Bird & Bird

UK & EU Data Protection Bulletin: December 2021

Welcome to your monthly newsletter from Bird & Bird's UK Data Protection team

In this month's newsletter, we bring you the following updates:

United Kingdom

ICO

UK Cases

EU

EDPB

EU Cases

UK Enforcement

ICO Enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
October	**ICO launches consultation on the Draft Journalism Code of Practice** On 13 October 2021, the Information Commissioner's Office ("**ICO**") opened a consultation seeking feedback on the **Draft Journalism Code of Practice** (the "**Code**"). The Code provides practical guidance for organisations processing personal data for the purposes of journalism, and is aimed at individuals with data protection responsibilities within controller organisations (such as legal teams, data protection officers and/or senior editorial staff) as opposed to those with more day-to-day journalistic roles. The Code is a successor to the ICO's previous guidance on this subject-area, **Data Protection and Journalism: a Guide for the Media**, which was issued following the Leveson enquiry; and follows a **Call for Views** to which responses were published in May 2019. The Code is a statutory code of practice which means the Commissioner must take the Code into account when considering whether an organisation has complied with its data protection obligations when processing for the purposes of journalism, and when considering its enforcement powers. If the Code is not followed, it may be more difficult for an organisation to demonstrate that its processing for journalism purposes complies with the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 (the "**DPA 2018**"). The provision of the DPA 2018 requiring the Commissioner to publicise such a Code emphasises that the Commissioner must have regard to the **special importance of the public interest in the freedom of expression and information**. This is a theme emphasised throughout the Code when considering the application of data protection law to journalistic activity. Key points include: • **Balancing journalism and privacy** – the Code gives guidance around the application of the "*special purposes exemption*", under which it is possible to disapply a broad range of UK GDPR provisions where their application would be at odds with a journalistic purpose. This involves consideration of (i) whether the processing is for the purposes of "*journalism*" (the more closely the processing resembles the activities of traditional sources of journalism such as broadcast media, the more likely it is to constitute journalism – though the ICO notes that the digital age has given rise to alternative channels which could in some (though not all) instances also constitute journalism, such as private individuals publishing public interest footage online); (ii) whether the processing is "with a view to publication"; (iii) whether it is reasonably believed that "*publication is in the public interest*" (both a subjective and an objective test, and less restrictive than other exemptions in the DPA 2018; the ICO notes that reference to existing defamation law will be of assistance when analysing this point); and (iv) whether it is reasonably believed that compliance with the relevant data protection provision would be "*incompatible with journalism*" (i.e., is it necessary not to comply with data protection law in order to achieve your journalistic purpose?). For organisations who need to evaluate whether or not data protection law would prohibit them from publicising certain journalistic material, this will be a useful section of guidance.

	• **Compliance with the principles in a journalism context** – the Code considers how controllers might comply with each of the UK GDPR principles when processing for the purposes of journalism. In particular, there is detailed discussion around the lawfulness, fairness and transparency principle, including reliance on the substantial public interest condition for the disclosure of special category/criminal data for the purposes of journalism in connection with unlawful acts and dishonesty. The ICO also confirms that from an accountability perspective, organisations will not need to conduct a fresh DPIA every time they create a story involving high-risk journalistic processing but can instead cover all such stories with a single DPIA (e.g. for "*investigative journalism*"). • **Individual rights** – the Code considers some of the specific issues which might arise in a journalism context when responding to requests from data subjects to exercise their rights under the UK GDPR. The ICO makes clear that organisations can likely be exempted from responding to rights requests in certain public interest scenarios, for example requests to erase data from news archives or access requests which would involve disclosing the identity of confidential sources; however, express reference to resourcing constraints as a ground for an exemption is only mentioned in the context of DSARs. • **Enforcement** – the Code sets out a reminder of the ICO's enforcement powers. It is worth noting that in the context of the special purposes exemption there has been little enforcement to-date (most notably the **ICO's decision to fine True Vision Productions £120,000** in connection with CCTV-style filming in hospitals in 2019 although noting that his penalty was reduced to £20,000 on appeal to the First Tier Tribunal in January 2021), and so the door remains open for further enforcement decisions to confirm how the ICO will apply the Code in practice. The ICO is also seeking views on the **Draft Economic Impact Assessment** which sits alongside the Code and provides a cost-benefit analysis of the Code's implementation as well as an analysis of the alignment of the Code's objectives with other key policy areas, for example online harms. The deadline for responses to the consultation is **10 January 2022** and can be submitted via an online or Word survey here.
October	**ICO publishes draft second chapter of its Anonymisation Guidance** The ICO has published the second draft chapter of its Anonymisation, Pseudonymisation and Privacy enhancing technologies guidance for consultation. This chapter looks at "*how do we ensure anonymisation is effective*" and has two parts: the first broadly follows the WP29 opinion on anonymisation techniques, and the second part provides detailed examples on how to anonymise in practice. In particular, the draft chapter explains the concept of identifiability and its key indicators such as **singling out**, **linkability** and **inferences**. The ICO states that an anonymisation process should seek to **reduce the likelihood** of someone being identified or identifiable to a sufficiently remote level while acknowledging that this level depends on a number of **context-specific factors**. In all cases, the ICO states that this assessment should consider: a. Whether there is additional information that may enable identification;

	b. Whether there are techniques that enable identification from the information in question; c. The extent to which the additional information or techniques are likely to be accessible to and used by somebody to re-identify – i.e. the ICO posits a "*motivated intruder*" test as an aid to assess whether an intruder would be able to achieve identification if they were motivated to attempt it. A copy of the chapter can be found **here**. The consultation closed on 28 November 2021. The first draft chapter was published in May and covered in our June 2021 Bulletin. Further chapters will be released over the coming months and will include: • Guidance on pseudonymisation techniques and best practices; • Accountability and governance requirements in the context of anonymisation and pseudonymisation, including data protection by design and DPIAs; • Anonymisation and research; • Guidance on privacy enhancing technologies (PETs) and their role in safe data sharing; • Technological solutions; and • Data sharing options and case studies.
October	**ICO responds to UK Government consultation on data protection reform** In September, the UK's Department for Digital, Culture, Media & Sport (DCMS) released a consultation document about the future of data protection law in the UK. The proposals were wide ranging, addressing both uncertainties and clarifications in data protection law as well as significant changes to the way the law operates in the UK. You can read our full summary and analysis of the proposal **here:** The consultation is now closed, and DCMS is currently analysing the responses it has received. The ICO responded promptly, publishing its response in early October. Its response to DCMS' proposals was mixed. The regulator was broadly supportive of making data protection law easier to understand, and simplifying compliance obligations, but warns against removing protections for individuals. In a number of cases (e.g. changes to cookie consent requirements or reliance of public interest as a legal basis) the ICO urged DCMS to provide further detail, to allow the proposal to be assessed more concretely. Deep concerns were expressed in relation to possible reforms to the application of the fairness principle to the use and development of AI systems, and changes to Article 22 UK GDPR (automated decision making provision). On some points, such as DCMS' sweeping proposal to replace the UK GDPR's accountability framework with a privacy management programme, the ICO deferred to the public's response to the consultation, and committed to working with Government to develop whichever option is preferred following the review of all consultation responses. The ICO also expressed strong concerns about the impact of DCMS' proposed reforms to the ICO's own structure and governance, though it was supportive of the proposal to move from a sole Commissioner to a statutory supervisory board with separate Chair and CEO.

October	**ICO's Opinion on Age Assurance for the Children's Code** On 14 October 2021, the ICO issued an opinion on Age Assurance for the Children's Code (the 'Opinion'). The Children's Code (or 'Age Appropriate Design Code'), which applies to online services likely to be accessed by children, requires online services to take a risk-based approach in recognising the age of their users, so as to ensure that they effectively apply the Code's standards to child users. The ICO acknowledges that age assurance is a developing area and has been a challenging topic for online service providers, who have during the transition period asked the ICO to provide further information and clarity on this point. The Opinion explains how the ICO expects online service providers to meet this age assurance requirement. More specifically, it: • examines the main approaches to age assurance • expands further on the requirement for a "risk-based" approach when it comes to age assurance • considers the data protection principles in the context of age assurance (lawfulness, fairness, transparency, accuracy, data minimisation, purpose limitation, storage limitation, security and accountability) • examines points relating to the use of AI as an age assurance measure, such as the processing of biometric data, the statistical accuracy of AI methods and the risks of algorithmic bias. The Opinion also contains an annex which examines current uses of age assurance, and an annex on the impact of age assurance on online service/age assurance providers, data subjects, the ICO and wider society. The ICO will review the Opinion in September 2022, as part of its overall review of the Children's Code. **What is age assurance?** The ICO uses the term "*age assurance*" to refer to methods used to provide assurance that children are unable to access adult, harmful or otherwise inappropriate content when using online services; and methods to estimate or establish the age of a user so that online services can be tailored to their needs and can apply protections appropriate to their age. **What are the main age assurance measures?** The Opinion examines the main four approaches to age assurance: **age verification, age estimation, account confirmation** and **self-declaration**. As age assurance methods involve the processing of personal data to verify or estimate age, they have their own data protection considerations and carry their own types of risk. For example, they may not be fool-proof and may be easily circumvented. They may be disproportionately intrusive, they may introduce risks of bias or inaccuracy and result in exclusion or discrimination of already marginalised groups. For example, age verification which usually depends on official documentation or credit history, would create an issue for young adults, people with protected characteristics or people from deprived backgrounds. Also, age estimation may carry risks from algorithmic bias; for example, systems based on hand or facial structure may perform poorly on people of non-white ethnicity, people with medical conditions or disabilities that affect physical appearance.

Risk based approach to age assurance

The Children's Code calls for a "risk-based" approach to age assurance: it establishes that service providers should either apply the standards of the Code to all users irrespective of their age, or establish the age of their users with a level of certainty that is "*appropriate to the risks*" that arise from the data processing. For high-risk processing, this means introducing age assurance measures that give the highest possible level of certainty on age of users, taking into account the products currently available in the market and the organisation's technical capabilities and resources. The ICO will not expect services to implement measures that are not currently technically feasible or pose a significant and disproportionate economic impact on their business; but it will expect online services to demonstrate that they have considered all available options and to evidence the disproportionate costs or impact on individuals, or the technical explanations why they are not using measures that may provide higher certainty.

Examples of activities that the ICO considers likely to result in high risk to children include:

- Large-scale profiling of children
- Invisible processing of children's data (e.g. list brokering, data sharing with third parties, and online tracking of children)
- Targeting of children (e.g. geolocation, web & cross-device tracking)
- Activities with risks of physical or developmental harm to children (e.g. data revealing children's physical location or health)
- Activities with risks of detrimental use (e.g. processing which is demonstrably against children's wellbeing, as defined by government advice or industry codes of practice).

For non-high risk activities, online services should use proportionate age assurance methods (unless they choose to apply the Code to all users irrespective of their age). For some low risk activities, the ICO accepts that self-declaration may be appropriate (alone or combined with technical measures).

Data protection compliance of age assurance methods

The Opinions also examines the main data protection principles and requirements that online service providers should take into account. Examples of data protection considerations in the context of age assurance include:

- taking action to scrutinise and minimise any potential bias in the age assurance method used;
- ensuring that users have an effective way to challenge an age assurance decision if they believe it is incorrect;
- providing information to individuals about the use of age assurance and the relevant data processing operations;
- not repurposing data collected for age assurance, for example, for profiling for advertising
- monitoring and considering carefully any challenges to the accuracy of data, to avoid situations where adults are wrongly identified as children and are denied access to certain platforms or services; or children are wrongly identified as adults or older than they are and can access restricted services.

November	**ICO's Opinion on "Data Protection and Privacy expectations for online advertising proposals"** • On Thursday 25 November 2021, the Information Commissioner published an Opinion entitled "Data protection and privacy expectations for online advertising proposals". This is part of the Information Commissioner's Office's ('ICO') broader adtech and real-time bidding ('RTB') investigation (here), which had been put on pause during the COVID-19 pandemic. **The content of the Opinion** • This Opinion is a reminder of the ICO's position that current approaches adopted within the adtech industry are not compliant with data protection law. However, perhaps more concerning for those providing or using adtech solutions is that the Commissioner believes new solutions in development - in part in response to the ICO's 2019 report on adtech and RTB (the 'Report') - still leave much to be resolved. This Opinion and its "privacy standards" are called a "warning" in the press release (here). • The Opinion is wide ranging, and cuts between summarising the state of play and a closer look at some key areas where there are specific concerns. The Commissioner explicitly repeats and reiterates points already made, signposts specific guidance and refers to previous work. • A consistent theme is the ICO's cross-over with the Competitions and Markets Authority ('CMA'), another regulator with a history of investigations into the adtech sector. The Opinion reflects the tensions at play between achieving compliant privacy solutions as against cultivating a fair and competitive landscape in the complicated adtech ecosystem. The ICO does believe that these differences can be reconciled and the two regimes, and their respective objectives, are not "tradeable". Please see our more detailed news alert on this: The ICO issues an Opinion on the privacy challenges impacting the adtech industry

UK Cases

Date	Cases
12 October 2021	**Fairhurst v Woodard (Case No: G00MK161)** *Fairhurst v Woodard* involved a dispute between two neighbours over the use of home security devices. The Court found that the use of such devices in this instance went beyond what was necessary and proportionate to achieve the aim of preventing crime and was therefore in breach of data protection laws. The Defendant, Mr Woodard, had told the Claimant, Dr Fairhurst, that he had installed various image and audio recording cameras around his property, such as a doorbell camera with video and audio capabilities, a driveway camera, and a shed camera which overlooked a communal park. Dr Fairhurst became alarmed when Mr Woodard boasted about the surveillance capabilities of the cameras, which could capture images of the Dr Fairhurst's property and garden, as they could capture images and soundbites of other communal areas. Mr Woodard also misleadingly told Dr Fairhurst that some of the cameras were only for "show" (i.e. to deter potential criminals and were not operational) when, in fact, those cameras were operational. Dr Fairhurst brought claims for breach of data protection laws, nuisance and harassment based on Mr Woodard's use of the cameras being an invasion of her privacy. The data protection claim argued that images and audio files captured by Mr Woodard's camera were personal data. Mr Woodard argued that he had a legitimate purpose collecting and processing the data to prevent crime. Dr Fairhurst's position was that the processing was unlawful and her right to privacy overrode Mr Woodard's purpose. The County Court therefore had to consider whether Mr Woodard had processed such personal data lawfully, in line with a legitimate purpose and proportional to the said purpose. The judge accepted that the image and audio recordings included Dr Fairhurst's personal data, but also found that Mr Woodard's purpose of preventing crime was legitimate. Despite this, the judge found that Mr Woodard had failed to act with transparency when collecting the data by actively misleading Dr Fairhurst about whether the cameras were operational and what they were capturing. Misleading the Claimant in this way undermined Mr Woodard's argument that he was collecting the data for a legitimate purpose. The Court also found that much of the image and audio collected was not necessary or proportional to achieving the purpose of preventing crime. For example, the range of audio that could be collected by the doorbell camera was over 50 feet, going beyond the boundary of Mr Woodard's property in a way that was not necessary to achieve his purpose. The Court actually considered that Mr Woodard's purpose could have been achieved without collecting audio at all. The Court concluded that Mr Woodard had breached the Data Protection Act 2018 and has now invited the parties to make further submissions in relation to damages and injunctive remedies. These damages are, however, likely to be higher than ordinary in data protection claims as Mr Woodard was also found liable for the harassment claim which is likely to lead to a higher damages award. In reaching its

Date	Cases
	conclusions the Court did not consider the social and domestic purposes exemption, nor was it invited to consider the CJEU Rynes case which had similar subject matter. Therefore, there may remain scope to distinguish cases where the use of home surveillance technology is more limited Whilst the County Court' decisions do not set binding precedents and this case concerned two individuals, the decision should be noted by businesses that are operating security cameras or other devices that capture information to identify individuals on or within their premises. Any business that operates such devices must remain mindful of individuals' privacy rights and whether images and audio files are being collected lawfully. The case illustrates the importance of proportionality when collecting video images and audio to prevent crime as a legitimate purpose. Businesses using video and audio equipment should be open and transparent to any individuals about this operation which could include providing appropriate notices to individuals entering premises and ensuring that the images and/or audio are collected strictly for that purpose.
29 October	**R (Open Rights Group & the3million) v Secretary of State for the Home Department and Others [2021] EWCA Civ 1573** On 29 October the Court of Appeal handed down its judgment on a suspension of relief, following an earlier judgment in May 2021 which found that the immigration exemption under Schedule 2 Paragraph 4 of the Data Protection Act 2018 is incompatible with Article 23(2) of UK GDPR. GDPR allows jurisdictions to incorporate exemptions to derogate from provisions in specific and limited circumstances according to criteria set out in Article 23(2). The Court held that the UK's immigration exemption was too broad and contained insufficient safeguards to be compatible with Article 23(2). The May judgment has drawn particular attention given the potential impact it has on other similarly drafted derogations under Schedule 2 of the Data Protection Act. In the October case, the Court of Appeal found that UK courts have the power to suspend relief in the application of retained EU law on a temporary basis. The Court suspended relief, and thus the disapplication of the immigration exemption, in order to allow time to draft and table new provisions before Parliament which correspond with Article 23(2). Here, the Court noted that suspending relief should only take place on a temporary basis and that "*it is not enough that the government would find it convenient to have more time, or that the period sought would be reasonable from an administrative point of view. The court must be satisfied that the period of suspension imposed is really needed, to avoid legal uncertainty*". When deciding the suspension itself, the Court considered arguments from the Appellants that the suspension of relief should apply only to public sector organisations and not the private sector, creating two regimes. The court rejected this argument as an immediate suspension of the immigration exemption would create a significant disruption to the private sector given the role it plays in immigration related enforcement together with the government. The Court has granted a suspension until 31 January 2022, to allow the Government to table a statutory instrument in Parliament and allow sufficient time for it to pass through its legislative procedure. In submissions, the Government outlined that it would aim to table a statutory instrument by mid-December 2021, in order to meet the 2022 deadline, and pass through affirmative legislative procedure which requires approval from both Houses.

Date	Cases
7 September **11 October** **16 November**	**Rolfe & Ors v Veale Wasbrough Vizards LLP** [2021] EWHC 2809 (QB), **Ashley v Amplifon Limited** [2021] EWHC 2921 (QB), [Judgement not yet on BAILII] **Johnson v Eastlight Community Homes Ltd** [2021] EWHC 3069 (QB) These cases all concern a single, accidental disclosure of small amounts of personal data to a third party, which were quickly rectified. All three were then brought before the High Court, with the data subject claiming damages under (at least) breach of UK GDPR, misuse of private information (MPI) and breach of confidence, with the defendant requesting summary judgement or striking out. In *Rolfe*, the request to strike out was wholly successful. However in *Ashley* it was only successful as far as getting a clearly erroneous negligence claim struck out, and in getting the remainder of the claims transferred to the County Court. Meanwhile in *Johnson* all but the GDPR breach was struck out, with this final remaining claim surviving "by a very narrow margin" and being transferred to the County Court. Facts In *Rolfe,* the data breach occurred when the defendant, VWV, sent a demand for payment of school fees to the claimants. However, due to an error in one letter of the email address, this was accidentally sent to a third party. The third party promptly notified VWV of the error, and quickly confirmed deletion at VWV's request. The demand for payment itself contained minimal personal details- only names, address, amount of the school fees, an account of the school fees and the demand for payment. In *Ashley*, contractual documents relating to one Amplifon employee ("Adrian A") were accidentally disclosed to another employee with the same forename ("Adrian B"). These documents contained Adrian A's name and address, and his contractual rights and obligations. This disclosure occurred in the context of a separate legal dispute between the two parties, the details of which were irrelevant to the case. It took a week for Amplifon to be made aware that the documents had been sent to the wrong person, but Amplifon then promptly contacted Adrian B who confirmed he had never opened the documents. He then confirmed deletion 6 days later. Amplifon claims they then phoned Adrian A to let him know they had been deleted, but Adrian A claims he never received such a call. In *Johnson,* a document containing rent statements for several renters (including the claimant) was accidentally sent to a different renter. The claimant's details were on pages 880-882, in a document almost 7,000 pages long. In less than 3 hours, the mistake was noticed and the recipient confirmed deletion. 19 days later the claimant was informed of the mistake and subsequent deletion. Judgements In *Rolfe*, Master McCloud dealt with the case quite shortly, and primarily by simply reciting and approving the defendant's skeleton argument. She notes that minimal personal data was transferred, that there was a prompt request to delete the personal data, and in turn this was promptly confirmed. As a result, she calls the claimants' suggestion that they were distressed by these events "frankly implausible". She notes that she considers the claimants bringing this claim to be inappropriate in any circumstances, and particularly inappropriate to bring before the High Court. As above, the claims were struck out entirely.

Date	Cases
	In *Ashley*, Mr Justice Kerr reached the opposite conclusion. He concluded that claims for MPI and breach of UK GDPR should not be struck out, and instead allowed to continue in the County Court. In doing so he noted that the distress the incident caused the defendant may have been aggravated by the context of the wider legal dispute between the parties. This, combined with the long gap between the third party being made requested to delete the emails and doing so and the lack of certainty over whether the claimant was ever made aware that Amplifon had received confirmation of deletion, led to a conclusion that the case deserved of proper consideration. In particular, he criticised Amplifon for not simply forwarding on the email confirmation of deletion to the claimant, and more broadly for not keeping the claimant updated as the mitigating steps progressed. As a result of all this, the claim was transferred to the County Court (except for a negligence claim which was readily abandoned by the claimant). *Johnson* then seems to present a borderline case between the two. Master Thornett helpfully affirmed that the common law "*Jameel*" test for striking out claims did still apply to the GDPR (contrary to claims by the claimant). He also found that the claimant's distress over the disclosure of her address seemed to be both hypothetical and historic, based on her current behaviour of being happy with its disclosure on court forms. However ultimately, the claimant's distress was such that he considered there was sufficient grounds for a trial to determine whether this distress had crossed the *de minimis* threshold. This resulted in the claim being referred to the County Court, amidst heavy criticism of the claimant's solicitors for "procedural abuse" in bringing the claim before the High Court. However claims for MPI and Breach of Confidence were not transferred with it, as the Master considered them likely to take up disproportionate and unreasonable time and costs. <u>Commentary</u> All three cases affirm that small-scale data breaches like this are not welcome before the High Court. In particular, in *Johnson* the Master had no trouble seeing through an inflated claim for legal fees and affirmed that the subject matter of such a claim does not entitle elevation to the High Court either. Furthermore, all three cases recognised that such claims could be struck out under *Jameel*, though this only happened in one. This seems to be a recognition of the levels of distress claimed in each. In *Ashley,* it was in question whether the claimant had been informed that the data had been deleted any time before bringing the case, and when combined with the aggravation of the wider legal dispute, this meant there was a very real possibility of significant distress which needed further consideration. In contrast in *Rolfe* there was minimal distress, with a finding that no person of "ordinary fortitude" would reasonably suffer much distress on these facts. In *Johnson* the level of distress that would normally have been caused by the breach and subsequent actions of the defendant would be expected to follow *Rolfe* more than *Ashley*. However here, the particular circumstances of the claimant aggravated this to just cross the threshold of "being worth the candle". This would appear unlucky for the defendant, but is in keeping with the "eggshell skull" principle in tort and the requirement in GDPR to take vulnerable people in consideration. However Eastlight are likely to be pleased with the striking out of all claims other than the GDPR breach (unlike in *Ashley*), which both minimises the costs and eliminates all possibility of recovering any ATE premium. As such the key takeaway is that taking steps to minimise the distress of data subjects in the event of a breach will be rewarded if the case comes to court, potentially to the level of striking out any case. This is paired with an affirmation that such cases are not welcome in the

Date	Cases
	High Court, and instead will be directed to the County Court- with the associated reduction in time, effort and legal costs for the defendants.

EU

EDPB

Date	Description
13 October	**EDPB adopts guidelines on restrictions on data subject rights under GDPR** Following public consultation, the European Data Protection Board ("EDPB") has adopted Guidelines 10/2020 on restrictions under Article 23 of the EU General Data Protection Regulation ("GDPR") (the "Guidelines"). Article 23 of the GDPR allows Member States to put restrictions on data subject rights (those set out in Articles 5, 12-22 and 34), to the extent such restrictions "*respect the essence of the fundamental rights and freedoms and [are] a necessary and proportionate measure in a democratic society to safeguard*" e.g. national security, defence or public security. The Guidelines note that the restrictions should be "*exceptions*" to the general rule encouraging the exercise of rights and obligations under the GDPR, and as such should be interpreted narrowly and only be applied in specific circumstances where certain conditions are met. According to the Guidelines, the restriction must be set out in a "*clear and precise*" legislative measure and its application must be "*foreseeable*" to those subject to it. The Guidelines also note that legislative measures containing restrictions must set out the information required under Article 23(2). The Guidelines indicate that this will enable permit data subjects to understand '*how and when*' the restriction might apply.
18 November	**EDPB adopts draft guidelines on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR** The EDPB has adopted draft Guidelines 05/2021 with the intent to clarify what constitutes an international data transfer in accordance with the GDPR (the "Guidelines"). The Guidelines are open to public consultation until the end of January. Chapter V of the GDPR sets out rules for the transfer of personal data to third countries or international organizations. However, the GDPR does not contain a definition of "transfer." The EDPB proposes **three cumulative criteria for transfers**: 1. A controller or a processor is subject to the GDPR for the relevant act of processing; 2. This controller or processor ("exporter") discloses that personal data by transmitting it, or otherwise making it available, to another controller, joint controller or processor ("importer"); 3. The importer is in a third country or is an international organization. This is true whether or not the GDPR is also applicable to the processing of personal data by the importer.

This approach '*deflates*' the GDPR bubble by confirming that a disclosure of personal data to an importer, to whom the GDPR is applicable on an extraterritorial basis, should still be regarded as a data transfer.

The draft guidelines note the EDPB is willing to collaborate on transfer tools for use with organizations to whom the GDPR applies under Article 3(2) (as the new standard contractual clauses do not cover this situation).

Other points the Guidelines confirm:

- **the concept of transfer only applies to disclosures between two different, separate parties, each of whom is a controller, joint controller or processor: the importer must be different from the exporter.**

- **where data subjects disclose data directly, on their own initiative, to a controller or processor in a third country, this is not a "*transfer*."**

For more information, see the full *Guidelines 05/2021*.

EU Cases

Date	Description
25 November	**Case C-102/20** In a ruling dated 25 November 2021, the CJEU broadened the typically-understood scope of EU/EEA anti-spam rules to include, for the first time at EU level, certain forms of web or in-app display ads. In this new ruling, dubbed *Pegnitz*, the CJEU held that an online display advert that was made to *look* somewhat like an ordinary email in a webmail user's inbox, fell within the scope of those anti-spam rules. Ads caught by those rules can only be shown with the recipient's prior opt in, or under the rules' limited "*soft opt in*" exception - if available. The Court emphasised that the notion of "*electronic mail*" is broad (it has long encompassed, for instance, SMS texts); and that in any event, the advertiser "use[d] the existence of the list of private emails, taking into account the particular interest and trust of the subscriber with regard to that list, to place their direct advertising, giving it the appearance of a real email." This was therefore "*using*" email to deliver the advert. It did not matter that the advert: 1. was not communicated via the email network (IMAP/POP/SMTP); 2. was dynamically generated/loaded (i.e. delivered by the ad server) by a request sent from the user's browser while loading the webpage – and not durably "stored in the network" e.g. in the user inbox (and did not count towards data limits or read/unread message counts for that inbox); 3. was sent to people *en masse*, selected at random, rather than targeted to particular recipients based on their personal data (the messages were still sent "directly" / individually to people, since they reached each person in "a private space reserved to him or her and which is intended for the consultation of private content, in the form of emails"); 4. did not behave like a typical email (it could be deleted, but not modified, archived or forwarded; and clicking it did not open a message, but rather led to the advertiser's web page); 5. was clearly marked as an advertisement (as per EU advertising rules that prohibit covert advertising) by replacing the "*sent*" date with the German word for "*advert*", and 6. had been further distinguished from real emails, by using alternative row colouring and not including a sender. The Court held that advertisers could be liable for breach of anti-spam rules without any need to show that the adverts were more than just a nuisance; and that repeatedly displaying this advert could also amount to a prohibited commercial practice under EU consumer law protections that prohibit 'persistent and unwanted solicitations', meaning liability under both anti-spam and unfair commercial practices legislation.

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
15 September	SportsDirect.com Retail Ltd	Monetary Penalty of £70,000	The ICO has fined SportsDirect.com Retail Limited ("Sports Direct") £70,000. From December 2019 to February 2020, Sports Direct sent more than 2.5 million emails to clients as part of a so-called "re-engagement campaign". Sports Direct argued that it relied on both soft-opt for some clients and on consent for others, but that it was no longer possible for them to retrieve the distribution list used for the said campaign. As such, the ICO concluded that Sports Directs did not seem to be able to rely on the soft-opt in exception in regulation 22(3) PECR.
15 September	Saga Group	Monetary Penalty of £225,000 (Comprising of £150,000 for Saga Services Limited and £75,000 for Saga Personal Finance) Enforcement Notice	The ICO has fined Saga Services Limited ("SSL") £150,000 and Saga Personal Finance ("SPF") £75,000. Both SSL and SPF are subsidiaries of Saga Group Limited ("Saga Group"). Between November 2018 and May 2019, SSL instigated more than 128 million emails using partner companies and their affiliates and SFP more than 28 million. It was argued that the partner companies and their affiliates were the instigators of the direct marketing, but the ICO took the view that SSL and SPF were the instigators as the emails would have not been sent without their involvement. Both SSL and SPF argued that they relied on indirect consent (i.e., where the intended recipient had told one organisation that he/she consents to receiving marketing from other organisations). However, the ICO recalled that indirect consent might not be valid in some circumstances. In this case, the ICO found that the partner companies and their affiliates' consent statements or privacy policies either: • did not specify that data subjects will receive marketing from SSL, • did not allow the data subject to select how they wish to receive marketing and from whom; • did not specify the third-party companies that may send marketing material; • made the consent to marketing a condition of subscribing to the service.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			As such, the indirect consent that SSL and SPF relied on was not valid consent. The ICO concluded that SSL and SPF instigated the sending of direct marketing emails contrary to regulation 22 of PECR. Indeed, per regulation 22 of PECR, the instigator of direct marketing (i.e. SSL and SPF) has to make sure that all requirements are met and emails sent only where valid consent was obtained. In addition, the ICO issued enforcement notices to both companies requiring them to stop any illegal direct marketing within 30 days or face court action.
15 September	We Buy Any Car Limited	Monetary Penalty of £200,000	The ICO has fined We Buy Any Car Limited ("WBAC") £200,000. From April 2019 to April 2020, WBAC sent more than 191 million emails and 3.6 million text messages to promote the We Buy Any Car service. <u>Concerning the marketing emails:</u> WBAC sent three types of emails, to either encourage customers to continue their valuation journey or promote the We Buy Any Car service: • Journey emails: sent to customers of its website in response to valuation requests; • Batch emails: sent to customers after the 30 day "journey" and up to 4 years since their last valuation was provided; • Good news emails: sent to inform customers that the offer for their vehicle has been increased. The ICO concluded that the first journey email sent for each customer is indeed solicited marketing, but that all the following journey emails, the batch emails and the good news emails were not and were, as such, caught by PECR rules. <u>Concerning the text messages:</u> Similarly, WBAC sent batch messages and good news messages for the same purposes as the emails. For both emails and text messages, WBAC stated that it relied on the soft opt-in exception. The ICO found that customers, while being informed that they will receive marketing communications, were not offered a way to opt-out at the point of collection of their details.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			Therefore, the ICO concluded that WBAC did not comply with the requirements of Regulation 22(3)(c) in relation to the timing of the opt-out and consequently failed to meet the soft-opt in requirements.
22 September	Your Home Improvements Ltd	Monetary Penalty of £20,000	The ICO has fined Your Home Improvements Ltd ("YHIL") £20,000. YHIL has made, between June 2020 and July 2020, 1,718 unsolicited calls to people who were registered with the Telephone Preference Service (TPS). These calls were made for direct marketing purposes in relation to boiler insurance. YHIL repeatedly claimed, including through a representation from their solicitor, that since 2018 they had not conducted any marketing for the boiler insurance business and did not hold client contact lists. However the ICO concluded this was incorrect on the balance of probabilities, particularly as the telephone numbers involved had been assigned to YHIL. The ICO concluded that YHIL negligently contravened regulation 21 of PECR as YHIL has been unable to provide any explanation for the calls nor demonstrate it held valid consent for the purpose of these calls. In particular, the ICO noted that there were failings in basic requirements for any organisation conducting a live direct marketing campaign, including: • the director had purchased the business with an existing customer base so should have been aware that such contraventions may occur, and had failed to carry out due diligence on purchase. • YHIL had not ascertained the source of the data or whether there was consent to make calls, and had not screened the data against the TPS every 28 days as required. • the director being unable to provide any explanation for the calls suggests a general lack of awareness of how the business is operating. The ICO then noted there were no mitigating factors and a number of aggravating factors including: • whilst there was no evidence of direct targeting of vulnerable individuals, the Commissioner noted that complainants mentioned persistence of calls for products which they had never had, in one instance, going so far as offering to take control over a laptop remotely. It is also concerning that complaints evidence that YHIL were seeking financial information including

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			sort codes and account numbers which, given the company's approach, poses a high risk of inadvertent disclosure or fraud; • the actions of YHIL were carried out to generate business and to increase profits, gaining an unfair advantage on those businesses complying with the PECR; • YHIL failed to co-operate with the Commissioner's investigation, initially declining to do so until the prospect of being served with an Information Notice. Even then, and despite having utilised the services of a solicitor, YHIL was unable to provide adequate answers to the Commissioner's enquiries or evidence consent to make the calls; • YHIL's director acknowledged that calls were made by staff using mobile telephones, however the ICO is unable to verify the extent to which such calls were made. Therefore, the true extent of the contravention is indeterminable.
22 October	HIV Scotland	Monetary Penalty of £10,000	The ICO has fined HIV Scotland £10,000. HIV Scotland is a charity which provides support for individuals living with HIV, individuals who may be at risk of HIV, and individuals who support those groups. In February 2020, HIV Scotland sent an email to the 105 members of its Community Advisory Network (a group of representatives of those impacted by HIV in Scotland) notifying them of the agenda of an upcoming meeting via Microsoft Outlook, however used CC instead of BCC. As a result, all email addresses were visible to the other recipients. 65 of the 105 members could be readily identified by their name in their email address. Although the actual data disclosed only consisted of email addresses, these could reasonably be inferred to be either HIV positive people, or those supporting HIV positive people, due to the knowledge of the purpose of the group. As such the email addresses were found to constitute special category data. The ICO considered this a negligent breach of the GDPR. In particular, they noted that this came in the context of an ongoing migration to a secure mailing service, which had begun 7 months earlier, and that the transfer of such a sensitive mailing list should have been prioritised. Instead HIV Scotland had deliberately deferred the transfer until after the meeting for convenience. However the ICO also recognised that the ongoing transfer showed that HIV Scotland recognised the deficiencies of their previous BCC policy, and that therefore it was also a mitigating factor.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
25 October	Unite the Union	Monetary Penalty of £45,000	The ICO has fined Unite the Union ("Unite") £45,000. Between 11 March 2019 and 11 March 2020, Unite made 57,665 unsolicited direct marketing calls to subscribers who were registered with the TPS. These calls were made to members of Unite to encourage them to join a life insurance scheme offered by a third party to members. These were being offered on an opt-out basis, since Unite claimed that they did not constitute direct marketing due to their rulebook requiring them to communicate information about this to members. The ICO confirmed that these calls were direct marketing, due to them offering a service from a third party whose business was to provide this service, and that the Unite rules are irrelevant as they cannot override the statutory protection in this area. As such this constituted a negligent breach of the Privacy and Electronic Communications Regulation (PECR). The ICO noted that the fact they had provided extensive advice and guidance on marketing calls (and direct marketing more broadly) was an aggravating factor, but also the fine was mitigated by Unite's prompt remedial actions after they flagged the contravention.

Information Tribunal Appeal Cases

Date	Appellant	Type of Case and Result	Summary of Case
17 September	Acute Recruitment Ltd	Appeal against Monetary Penalty Notice for failure to pay registration fee. Appeal Dismissed	The Appellant appealed a monetary penalty notice for failure to pay its registration fee. Itclaimed that it had failed to receive the notice of intent, which was sent by post to its registered business address, due to the company having recently moved offices. However the company did not contest having received reminder emails from the ICO prior to the notice of intent, nor the ultimate penalty notice, and had still not updated its address with the ICO.

Date	Appellant	Type of Case and Result	Summary of Case
			The Tribunal found that the onus was on the Appellant to make sure that properly served notices are received, and that the ICO had properly served it by sending it to its registered business address. The Tribunal questioned in particular why the Appellant had failed to respond the reminder emails that the ICO had sent (despite not being obliged to), and instead had only paid the fee when they received the penalty notice.
29 October	Studios MG Ltd	Appeal against Monetary Penalty Notice for sending unsolicited marketing emails. Appeal Dismissed.	The Appellant appealed against the amount of a monetary penalty notice issued for sending unsolicited marketing emails in breach of the PECR. Studios MG had sent around 9,000 unsolicited marketing emails advertising face masks for sale at a heavily inflated price in April 2020, attempting to exploit the circumstances of the pandemic, but the exact extent of the breach could not be determined due to the companydeliberately deleting the data after being contacted by the ICO. Studios MG appealed, claiming that the impact of the pandemic and the urgency of the situation made the breach less serious, that further weight should be added to their admission of liability, that the Information Commissioner acted less than impartially in its findings, and that the Information Commissioner should have found the breach to simply be "negligent" rather than "deliberate". In response, the Information Commissioner reduced the penalty from £40,000 to £30,000, but insisted this new amount was reasonable. The Appellant also claimed that it was unable to pay a sum of more than around £5,000, but failed to provide any financial documentation to prove this and the information available to the Commissioner suggested that Studios MG was in a good financial position. The Tribunal ruled in favour of the Commissioner on all points, finding the breach serious and deliberate and flagging in particular the Appellant's deliberate attempts to frustrate the investigation (including by deleting relevant information and failing to make a full and frank statement of the relevant facts).
22 Novembe	Bright Jemwa	Application for an Order to Progress a Complaint under s166 DPA 2018.	The Applicant applied to the Tribunal for an order to progress a complaint (under s166 of the Data Protection Act 2018). However the outcome of the complaint had already been communicated to the Appellant, and so instead the Applicant was looking for the Tribunal to order the rectification of his personal data. The Tribunal noted that this was not within its power

Date	Appellant	Type of Case and Result	Summary of Case
		Struck Out (no reasonable prospect of success)	to do, and instead the Applicant should have brought a case before the High Court against the data controller. As such the application was struck out.

Upper Tribunal (Administrative Appeals Chamber)

Date	Appellant	Type of Case and Result	Summary of Case
17 September	Joined Cases: Killock and Veale, EW, and Coghlan (on behalf of C)	<u>Killock and Veale:</u> Application for an Order to Progress a Complaint under s166 DPA 2018. Application Dismissed. <u>EW:</u> Application for an Order to Progress a Complaint under s166 DPA 2018. Application Granted. <u>Coghlan:</u> Appeal against refusal to extend time limit on an application for an Order to Progress a Complaint under s166 DPA 2018 (Coghlan) Appeal Dismissed.	These three cases all covered overlapping aspects of the s166 DPA order, where the Tribunal is able to issue an order to the Commissioner to progress a complaint. The Tribunal discussed prior case law on the matter, before affirming that this procedure entitled the Tribunal only to correct a procedural defect in the Commissioner's investigation of a complaint. This is as opposed to a substantive defect, e.g. with the outcome of a complaint, which must be brought before the Courts. It was noted that the Tribunal must be careful not to allow a complaint that purported to be procedural, but was actually intended to abuse the process to change the outcome of an investigation. Furthermore, the Tribunal noted that it would review such procedural complaints only in the context of considering the Commissioner's "institutional competence" and other considerations that the Commissioner may have, such as its regulatory priorities and decisions on how best to target its limited resources. These three cases show that the Tribunal will interpret its rights under s166 narrowly in order to limit it to true procedural defects. Attempts to expand it into cases where the actual issue was an attempt to appeal the outcome, argued through references to EU principles on effectiveness and comparison with Freedom of Information Act remedies, were swiftly rebuffed. <u>Killock and Veale</u> Killock and Veale's case concerned a complaint about the handling of personal data by adtech companies, particularly in relation to the Real Time Bidding ("RTB") technique. In response, the Commissioner invited Killock and Veale to participate in its ongoing investigations in this area, but ultimately closed thecomplaint with no action since it did not complain about any specific

Date	Appellant	Type of Case and Result	Summary of Case
			activity. This is despite the Commissioner continuing to investigate and raise concerns about the adtech industry. The Applicants complained that the Commissioner had failed to keep them updated with its work on adtech enforcement prior to closing their complaint, in particular failing to contact them for their input before publishing a blog post on adtech, and had given them notice of closing their complaint while the Commissioner's investigations into the adtech industry are ongoing. The Tribunal readily found the Commissioner's actions reasonable. In particular, it noted that entering a complaint did not entitle the Applicants to be involved in the ICO's wider investigations into the same topicas the complaint, and that the Commissioner had taken extensive steps to involve the Applicants in itsinvestigations. <u>EW</u> EW's case concerned repeated Subject Access Requests submitted to her local council. In each case the council refused to provide any data, citing an exemption, but the Commissioner refused to consider EW's complaints as they came more than 3 months after the council's responses. In this case the Tribunal found that the Commissioner had acted improperly. The Commissioner's policy only noted that it may refuse to act after 3 months, yet the replies to EW suggested she believed she had to refuse to act after 3 months. The Tribunal found this to be the proper type of procedural defect for them to fix, and ordered the Commissioner to reconsider EW's case. <u>Coghlan</u> In Coghlan's case, the Commissioner had refused to investigate her complaint but had noted that Coghlan could not initiate Judicial Review of this complaint unless she first went through the Commissioner's internal review process. Coghlan followed this process, which affirmed the original decision. Rather than applying for Judicial Review, Coghlan chose to request a s166 order that the Commissioner must investigate the complaint. However this was requested beyond the time limit of 6 months and 28 days for such a request. The Tribunal noted that the original refusal from the Commissioner was within the time limit, and while she was directed to not judicially review at that stage she could have asked for a s166 order then. As such, the Tribunal confirmed that the internal review process does not extend the

Date	Appellant	Type of Case and Result	Summary of Case
			deadline, and that it would not exercise its discretion to allow an out-of-time application. The Tribunal also noted that the Commissioner's reasoned explanation of why itwould not investigate her complaint was also sufficient anyway as far as procedural concerns went, so the request lacked merit even if it had been within time.

Other recent articles

Filling in the blanks: What is the transfer of personal data and when will Chapter V obligations be applicable? (twobirds.com)

How does the new UAE Federal Decree Law on Personal Data Protection compare against the GDPR?

Employee data protection series (iv): processing a candidate's personal information during recruitment

Global Cookie Review (twobirds.com)

Security of Critical Infrastructure Act 2018 (Cth) Reforms in Force

Working with Data - From Reactive to Strategic

Inspection activities of the Czech Data Protection Authority in 2021 – what are the key findings?

Cookies in 2022: Amendment to the Electronic Communications Act

Employee Data Protection Series (III): Impact of Personal Information Protection Law on Employer's Internal Investigations

China Cybersecurity and Data Protection: Monthly Update - November 2021 Issue

The ICO and the Proposed Competition Duty

Changing direction? UK consults to reform its data protection law