March 2018

Page

1. Contractual interpretation / limitation of liability

Royal Devon and Exeter NHS Foundation Trust v ATOS IT Services UK Ltd [2017] EWCA Civ 2196 3

2. Penalties

Holyoake and another v Candy and others [2017] EWHC 3397 (Ch) 5

3. Contractual interpretation / implied terms

Kason Kek-Gardner v Process Components [2017] EWCA Civ 2131 7

4. Good faith / duress

Al Nehayan v Kent [2018] EWHC 333 (Comm) 9

5. Termination

Assessing damages for termination – Phones 4U Ltd (in administration) v EE Ltd [2018] EWHC 49 11

6. Confidential information / trade secrets

IPO publishes consultation on Trade Secrets Directive (EU/2016/943) 13

7. Trade marks / passing off

Caspian Pizza Limited & ors v Shah & & another [2017] EWCA Civ 1874 15

8. Data protection

Vicarious liability for deliberate data breaches – Various Claimants v WM Morrisons Supermarket PLC [2017] EWHC3113 (QB) 17

ICO publishes draft guidance on children and the GDPR 19

Article 29 Working Party publishes guidelines on consent under the GDPR 22

Article 29 Working Party adopts guidelines on Data Protection Impact Assessments 26

Article 29 Working Party publishes draft guidelines on transparency under the GDPR *28*

Article 29 Working Party publishes guidelines on data breach notifications under the GDPR *31*

ICO fines Carphone Warehouse £400,000 following systemic data failures *34*

Court of Appeal declares the Data Retention and Investigatory Powers Act 2014 unlawful – Secretary of State for the Home Department v Watson MP and others [2018] EWCA Civ 70 *37*

9. Online platforms

Government publishes Digital Charter *39*

10. Consumer

Update of the Guidance for Traders on Pricing Practices *42*

11. ASA

ASA guidance on promotional marketing for subscription models *43*

ASA ruling on Ryanair's claim: "Europe's number one airline"? *45*

ASA ruling on Amazon TV ad interacting with AI *48*

ASA call for evidence on recognition and labelling of online ads *50*

Key principles of ad disclosure *52*

Contractual interpretation / limitation of liability

Royal Devon and Exeter NHS Foundation Trust v ATOS IT Services UK Ltd [2017] EWCA Civ 2196

The question

How will the Court interpret limitation of liability clauses?

The facts

An NHS Trust and ATOS entered into a contract for ATOS to provide an IT system which would allow for electronic document management and scanning. The NHS Trust later terminated the contract, alleging defects with the system which ATOS had failed to remedy. The NHS Trust alleged that the limitation of liability clause contained in the contract was unenforceable, as it was ambiguous or uncertain.

The relevant clause stated:

> "*9.2 The aggregate liability of the Contractor in accordance with sub-clause 8.1.2 paragraph (b) shall not exceed:*
>
> *9.2.1 for any claim arising in the first 12 months of the term of the Contract, the Total Contract Price as set out in section 1.1; or*
>
> *9.2.2 for claims arising after the first 12 months of the Contract, the total Contract Charges paid in the 12 months prior to the date of that claim*."

The High Court ruled in ATOS' favour and dismissed the NHS Trust's claim that paragraph 9.2 was not capable of being construed. The Court also concluded that the commercially sensible interpretation of the clause was to impose a single cap on liability. This cap could be either the cap in 9.2.1 or the cap in 9.2.2 depending on the circumstances, ie when the claim arose.

The NHS Trust appealed the second point, arguing that paragraph 9.2 in fact imposed two caps.

The decision

The Court of Appeal found in favour of the NHS Trust and allowed the appeal. The Court stated that clause 9.2 contained two separate caps because:

- although the High Court considered the phrase "*aggregate liability*" pointed towards one cap on liability rather than two, this was not necessarily the case. It could also mean the aggregate of the sums under paragraphs 9.2.1 and 9.2.2;
- the word "or" at the end of paragraph 9.2.1 could be read disjunctively or conjunctively;
- the language of the clause strongly emphasised that there were two separate caps. For any default occurring in the first year of the contract, ATOS' liability was capped at the contract sum. For any default after that, ATOS' liability was capped at the amount of contract charges paid in the previous 12 months. If there were defaults in each period, then ATOS' liability for the default in the first 12 months was capped at the contract price, and for subsequent defaults it was capped at the amount of contract charges paid in the relevant 12 month period;
- this interpretation made the most sense commercially. ATOS' work in the first 12 months was high value with potentially very expensive consequences. Its work after that period for the NHS Trust was lower value work with less expensive potential consequences.

Why is this important?

This case demonstrates how precisely limitation clauses must be drafted. The dispute arose from the lack of clarity in one paragraph of the clause which allowed for multiple interpretations.

It also highlights the risk of leaving the Court to interpret a clause by reference to commercial sense. The High Court came to its decision because it believed that imposing one cap made the most commercial sense. However, the Court of Appeal came to the opposite opinion by applying what it considered to be the clear direction of the drafting and an outcome it said was consistent with commercial common sense.

Any practical tips?

Be extra careful with drafting exclusion and limitation clauses!

Limitation clauses that deal with aggregate financial caps, different caps for different claims, the timing of when claims "arise" and connected claims are often problematic. Consider stress-testing key clauses with hypothetical disputes and claims to see how they operate in practice. If in any doubt, seek a legal colleague's opinion or specific advice…it could prove (very) expensive not to!

Penalties

Holyoake and another v Candy and others [2017] EWHC 3397 (Ch)

The question

Does the rule against penalty clauses apply to repayment obligations?

The background

Mr Holyoake, a property developer, sought to purchase Grosvenor Gardens House through a company, Hotblack Holding Limited (HHL). To finance the purchase, Mr Holyoake agreed an unsecured personal loan with Christian Candy for £12,000,000.

Mr Holyoake defaulted on the loan and the property was sold without having been redeveloped to repay the loan. Part of the resulting claim was that the loan contained wrongful penalty clauses:

- the borrower was required to pay a redemption amount in the event of an early repayment (which included interest for the two year period of the loan, for a total of £17,740,000);
- the escrow deed provided that if the borrower did not repay the debt and complete relevant documents, a new debt of £17,740,000 would arise;
- the borrower was required to pay certain extension fees under loan extension agreements.

The decision

The Court concluded that the clauses were not penalties. The clauses were not triggered by a breach of contract and so the penalty rule was not engaged (applying *Cavendish v El Makdessi and Parking Eye v Beavis* [2015] UKSC 67).

The redemption clause was triggered by the borrower exercising the option to repay the loan early, not a breach of contract. The requirement to pay the interest which would have accrued over the term of the loan was a primary obligation.

Similarly, the escrow deed clause operated on a failure of a condition, rather than a breach of contract and was therefore not caught by the penalty rule. The way the clause was drafted gave the effect that the borrower had agreed to pay £17,740,000 if he did not complete the relevant documents or refinance the loan.

The extension fees were also construed as primary obligations, as they were payment for consideration ie an extension of time for repayment of the loan.

Why is this important?

This case demonstrates that it is possible to circumvent the penalty rule with careful drafting, for example, when a clause can be drafted as a primary obligation, which operates on a particular event or condition, as opposed to being triggered by a breach of contract.

The penalty rule only applies to a breach of contract, so if a clause is not triggered by a breach of contract the penalty rule is not engaged.

Any practical tips?

Consider whether the consequences of a default can be drafted as primary obligations (eg obligations to pay or indemnities) that arise on particular events. If the financial consequences do follow a breach, include appropriate wording to justify the imposition of those consequences (eg legitimate interests in performance, the benefits to both parties of certainty, etc).

Contractual interpretation / implied terms

Kason Kek-Gardner v Process Components [2017] EWCA Civ 2131

The question

How will the Court approach interpretation of related agreements and implying terms for "business purposes"?

The background

Kemutec Powder Technologies Ltd (KPTL) ran into financial difficulties and entered administration. Process Components Limited (PCL) and Kason Kek-Gardner Ltd (KGL), both companies formed by former directors of KPTL, entered into asset sale agreements with KPTL for parts of the business and certain intellectual property rights.

PCL and KGL subsequently entered into a licence agreement under which KGL licensed PCL to use IP formerly belonging to KPTL. The licence included a termination clause for any material breach of the parties' obligations under the agreement. When PCL was later acquired, it disclosed a copy of the licence to the purchaser. KGL terminated the agreement on the basis that a confidentiality clause had been breached through this disclosure.

The issues included interpretation of contractual provisions, what IP had KGL acquired, and was PCL estopped from asserting certain rights. There were also issues regarding implied terms and termination of the licence between KGL and PCL.

PCL argued that both sale agreements should be read together and, in the light of the overall administration, it made 'commercial common sense' that PCL would have received the IP relevant to the parts of KPTL's business that it had purchased. PCL also argued that a term should be implied in the licence to permit it to disclose the contents of the licence 'for necessary business purposes'.

The decision

The Court of Appeal clarified several points on contractual interpretation, as follows:

- the parties' conduct after concluding an agreement could not be used to affect the interpretation of that agreement. As such, PCL's sale agreement, concluded 10 days after KGL's, could not be used to interpret the initial agreement;

- the 'admissible background' to be considered in contractual interpretation is limited to facts known or reasonably available to both or all parties and it is not right to take into account facts known by only one party;
- relying on 'commercial common sense' and the background of the agreements devalued the importance of the language of the contractual provisions in question;
- an implied term will not be implied into a detailed commercial contract unless it is necessary to give the contract 'business efficacy' or it was so obvious it went without saying. The Court rejected PCL's proposed test that a term could be implied as it was reasonable for 'necessary business purposes', as an implied term must be necessary for the business efficacy of the contract rather than a wider business purpose of a party.

When interpreting the agreement under these principles, PCL had not acquired the IP in the divisions of KPTL it had bought. There was also no implied term in the licence upon which PCL could rely and so the licence was validly terminated.

Why is this important?

The Court of Appeal decision is a useful summary of existing principles of contractual interpretation. It confirms that, for background knowledge to be admissible in the interpretation of contractual provisions, such knowledge must be known to all parties. Background and commercial common sense should not be used to devalue the actual language of the contractual provisions being considered.

Any practical tips?

As always, the wording of the agreement should properly capture the deal. If there are commercial considerations/background that should be taken into account, include this within the recitals.

Also remember that terms will only be implied in limited circumstances – eg they must be necessary to give business efficacy to the agreement, not because they are of wider assistance to the business.

Good faith / duress

Al Nehayan v Kent [2018] EWHC 333 (Comm)

The question

When will the Court imply a duty of good faith?

The facts

In 2008, Al Nehayan entered into an oral joint-venture with Mr Kent, to invest in Mr Kent's hotel business (Aquis) as an equal shareholder. Al Nehayan's investment was later expanded to include an online travel business called YouTravel.

Al Nehayan (through his representatives) provided further support by way of loans and share capital to the businesses over the years as they experienced financial difficulties. By April 2012, Al Nehayan's representatives sought to separate his interest from Mr Kent's by restructuring Aquis and YouTravel and seeking repayment of Al Nehayan's contributions. After meetings, where Mr Kent was allegedly threatened with physical violence, he made two agreements with Al Nehayan to implement this proposal, a promissory note and a framework agreement (the **Agreements**).

Al Nehayan later sued Mr Kent for payments he claimed were owed under the Agreements. Mr Kent counterclaimed on the basis that, under the original joint venture, Al Nehayan owed Mr Kent various fiduciary and contractual duties, including a duty to act in good faith and that, but for breaches of these duties, Mr Kent would not have entered into the Agreements. Mr Kent also claimed that he entered into the Agreements by duress, and that this duress was actionable.

The decision

The Court held that Al Nehayan was not entitled to be paid sums under the framework agreement, but was entitled to damages of the value of the promissory note.

The Court also accepted various elements of Mr Kent's counterclaim, concluding that:

- Al Nehayan did not owe any fiduciary duties to Mr Kent;
- due to the nature of the parties' relationships, as participants in a joint-venture, it was essential to imply a duty of good faith into the contract to give effect to the parties' reasonable expectations. The Court viewed the relationship as "*a classic instance of a relational contract*" in which the parties "*naturally and legitimately expected of each other greater candour and co-operation and greater regard for*

each other's interests than ordinary commercial parties dealing with each other at arm's length";

- Al Nehayan's representatives induced Mr Kent to enter the Agreements by conduct which breached the implied contractual duty of good faith;
- this inducement also amounted to duress. No legal basis for demanding repayment by Mr Kent was identified, meaning the demand was illegitimate. This illegitimate demand was reinforced with threats to Mr Kent;
- Mr Kent's loss was the entry into the Agreements. This meant that any payment under the promissory note made by Mr Kent to Al Nehayan would give rise to an equal and opposite liability of Al Nehayan to Mr Kent.

The overall effect of the Court's finding was that neither party was entitled to recover money from the other.

Why is this important?

This decision is an example of the Court finding that a contractual duty of good faith should be implied, as well as finding that a joint venture arrangement is a "relational contract" that gives rise to higher standards than ordinary commercial dealings. The Judge (Leggatt J) also found an implied duty of good faith in *Yam Seng*, which involved a long term distribution agreement – although this approach (including as to "relational contracts") has not found favour with the Court of Appeal.

Any practical tips?

Express obligations to provide information, cooperate, etc will always be preferable to relying on implied terms, particularly as to good faith. But bear in mind that there may still be a willingness, at least among some judges, to find a duty of good faith to deal with unreasonable or unconscionable behaviour – particularly in long term or so-called "relational contracts".

Termination

Assessing damages for termination – Phones 4U Ltd (in administration) v EE Ltd [2018] EWHC 49

The question

How will the Court assess damages for termination on an express contractual right?

The background

Phones4U ceased trading and went into administration in September 2014. Following this, EE terminated its trading agreement with Phones4U on the basis of an express contractual provision, entitling EE to terminate on an insolvency event. The termination notice made it clear the termination was on this basis, and was irrespective of breach by Phones4U.

Phones4U subsequently claimed £120million in unpaid commission from EE under the trading agreement. In response, EE counterclaimed for £200million of damages at common law for loss of bargain resulting from repudiatory breach of the trading agreement. In particular, EE argued that the Phones4U's cessation of trading (on 15 September) and EE's termination notice (on 17 September) amounted to repudiatory breach of Phones4U's obligations under the trading agreement to market and sell products.

The decision

On an application of summary judgment, the Court confirmed that EE needed to show that the termination notice was an exercise of EE's common law right to terminate for repudiatory breach, not simply an exercise of a contractual right to terminate the trading agreement, in order to recover damages for loss of bargain.

The Court decided that EE's termination letter had communicated expressly and unequivocally that EE was terminating on the basis of its contractual right under the trading agreement, irrespective of any breach by Phones4U. This termination right was independent of any breach, and EE's common law right to terminate for repudiatory breach. It was clear that the circumstances of termination and consequential loss of bargain did not result from a repudiatory breach.

Although the termination notice had 'expressly reserved all rights and remedies', this did not assist EE as 'a right merely reserved is a right not exercised'.

As such, EE's counterclaim had no prospect of succeeding and was summarily dismissed.

Why is this important?

This decision confirms that if a termination notice states that a party is terminating on the basis of a contractual right to terminate only, the terminating party will lose its right to claim common law loss of bargain damages for repudiatory breach. This may have very significant commercial consequences.

Any practical tips?

Make sure all grounds of termination are covered in any termination notice. Where appropriate, a termination notice should be clearly drafted to confirm that termination is based not only on a contractual right to terminate, but also on repudiatory breach of contract – particularly if there is a possibility of a damages claim in the future (by either party).

Confidential information / trade secrets

IPO publishes consultation on Trade Secrets Directive (EU/2016/943)

The question

How will the UK implement the Trade Secrets Directive?

The background

On 8 June 2016 following a proposal from the European Commission, the European Parliament and Council adopted a Directive that aims to harmonise the national laws in EU countries against unlawful acquisition, disclosure and use of trade secrets.

The Trade Secrets Directive (EU/2016/943) will harmonise the definition of trade secrets across member states in accordance with existing international standards. That definition will essentially amount to "confidential information" under English law (ie not limited to the narrower concept of "trade secrets" as understood under English law).

The Directive aims to: (1) stop unlawful use and further disclosure of misappropriated trade secrets; (2) remove goods that have been manufactured on the basis of wrongly acquired trade secrets (3) provide a right of compensation for the damage caused by unlawful use or disclosure of trade secrets.

EU member states are required to bring into force the national law(s) necessary to comply with the Directive by 9 June 2018.

The development

The UK Intellectual Property Office (IPO) published a consultation on the implementation of the Trade Secrets Directive and the draft UK regulations in February 2018.

The IPO believes that the majority of the substantive provisions of the Directive already exist in UK law; so the draft regulations do not contain provisions dealing with the acquisition, use or disclosure of illegally acquired trade secrets. The proposed draft regulations are concerned primarily with limitation and prescription periods, procedural issues and remedies.

Why is this important?

The Trade Secrets Directive will provide more consistent and effective remedies for unauthorised use or disclosure of confidential information across the EU. The UK has confirmed that it will be implementing the Directive (notwithstanding Brexit).

Although the Directive is unlikely to result in significant changes in UK law or procedures that apply to confidential information claims, it will have a greater impact in some EU member states and it may increase awareness and focus on confidential information issues generally.

What next?

The closing date for responding to the IPO was 16 March 2018, after which the responses will be published in due course.

The Directive is to come into force any time between now and 9 June 2018, however no definitive date on implementation into UK law has been confirmed.

Trade marks / passing off

Caspian Pizza Limited & ors v Shah & & another [2017] EWCA Civ 1874

The question

Can localised goodwill prevent the registration of a UK trade mark?

The facts

The claimants started a pizza business in Birmingham in 1991, registering the word mark CASPIAN in 2005 and a device mark featuring the words CASPIAN PIZZA alongside an image in 2010.

The defendants were also in the pizza business and had operated a restaurant in Worcester called Caspian Pizza since 2004.

The claimants brought a claim for trade mark infringement and passing off, with the defendants counterclaiming that the claimants' trade marks were invalid. At first instance, the judge found that the defendants had acquired localised goodwill in the name CASPIAN for a pizza restaurant in Worcester.

The defendants could therefore rely on the locality defence at s11(3) of the Trade Mark Act 1994 in response to the infringement proceedings. The judge also found that the claimants' word mark was invalid based on this earlier passing off right, but that their device mark was valid.

The claimants appealed for the validity of their word mark, whilst the defendants cross-appealed that the claimants' device mark was also invalid.

The decision

The Court of Appeal confirmed that:

- the defendants could rely on the locality defence, despite the claimants having goodwill in the word CASPIAN in Birmingham since 1991;
- the relevant threshold for goodwill in a mark is "*over an identifiable geographical area that would qualify for protection in passing off proceedings*";
- goodwill in a particular locality, and not throughout the UK, would be enough to prevent another party registering a UK trade mark;
- the Trade Mark Act 1994 does not allow for a partial declaration of invalidity; and

- a party cannot retrospectively remove locations from the geographical scope of their trade mark registration, the trade mark owner would have to pre-emptively remove areas from the scope of the registration.

The Court of Appeal therefore dismissed the appeal, and accepted the cross-appeal and declared that the claimants' CASPIAN PIZZA device mark was also invalid.

Why is this important?

This decision highlights that a localised passing off right can be relied upon to invalidate a registered UK trade mark (which provides national protection).

Any practical tips?

Consider carrying out common law as well as registry searches and evaluate trade mark use, even if only on a localised basis. Depending on the results, consider whether registered rights should be subject to a limitation or disclaimer. Above all, apply to register marks early!

Data protection

Vicarious liability for deliberate data breaches – Various Claimants v WM Morrisons Supermarket PLC [2017] EWHC3113 (QB)

The question

Can a business be held vicariously liable for the actions of an employee who deliberately breaches its employer's data protection policies and data protection law?

The background

In late 2013 the Defendant, Morrisons, had tasked one of its senior IT auditors, Andrew Skelton, with providing KMPG a copy of its payroll master file for the purpose of its annual statutory audit process. Without Morrisons' knowledge, Andrew Skelton retained a copy of the payroll master file and later posted the payroll data to a file-sharing website and sent copies of the data to various newspapers. The data concerned almost 100,000 employees.

The newspapers alerted Morrisons to the data breach and Andrew Skelton was subsequently arrested and convicted of criminal offences in relation to his misuse of the payroll data. Mr Skelton's motive was found to be malicious and in response to a disciplinary sanction imposed by Morrisons earlier in 2013. Despite Morrisons acting quickly to protect the affected employees upon learning of the data breach, just over 5,500 employees brought claims against Morrisons.

The Claimants brought a claim for compensation for breach of statutory duty under s.4(4) DPA, and at common law for misuse of private information and breach of confidence. They argued that Morrisons bore both primary and vicarious liability for Skelton's acts.

The decision

Langstaff J found that Morrisons was not liable for any direct breach of the DPA which would have caused the unauthorised disclosure of the employees' personal data. In particular, he found that the extraction and transfer of the data to Skelton had been secure and, even if it had not been, was not the cause of the publication of the unauthorised data online. There had been no breach of the seventh principle in permitting Skelton access to the data.

While Morrisons were not liable under the DPA, the Claimants did succeed with their alternative argument that Morrisons should be vicariously liable for the actions of Mr Skelton.

Langstaff J found that "there was an unbroken thread that linked" Skelton's work to the disclosure, that Skelton had been deliberately entrusted with the data by Morrisons, and was acting as an employee when he received the data. The Judge rejected the contention that the fact that the disclosures were made at the weekend, using personal equipment at home, disengaged them from his employment. Skelton's motive was irrelevant in determining vicarious liability.

Why is this important?

The implication of the judgment is that, notwithstanding an organisation achieving compliance with its obligations as a data controller, at not insignificant expense, data controllers may nevertheless be held liable for the conduct of an employee acting on their own account even where those actions are criminal and deliberately targeted at harming the organisation; there is an obvious tension in such a finding.

Any practical tips?

Where regulatory compliance may save a data controller from the abundant fines available to the ICO under the GDPR, this will not be sufficient to avoid the prospect of liability for compensation and costs in group litigation, whether brought by individuals themselves or by a not-for-profit on their behalf under the new rights afforded by the GDPR. Businesses need to take appropriate steps to prepare for such potential liability, in particular obtaining insurance cover against the risks and having robust processes in place to mitigate the risks when a data breach occurs.

Data protection

ICO publishes draft guidance on children and the GDPR

The question

What extra requirements must be met when processing the personal data of a child under the GDPR?

The background

Upon coming into force on 25 May 2018, the GDPR will introduce new, specific legal responsibilities for organisations that are processing children's data. On 21 December 2017, the ICO published draft guidance on children and the GDPR, intended to provide more detailed, practical guidance for UK organisations that are processing children's personal data under the GDPR.

The development

The GDPR contains provisions intended to enhance the protection of children's personal data. The draft guidance focusses on the additional, child specific considerations necessitated by those provisions. From a policy perspective, child specific provisions are provided by the GDPR on the basis that children require more particular protection regarding collection and processing of their personal data, as they are likely less aware of the risks involved than an adult. The guidance broadly splits the relevant requirements of the GDPR into five categories:

1. Bases for processing a child's personal data

Organisations need a lawful basis for processing a child's personal data. Broadly, there are three bases upon which an organisation can rely:

- Consent – when relying on this basis, an organisation should ensure a child understands what they are consenting to, and there is no exploitation of any imbalance in power which may exist between the child and the organisation.
- "Necessary for the performance of the contract" – when relying on this basis, it is important that the organisation consider the child's competence, or otherwise, to understand what they are agreeing to, and their competence to enter into a contract.
- "Legitimate interests" – when relying on this basis, the organisation should ensure it takes responsibility for identifying the risks and consequences of the data processing, and ensure age appropriate safeguards are in place to protect the child.

2. Offering an Information Society Service (ISS) directly to a child, on the basis of consent

- When offering an ISS (online service) to a child, located in the UK and on the basis of consent, an organisation must make reasonable efforts to ensure that anyone providing their own consent is 13+ years old (noting that the UK has adopted 13 as the age of consent).
- Where a child is under the age of 13, an organisation must obtain the consent of the person with parental responsibility over that child when offering the ISS, and make reasonable efforts to verify that the relevant person does indeed hold parental consent over that child. Note that age verification or parental consent is not required when the ISS (online service) offers online preventative or counselling services to the child.

3. Marketing

- If an organisation is marketing to children, it should take into account a child's reduced ability to recognize and critically assess the purpose behind any processing, and consider any potential consequences of children providing their personal data as part of that marketing.
- An organisation should also take into account sector specific guidance on marketing, for example that issued by the ASA, in order to make sure children's personal data is not used in a way which could lead to their exploitation.
- Where a child asks that an organisation stop processing their personal data for the purposes of direct marketing, it should do so.
- An organisation should comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (**PECR**).

4. Solely automated decision making

- Children have a right not to be subject to decisions based solely on automated processing if these have a legal or similarly significant effect on them.

5. Privacy notices

- Privacy notices should be clear, and written in plain, age-appropriate language.
- To assist with this, child friendly ways of presenting privacy information should be implemented. Examples could include: diagrams, cartoons, graphics or videos.
- If an organisation requires children's personal data, it should explain why it is required, and what it will be used for, in an age appropriate manner.
- Where relying upon parental consent to process a child's personal data, offer two different versions of privacy notices: one aimed at those holding parental responsibility, and one aimed at children.

More generally, children have the same rights as adults over their personal data. These rights include the rights of access to personal data, request rectification, the right to object to processing and the right to erasure of personal data.

If the original processing was based on consent provided when the individual was a child, an individual's right to erasure is particularly important and should be complied with.

Why is this important?

The GDPR does not represent a fundamental change to many of the rights held by children over their personal data; children already enjoy rights under the Data Protection Act (1998) (the **DPA**), which applies to children as individuals in their own right. However, the DPA does not provide explicitly for the protection of children's data in the detailed and specific manner which the GDPR does; the GDPR can be said to be more detailed, tailored and widely encompassing in the protection it provides to children, as compared to the DPA. It also provides more clarity and certainty for organisations. By reference to the GDPR, organisations can now be more certain that they are doing enough to protect children's data.

Any practical tips?

The fact that the DPA already provides some protection to children, albeit as individuals in their own right, means that an organisation may well have already adopted procedures that comply with the more detailed requirements of the GDPR. Nevertheless, it is critical that data processing procedures are reviewed in light of the detail provided, to be sure of GDPR-level compliance. Perhaps of all areas, children's data collection is one where a 'privacy by design' approach should be adopted when designing and updating systems, and consideration given to the need for Data Protection Impact Assessments. Given the clear prescriptive guidance now issued by the ICO, it is hard to see her giving much leeway to any businesses that ignore or side-step them.

Finally, don't forget to read the guidance in line with other guidance which overlaps. For example, the Article 29 Working Party has recently released guidance on consent under the GDPR, and that includes interesting commentary on children and consent – for example, where parental guidance has been obtained, the need for fresh consent to be sent to children when they reach the age of consent.

Data protection

Article 29 Working Party publishes guidelines on consent under the GDPR

The question

What exactly are the higher standards of consent under the GDPR?

Definition of consent

The GDPR defines consent as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4(11).

Interpreting the consent definition

The WP29 has now thrown light on what all these different elements mean, namely:

- **Freely given**: this must imply real choice and control for individuals. As the WP29 says: "If consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given". Data subjects have to be able to refuse or withdraw consent without detriment and there should be no "imbalance of power". Note that such an imbalance of power will often be presumed in relationships between a public authority and a data subject, and between and an employer and an employee. Equally, "bundling" consent with acceptance of terms and conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data not necessary for the performance of that contract or service, is also presumed not to be freely given. See Example A below;
- **Specific**: separate consent should be gained for separate processing purposes; vague and blanket consent to a bundle of processing purposes is not sufficient. So controllers must apply (i) purpose specification as a safeguard against function creep; (ii) granularity in consent requests; and (iii) clear separation of information in obtaining consent for data processing from information about other matters. Also, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose (plus specific information for each purpose);
- **Informed**: sufficient and accessible information should be provided so that an informed decision about consent can be made, it is clear what is being consented to and, for example, that there is a right to withdraw consent effectively. This means providing the name of your organisation, the name of any third party controllers who will rely on the consent, why you want to process the data and what you will do with

it. You must use clear and plain language, avoiding long, illegible privacy policies and legal jargon; and

- **Unambiguous**: a statement or clear, affirmative action is required, signifying agreement to the processing of personal data for the purposes specified. An opt-in box may be used (whereas pre-ticked boxes, opt-out boxes or other default settings should not be used). Interestingly, the WP29 suggests that other actions (eg swiping a screen or waving in front of a smart camera), can qualify as clear affirmative action.

A request for consent should be presented in a manner which is clearly distinguishable from other matters (such as terms and conditions) using clear and plain language.

If, having obtained consent to use data for a particular purpose, you wish to use the data for a new purpose, a new consent will be required unless an alternative lawful ground can be established.

Explicit consent

The GDPR does not define "explicit consent". However, under the GDPR, explicit consent is required where heightened data protection risks exist (for example, when processing special categories of personal data, which includes personal data relating to religious beliefs, sexual orientation or health). In this situation, consent should be given in an expressed statement, such as a written confirmation, rather than by any other positive action. In an online context, the WP29 says that filling in an electronic form or sending an email also works.

Demonstrating consent

You must be able to demonstrate that valid consent has been given (eg that it was possible for the data subject to refuse or withdraw consent without suffering any detriment, that the right to withdraw consent was explained, that the request was clearly distinguishable from other matters etc). In practice, demonstrating consent when it is given means keeping records to evidence consent – who consented, when, how, and what they were told. There is no specific time limit in the GDPR for how long consent will last, but the WP29 suggests that consent should be refreshed at regular intervals.

Existing consent

Consent which has been obtained prior to the GDPR continues to be valid but only if it meets the criteria laid down in the GDPR. So checks need to be made to see how much reliance can be placed on existing processes. If the conditions are not met, or the consent is poorly documented, either: a fresh GDPR compliant consent should be obtained; a different lawful basis for the processing considered; or the processing stopped. Remember that being able to demonstrate consent is critical and that all presumed consents of which no references are kept will need to be renewed.

Withdrawing consent

An individual has the right to withdraw consent to the processing of his or her personal data at any time. In line with the fact that consent must be freely given, it should also be made possible (and easy to) withdraw consent. Withdrawal of consent must be as easy as the process by which the consent was originally obtained. See Example B.

Compliance with other principles

Even if a valid consent is obtained, this does not negate or diminish the requirement to comply with other fair processing principles, such as fairness, necessity and proportionality. For example, holding a consent would not legitimise the collection of data that is unnecessary for the stated purpose. Furthermore, if the performance of a contract, including the provision of a service, is conditional on consent to data processing that is not necessary for the performance of the contract, this will undermine the validity of the consent. Put another way, in the WP29's words: "..it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent".

Children

There are no overall rules on children's consent under the GDPR, but there is a specific provision in Article 8 on children's consent for 'information society services' (services requested and delivered over the internet). Note that the GDPR sets the age of consent at 16, but allows individual Member States to lower this. The UK is adopting the age of 13. The language must be plain and clear for children. In terms of obtaining parental consent where necessary, the WP29 recommends a proportionate approach (ranging from email consent to more concrete proof).

One important point around children is that, as the WP29 points out, parental consent will expire once the child reaches the age of digital consent. It states: “From that day forward, the controller must obtain valid consent from the data subject him/herself. In practice this may mean that a controller relying upon consent from its users may need to send out messages to users periodically to remind them that consent will expire...”. This means that controllers will need to find a way of tracking when a child reaches the age of consent, and then refresh the consent with the individual when that age is reached.

Why is this important?

Consent under the GDPR requires higher standards and the WP29 guidelines reinforce just how tricky this area can be, and why (of all areas) any business which relies on consent to run its operations needs to study the advice carefully, and in good time before the GDPR lands. From a marketing perspective, we await the finalisation of the ePrivacy Regulation, but any hope that this will create a gentler regime for marketing consents has already been dashed now that the draft is in circulation.

Any practical tips?

Watch consent like a hawk! It is an area of the GDPR which is likely to surprise many, especially those in the marketing industry – and not in a good way. Early consideration/action, particularly around the ongoing validity of existing databases after 25 May, is essential. And look out also for the hidden traps. For example, refreshing a child's consent when he/she reaches the age of digital consent – that requirement alone will result in the need for tech developments to ensure that controllers find a way of (automatically) refreshing their databases.

Example A

A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation nor online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

Example B

A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, and this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.

Data protection

Article 29 Working Party adopts guidelines on Data Protection Impact Assessments

The question

When should a data controller conduct a Data Protection Impact Assessment (DPIA)?

The background

DPIAs are a tool for data controllers to build and demonstrate compliance with the GDPR. The process is designed to encourage organisations to describe and audit their processing activity, consider its proportionality, and balance its necessity against the risks to the rights and freedoms of their data subjects.

While the Information Commissioner's Office (ICO) has long been advocating DPIAs as best practice, it is only now, under the GDPR, that DPIAs have become compulsory in certain circumstances.

The development

Article 35 of the GDPR indicates that DPIAs will only be required when a data controller envisages that its processing is "likely to result in a high risk to the rights and freedoms of natural persons". To ensure a consistent interpretation of the circumstances in which a DPIA is mandatory, the WP29 has released guidelines which clarify and expand upon the examples of 'high-risk' processing outlined in the GDPR.

In brief, an organisation's processing is likely to result in a high risk to data subjects if it involves:

- evaluation or scoring (including profiling and predicting);
- automated decision making with legal or similar significant effect;
- systematic monitoring;
- sensitive data or data of a highly personal nature;
- data processed on a large scale;
- matching or combining data sets;
- data concerning vulnerable data subjects;
- innovative use or new technological or organisational solutions; or
- barriers preventing data subjects from exercising a right or using a service or contract.

As a rule of thumb, the WP29 considers that a processing activity meeting two (or more) of the above criteria will require a DPIA. If it is not clear whether a DPIA is necessary, the WP29 recommends that one is carried out nonetheless. As ever, organisations should adopt the 'data protection by design' approach – ie starting early (and in any case always prior to the commencement of processing), and treating DPIAs as a continual and evolving process rather than a one-time exercise.

While the GDPR is flexible as to the methodology used to undertake DPIAs, it does dictate some minimum required features:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the data processing;
- an assessment of the risks to the rights of the individuals affected; and
- measures envisaged to address the risks and demonstrate compliance with the GDPR.

If, after the DPIA has been completed, the data controller considers that it will not be able to sufficiently address the risks identified, it must consult its supervisory authority.

Why is this important?

Non-compliance with DPIA requirements under the GDPR (ie failure to carry out a DPIA when mandatory, carrying out a DPIA incorrectly, or failing to consult the relevant supervisory authority) can result in fines of up to €10m or 2% of total worldwide annual turnover, whichever is higher. And remember that a DPIA-level fine would be additional to the higher level fines (€20m or 4% of global turnover) which could follow the identification of other breaches under the GDPR (ie for the underlying cause of a breach itself).

Any practical tips?

Data controllers should take note of the nine criteria outlined by the WP29, and consider them each time a new processing activity is undertaken. In case of any doubt, it is better to be safe than sorry and conduct a DPIA – no one will blame you for properly stress-testing a new data activity with the threat of GDPR-level fines looming overhead.

Data protection

Article 29 Working Party publishes draft guidelines on transparency under the GDPR

The question

In accordance with the GDPR's new obligation of transparency, what do the WP29 draft guidelines suggest you put in your organisation's privacy policy and other privacy notices?

The background

The WP29 has adopted draft guidelines aimed at providing practical guidance and interpretive assistance on the new obligation of transparency concerning the processing of personal data under the GDPR. The draft guidelines describe transparency as an overarching obligation that applies to three central areas:

- the provision of information to individuals relating to fair processing;
- how data controllers communicate with individuals in relation to their rights: and
- how data controllers facilitate the exercise by data subjects of their rights. The guidelines are particularly relevant in the context of drafting privacy policies and notices.

The development

The transparency requirements, which derive from Articles 12-14 of the GDPR, apply from the point that personal data is collected or obtained, throughout the whole processing period and at specific points in the processing cycle.

Article 12 sets out the general rules which apply to the provision of information to individuals under Articles 13 and 14. Articles 13 and 14 prescribe the information to be provided when data has been collected from the individual or obtained from elsewhere, respectively.

Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible;
- clear and plain language must be used;
- the requirement for clear and plain language is of particular importance when providing information to children;
- it must be in writing "or by other means, including where appropriate, by electronic means";
- where requested by the data subject it may be provided orally; and

- it must be provided free of charge.

Under Articles 13 and 14, information is to be provided where personal data is collected from the data subject (Article 13), or where it is not (Article 14).

While the GDPR does not prescribe the format or modality by which information under Articles 13 and 14 should be provided, it does make clear the data controller's responsibility to take "appropriate measures" in relation to the provision of required information for transparency purposes.

As regards the timing for provision of information under Articles 13 and 14, the WP29 notes that while information must be provided under Article 13(1) "at the time when personal data are obtained", the general requirement under Article 14 is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, depending on the specific circumstances in which the data is processed.

Similarly, in relation to the notification of changes to Article 13 and 14 information, the WP29 says that if the change to the information is indicative of a fundamental change to the nature of the processing, such as enlargement of the categories of recipients or introduction of transfers to a third country, then that information should be provided to the individual "well in advance of the change actually taking effect".

Articles 13 and14 also contain similar provisions requiring the data controller to inform the individual if it intends to further process their personal data for a purpose other than that for which it was collected or obtained in the first place.

The WP29's robust position is that data controllers should provide individuals with an explanation as to how the processing for other purposes is compatible with the original purpose where a legal basis other than consent or applicable law is relied on for the new processing purpose.

The only exception under Article 13 is "where and in so far as, the data subject already has the information".

The WP29 notes that Article 14 carves out a much broader range of exceptions including where the provision of information is impossible or would involve disproportionate effort. A further exception under Article 14(5)(d) applies where the personal data "must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."

Why is this important?

The provision of guidance as to the GDPR's new obligation of transparency is particularly important in the context of privacy policies and privacy notices, and provides clearer guidance as to the level of transparency which the GDPR requires organisations to comply with.

Any practical tips?

When drafting your privacy policy or notice, remember to check the guidance provided on the requirements of Article 12-14 of the GDPR. As a rule of thumb, simplification of language will almost certainly aid the clarity and accessibility of such policies / notices. Basically, keep it simple and don't over-lawyer! This may feel like a hard balance to achieve, especially given the prescriptive nature of the GDPR's requirements on transparency. Having said this, clarity and transparency are what the regulators are looking for and, in any event, clearly makes sense from the perspective of engaging and building trust with your customers.

Data protection

Article 29 Working Party publishes guidelines on data breach notifications under the GDPR

The question

What data notification procedures should data controllers and processors have in place by 25 May 2018?

The guidelines

The key elements of the guidelines include:

Types of data breach

Breaches could relate to the confidentiality, availability and/or integrity of personal data. A breach could relate to any one of these types of breach, or any combination of these. Taking each in turn:

- confidentiality: the disclosure to or access by someone who does not have authority to access the data;
- availability: a loss of access to or the unintended destruction of personal data;
- integrity: the alteration of personal data either by an unauthorised person or by accident.

When to notify a data breach

The GDPR requires data controllers to notify the relevant supervisory authority where it becomes aware of a personal data breach which is likely to result in a risk to the rights and freedoms of individuals. The notification should be made without undue delay and where feasible within 72 hours of it becoming aware of the breach. The controller becomes "aware" once it has a reasonable degree of certainty that (i) a security incident has occurred and (ii) the breach has led personal data being compromised. The investigation should commence promptly and should only be for a short period to establish whether a data breach has occurred. A more detailed investigation can follow the notification to the relevant supervisory authority. A "bundled" notification can be made where the data controller becomes aware of multiple, similar breaches over a short period of time which leads to a longer initial investigation. A "bundled" notification can be made within 72 hours (if appropriate) but should not be made where multiple breaches concern different types of data.

The information to provide alongside the notification

WP29 suggest that a description of the types of individual whose personal data has been affected should be identified. Examples of the types include vulnerable individuals (such as children), people with disabilities, employees and customers. The type of personal data should be identified (eg health data, educational records, social care information, financial details, bank account numbers and passport details). The notification should outline, where appropriate, any particular risk to the data subject because of the breach (eg identity theft, financial loss and threats to professional secrecy). The focus should not be on providing precise information (unless this is available) and should be on addressing the adverse effects of the data breach and ensuring timely notification. Further details can be provided once the notification has been made and further investigations into the breach are underway.

Breaches concerning multiple Member States

Data controllers are required to notify the lead supervisory authority if a data breach occurs. The supervisory authority of the main establishment of the business will be the lead authority. Data controllers may opt to notify the lead authority and the supervisory authorities of the Member States affected by the breach. Should the data controller decide to only notify the lead authority, it should state the affected Member States - and how they have been affected - in its notification to the lead authority.

When a notification is not required

A notification does not need to be made if a breach is "unlikely to result in a risk to the rights and freedoms of natural persons". For example, (i) where a breach relates to personal data which is publicly available so will not constitute a likely risk to the individual and (ii) the loss of encrypted data where a backup is accessible in a timely manner. Where no back-up is available at all or the backup is not available in a timely manner a notification would need to be made. A notification may need to be made some time after a breach occurs if data which was securely encrypted may have been compromised or the encryption software is later known to have vulnerabilities.

Notifying the data subject of a personal data breach

In addition to notifying the relevant supervisory authority in circumstances where a breach is likely to pose a risk to an individual, the individual must be notified where there is a high risk of the individual's rights and freedoms becoming affected by the data breach. Information to be provided should include the nature of the breach, the name and contact details of the data protection officer or other contact point and the likely consequences of the breach, including, where appropriate, measures to mitigate its possible adverse effects. The notification should be made directly to the individuals unless this would result in a disproportionate effort. The communication should be clear and transparent (possibly provided in multiple languages). Controllers should try to maximise the chance of contacting affected individuals (eg by using multiple contact channels to communicate the breach).

A notification does not have to be made to an individual in circumstances where: (i) the controller has applied measures to protect the individuals data in advance of the breach (eg encryption); (ii) the controller has taken steps following the breach to ensure that the high risk threat is unlikely to materialise; and (iii) it would involve a disproportionate effort to notify individuals and the data controller elects to utilise another form of public communication to notify the individual.

Record keeping

Data controllers should keep a record of all data breaches irrespective of whether they notify their relevant supervisory body or not. The record should include the effects and consequences of the breach and details of any remedial action the controller takes. The record should also detail the reasoning behind any decisions the controller takes – especially if the controller decides not to notify the relevant supervisory authority.

Why is this important?

A failure to report a personal data breach in accordance with the GDPR may result in a fine (up to €10 million or 2% of the firm's global turnover) - which would be in addition to a fine for the actual data breach (which could be as much as €20 million or 4% of the firm's global turnover). So knowing when and how to notify is key to avoid aggravating what could already be a painfully expensive fine.

Any practical tips?

Knowing how to promptly detect, notify and investigate data breaches is critical. And systems should be tested regularly to ensure that the right team (including a member of senior management) knows what to do in a crisis.

There is no penalty for reporting incidents which do not amount to a data breach. This makes the chances of the ICO's team being flooded (almost literally!) with breach notifications pretty high. And with many of her senior staff leaving for highly paid jobs in private business, one wonders how she will be able to focus on anything but the biggest, most damaging data breaches.

Data protection

ICO fines Carphone Warehouse £400,000 following systemic data failures

The question

Need an example of how not to protect your customers' and employees' data? Then, read on!

The background

In 2015, Carphone Warehouse was the victim of a cyber-attack, giving intruders access to personal data of more than three million customers and 1,000 employees as well as historic transaction details spanning over 18,000 payment cards for the period March 2010 - April 2011. The card data comprised card holder names and addresses, card expiry dates and card numbers.

The security breach concerned a specific Carphone Warehouse computer system, which was overseen by a specific division of Dixons Carphone plc.

From 21 July to 5 August 2015, the system was subject to an external cyber-attack originating from an IP address in Vietnam. The attacker made a scan of the system server using Nikto, a "relatively commonplace" penetration testing tool for testing security issues such as outdated software and other vulnerabilities. One of the vulnerable points was an installation of the content management system WordPress on one of the websites maintained on the system. Via the WordPress installation, the attacker entered the system and uploaded "web shells" designed to provide the attacker with, among other things, basic file management and database functionality over the contents of the system.

The decision

On the evidence, the ICO found that Carphone Warehouse had committed a serious breach of the seventh data protection principle (Principle 7) in that:

- important elements of the software in use on the system were many years out of date;
- Carphone Warehouse's approach to software patching was "seriously inadequate". Although a "Patch Management Standard" was in place, it was not being followed by the relevant business area;
- Carphone Warehouse needed to have, but did not have in place rigorous controls over who had WordPress login credentials;

- inadequate vulnerability scanning and penetration testing measures were in place at the time. It appeared that no routine testing procedures were in place and no internal or external penetration testing had been conducted in the 12 months leading up to the attack;
- at the time of the attack, Carphone Warehouse had no Web Application Firewall (WAF) for monitoring and filtering traffic to and from its web applications;
- contrary to Carphone Warehouse's internal policy none of the servers that made up the system had antivirus technology installed;
- it was some 15 days after the system was first compromised that the attack was noticed, suggesting inadequate technical measures were in place for detecting attacks;
- the operating system on the servers making up the system all had the same root password which was known and used by some 30-40 members of staff;
- there was no good reason for the retention of large volumes of historic transactions data. Inadequate measures were in place to identify and purge such data;
- while the historical transactions data was encrypted, encryption keys were stored in plain text within the application's source code. In terms of data security, plain text storage for encryption keys was inadequate, particularly for data relating to individuals' financial transactions.

The ICO was satisfied that the contravention warranted a monetary penalty under s 55A of the Data Protection Act 1998, and imposed a fine of £400,000. This was on the basis that, cumulatively, this "multi-faceted contravention" was extremely serious.

Why is this important?

This decision provides a clear example of the types of systemic failures and deficiencies that the ICO will consider to be a breach of data protection principles under the Data Protection Act, and inevitably, under the GDPR also. In that sense, it provides a ready-made checklist of possible contraventions which organisations, or rather their tech teams, need to protect against.

Any practical tips?

£400,000 is a big fine under the ICO's current fining powers (which currently go up to a maximum of £500,000). Come 25 May, she will be able to pull the lever on fines of up to €20m or 4% of global turnover. Against that backdrop, tech directors (whatever their sector) should be thinking seriously about what they should be doing now to make their systems more robust.

Lawyers can't implement technical measures themselves, but they can inform and warn. So consider sharing this report on technical deficiencies with your tech team. The sooner that everyone in the organisation, especially the tech specialists, get a grip on the seriousness of the new GDPR world order, the safer your business will be.

Data protection

Court of Appeal declares the Data Retention and Investigatory Powers Act 2014 unlawful – Secretary of State for the Home Department v Watson MP and others [2018] EWCA Civ 70

The question

Is section 1 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) inconsistent with EU law?

The background

Two British MPs commenced judicial review proceedings to challenge the validity of the powers under section 1 of DRIPA (now replaced by the Investigatory Powers Act (IPA) 2016, the so-called "snooper's charter" which contains similar provisions). This section allows the Home Secretary to require communication service providers to retain communication data for up to twelve months for various purposes, including national security and the detection and prevention of crime.

The ECJ's finding

In 2016, in response to questions referred from the Court of Appeal, the European Court of Justice (ECJ) declared that EU law precludes national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of traffic and location data (ie metadata). Such legislation would be incompatible with the Privacy and Electronic Communications Directive (PECR) and the Charter of Fundamental Rights.

It further noted that any legislation which gives a public authority the power to access retained data must be subject to some restrictions. Such a power must be exercised according to criteria now known as the 'Watson requirements':

- only for the purpose of fighting serious crime;
- only with prior approval from a court or an independent authority; and
- ensuring that the data remain within the EU.

With this clarification, the case was referred back to the Court of Appeal for a further hearing.

The Court of Appeal's decision

The Court granted a declaration stating that section 1 of DRIPA was inconsistent with EU law in that, for the purposes of prevention and detection of criminal offences, it permitted access to

retained data where (i) the object of that access was not solely to fight serious crime; and (ii) access was not subject to review by a court or independent body.

Many other aspects of the ECJ's response (eg does it create an absolute bar on bulk communications data leaving the EU? Do the Watson requirements equally apply to retention for the purpose of national security?) were not discussed by the Court, which observed that these issues will likely be considered as a result of yet another ECJ referral – this time from the Investigatory Powers Tribunal (see Privacy International v IPT [2017] EWCA Civ 1868).

Why is this important?

Yet again, a UK court has ruled that the government's proposed mass surveillance regime is unlawful. While the decision is somewhat academic (since it relates to law which has since been repealed), it will still have implications for the IPA 2016 and the government's proposed changes to it in its recent consultation.

The several ongoing legal challenges concerning both the ECJ's judgment and the IPA 2016 (eg campaign group Liberty's judicial review claim) are symptomatic of a bigger problem, and suggest more polemics to come – especially at a time of heightened sensitivity in all things data.

Any practical tips?

Communication service providers will be particularly affected, as the judgment creates a difficult balance – retention notices issued under the IPA 2016 may require them to retain customer data for potential access by various public bodies; however, the ECJ has made clear in its ruling that blanket retention of such data is not acceptable.

On a bigger scale, what does all of this mean for Brexit, and in particular data transfers once the UK sits outside the EU? How will the UK meet adequacy requirements with this type of legislation in play? As if GDPR wasn't complicated enough, could the UK be facing similar difficulties to those which ultimately saw the death of the Safe Harbour in the US?

Online platforms

Government publishes Digital Charter

The development

On 25 January 2018, the Department for Media Culture and Sport ("DCMS") published the Digital Charter that was announced in the 2017 Queen's speech. The Charter sets out a programme of work intended to make the UK both the safest place to be online and the best place to start and grow a digital business.

Background

The DCMS set out in their Policy Paper that they are determined that the UK should lead the world in innovation-friendly regulation that encourages the tech sector and provides stability for businesses. The aim is to increase public confidence and trust in new technologies, and therefore create the best possible basis on which the digital economy can thrive.

Recognising that the internet is a powerful force for good that creates new opportunities, the DCMS also recognises that it presents challenges and risks and that tackling these challenges in an effective and responsible way is critical for digital technology to thrive.

The Digital Charter is the response of the DCMS to these issues. It creates a programme of work to agree norms and rules for the online world and put them into practice. It considers the need to shift expectations of behaviour, agree new standards and update laws and regulations. The starting point of the Digital Charter is that it should be possible to have the same rights and expect the same behaviour online as offline.

The principles

The Charter sets out the principles that will guide the work of the DCMS. The principles are that:

- the internet should be free, open and accessible;
- people should understand the rules that apply to them when they are online;
- personal data should be respected and used appropriately;
- protections should be in place to help keep people safe online, especially children;
- the same rights that people have offline must be protected online; and
- the social and economic benefits brought by new technologies should be fairly shared.

Work programme

The Charter has outlined an on-going programme of work that will evolve as technology develops. However, the current priorities include:

- digital economy – building a thriving ecosystem where technology companies can start and grow;
- online harms – protecting people from harmful content and behaviour, including building understanding and resilience, and working with industry to encourage the development of technological solutions;
- liability – looking at the legal liability that online platforms have for the content shared on their sites, including considering more effective action through better use of the existing legal frameworks and definitions;
- data and artificial intelligence (AI) ethics and innovation – ensuring data is used in a safe and ethical way, and when decisions are made based on data, these are fair and appropriately transparent;
- digital markets – ensuring digital markets are working well, including through supporting data portability and the better use, control and sharing of data;
- disinformation – limiting the spread and impact of disinformation intended to mislead for political, personal and/or financial gain;
- cyber security – supporting businesses and other organisations to take the steps necessary to keep themselves and individuals safe from malicious cyber activity, including by reducing the burden of responsibility on end-users.

Progress to date

The DCMS states that there has already been good progress under the Charter's work programme, including movements to:

- give people more control over their personal data through the Data Protection Bill;
- protect children and vulnerable adults online through the Internet Safety Strategy;
- create a new Centre for Data Ethics and Innovation to advise government and regulators on the implications of new data-driven technologies, including AI; and
- build international pressure and consensus to tackle terrorist use of the internet and support the establishment of an international industry-led forum to look at it

Why is this important?

The Charter will not be developed by government alone. It will look to the tech sector, businesses and other interested parties to find solutions.

As work on the Charter continues, the DCMS are committed to:

- harnessing the ingenuity of the tech sector, looking to them for answers to specific technological challenges, rather than government dictating precise solutions;
- considering the full range of possible solutions, including legal changes where necessary, to establish standards and norms online;
- leading by example, including through procurement policy;
- building an international coalition of like-minded countries to develop a joint approach.

The Charter will develop alongside technology and is a document that will be updated as progress is made on the work programme. While the plans are still high level, it will be interesting to see how much input will be sought from platforms and tech companies under this initiative.

Consumer

Update of the Guidance for Traders on Pricing Practices

The question

What changes have been made to the guidance since the latest version was published in December 2016?

The background

The Chartered Trading Standards Institute (**CTSI**) published its "Guidance for Traders on Pricing Practices" in December 2016. This was at the request of the Department of Business, Energy and Industrial Strategy (**BEIS**) and the Consumer Protection Partnership, and followed a series of consumer complaints focused on misleading practices, and a super-complaint from the Consumers Association, Which?.

The development

Recent changes to the guidance have been made following the introduction of the EU Payment Services Directive into UK law. This directive has banned businesses from charging fees for using credit cards when making payments.

The original guidance only stated that a business could not charge the consumer a fee in excess of the fee the business had to pay. Now the guidance has been updated on page 6 to say "DON'T charge consumers a fee for using a credit card or debit card".

Why is this important?

There was no announcement by CTSI that the guidance had been updated and unless you were watching the Payment Services Directive, this change might have passed you by.

Any practical tips?

Do not charge consumers a fee for using a credit or debit card. But remember that not all fees have been banned. So booking fees applied to all transactions regardless of payment method still stand. The trick on the latter is to be aware that a fee which is always payable in all cases will almost undoubtedly impact on the headline price. As the guidance itself states, an additional charge must be included in the up-front price if that charge is compulsory and a failure to do so would breach the Consumer Protection Regulations (see page 24 of the guidance).

ASA

ASA guidance on promotional marketing for subscription models

The question

What guidance does the ASA provide regarding advertising for 'free trials' (and similar promotional techniques) for subscriptions?

The background

The ASA is concerned that ads for 'free trials' or other such promotional subscription offers, which fail to make clear that the customer will be subsequently enrolled in an ongoing subscription arrangement, have the potential to mislead consumers.

The development

A 'free trial' is where a consumer enrols in an ongoing payment arrangement to take advantage of a free trial product offer, test subscription, or other promotional benefit. Importantly, if a consumer does not cancel the trial, they become liable to make a payment, or ongoing payments, as part of the subscription plan to which they signed up, whether knowingly, or otherwise.

While not considered 'intrinsically problematic' by the ASA, these ads do manifest as problematic where a consumer unknowingly agrees to an ongoing payment plan, as a result of the ad:

- omitting significant conditions, or;
- not making significant conditions sufficiently clear for the consumer.

Where the ad misleads in such a way, the ad itself is known as a "subscription trap".

To avoid misleading consumers, the ASA's guidance suggests that:

- an ad must make clear all significant conditions, where their omission would be likely to mislead; and
- any statement regarding the significant conditions should be sufficiently prominent that consumers are not likely to miss it - the positioning will vary depending on the individual ad and medium in which it appears.

Significant conditions

Ads for a 'free trial' or promotional subscription offer should communicate all significant conditions likely to affect a consumer's decision to participate. Stating that 'T&C's apply' is not sufficient. More specifically, the ads must make clear:

- whether a paid subscription starts automatically after the trial, unless cancelled;
- the extent of the financial commitment if the consumer does not cancel; and
- any other significant conditions, for example, significant costs to participate.

Placement of significant conditions

In relation to marketers' own websites, the Guidance suggests that significant conditions should be prominent, and distinct from other information. They should also immediately follow the most prominent references to the trial or offer. Significant conditions should be clear and legible in both size and clarity of font, as well as immediately visible; pop ups are not sufficient.

In relation to marketing communications, if they are significantly limited by time or space, the communication must include as much information about significant conditions as is practicable. The ASA has suggested that, in Twitter ads, marketers could include an image that clearly states the relevant conditions. The ASA considers that the following non-exhaustive list of communications will be unlikely to be considered significantly limited by time or space: emails, direct mailings, press and magazine ads, leaflets, posters and ads in social media not constrained by low character limits. Only in extreme circumstances will a media type be considered to be significantly restricted by time or space. Examples may include sponsored ads on search engine sites, and extremely small banner ads.

Why is this important?

The 'free trial' or promotional subscription model is frequently deployed as an effective hook to fish for new consumers. The guidance provides clarity for those circumstances where the ASA considers a 'subscription hook' to in fact be a 'subscription trap' for consumers.

Any practical tips?

Clarity is crucial; if the ad is a 'free trial' or a promotional subscription offer, include clear, simple and prominent wording to that effect. If you are unable to include significant conditions within an ad, you should perhaps consider whether the media type you wish to use is in fact suitable for this type of promotion.

ASA

ASA ruling on Ryanair's claim: "Europe's number one airline"?

The question

How will the ASA interpret a claim to be "number one" in the context of widespread negative publicity?

The facts

The ruling related to three ads for Ryanair in September and October 2017:

- a TV ad, which featured images of people travelling on a Ryanair plane. The voice-over stated "Discover why more and more people are choosing Europe's number one airline." On-screen text stated "IATA Scheduled passengers carried: 2016".
- a radio ad, which featured the claim "Discover why we're Europe's number one airline."
- a poster, seen on the London Underground, which featured the claim "EUROPE's NO.1 AIRLINE".

The complaint

Thirteen complainants (who noted that Ryanair had cancelled many of its flights in September and October 2017) challenged whether the claim "Europe's number one airline" in the above ads was misleading.

The response

Ryanair said that the claim "Europe's number one airline" was a statement of fact, supported by a third-party statistical report, and was therefore not misleading. Ryanair said that the claim was based on the most recent International Air Transport Association (IATA) World Air Transport Statistics 2017 report for air travel in 2016, which found that Ryanair was the world's largest airline for international flights and Europe's largest airline for international and domestic flights combined.

Ryanair said that its cancellations of flights in late 2017 did not materially alter that statement of fact. The cancellations affected less than 0.5% of its 129 million customers in 2017. Further, Ryanair's October 2017 traffic grew by 8% even when the flight cancellations were included.

Ryanair contended that the on-screen text "IATA Scheduled passengers carried: 2016" in the TV ad was sufficiently clear to communicate the basis of their claim. The radio ad had directed consumers to the Ryanair website for full details of what the claim was based on. Ryanair conceded that, due to an oversight, the same qualification was not included in the poster ad, but said that they had taken steps to ensure that it did not happen again.

The decision

Not upheld.

The ASA considered that consumers were likely to interpret the claim "Europe's number one airline" in each ad to mean that, over a reasonable period before the ads were produced, Ryanair had carried more passengers than any other European airline. That was an objective claim. The ASA acknowledged that many of the complainant's views were that it was not their personal number one airline due to the recent cancellations. Nevertheless the ASA considered that the complainants and other consumers would still interpret the claim to be an objective statement about the number of passengers carried.

The IATA report showed that Ryanair had carried more scheduled passengers on domestic and international flights combined than any other European airline and was appropriate to substantiate the claim. The ASA considered that the most recent report from IATA was appropriate to substantiate the claim.

Further, there was no indication that the flight cancellations would affect the accuracy of that claim. The ASA noted that Ryanair had carried over 40 million passengers more than the European airline ranked second by IATA, and the number of flight cancellations in 2017 was less than 645,000.

Because the most recent available figures showed that Ryanair had carried more passengers than any other European airline, the ASA concluded that the claim "Europe's number one airline" was unlikely to mislead consumers.

Why is it important?

Consumers will almost always interpret a 'number one' claim to be an objective statement about market position, akin to 'best-selling'. That is the view of the ASA, underscored by this ruling. The effect of this is two-fold. Firstly, any advertiser using a 'number one' claim must be able to substantiate it with evidence. Often this evidence will be in the form of an advertiser's own research into its position in the market in relation to its competitors, although it may be acceptable to rely on independent third party data. Secondly, an objective 'number one' claim will not be held to be misleading simply because of the subjective views of consumers.

Any practical tips?

This decision is a reminder of the benefits to advertisers of treating 'number one' claims with caution. It is essential to hold appropriate substantiating evidence, refer to that evidence in the ad, and use adequate qualifications (eg *Europe's* number one airline). Exercising good discipline from the outset should help prevent complaints arising in the first place, noting that these complaints had come at a particularly difficult time for Ryanair, with negative reports on social and mainstream media regarding its cancelled flights.

Advertisers will take comfort from the fact that they can still be 'number one' in the context of negative publicity and the subjective views of the public. But note that it's generally wise to only use 'number one' when you mean 'best seller'. The ASA has consistently held that consumers will interpret 'number one' to mean the market leader, so consider using different language if the intention is to make some other claim.

ASA

ASA ruling on Amazon TV ad interacting with AI

The question

Was a TV ad which interacted with an Amazon device to place an unwanted order socially irresponsible?

The complaint

A TV ad for the Amazon Echo Dot featured a man's voice instructing: "Alexa, re-order Purina cat food". The "Alexa" virtual assistant responded: "I've found Purina cat food. Would you like to buy it?" The complainant argued that the statement: "Alexa, re-order Purina cat food" was socially irresponsible, on the basis that the complainant's Echo Dot had placed an order for cat food after the ad had played.

The response

Amazon confirmed that the complainant's device had a purchase order for Purina Cat Food on the day the ad was seen. However:

- Amazon had technology in place which should prevent its ads from interacting with customer devices. Advertisements were "marked" so that they did not trigger any responses from Amazon devices when broadcast;
- if this technology did not work, Amazon had implemented further processes to ensure that an accidental purchase was not made. Customers had to verbally confirm that they would like to make a purchase for any order to become effective. If confirmation was not given, the order would be automatically cancelled;
- in this instance, the order was expressly and immediately cancelled by the customer. However, had this had not happened, it would have been automatically cancelled due to lack of customer authorization.

Clearcast stated that they were satisfied that the ad was not socially irresponsible. They had been assured during the clearance process that there was: (i) a security step in place so that customers would have to verbally confirm an order placed via the Echo, and (ii) technology in place to prevent the advertisement engaging with devices in customers' homes.

The decision

The ad was investigated under BCAP Rule 1.2 (social responsibility). The ASA ruled that:

- Amazon had taken security measures to ensure their ads did not interact with artificial intelligence devices which may overhear them. In this instance, the technology had failed, causing the device to initiate an order not sought by the customer;
- however, the additional requirement for the customer to actively confirm their order before a transaction was undertaken meant that it would not be possible for a purchase to be made without the account owner's knowledge, even in cases where technology, implemented to prevent ads and devices interacting, had failed;
- the ad was not socially irresponsible and did not breach the Code.

Why is it important?

The decision illustrates that including a requirement for active customer consent provides an additional layer of protection for companies producing interactive devices. However, the decision also highlights the importance of getting the technology right the first time.

Clearly there is a fine line between a successful interactive AI device and one which is distrusted by consumers for fear that it encroaches on their privacy. In this instance, even though the purchase was never made, the consumer may have felt uneasy that the device had the potential to make the order in the first place.

Any practical tips?

Providing the assurance that a device is unable to "spy" on a consumer in their own home is increasingly important in today's climate, as concerns about protection of private information and personal data are frequently driven from the ground-up.

Ensure that any interactive devices include extensive control mechanisms, which not only require the customer to actively consent to any purchases, but also prevent intrusion by the device into the customer's private sphere.

ASA

ASA call for evidence on recognition and labelling of online ads

The question

Do consumers have a clear understanding of the labelling used for online ads?

The background

One of the fundamental rules of advertising is that ads must be obviously identifiable as ads. For some time the ASA has been pushing hard for consumers to be able to distinguish between ads and editorial content. They are increasingly concerned with the lines being blurred due to the rise in advertisers' use of online platforms and online content to reach consumers – using tactics such as native marketing (brand-generated content that looks at home in the context in which it is being viewed) and influencer marketing (paid-for content appearing in tweets, blogs, vlogs, etc.).

The development

To combat this blurring, the ASA has in recent years issued multiple rulings calling out incompliant advertisers, and released guidance to assist those wishing to ensure compliance. It has now gone one step further, issuing a call for research and evidence on consumer understanding of the labelling of online ads. In particular, the ASA is interested in information regarding:

- the level and type of commercial influence over editorial content people expect to be informed about, through an ad label or other method;
- how people interpret specific labels (eg #ad and #spon), and the extent to which wording, placement, visibility and style might impact a consumer's ability to identify an ad;
- the extent to which some groups are more or less likely able to distinguish advertising from non-advertising content; and
- current practices for the labelling of online ads (eg national and international examples).

Why is this important?

This call for evidence is a clear statement of intent from the ASA, reinforcing its general direction of travel when it comes to the regulation of online advertising. A quote in an interview with Guy Parker, the ASA Chief Executive, on the new initiative really drives home the point: "social influencer and native advertising might be relatively new but the advertising

rules haven't changed – people shouldn't have to play the detective to work out if they're being advertised to."

Following this initial process, and based on the information it receives, the ASA will commission its own research into public perception and understanding. Depending on its satisfaction with consumer understanding of labels, it may choose to alter or strengthen the methods through which it regulates the issue. If advertisers don't respond to what the ASA is calling its constructive, cooperative, guidance-based approach, it may need to take a harder line – perhaps even by formalising online advertisement rules into the CAP Code.

Any practical tips?

Until the ASA announces the outcome of its call for evidence and further research, continue to think carefully about any advertising labels used for online content. In each case, consider whether the consumer knows they are being advertised to – is the ad obviously identifiable? If not, a label will be required, and it will need to be appropriate, unambiguous, noticeable and available to the consumer *before* they engage with the content. Overall, err on the side of caution, and if in doubt…use 'ad'!

ASA

Key principles of ad disclosure

The question

What are the rules around disclosure of marketing communications?

The background

Over the past few years, there have been a number of challenges to advertising communications on the basis that they are not "obviously identifiable". The three areas that have attracted particular regulatory attention in this context are:

- **traditional media (newspapers, magazines etc)** – in the context of whether advertorial content is clearly recognisable as a marketing communication, rather than being confused with pure editorial content;
- **bloggers/vloggers** – for failing to disclose the existence or extent of the commercial relationship they have with brands whose products they have endorsed or featured on their channels; and
- **affiliate marketing** – for failing to ensure that additional disclosure is present when the affiliate content is not obviously identifiable as a marketing communication (eg performance-based marketing where an affiliate is rewarded by a business for new customers attracted by the affiliate's marketing efforts, whether by news outlets, blogger/vloggers or commercial websites such as voucher sites).

Consequently, there have been a number of rulings on the adequacy of particular labels to identify advertising materials. The following are some of the key principles derived from rulings and various CAP help/guidance notes.

Ad disclosure: key principles

- The starting point is whether the marketing communication is already obviously identifiable as an ad. If it is, no further action is required (see CAP Advice Online – Online Affiliate Marketing);
- If not already clear from the context, an appropriate label should be used to indicate the nature of the relationship to the consumer (see CAP News: Is your ad 'obviously identifiable?' Here's why 'Spon' is not 'ad');
- Sponsorship and advertising are treated as having different meaning to consumers. The key distinction is whether any editorial control over content is exercised by the brand (advertising) or whether there is only a payment element with ultimate control

remaining with the publisher/vlogger etc (sponsorship) (see Advice Online: Recognising Advertisement features);

- If labelling is required, companies should avoid the use of ambiguous or confusing statements which do not make it clear whether the piece in question is advertising or sponsorship (see CAP Advice Online: Video blog scenarios);
- When labelling is required, it should be placed somewhere consumers will be able to see it before they choose to read, watch, or listen to that content (see CAP News: Is your ad 'obviously identifiable?' Here's why 'Spon' is not 'ad').
- In the context of affiliate marketing, where only some of the links on the affiliate's website are advertising then it needs to be obvious which links are advertising and which are not (see CAP Advice Online – Online Affiliate Marketing).

Each are discussed in turn below.

Is the marketing communication obviously identifiable as an advert?

Labelling is only required if the content in question is not already obviously identifiable as an advert. Even when presented alongside editorial/native content, CAP has acknowledged that "*it is feasible that the overall presentation and context could make it sufficiently clear [that a particular piece is a marketing communication]*". In a 2013 adjudication against Haywood & Co (not upheld) the ASA found that the advert (which had featured in a regional newspaper) had been presented in a way that was obvious to readers that the advertorial had been paid for and written by Haywood & Co. In particular, the ASA noted that the advert had been separated from editorial content by being bordered in a blue box and that "there was nothing in the ad to suggest it had been produced by anyone other than the advertisers".

If not already clear from the context, appropriate labelling is required

CAP Guidance suggests that this "*will particularly be the case where the individual concerned is primarily a creator of non-commercial content or where the overall impression is of editorial independence*". The purpose of the label is to clearly indicate to the consumer that what they are in fact viewing is an advert when the context and presentation alone does not facilitate this.

'Sponsorship' vs advertising

CAP has sought to clarify the difference between advertising and sponsorship in a series of help notes (see for example, CAP News: Is your ad 'obviously identifiable?' Here's why 'Spon' is not 'ad' and CAP Advice Online: Video blog scenarios). Essentially, the position is that when there is a financial arrangement or other incentive with the brand, but the brand has no control or input into the content, then this may be considered (and labelled) "sponsorship". An example of this cited by CAP includes when a company provides a travel writer with a free holiday, but has no input or control over any resulting article. In contrast, where a degree of control over the content is exercised by the brand then this is an advert or advertorial, and must be clearly labelled as such.

CAP Guidance has suggested that the threshold for "editorial control" is usually based on whether or not the brand has final approval of text and visuals. However, this is not definitive and in 2009 the ASA made a series of rulings against Express Newspapers for publishing seemingly editorial articles alongside pure adverts for a number of companies. The brands featured were only permitted to see the final copy of the editorial piece in order to correct factual inaccuracies. Nevertheless, the ASA considered that because the articles were uniquely favourable to the product featured in the accompanying ad, editorial control was still being exercised by the relevant brand and so the whole feature should have been disclosed as an ad (see commentary under heading "Remember that the spirit of the Code applies..."). Additionally, instances where key messaging has been provided by the brand to the publisher, even if the brand was not permitted 'final' editorial approval, has been considered by the ASA to sufficiently meet the threshold for editorial control (Ruling on ASDA Stores Ltd and MGN Ltd, December 2017). When considering whether there is editorial control by the brand the ASA may look into the parties' rights and obligations under the contract (Ruling on Wahoo Fitness (UK) Ltd, March 2018).

Whilst pure sponsored material is not covered by the CAP Code, it has been recognised that the CMA would expect disclosure of a commercial relationship with a brand in order to comply with consumer protection legislation (CAP Advice Online: Videoblog scenarios).

General comment: It appears that the ASA and CAP are keen to ensure that the delineation between advertising and sponsorship is maintained, so that if something is in reality an 'advert' it cannot also be 'sponsored', and labelling it as such is likely to mislead.

Using an appropriate label when not obviously identifiable

If content requires a label to disclose the commercial relationship between the two brands, then the label used must be appropriate. The ASA has repeatedly upheld complaints against companies and individuals who have incorrectly labelled content, even when the labelling has been clear and prominent – see, for example the Ruling on Michelin Tyre plc and Telegraph Media Group Ltd, December 2015. This was upheld against the organisations despite the advertorial piece appearing within the 'sponsored' section and the presence of the phrase "in association with Michelin" was prominently included. The ASA considered that whilst these "may have served to show that a financial arrangement was in place, they were insufficient to identify the content specifically as an ad (as opposed to, for example, material that had been financially sponsored, but over which the creator retained editorial control)".

Additionally, the ASA has confirmed that labels where the exact nature of the relationship is not entirely clear to the consumer (ie they would be unable to tell if the content was sponsored or advertorial) would likely breach the CAP Code. Consequently, statements/phrases such as '[brand name] partnership' (Ruling on ASDA Stores Ltd and MGN Ltd, December 2017); 'brought to you by', (Ruling on Procter & Gamble, May 2015) 'in association with' (Ruling on

Michelin Tyre plc and Telegraph Media Group Ltd, December 2015) and 'thanks to [brand]' (Ruling on Mondelez UK Ltd, November 2014) have all been ruled as ambiguous and in breach of the Code.

General comment: Labels such as "advertisement", "advertisement promotion", "advertising feature" and "ad" are normally acceptable, suggesting that anything without "ad" as the prefix is unlikely to be acceptable when the content is found to be advertising.

Positioning, prominence and timing of the label

If a label is required to indicate that the consumer is in fact viewing an advertisement, the regulator will take into account the presentation, positioning and noticeability of the label itself.

Labels should be "prominently placed"; for instance, the Ruling on ASDA Stores Ltd and MGN Ltd, December 2017 establishes that a label in small grey font above a much larger article headline will not attract the readers' attention. Similarly, the ASA has ruled that if a description box featuring the label is not immediately visible (particularly when viewing the site through a tablet, mobile browser or app) it will be insufficient (Ruling on Wahoo Fitness (UK) Ltd, March 2018). On the other hand, the ASA found that a banner at the top of the relevant page stating "the page that you are currently reading is an ad feature" to be sufficient given the prominence of the positioning and the fact that readers were likely to see it before engaging with the ad (Ruling on Marcândi Ltd t/a MadBid, March 2014).

It must also be clear prior to consumer engagement that the content in question is advertising. This will be particularly relevant if the relevant advertising content features video and/or sound. In a ruling against Mondelez, the ASA considered it insufficient for disclosure statements to be made at the end of the video given that the consumer had already engaged with the content before the disclosure was made. This was therefore not obviously identifiable at the outset, and would deprive the consumer of the opportunity to decide whether or not to engage with the advert in question.

General comment: It seems that best practice for compliance purposes is to place disclaimers prominently at the top of the ad, or above/next to the links to the relevant article, and/or before the consumer engages with any audio/video content.

If only some links on a website are advertising, they need to be clearly identifiable

Where there is an affiliate marketing relationship on a website and only some of the content or links featured on the website are advertising then this needs to be clear to consumers so that they are able to easily distinguish these from native links/content. Whilst CAP Guidance states that affiliate marketers are free to highlight this commercial relationship how they would like, it then goes on to suggest that a way of achieving this could include "placing a label, for example 'Ad', in or around the title".

Why is this important?

This is currently a very hot topic for regulators who are keen to ensure that there is consistency over how and when advertising is disclosed to consumers. Indeed, CAP are currently calling for evidence people's understanding of labels and other identifiers that are intended to indicate that online content is advertising.

Snapshot created March 2018