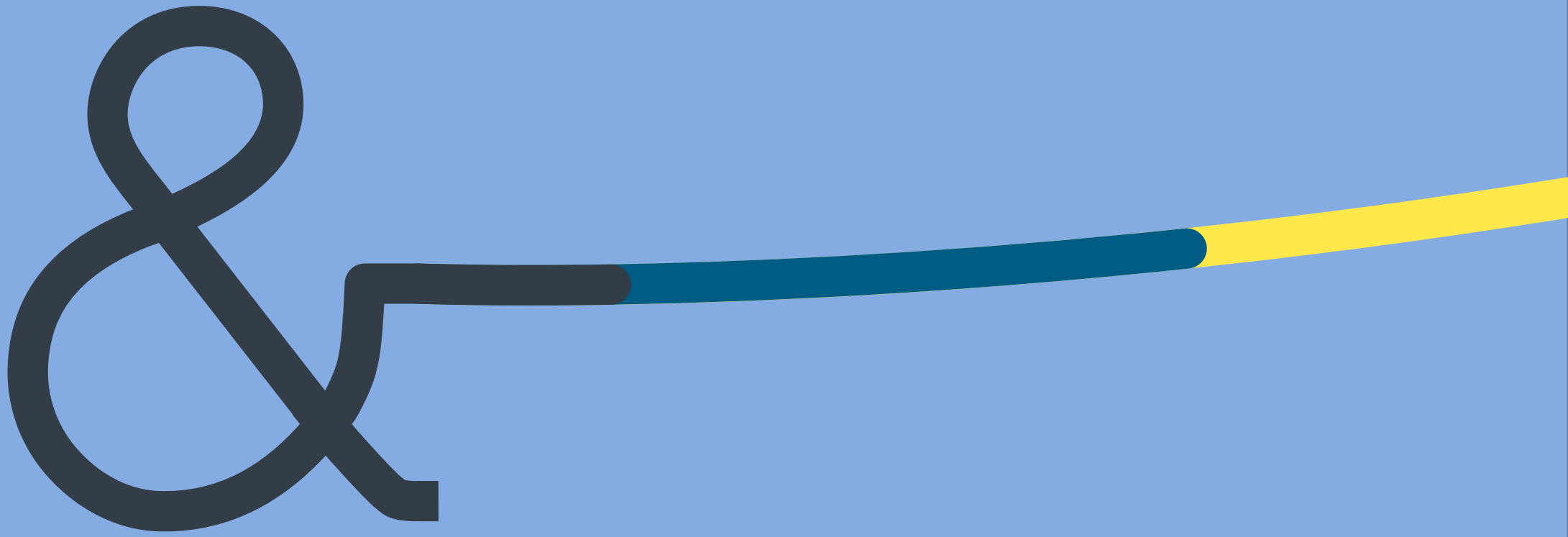
Bird & Bird

March 2022

UK & EU Data Protection Bulletin



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

EUROPE

EDPB

CJEU Cases

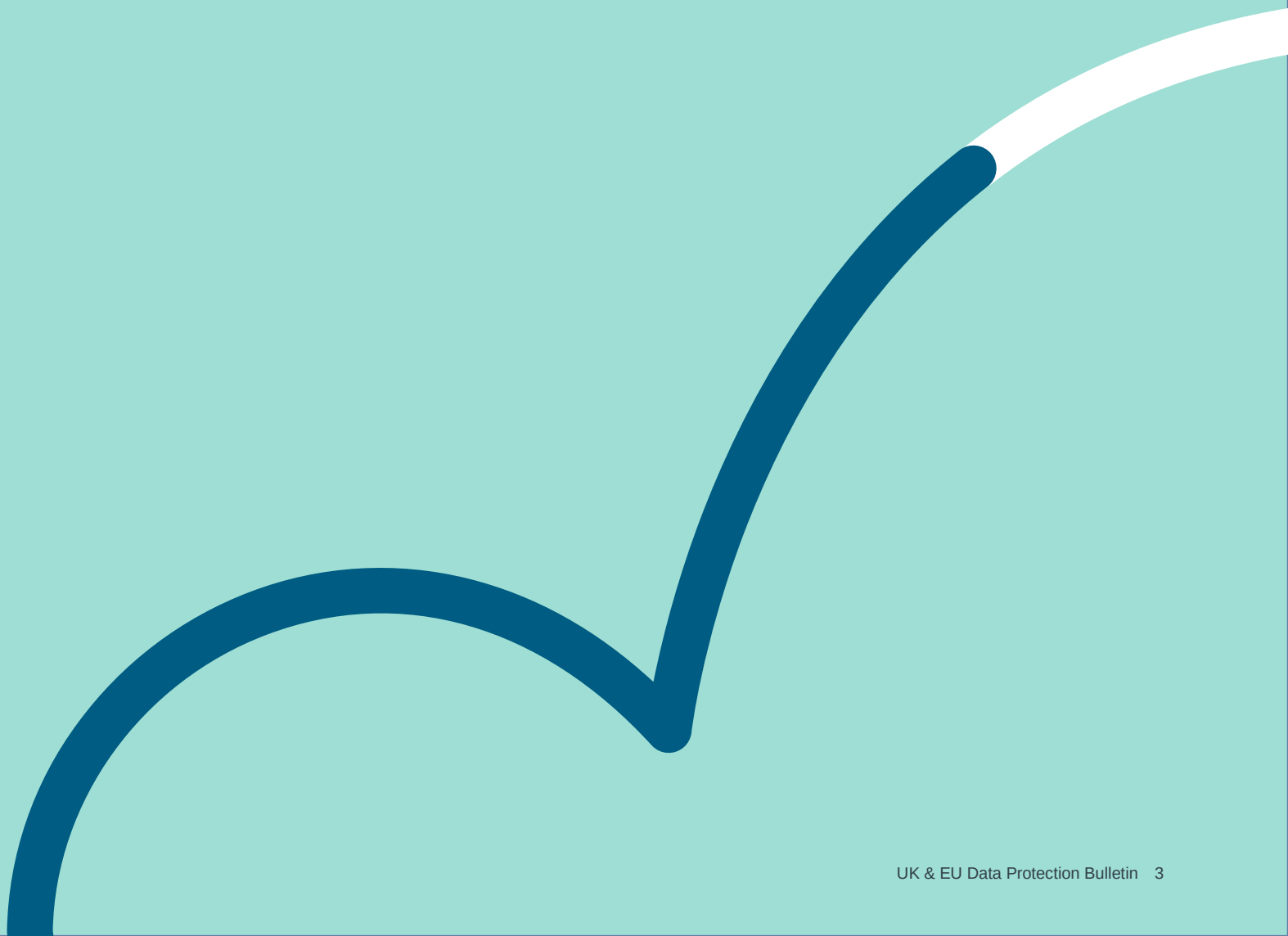
ECtHR Cases

UK Enforcement

ICO Enforcement

Information Tribunal Appeal Cases

United Kingdom



Information Commissioner's Office (ICO)

Date	Description
November	**ICO issued provisional notice to fine Clearview AI over £17 million for scraping images from the internet and offering biometric services to its customers** Following a joint investigation between the ICO and the Office of the Australian Information Commissioner ("OAIC"), on 29 November 2021, the ICO announced its intent to impose a fine of just over £17 million on Clearview AI Inc, as well as issuing a provisional notice to ClearView AI to stop further processing of the personal data of people in the UK and to delete data. This follows alleged serious breaches of the UK's data protection laws. The investigation focused on Clearview AI's use of images, data scraped from the internet, and the use of biometrics for facial recognition of the individuals found on the internet. Whilst Clearview AI argued that the images it scraped and the web URL attached to the images did not constitute personal data, neither the ICO nor the OAIC agreed with these views. Clearview AI's customers can also provide images to the company for it to carry out biometric searches (including facial recognition searches) on their behalf to identify relevant facial image results against a database of over 10 billion images. The images are likely to include the data of a substantial number of people in the UK whose data may have gathered without their knowledge from publicly available sources. Clearview argued that it was only offering its biometric search services to law enforcement agencies and that this was a justifiable use; however Clearview's patent application made it clear that its technology could be used for a variety of other use cases such as dating or identifying people who are homeless or use drugs which was found to be outside the scope of services offered to law enforcement agencies. Findings of the ICO The ICO's preliminary view is that Clearview AI appears to have failed to comply with UK data protection laws in several ways including by failing to: • process the information of people in the UK in a way they are likely to expect, or that is fair; • have a process in place to stop the data being retained indefinitely; • have a lawful reason for collecting the information; • meet the higher data protection standards required for biometric data, which is classed as special category data under GDPR and the UK GDPR;

	• inform people in the UK about what is happening to their data. In addition, ICO found that where individuals sought to exercise their rights, Clearview asked for additional personal information, including photos, which may have acted as a disincentive to individuals who wish to object to their data being processed. Clearview AI can make representations in respect of the above alleged breaches and a final decision is expected to be made by mid-2022.
December	**On December 20, 2021, the UK Information Commissioner's Office ("ICO") launched a public consultation on its regulatory approach.** The ICO has launched a consultation looking at three new draft documents addressing its regulatory approach – the ICO's Regulatory Action Policy ("RAP 2021"), Statutory Guidance on the ICO's Regulatory Action, and Statutory Guidance on the ICO's PECR Powers. The ICO's current Regulatory Action Policy was adopted in September 2018 ("RAP 2018") following the implementation of the GDPR and the DPA 2018 and is a single guidance document which included statutory guidance relevant to the DPA 2018. The ICO committed to review the RAP 2018 in order to take account of learnings from the first year of its implementation and this is the purpose of this recent consultation. As part of the updates, the ICO has decided to separate the statutory guidance from the RAP 2018 and create two new draft documents: the RAP 2021 and the Statutory Guidance on the ICO's Regulatory Action. When the ICO implemented the RAP 2018, it retained the preceding statutory guidance in respect of how it determined penalties under the PECR. Those penalties are still determined under the old DPA 1998. The ICO has now updated that guidance, which now also deals with its powers to serve a monetary penalty on an officer of a body for data protection failures in respect of the PECR (as well as on a person). This draft guidance is now called the Statutory Guidance on the ICO's PECR Powers and is intended to replace the earlier guidance on that topic. The purpose of the RAP 2021 is similar to the RAP 2018. It sets out the ICO's approach to regulatory action, explaining various factors the ICO takes into consideration during regulatory action and how it enforces the legislation for which it is responsible; as well as how the ICO works with other regulators. As well as splitting out the Statutory Guidance on the ICO's Regulatory Action into a separate document, the RAP 2021 departs from the RAP 2018 in a number of ways: • The RAP 2021 calls out the ICO's legal obligations including the obligation to comply with the Regulators' Code; • Additional aggravating factors are called out, including: - where there is a high degree of damage to the public (which may include distress or embarrassment); - where the data protection legislation breaches result in a relatively low degree of harm but affect many people;

- where the person or organisation significantly or repeatedly fails to follow the good practice set out in the codes of practice the ICO is required to promote.

- Additional mitigating factors have also been identified, including:

  - if the person or organisation notifies the ICO of the breach or issue early and has been open with the ICO;
  - any early action the organisation has taken to ensure future compliance with a relevant code of practice.

- Further, the RAP 2021 mentions other factors that might be considered, including:

  - any action the organisation took to report the breach to other appropriate bodies (such as the National Cyber Security Centre (NCSC)) and to follow their advice;
  - If the ICO finds that a person or organisation has profited from the misuse of data, then the ICO can work alongside agencies who can confiscate money made from data misuse under the Proceeds of Crime Act.

- The RAP 2021 provides greater detail on the Office's cooperation with other regulators, in terms of their international counterparts, other UK based regulators, and various regulatory networks.

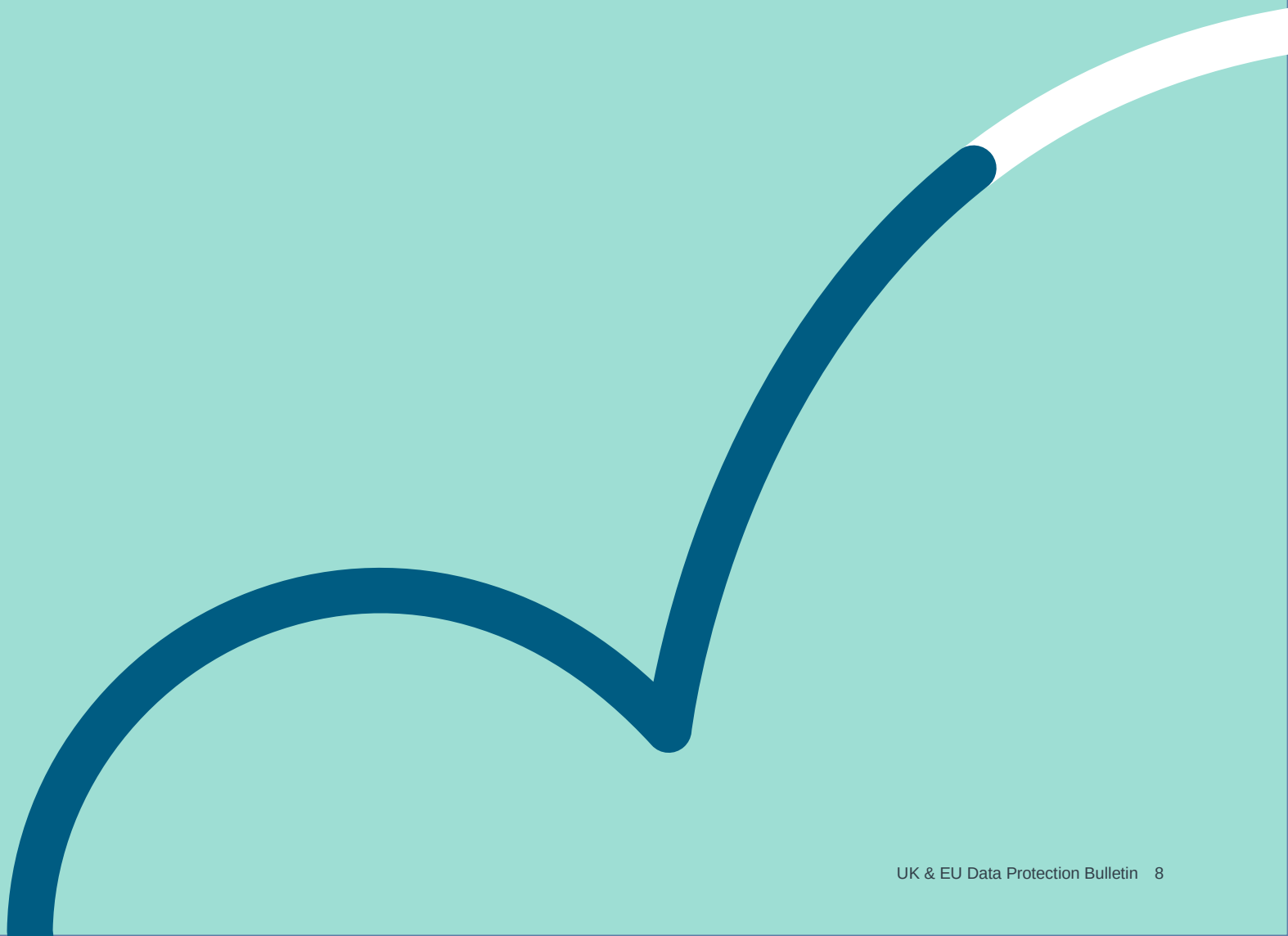
The ICO indicated that the purpose for updating these documents was to provide clarity on how it will exercise its regulatory powers and stakeholders should bear this in mind when considering their responses to the consultation. We consider that there are some significant blind spots in the RAP 2021. For example, it does not clarify how data controllers can challenge softer decisions made by the ICO (including warnings and reprimands). This is significant given such decisions could be an aggravating factor in any future enforcement.

The ICO's public consultation will conclude on March 24, 2022.

UK Cases

Date	Cases
December	**UK Court of Appeal considers territorial scope of data protection in allowing service out of jurisdiction (Soriano v Forensic News 2021 EWCA Civ 1952)** In this recent case, available here, the Court of Appeal overturned the High Court's decision to refuse permission to serve GDPR claims out of jurisdiction on US website publishers. More information on the High Court's decision can be found in our February 2021 bulletin here. Warby LJ's decision considered the potential application of the GDPR to the US websites activities, under Articles 3(1) and 3(2). In assessing the territorial scope of GDPR, Warby LJ emphasised that the Court merely needed to determine whether the argument that the GDPR applied to the defendants was fanciful, under either Article 3(1) or Article 3(2), as this would prevent service being granted out of jurisdiction. He concluded, in the sole judgment in the case, that: • Article 3(1) (processing in the context of the activities of an establishment in the UK) might potentially be capable of applying, notwithstanding that the defendant had no physical establishment in the EU or United Kingdom, given the website's support through Patreon subscriptions from EU and UK users.This is a surprising reading of the CJEU's judgment in *Weltimmo* and of Recital 23 of the GDPR (which applies more clearly to Article 3(2)(a)); • Article 3(2)(a) (targeting) might potentially apply in this case, despite the fact that the claimant was not a data subject who was targeted under Article 3(2)(a) – he was instead a subject of the defendants' articles that are targeted at a UK/EU audience; • Article 3(2)(b) (monitoring) might potentially apply to the use of the internet "to collect information about the behaviour in the EU of an individual who is in the EU" when this is followed by assembly, analysis and ordering "for the purposes of writing and publishing an article about that behaviour in (among other places) the EU." Some of these conclusions are likely to surprise many privacy practitioners. It is not clear that these ought to be given any binding precedence - in particular, Warby LJ explicitly resisted a suggestion that the court should "decide these questions definitively" and also called for "further and definitive consideration" of the application of the GDPR within any substantive case before suggesting that the Information Commissioner was called to intervene in such litigation. As a result, whilst it is possible courts may turn to this judgment for guidance in the future, it should not be considered as the primary source for any controller's analysis at this stage.

EUROPE



EDPB

Date	Description
18 January	**EDBP Guidelines on Examples regarding Personal Data Breach Notification** In January, the EDPB published its Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. These Guidelines provide detailed examples of personal data breaches and comment on the actions that controllers should take covering: 1) **Internal documentation**, 2) **Notifications to supervisory authorities**, and 3) **Communication of the breach to data subjects**. Previous guidance from the Article 29 Working Party commented on the application of articles in GDPR but gave little in terms of practical examples. The only case in previous guidance where it was not necessary to notify supervisory authorities and data subjects was where a data breach occurs with a 'trusted third party'. **These new Guidelines go further and give more detailed examples** categorised under different types of data breach such as ransomware attacks, data exfiltration attacks, internal human actions, lost or stolen devices and documents, mis-postal of data and an 'other' category. As a baseline, the Guidance requires that controllers cover data breaches in their internal documentation, but **there are examples where the EDPB does not think it necessary to notify supervisory authorities or communicate the breach to data subjects**. For example, where encryption at rest means that data which falls into the hands of an attacker cannot be used, and backup systems mean that the controller can quickly restore its own access to such data. Others deal with breaches that do not have a significant effect on data subjects or a risk to their rights and freedoms, such as inadvertently sending personal data to all those attending a particular course by email. There are limitations in the Guidelines and in parts the EDPB avoids commenting on specifics and instead argues that controllers will have to decide on a case by case basis. A final point is that the **Guidelines give non-exhaustive examples of measures that controllers should take to mitigate the effects of data breaches** – focusing on technical measures such as encryption and strong authentication methods, as well as organisational procedures with training, audits and penetration testing.
28 January	**EDPB Publishes Guidance on Right of Access** On the 28th January, the EDPB published a draft version of its Guidelines on the Right of Access. This version is subject to a public consultation, concluding on the 11th March 2022. These Guidelines step through the stages of a Data Subject Access Request (DSAR), providing guidance on what is required of companies in replying to the DSAR at each stage, in particular: - clarifying how the request can be received;

- providing more information on when it is appropriate to confirm the identity of the requestor, and if so how to do so;
- what information needs to be shared with the data subject, both in terms of the personal data itself and the covering information;
- how to provide this information to the requestor; and
- further clarifications on the limits and restrictions on the right of access.

In doing so, the EDPB repeatedly confirm this right as being broad and with the interests of the data subject foremost. For example, the EDPB notes that extensions beyond the initial month should never be routine and, if they become so, the controller should put further "routines and mechanisms" in place to be able to respond to ensure that requests can be handled within the first month in normal circumstances. The Guidelines also clarify that the contextual information, to be provided alongside a copy of the data, needs to be customised and targeted to the individual data subject. In particular, using some or all of a generic privacy policy designed at, for example, a range of employees or service users, is unacceptable if it could be narrowed down or refined based on the particular context of the data subject. As such, these guidelines undermine common measures used to alleviate the significant burden DSARs put on controllers.

However, the improved certainty on a wide range of points is still to be welcomed. In particular, these Guidelines provides further information on how to handle various fringe circumstances, such as where the subject access request follows suspected identity fraud, and examples of how to approach situations where the controller's own rights and freedoms compete with those of the data subject. There is also a new limitation, albeit likely of limited use, suggesting a controller can ignore requests sent to a plainly irrelevant contact point when a specific contact point is advertised (though other reasonable contact points must remain acceptable- e.g. a general queries email address must be able to accept DSARs, but an email address to report cleanliness of changing rooms does not).

CJEU Cases

Date	Description
February 2021	**C-77/21: Hungarian Data Protection Authority requests a preliminary ruling from the Court of Justice of the European Union (CJEU)** In June 2020, the Hungarian Data Protection Authority (NAIH) imposed a record breaking administrative fine of approx. EUR 290,000 on Digi Távközlési Zrt. (Digi), a major e-communications provider in Hungary, as a result of a website security vulnerability. In summary, the main reason for the record fine was that Digi created a test database to which it had copied the personal data of around 322,000 subscribers. An ethical hacker found and accessed this test database, which contained among other data, names, numbers of id cards, email addresses and phone numbers. The NAIH's main reasoning for the fine was that the test database was created for a different purpose, which was an infringement of the principle of storage limitation and that appropriate security measures were not put in place. (For details, please read our earlier article on the decision). Digi has now commenced an administrative-law action at the Metropolitan Court in Budapest against the decision. Digi claimed that: (i) the creation of a test database did not change the original purpose for the personal data was collected, because the principle of purpose limitation does not indicate in which internal system the controller may process the personal data; and (ii) the test database itself was created for security purposes to ensure the compliance with Article 32 (Security of processing) of the GDPR. Digi also requested that court submit a request to the CJEU for preliminary ruling. The Metropolitan Court requested that the CJEU provide guidance on the following: 1. whether the copying of data to another internal database which were collected for a limited purpose changes the purpose of collecting and processing the data. It also asks whether the fact of creating a test database (i.e.keeping data collected for a limited purpose in another internal system) and continuing to process the data in that way is compatible with the purpose of collecting the data. The Court takes the view that the principle of purpose limitation does not provide any clear indication as to which of the controller's internal systems are ones in which the controller may process legitimately collected data, or whether that controller may copy such data to a test database without changing the purpose of collecting the data; and 2. if creating a test database is not compatible with the purpose of collecting the data, then how should the principle of storage limitation be determined in respect of that separate database? For further details, please see here. This ruling of the CJEU will have significant consequences for parallel datasets and duplicating databases.

ECtHR Cases

Date	Description
January 2022	**Ekimdzhiev v Bulgaria (Application No. 70078/12) (ECtHR): When surveillance safeguards fail** The 11 January 2022 Chamber judgment of the European Court of Human Rights (ECtHR) in Ekimdzhiev v Bulgaria (Application No. 70078/12) reads like an abject lesson in what can go wrong with surveillance powers when safeguards, such as having to apply to court for a warrant, break down. The historic failures recorded in the judgment included a court issuing warrants without sufficient foundation at a time when it was the main warrant-issuing court, the president of that court being criminally convicted of deliberately issuing a warrant for a period exceeding the statutory maximum, and courts issuing boilerplate interception and surveillance warrants distinguishable from each other only by the application number and date. These was also evidence that the current specialist court was under-staffed and resourced to deal properly with the volume of applications. The ECtHR concluded that: > "no proper reasons have been given for the decisions to issue the vast majority of all surveillance warrants issued in Bulgaria in the past decade." It went on: > "This is of particular relevance as the contemporaneous provision of reasons is a vital safeguard against abusive surveillance. … This is because the provision of reasons, even if succinct, is the only way of ensuring that the judge examining a surveillance application has properly reviewed the application and the materials which support it, and has truly directed his or her mind to the questions…". This was against a background of apparently corroborated allegations that it was possible to open frivolous and abusive criminal prosecutions, chiefly with a view to making it possible to place someone under surveillance for ulterior motives. Against this background, and in view of several other shortcomings in procedure and oversight, the Court held that although for the most part the legislation was clear about the grounds on which surveillance could be authorised and against whom, and if strictly adhered to the authorisation procedure provided substantial safeguards against arbitrary or indiscriminate surveillance, those safeguards were not properly applied in practice and did not provide adequate guarantees against abusive surveillance. They appeared to have had an actual impact on the operation of surveillance in Bulgaria.

The second half of the judgment examined the Bulgarian regime requiring telecommunications operators to retain all communications data of all users for six months. This was a blanket bulk retention requirement, applicable to all operators, of the kind that the CJEU invalidated in Tele2.

The Court observed that although the interference with privacy was carried out by private persons – telecommunications operators – it was required by law so was attributable to the Bulgarian State.

The main point of principle that the Court laid down was that mandatory general retention of communications data and its access by the authorities in individual cases must be accompanied by the same safeguards, mutatis mutandis, as secret surveillance.

Some aspects in which the Bulgarian regime fell short were:

- The authority seeking access was under no duty of full and frank disclosure to the judge of all relevant matters, including matters which may weaken its case.
- The law did not require that supporting materials be enclosed with the application for access.
- The law did not require judges examining applications to give reasons explaining why they have decided that access was truly necessary.
- The procedures therefore did not guarantee that access to retained data was granted in each case only when genuinely necessary and proportionate.
- The Court also noted lacunae in rules for storage and destruction of accessed data, inadequate oversight arrangements and lack of effective remedies.

In both the surveillance and the data retention limbs of its judgment, the Court also relied on lack of provision for notification to subjects that authorities had lawfully been given access to data about them, once that could be done without jeopardising the purpose of the measure. That, however, was in the context that no effective remedies were available without notification.

Implications for UK legislation

As with any Strasbourg judgment in this area, it is almost impossible to tease out hard and fast consequences for other legislative regimes. The Court takes a holistic, multi-factor approach in which deficiencies in one area can be compensated by safeguards in another. So a specific weakness cited as a reason for finding a violation in one case may not be conclusive in another case.

That said, two of the Court's grounds could give pause for thought.

The first is the requirement to give reasons. Under the Investigatory Powers Act 2016, an obligation to give reasons applies only when a Judicial Commissioner refuses approval of various kinds of warrant or notice. The March 2018 IPCO (Investigatory Powers Commissioner's Office) Advisory Notice elaborates:

> "45. Judicial Commissioners will record their decision on the relevant form, always with reasons if the warrant is refused and at their discretion if it is approved. The nature and extent of those reasons is a matter for the Judicial Commissioner though in complex, novel or contentious matters it is anticipated that a detailed record of the decision will be made."

There is no statutory obligation on OCDA (the Office for Communications Data Authorisations) to give reasons either for authorising or refusing to authorise an application to obtain communications data. A requirement to give reasons in all cases (even if succinct) could be challenging in the context of the volume of decisions made (some 223,000 in 2020).

The second ground of interest, but probably of less significance in the light of the Codes of Practice issued under the 2016 Act, is the obligation of full and frank disclosure. The 2016 Act itself places no such obligation on the applicant for a warrant or for a communications data authorisation. However the Interception Code of Practice states:

> "5.30 When completing a warrant application, the intercepting authority must ensure that the case for the warrant is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which weakens the case for the warrant. "

The IPCO March 2018 Advisory Notice records that:

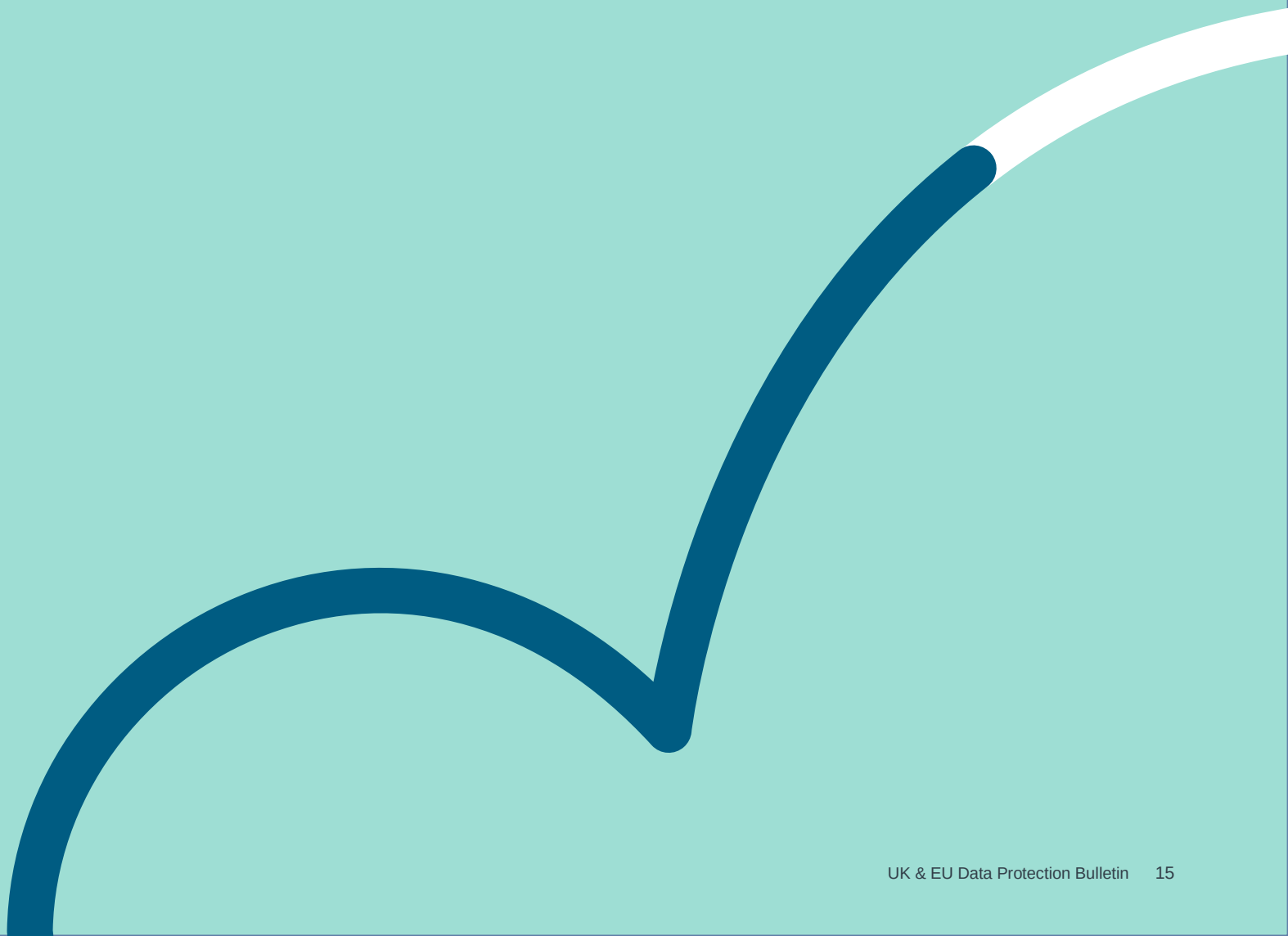
> "34. Those requesting a warrant will confirm as part of the application that, in accordance with the applicable Code of Practice, they have made all reasonable efforts to take account of information which may weaken the case for the warrant."

Similarly the Communications Data Code of Practice states that an applicant to acquire communications data must:

> "present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorization."

The Investigatory Powers Act comes up for its statutory review later this year. It will be interesting to see what, if anything, is said about these points.

UK Enforcement



UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
1 December	EB Associates Group Limited	Monetary Penalty of £140,000 Enforcement Notice	The ICO has fined EB Associates Group Limited ("EB") £140,000 for violations of Regulation 21B of the PECR. The ICO has also issued an Enforcement Notice ordering EB to stop making further calls of this type. Between 11 January 2019 and 30 September 2019, 107,003 unsolicited direct marketing calls were made to subscribers in relation to occupational or personal pension schemes. These calls were instigated by EB without valid consent. Following investigation, the ICO concluded that EB positively encouraged lead generators to make calls on its behalf, as evidenced by payment of a fixed fee for each referral made of up to £750. The calls instigated by EB were direct marketing in relation to occupational pension schemes or personal pension schemes within the definition of Regulation 21B PECR. Such calls can only be made by an authorised person or a person who is the trustee manager of an occupational pension scheme or personal pension scheme. The lead generators who carried the calls out on EB's behalf were not included in the categories of authorised persons. The ICO also found that EB did not have valid consent to instigate the making of the calls.
2 December	Cabinet Office	Monetary Penalty of £500,000	The ICO has fined the Cabinet Office £500,000 for disclosing postal addresses of the 2020 New Year Honours recipients online. On 27 December 2019, the Cabinet Office published a file on the government website containing the names and unredacted addresses of more than 1,000 people announced in the New Year Honours list. People from a wide range of professions across the UK were affected, including individuals with a high public profile. The personal data was available for nearly two and a half hours and was accessed 3,872 times. The Honours and Appointments Secretariat ("HAS") within the Cabinet Office had implemented a new IT system in 2019 to process the public nominations for the New Year Honours list. However, the IT system was not set up correctly by the Cabinet Office which led to the system generating a file that included postal address data. As time was tight to get the list published, the HAS operations team decided to amend the file instead of modifying the IT

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			system. Each time a new file version was generated, the postal address data was automatically included in the file. At the time, there was no process in place within HAS to sign off on documents and content containing personal data prior to publication. The ICO found that the Cabinet Office had failed to put appropriate technical and organisational measures in place to prevent the unauthorised disclosure of people's information.
8 December	Virgin Media Limited	Monetary Penalty of £50,000	The ICO has fined Virgin Media Limited ("Virgin") £50,000 in connection with 451,217 marketing emails sent to persons who had previously opted out of marketing communications from Virgin. The relevant emails informed their recipients of a price freeze being implemented by Virgin. The end of the email then informed the recipient that as they had opted out of marketing messages Virgin could not keep them up to date with their latest news and offers, before providing a link which would enable the recipient to change their marketing preferences. The ICO concluded that this sought to entice or encourage customers to update their marketing preferences while also marketing Virgin's commercial offerings. These were direct marketing for the purposes of DPA 2018 and PECR. Virgin did not have consent to send these directing marketing emails and therefore acted in breach of Regulation 22 PECR.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
17 December	Northern Gas & Power Ltd	Monetary Penalty of £75,000 Enforcement Notice	The ICO has fined Northern Gas & Power Ltd ("NGP") £75,000 in relation to the making of direct marketing calls without valid consent. The ICO has also issued an enforcement notice ordering that NGP stop making further calls. Between 1 May 2019 and 31 March 2021, NGP used a public telecommunications service for the purpose of making unsolicited direct marketing calls to subscribers who had a telephone number registered with the Telephone Preference Service ("TPS") or Corporate Telephone Preference Service ("CTPS") and where the number concerned had already notified that calls should not be made. The ICO also found that NGP had not been able to demonstrate that the TPS or CTPS subscribers had given prior notification or valid consent to receive the direct marketing calls. To be valid, the notification must clearly indicate the individual's willingness to receive marketing calls from that company specifically. Companies cannot rely on individuals opting into marketing communications generally, unless it is clear that this will include phone calls and notifications will not be valid where individuals are asked to agree to receive marketing calls from "similar organisations" or other similar generic descriptions. ICO therefore found that NGP had contravened Regulation 21 PECR. In determining the appropriate fine the ICO considered that the number of complaints was likely to be only a small proportion of the actual number of breaches. There were, however, also mitigating factors, including that NGP confirmed that it had purchased its own TPS licence, as well as call screening and blocking software.
18 January	Ministry of Justice	Enforcement Notice	On 21 December 2017, the Ministry of Justice ("MoJ") was issued with an Enforcement Notice following a conclusion by the ICO that it had failed to comply with a large number of data subject access requests ("DSARs") without undue delay, in contravention of data protection legislation. The MoJ complied with the terms of that earlier Enforcement Notice within the timeframes required of it. On 7 January 2019, the ICO was made aware by the MoJ that a backlog of DSARs had again accrued. A year of correspondence between the MoJ and ICO followed until the pandemic led to a shift in the ICO's approach to regulatory action in March 2020.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			On 20 October 2020, the MoJ were contacted by the ICO and asked to provide an update on its processing of DSARs. The MoJ explained that the pandemic had affected its operations, but it had sought to prioritise responses to DSARs where the request related to urgent matters (e.g. legal proceedings, immigration hearings or police investigations). On 16 April 2021, the ICO was advised that, at 31 March 2021, the MoJ had 5,956 DSARs outstanding to which it had only partially responded, with 372 of those dating back to 2018. By 16 August 2021, the number of DSARs overdue had risen to 7,753. While the ICO acknowledged that the MoJ faced certain difficulties during the pandemic and that it had co-operated with the ICO's investigation, it concluded that the MoJ had contravened Article 15 EU and UK GDPR by failing to inform relevant data subjects whether their personal data is being processed without undue delay and had failed to provide access to that personal data. The ICO issued an Enforcement Notice requiring the MoJ to: a. by no later than 31 December 2022, have informed the 7,753 data subjects who have made a DSAR whether the MoJ is processing their personal data and, if so, provide a copy of that data (subject to any exemptions); and b. by 31 December 2022 at the latest, the MoJ is to carry out changes to its internal systems, procedures and policies to ensure that future DSARs are complied with in accordance with Article 15 UK GDPR.
20 January	Energy Suite Limited	Monetary Penalty of £2,000	The ICO has fined Energy Suite Limited ("Energy Suite") £2,000 for making over 1,000 unsolicited direct marketing calls to subscribers who were registered with the Telephone Preference Service ("TPS") and who had not notified Energy Suite that they were willing to receive such calls which led to 3 complaints being made. The ICO found that the contravention by Energy Suite took place between 1 March 2020 and 13 November 2020, during which period Energy Suite used a publication telecommunications service for the purposes of making at least 1,246 connected calls to subscribers whose numbers were listed in the TPS register. In the absence of any evidence from Energy Suite, the ICO concluded that on the balance of probabilities, most or all of the numbers on the TPS register were not allocated to people who had notified Energy Suite (via the contact form on its website) that they did not object to being contacted.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			This, among other factors, led to a conclusion that Energy Suite had committed multiple breaches of Regulation 21 PECR. When considering the level of fine to impose the ICO took into account: (a) the small size of the company; (b) that Energy Suite had sought to cooperate to some degree with the ICO (albeit its responses were deemed unsatisfactory); and (c) the volume of calls in this case was comparatively low compared to others that the ICO had seen previously.
2 February	Home2sense Limited	Monetary Penalty of £200,000 Enforcement Notice	The ICO has fined Home2Sense Ltd ("H2S") £200,000 for making more than 675,478 unsolicited marketing calls between June 2020 and March 2021, offering insulation service to individuals registered with the Telephone Preference Service. H2S came to the ICO's attention following an analysis of complaint trends which indicated an increase of complaints about unsolicited calls relating to loft insulation. Various trading names were provided on calls which were complained about, including Cozy Loft, Warmer Homes and Comfier Homes. The ICO used a third-party information notice issued to the relevant communications service provider to identify H2S as the entity behind the calls. The ICO found H2S to be in contravention of Regulations 21 and 24 PECR. Between June 2020 and March 2021, H2S made the unsolicited calls for direct marketing purposes to subscribers. The ICO was satisfied that the calls were made to those who had not notified H2S that they did not object to receiving such calls; those individuals had not taken clear and positive action to indicate their willingness to receive marketing calls from the company. The ICO also found evidence that H2S failed to provide the recipient of calls with the particulars specified at Regulation 24(2) PECR; in particular, when it did provide subscribers with the name of the caller, it used seemingly interchangeable trading names which could not be readily identifiable as H2S. The ICO also expressed concern at H2S's failure to engage with its investigation and its attempts to deflect responsibility for compliance with the law onto its staff, including indicating that it was beyond its control to ensure staff screened data against the TPS register prior to making calls. The ICO has also issued H2S with an Enforcement Notice ordering them to stop making unsolicited marketing calls.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
9 February	Tempcover Ltd	Monetary Penalty of £85,000	The ICO has fined Tempcover Ltd ("Tempcover") £85,000 for sending a total of 29,970,419 unsolicited direct marketing messages without valid consent between 26 May 2019 and 26 May 2020. It became apparent during the ICO's investigation that at the time an individual provided their details to Tempcover, they were not provided with a separate option to either opt-in or opt-out of direct marketing. Instead, Tempcover used an individual's mandatory agreement to its website's terms and conditions/privacy policy as the basis on which to conduct its direct marketing campaign, acting under the belief it could rely on a 'legitimate interest'. The ICO found that Tempcover had breached Regulation 22 PECR by the sending of the unsolicited direct marketing messages (which were predominantly emails but also text messages). Tempcover did not hold valid consent to send these messages as it sent the messages unsolicited to subscribers who had entered their details on Tempcover's website with a view to obtaining insurance. Tempcover failed to provide an opportunity to opt-out of direct marketing when first obtaining these details and effectively made agreement to direct marketing a condition of service. The subscriber was therefore not given an active choice and the consent relied upon cannot be deemed sufficiently 'specific'. The ICO considered whether the soft opt-in under Regulation 22(3) might apply. The ICO accepted that it appeared Tempcover satisfied the first two limbs of the Regulation 22(3) test, in that it: (a) obtained the contact details for intended recipients in the course of a sale (or negotiation for a sale) of a product/service; and (b) used the unsolicited direct marketing as a way of marketing only its own similar products/services. However, the third limb of the test was not satisfied, as Tempcover failed to provide individuals with a simple means of refusing the use of their contact details for direct marketing at the time the details were initially collected. As all three parts of the test have to be satisfied, the criteria under Regulation 22(3) were not met. The ICO reiterated that 'legitimate interest' is not a lawful basis which can be relied upon under PECR in relation to direct marketing message. These messages can only be sent with valid consent or whether the soft opt-in applies. When considering the level of fine, the ICO considered as a mitigating factor that Tempcover has made changes to its practices in light of the ICO investigation and now allows subscribers the ability to opt-out of unsolicited direct marketing messages at the point which consent is obtained.

Information Tribunal Appeal Cases

Date	Appellant	Type of Case and Result	Summary of Case
7 December	Brandon Dolby	Application for an Order to Progress a Complaint under s166 DPA 2018 Dismissed	The Applicant said he was seeking "to raise a right of rectification in relation to data sharing regarding a subject access request" and that he wished the ICO to investigate to whom certain CCTV footage was disclosed and/or whether it was disposed of. The remedy sought was "Compliance orders". The Tribunal interpreted the application as one made under s166 DPA 2018. The ICO sought for the application to be struck out on the grounds that there is no reasonable prospect of it succeeding. The Tribunal noted that the Upper Tribunal have previously stated that if the ICO goes outside its statutory powers or makes any other error of law, it is for the High Court to correct the ICO on ordinary public law principles in judicial review proceedings. The Tribunal further noted that a person who wants a data controller to rectify personal data, compensate them or otherwise comply with data protection legislation must go to the civil courts, not the Tribunal. The Tribunal concluded it had no power to do what the Applicant was asking of it as it has no power to investigate a data subject's allegations of dishonesty, interference with or loss of data, nor does it have jurisdiction to provide rectification or compliance. The Tribunal therefore dismissed the application and declined to make an order under s166(2) DPA 2018.
14 December	Price Forbes & Partners Limited	Appeal against a Monetary Penalty Notice for failure to pay registration fee. Dismissed.	The Appellant challenged a monetary penalty notice issued in connection with its failure to pay the ICO the Data Protection Fee required under the Data Protection (Charges and Information) Regulations 2018. It was not disputed that the Appellant was liable to pay a fee of £2900 and failed to do so. The fee was due to be paid by 18 October 2020. Until September 2020, the Appellant's DPO was Ian Whitt. The Appellant emailed the ICO on 11 November 2020 to advise of a change of DPO to Neil Isherwood. The Appeal was brought on the basis that the ICO failed to take adequate measures to inform the Appellant of the Notice of Intent and that the ICO had sent email correspondence to the former DPO to which it would have received a bounce back notification. Other grounds included that there had been a series of errors by the ICO and that the fine imposed was excessive.

Date	Appellant	Type of Case and Result	Summary of Case
			The ICO's position was that no reasonable excuse for failing to pay the charge had been put forward and that the ICO was under no obligation to remind a controller of their legal liabilities to pay a charge. Reminders were sent by email (although the ICO stated it had no way of monitoring undelivered emails due to the volume sent daily) and by post to the registered office address. The Tribunal concluded that issuing the Penalty Notice was appropriate absent a reasonable excuse for the Appellant's failure to comply with the requirements of the Regulations. The Tribunal said that even with the departure of the previous DPO, it was not reasonable for the Appellant to have no system for monitoring emails sent to a former DPO, particularly where that email address has been provided to the ICO as the organisation's contact details. The Tribunal did not accept that the ICO failed to take adequate measures to inform the Appellant of the Notice of Intent and in any event it was under no obligation to do so. The appeal was dismissed and the £4000 fine upheld.
11 January	Eric Prizkalns	Application for an Order to Progress a Complaint under s166 DPA 2018 Dismissed	The Applicant applied to the Tribunal for an order under s166(2) and 166(3) DPA 2018 to direct a response from the ICO. The application related to a complaint made to the ICO concerning how an organisation based in the USA had processed his (and others) personal data by allowing access by the participants in webinars to the email address of every other participant. The complaint was made on 1 February 2021, with follow up complaints on 5 March 2021 and 26 March 2021. Having not received a response, the Applicant complained to the Tribunal. On 16 June 2021, the ICO told the Applicant that there was insufficient evidence of the data protection concerns and he should provide further material. The Applicant subsequently provided further information. On 30 June 2021, the ICO informed the Applicant that the material provided did not constitute evidence of an infringement, in particular because it was insufficient to ascertain that the organisation was offering services to natural people in the UK. The Tribunal made clear that the s166 provision is concerned with remedying ongoing defects that impede the resolution of a complaint rather than assessing the appropriateness of an outcome of a complaint. In this

Date	Appellant	Type of Case and Result	Summary of Case
			case, the Applicant was not satisfied with the outcome of the ICO's investigation and was effectively trying to "turn back the clock" in order to change the outcome which is not permitted under s166. The Tribunal therefore dismissed the complaint on the basis it has no power to decide the merits of the outcome reached by the ICO. There was no basis for the Tribunal to make an order under s166(2) DPA 2018. Any further remedy for the Applicant would be more appropriately sought from the Civil Courts.

Other recent articles

- Positive news for data controllers in the much-anticipated Lloyd v Google Supreme Court judgment (twobirds.com)
- Filling in the blanks: What is the transfer of personal data and when will Chapter V obligations be applicable? (twobirds.com)
- New UK Standard Contractual Clauses for Personal Data Transfers - Bird & Bird (twobirds.com)
- The EU Data Governance Act: what privacy professionals need to know - Bird & Bird (twobirds.com)
- Compliance Guide on Personal Information Protection for SMEs

twobirds.com

● Abu Dhabi ● Amsterdam ● Beijing ● Bratislava ● Brussels ● Budapest ● Casablanca ● Copenhagen ● Dubai ● Dusseldorf ● Frankfurt ● The Hague ● Hamburg ● Helsinki ● Hong Kong ● London ● Luxembourg ● Lyon ● Madrid ● Milan ● Munich ● Paris ● Prague ● Rome ● San Francisco ● Shanghai ● Singapore ● Stockholm ● Sydney ● Warsaw