikTok has now earned its very own guidance note from the advertising regulator.

The guidance

Make it clear when a TikTok is an ad
Whether the advert is a "Top View" ad (ie seen when the app is first opened), a branded effect, a TikTok posted by a brand or influencer or affiliate marketing content, it must be obviously identifiable that it is advertising. CAP acknowledges that most ads within TikTok's own ad formats, as well as TikToks posted by a brand's own TikTok page, are generally recognised as advertising from the context and the labelling applied by TikTok and the brand. However, research by the Advertising Standards Authority (ASA) found that some users struggled to identify when a TikTok post made by an influencer was an ad. For example, in the ASA's ruling on Jamella, a TikTok made by influencer, Emily Canham, which promoted the GHD brand and included a personalised discount code, was found to not be sufficiently clear as there was nothing in the content to indicate that it was an ad. Any TikToks uploaded by influencers (and others) which contain advertising or affiliate marketing therefore need an additional label to distinguish them as ads.

As a minimum, CAP recommends a prominent "Ad" label in any influencer and affiliate marketing TikToks in order for the advertising to be "obviously identifiable" as an advert; this label must be upfront in the content or in the accompanying caption. Additionally, the label must not be hidden or obscured (ie the label cannot be too small or be in a similar colour to the background). If the label is not clear, then the TikTok is unlikely to be "obviously identifiable" as an ad.

Capture the right audience
The ASA expects marketers to have taken all reasonable steps to avoid their ads being seen by someone who shouldn't (eg due to their age). Marketers will not be able to rely on the argument that less than 25% of a platform's total audience is under-age or based on self-reported user ages. Many social media ads can be (and usually are) targeted at a defined set of users. Therefore, the ASA will expect marketers to target their ads appropriately and to use all the tools available to exclude under-age consumers from their targeted audience. Audience demographic data relating to an influencer's own account may be enough evidence of responsible targeting.

However, marketers will also need to consider the type of content that the ad appears in or around.

Always use a CAP Code lens on advertising content
The general and sector-specific rules that apply to different ads and products apply equally on TikTok – so, CAP stresses the need to look out for rules that relate to the food and drink sector as well as avoiding materially misleading consumers or causing serious or widespread offence.

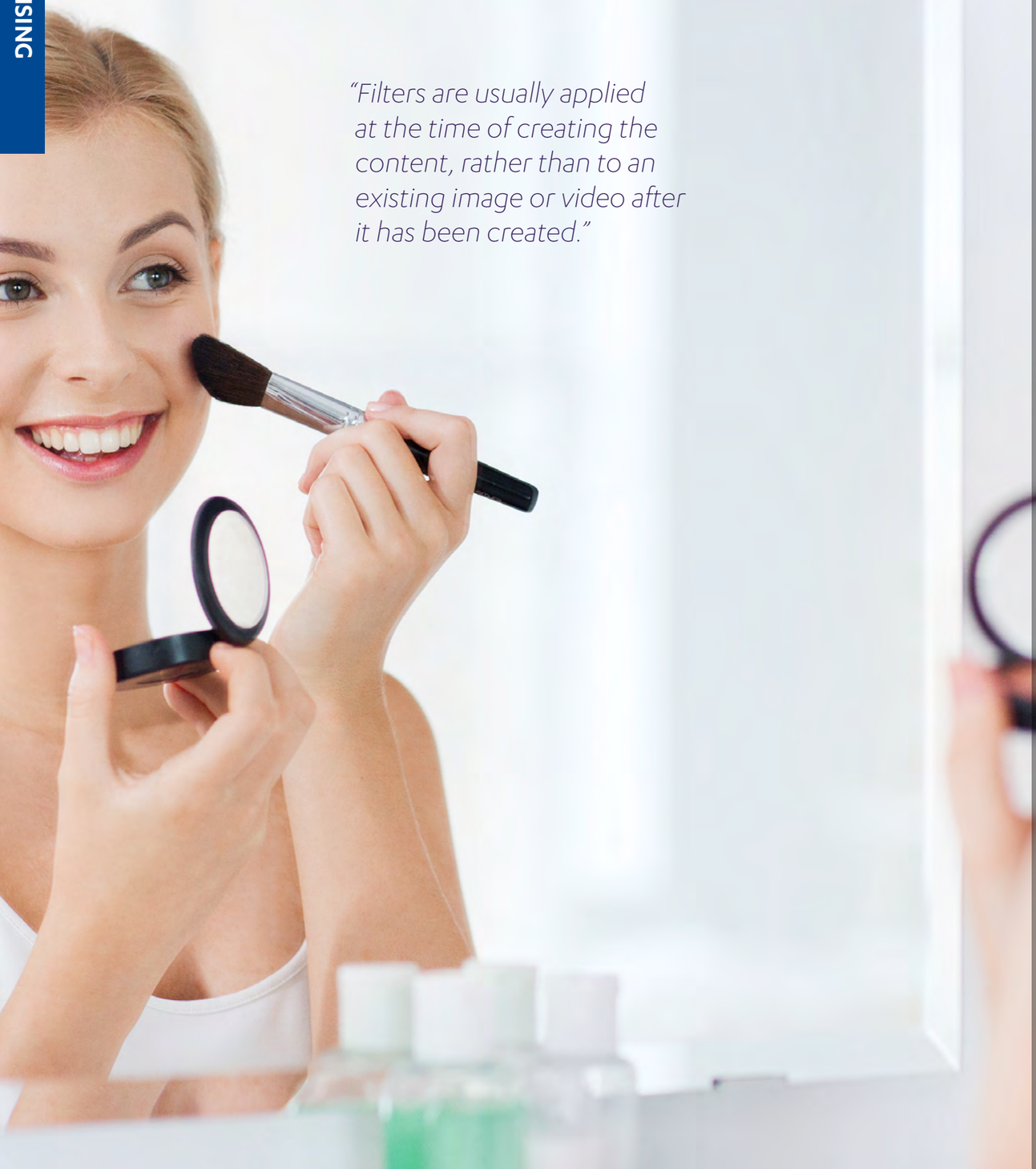
Why is this important?

The guidance reminds us just how flexible the principles within the CAP Code are, and that they apply to you however new and innovative your service may be.

Any practical tips?

You still need to follow the rules, irrespective of the type of advertising. Essentially, remember that any form of ad:

- needs to be obviously recognisable as such
- must not mislead consumers materially
- must not cause harm or serious or widespread offence
- needs to comply with any sector-specific Code rules that apply.



"Filters are usually applied at the time of creating the content, rather than to an existing image or video after it has been created."

ASA upholds use of filters in social media beauty ads as misleading

The question

Should influencers be allowed to use filters when advertising cosmetic products?

Key takeaway

Filters should not be used to advertise products on social media if they exaggerate the effect of the product. Influencers and advertisers promoting beauty products should avoid applying filters to photos or videos which are directly relevant to the product being advertised to avoid potentially misleading consumers.

The two recent ASA cases

In 2011, the ASA released guidance on the use of pre and post-production techniques in ads for cosmetics, which established that the re-touching of images requires particular attention to avoid misleading consumers, and visual claims should not misleadingly exaggerate the capabilities of the product. The guidance was published well before in-app beauty filters became available on social media and the historic rulings in this area tended to focus on post-production techniques for cosmetic products in TV ads; nonetheless these are useful in setting a baseline.

More recently, the ASA applied its core principles to two rulings against ads from Skinny Tan Ltd and We Are Luxe Ltd. Both ads consisted of Instagram stories by influencers promoting tanning products. In both cases, the influencers featured had applied beauty filters that made their skin tone appear darker than it would have without the filters. The ASA considered that, because the filters were directly relevant to the performance of the products being advertised, they were likely to have exaggerated the efficacy of the products and materially misled consumers.

Why is this important?

Using filters in ads is not inherently problematic but is likely to cause issues if a filter exaggerates the effectiveness of the product being advertised. It will be the advertiser's responsibility to demonstrate that is not the case. Even if an advertiser was able to create a filter which accurately reflects the efficacy of their product, the onus would still be on the advertiser to hold evidence to show that any visual claims made are unlikely to mislead.

Any practical tips?

Filters are usually applied at the time of creating the content, rather than to an existing image or video after it has been created. As such, it's unlikely that there will be "before" material which could be retained by an advertiser to demonstrate the effect of the filter and show that it wasn't likely to mislead. Advertisers could consider retaining such images or taking comparison ones before the application of any filters, to better ensure compliance or an adequate response to any ASA inquiry.

It's important to remember that the responsibility ultimately lies with the advertiser where the use of a filter is likely to mislead consumers about the efficacy of a product. Brands may therefore wish to clarify in their commercial agreements with influencers their responsibilities when marketing cosmetic products on social media and advise them against the use of beauty filters if they are likely to exaggerate the efficacy of the advertised product.

Avoiding "Fake Views" – CAP publishes guidance on testimonials and endorsements

The question

What enforcement options are available against marketers who use fake reviews to promote their goods or services?

Key takeaway

The Committee of Advertising Practice's (CAP) guidance reminds marketers of the need to be proactive in ensuring that they do not use fake reviews, either directly or indirectly due to a failure to verify. Remember, incoming European legislation, in the form of the Omnibus Directive (due to land in 2022), is set to give regulators real teeth to the enforcement options available to them against those who engage in fake reviews.

The new guidance

CAP has published guidance on Testimonials and Endorsements and specifically why not to use "fake views". The guidance contains seven common-sense steps towards compliance:

1. **Demonstrate they're genuine**: this is self-explanatory, but the ASA also advises retaining the contact details of the person featured for as long as the ad is used
2. **Obtain consent**: there are limited exceptions to this rule (see CAP Code rule 3.48)
3. **Make sure they're relevant**: eg don't use endorsements or testimonials in a way that misleads consumers as to the efficacy of a product (such as inaccurate before and after photos for weight loss products)
4. **Don't be sad, use #ad**: the ASA has produced a wealth of guidance around the use of appropriate marketing hashtags
5. **Avoid incentivising positive endorsements**: this could take the form of either encouraging consumers to post positive reviews in such a way that breaches the code, or amending or deleting negative reviews to give a misleading positive impression;
6. **Be aware of restricted categories**: for example, neither health professionals nor celebrities should be used to endorse medicines
7. Ensure all testimonials and endorsements comply more generally.

Given the importance of consumer reviews to business success, and their use as a legitimate method of promoting products or services, this is one area where it could be tempting to artificially bolster reviews. In 2019, the CMA investigated this exact practice and its prevalence on large online platforms such as Facebook and eBay. Its finding was that there is a "thriving marketplace for fake and misleading online reviews". The CMA also secured commitments from Instagram, Facebook and eBay to tackle the risk of fake reviews being bought and sold through their platforms.

The Omnibus Directive

CAP's advice is a salient reminder for brands to get their customer review processes in place before new European legislation in the form of the "New Deal for Consumers" lands next year. This package of legislation is intended to enhance and modernise the EU's consumer protection regime by increasing powers against non-compliant businesses and bringing regulations up to date for a modern, digital focussed market. Of relevance to the field of consumer reviews is the "Directive on better enforcement and modernisation of EU consumer protection rules"; more commonly known by its catchier title of the Omnibus Directive.

The Omnibus Directive seeks to increase transparency around consumer reviews. It will require traders to publicly provide information around how they have ensured that the consumer reviews they publish have been produced by verified product or service users. Further, the Omnibus Directive has expressly blacklisted certain activities, which will be added to the existing list of banned practices under the Unfair Commercial Practices Directive 2005. These include prohibitions on:

- the procurement and/or posting of false reviews
- the deletion of negative reviews to manipulate the consumer's product perception
- the transferal of endorsements from one product to another
- claiming that consumer reviews are authentic when this has not been verified.

The concept behind this new legislation is to ensure that consumers are presented with the most accurate account possible and are not misled by marketers when purchasing goods or services online.

Member States must adopt the Omnibus Directive by 28 November 2021 and must apply the rules of the Directive by **28 May 2022** at the latest. Despite the UK no longer being bound to implement the Omnibus Directive following Brexit, businesses who market their products or services to EU based consumers will still be caught by its provisions and expected to comply. Further, the UK Government published the Green Paper "Modernising Consumer Markets" in early 2018. This broadly mimics the Omnibus Directive but currently the proposal is for a cap on financial penalties of 10% of a firm's worldwide turnover.

Why is this important?

Looking at the broader picture of developing European consumer protection legislation, the CAP guidance note is helpful. It gives clear guidance on how a good customer review process should run and is a great reminder about the importance of achieving compliance before the arrival of the Omnibus Directive next year.

Put another way, using the guidance to help get your review processes in shape now will pay dividends later when the Omnibus Directive lands with its GDPR-level fines for non-compliance. Member States have the power to assess the gravity of a breach and, in the most serious cases can issue a fine of up to 4% of the annual turnover of the marketer "in the Member State or Member States concerned" or €2,000,000 if this figure cannot be calculated. As mentioned, while the UK itself will not be bound by the Directive, organisations who target EU-based consumers will be.

Any practical tips?

The ASA has for a long time warned marketers that they should be prepared to substantiate review claims used in promotions, whether made by influencers or members of the public. This advice is more relevant now than ever before, with the Omnibus Directive now racing down the track towards us. Considering the substantial potential fines for those found to be in breach under the Directive, ensuring that reviews used to market goods and products are legitimate and verifiable is quickly becoming a critical area for all consumer brands to focus on.

ASA upholds Ladbrokes gambling ad as socially irresponsible for problematic behaviour

The question

Is a gambling ad that features potentially problematic behaviour socially irresponsible?

Key takeaway

Advertisers must ensure that any ads associated with gambling do not highlight any problematic behaviour, such as detachment from surroundings and preoccupation with gambling, to avoid the ad being found socially irresponsible.

The ad

On 25 October 2020, All4 played a Ladbrokes video-on-demand ad which showed various people using the Ladbrokes app on their mobile phones. One scene showed a clip of a horse race, before showing a man in a café with several other people watching the horse race. The man is shown shaking the table with his knee and is described as "a bag of nerves". A woman turns to him and says, "Really?" which captures his attention briefly, but he then subsequently turns away. The man's food remains untouched and his interaction with others is brief, indicating that he is too preoccupied with the outcome of the race to eat or chat.

The complaint

The complainant challenged whether the ad depicted gambling behaviour that was socially irresponsible.

The response

Ladbrokes did not believe the ad depicted socially irresponsible behaviour because the character was not shown gambling or talking about gambling – the scene in question only showed the character waiting for the race to start. Ladbrokes also argued that nerves before a sporting event were a natural reaction – whether the person was gambling or not – and that it was the character's nerves that were being highlighted in the ad, as opposed to unhealthy gambling behaviour. They claimed that the scene did not indicate that nerves or gambling caused harm or distress for the character and that the character did not demonstrate any behaviour that could be considered socially irresponsible. They argued that the ad featured people in everyday situations and characters continuing with life in normal day-to-day activities – ie the character was in a social environment with friends eating a meal waiting for a race to start. In addition, the ad intended to convey that enjoyment that can be had from gambling and it portrayed using the app as fun and entertaining.

The decision

The ASA concluded that the ad depicted gambling behaviour that was socially irresponsible, breaching CAP Code rules 16.1 and 16.3.1. It noted Clearcast's view, which was that the ad implied the man was watching a race on TV. It agreed that, based on the scene and the simultaneous voice-over, viewers were likely to interpret the ad as showing him watching the television as the race was about to begin. The ASA noted that he was watching intently, and his shaking the table with his knee which, while clearly intended to be humorous, suggested he was preoccupied with the race as his food remained untouched.

The ASA also took the view that the character was so engrossed in the race that his companion had to point out his actions to draw his attention away from watching the television. The ASA noted that, after responding to his companion, the man appeared to turn away, though the shot was brief, and he was looking down. The ASA disagreed with Clearcast's view that the man was not disconnected from his companion, or from the room, but that viewers would assume from his behaviour that he was preoccupied with the outcome of the race in relation to a bet he had placed. Finally, the ad described the character as being a "bag of nerves", which the ASA believed viewers were likely to interpret as a result of him having placed a bet on the race.

Why is this important?

The ASA upholding the complaint is a clear warning to marketers that, even if a depicted scenario is intended to be humorous, an ad must not portray, condone or encourage gambling behaviour that is socially irresponsible or could lead to financial, social or emotional harm.

Any practical tips?

Marketers should refer to CAP's 2018 "Guidance on Gambling advertising: responsibility and problem gambling", which makes it clear that ads which portray or otherwise refer to individuals displaying problem gambling behaviours or other behavioural indicators linked to problem gambling are likely to breach the CAP Code.

Behaviours associated with people displaying or at risk from problem gambling include detachment from surroundings and preoccupation with gambling. Marketers should take care to avoid any implication of such behaviours, including outwardly light-hearted or humorous approaches that could be regarded as portrayals of those behaviours.

ASA rules "was" pricing claim by Watches of Switzerland as misleading

The question

How long does it take for a lower price claim to become the "usual" selling price for a product? What if the previous higher price ran for three years, and the lower price is in place for ten months? Does this period of time negate the ability to use the higher price as a "was" price comparison?

Key takeaway

An ad that included an old price as a "was" price, although used for three years prior, was deemed to be misleading by the ASA. The ruling held that ten months was enough time for the new discounted price to become the usual price for the goods and comparing against the older, higher price would mislead consumers and be in breach of the CAP Code.

The ad

Watches of Switzerland (WS), trading as Goldsmiths, sold jewellery and other items on their website www.goldsmiths.co.uk, which included a pair of "Mappin & Webb Fortune White Gold and Diamond Hoop Earrings" priced at £3,375. The price was listed next to an older "was" price of £7,500, which was crossed out.

The complaint

A complaint was made that the savings claim for the earrings was misleading, as the purchaser had never seen them being sold at the old, higher price.

The response

WS argued that the older retail price had fluctuated over the years due to the price of gold and diamonds, having first been advertised in 2013. The price of £7,500 was advertised during the period of November 2016 to December 2019. This had been the retail price for the three years prior to the earrings being bought by the complainant at the discounted price. They said that they followed the relevant pricing guidance and ensured that the full price had been advertised for a longer period than the discounted price, and the period during which the discounted price was offered was shorter than the period that the product was offered at the full price.

The decision

The ASA considered that consumers would understand from the ad that the usual price for the goods was £7,500 and that the advertised reduced price of £3,375 was the genuine level of savings they would achieve at that time. It considered that the ten months the earrings were advertised at the lower price was enough for it to establish that price as their usual selling price. Because of this, consumers would understand the higher price to still be the usual price for the earrings and the savings claim would be misleading. The ASA therefore upheld the complaint and deemed WS had breached rules 3.1 and 3.17 of the CAP Code.

Why is this important?

The decision showcases that the ASA will enforce its rules against any price listings that are not genuine representations of the actual price of the goods at the time of the ad. This includes any old data that is used as a comparative tool to show any potential savings against a reduced price, particularly for any goods where the price fluctuates because of raw materials.

Any practical tips?

Beware sticking to the maxim that you can run a price comparison if the full price has been advertised for a longer period than the discounted price. Here the period during which the discounted price was offered was shorter than the period that the product was offered at the full price. However, ten months is a long time and it was enough for the lower price to be established as the "usual" selling price – thereby making the use of the higher price as a "was" price misleading.

ASA upholds misleading "Jab & Go" claim against Ryanair

The question

How careful do you need to be in your ads when using phrases such as "Jab & Go" or "Vaccine?"

Key takeaway

Advertisers must take care to avoid encouraging viewers to act irresponsibly in relation to government guidelines on vaccinations and travel restrictions. Ads which suggest that you can get vaccinated ahead of government plans in pursuit of travelling abroad on holiday or suggesting that holidays will be free of travel restrictions before government announcements may be regarded as misleading.

The ad

Ryanair aired two TV ads. The first ad aired on 26 December 2020 featured an image of a medical syringe and a bottle labelled "VACCINE" and large on-screen text which stated "VACCINES ARE COMING". A voice-over stated, "*Covid vaccines are coming. So book your Easter and summer holidays today with Ryanair. £1m seats on sale from £19.99 to sunshine destinations in Spain, Italy, Portugal, Greece and many more. So you could jab and go!*" Footage showed groups of people in their twenties and thirties enjoying the holiday destinations. The voice-over continued, "*Book today on Ryanair.com and if your plans change, so could your booking*". Large on-screen text appeared which stated "JAB & GO!". The second ad, seen from 4 January 2021 included the same imagery, on-screen text and voice-over, except it referred to a different price offer.

The complaint and the response

The ASA received 2,370 complaints, falling into three categories:

1. complainants who felt the ads and particularly the claim "Jab & Go" implied that most of the UK population would be successfully vaccinated against COVID-19 by spring/summer 2021 and would be able to holiday unaffected by travel or other restrictions, challenged whether the ads were misleading
2. complainants who felt the ads trivialised the ongoing restrictions and effects of the pandemic on society and individuals, challenged whether the ads were offensive, and particularly the claim "Jab & Go"
3. complainants also challenged whether the ads, and particularly the claim "Jab & Go", were irresponsible.

Ryanair responded stating that:

- viewers would understand the ads envisaged a hypothetical Easter or summer holiday and considered that the average UK consumer was familiar with information about the vaccines, their rollout schedule, travel restrictions and the inherent uncertainty in the travel industry. In that context, Ryanair believed the ads' claims that use of phrases such as "vaccines are coming" and that "you could jab and go" were not misleading to consumers, who would be able to make an informed decision about whether they wished to book flights
- the use of "vaccines are coming" was not a claim concerning who would be vaccinated, when they would be vaccinated, how vaccines were to be administered or how long it would take to achieve maximal protection once vaccinated. Nor did they claim that vaccinations were a prerequisite to travel. The ads did not make any representations about the travel or social distancing restrictions that might be in place in spring and summer 2021; it would be misleading for them to try to speculate about what arrangements might be in place
- the ads were uplifting and encouraged viewers to consider a brighter future when restrictions were lifted, and people could go on holiday again. The term "jab" had been used widely to describe vaccines, including by the Government, and so they did not consider the language used was insensitive. Also, there was nothing to suggest those who were not vaccinated would not be able to travel abroad or that unvaccinated people would not be able to take advantage of the discounted prices advertised
- the ads did not trivialise the need to prioritise the rollout of the vaccine to vulnerable individuals or encourage individuals to try to "jump the queue". They highlighted that was not possible given that the vaccine was only available to those invited to make an appointment by the NHS based on the phased rollout schedule, and they considered the public was aware of that.

The decision

Were the adverts misleading?
ASA acknowledged that information about COVID-19 vaccines, the UK's vaccination rollout, and travel and other restrictions was available from a wide range of sources, and that the pandemic was the focus of the news and government messaging from November 2020 to January 2021. However, the situation was complex and constantly evolving throughout that time period. In that context, the ASA considered that consumers could easily be confused or uncertain about the situation at any given time and how it might develop throughout 2021. It was therefore important that advertisers were cautious when linking developments in the UK's response to the pandemic to specific timeframes around which life might return to some level of normality, particularly when linking it to how confident consumers could be when making purchasing decisions. The ASA further considered that the specific references to Easter and summer holidays directly linked the rollout of the vaccine to the implication that many people who wished to go on holiday during those periods would be able to do so as a direct result of being vaccinated. The ASA considered that the clear link made in the ads between the vaccine rollout and being able to holiday at Easter or summer 2021 provided reassurance to viewers that they could feel confident about booking flights, because they would be vaccinated by the time of their holiday. The ASA also understood that while the vaccines were proven to provide protection for individuals against developing serious illness, vaccinated individuals might still be infected with, or spread, the virus and were therefore advised to continue social distancing and mask-wearing. In that context, the ASA understood that any travel restrictions (either on leaving the UK or entering other countries) and other restrictions such as social distancing and mask-wearing were likely to remain the same for both vaccinated and non-vaccinated individuals in at least the short to medium term.

The ASA therefore concluded that the implication in the ads that most people who wished to go on holiday at Easter or summer 2021 would be vaccinated in time to do so, and that being vaccinated against COVID-19 would allow people to go on holiday without restrictions during those periods, was misleading and therefore breached BCAP Code rule 3.1.

Were the adverts offensive?
In relation to whether the ads trivialised the pandemic and caused harm or offence, the ASA did not uphold the complaint. Many complainants felt that the way in which the ads linked the start of the vaccine rollout to being able to go on holiday trivialised the need to prioritise the vaccine to those who were most medically vulnerable, and was insensitive to the pandemic's impact on those who had been ill or who had lost someone to COVID-19, who worked on the frontline or who would not be able to be vaccinated. However, the ad did not make any reference to those groups and whilst the tone was celebratory, the ASA did not consider it trivialised the wider impacts of the pandemic. The ASA considered they were unlikely to cause serious or widespread offence and were therefore not in breach of BCAP Code rule 4.2.

Were the adverts irresponsible?
Finally, the ASA upheld the complaints that the campaign was irresponsible. The ASA considered some viewers were likely to infer that by Easter and summer 2021 it would be possible for anyone to get vaccinated in order to go on a booked holiday, that maximal protection could be achieved immediately through one dose of the vaccine, and that restrictions around social distancing and mask wearing would not be necessary once individuals were vaccinated. The ASA considered this could encourage vaccinated individuals to disregard or lessen their adherence to restrictions, which in the short term could expose them to the risk of serious illness, and in the longer term might result in them spreading the virus. As such, the ASA considered the ads could encourage people to behave irresponsibly once vaccinated.

The ASA further considered the ads encouraged people to behave irresponsibly by prompting those who were not yet eligible to be vaccinated to contact GPs or other NHS services in an attempt to arrange vaccination, at a time when health services were under particular strain. For those reasons, the ASA concluded the ads were irresponsible and breached BCAP Code rule 1.2.

Why is this important?

The ruling highlights the importance of subject matter and the need to take care in wording to avoid being regarded as suggesting socially irresponsible conduct or misleading the public during a particularly sensitive time.

Any practical tips?

Take care to avoid claims that could be seen to encourage consumers to disregard the rule or the spirit of Government legislation and safety recommendations (including those relating to vaccinations and travel restrictions). Doing so is likely to be construed as socially irresponsible.

ADVERTISING

Three Mobile claim to be "the best network for data" misleading

The question

What are the limits and substantiation requirements on advertisers in relation to claims on being the "best network for data" in the telecommunications sector?

Key takeaway

A TV, website and paid-for search ad by Three Mobile were banned for failing to produce adequate substantiation to support the claim that they were the "best network for data".

The ad

The ruling concerns three ads for Three Mobile. The first was a paid for search ad, the second a website page, and the third a TV ad with voiceover. All three ads included some variation of the message "*The Best Network for Data*".

The complaint

Competitor EE challenged whether this message used in all three ads was misleading, whether it could be substantiated or whether it was verifiable.

The response

Three Mobile provided a lengthy and substantive response in which it explained that the claim was predominantly based on them winning the Best Network for Data award at the Mobile Consumer Choice Awards and their belief that consumers would not see the Best Network for Data award as a technical award based on objective measures. Further, Three Mobile claimed that nothing in the ads' context suggested that the award was based on technical performance characteristics. Clearcast and Mobile Choice Awards both fed into the response also, finding that the Mobile Choice Consumer Awards was a well-established and respected independent mobile phone awards organisation.

The decision

The ASA gave a lengthy ruling and found the ads to be in breach of the CAP Code for a number of reasons, namely: (i) it often wasn't clear in the ads that the claim was based on the Consumer Choice Award; (ii) the use of the word "data" was likely to give consumers the impression that the rating was based on the technical performance of the network, rather than factors relating to the company more widely, such as customer service; and (iii) the details of the basis for the comparison in the ads were not readily accessible.

Why is this important?

The ruling highlights the need for clarity in any claims regarding goods or services being the "best" in a category. Ads using this kind of wording need to be clear on the metrics used to decide why the goods or services are the best, especially when this could be in relation to technical performance over, for example, consumer perception or popularity.

Any practical tips?

If you make any claims of being the "best" in your advertising, whether it is to do with goods or services, be mindful of substantiation and clarity in relation to those claims to not potentially mislead consumers. "Best" claims are comparative claims, and you need to set out the basis of the comparison in an intelligible way to consumers, and if you are relying on an award to make the claim, lock in reference to that award in your advertising to ensure the basis of the claim is expressly clear.

DCMS begins inquiry into influencer culture and the power of influencers in marketing

The question

What are the UK government's future plans for influencer marketing?

Key takeaway

The government is clearly keeping a keen eye on influencers and their impact on society at large, including in the sphere of influencer marketing. The Department for Digital, Culture, Media and Sport's (DCMS) inquiry will shape potential future legislation, so all relevant stakeholders are encouraged to participate to allow for proper input from the industry.

The background

The DCMS has recently started an inquiry into the power of influencers on social media, how influencer culture operates and the absence of national regulation on the promotion of products or services on social media. The inquiry is also set to look at influencers' impact on media and popular culture, as well as the positive role they can play through raising awareness of specific issues.

The inquiry follows on from the ASA's report earlier this year, which shows a high level of non-compliance by influencers on appropriately labelling advertising posts as such. The CMA also found similar levels of non-compliance in their research into influencer marketing (with 75% of influencers "burying" their disclosures in their posts).

The inquiry

The DCMS is inviting written submissions from stakeholders, for example social media platforms and services like YouTube where influencers are featured prominently. The questions are:

- how would you define "influencers" and "influencer culture"? Is this a new phenomenon?
- has "influencing" impacted popular culture? If so, how has society and/or culture changed because of this side of social media?
- is it right that influencers are predominantly associated with advertising and consumerism, and if not, what other roles should influencers fulfil online?
- how are tech companies encouraging or disrupting the activities of influencing?
- how aware are users of the arrangements between influencers and advertisers?
- should policymakers, tech companies and influencers and advertisers themselves do more to ensure these arrangements are transparent?

Why is this important?

The inquiry appears to signal intent by the government to propose further legislation around influencers in the future, which will undoubtedly apply to brands as well as influencers.

The DCMS has indicated that it is looking into further regulation around a lack of transparency around the promotion of products or services by influencers on social media (potentially including the specific terms under which companies and influencers collaborate on social media). The extent of any future legislation remains to be seen and will be shaped by the inquiry and answers DCMS receive from stakeholders.

Any practical tips?

The deadline for the submission of answers to the DCMS' queries was on 7 May 2021, and the DMCS' findings will be hotly anticipated in the near future.

Global Expertise.
Local Connections.
Seamless Service.

TERRALEX

www.terralex.org

rpc.co.uk