Bird & Bird

UK & EU Data Protection Bulletin: April 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

UK Law

EU

EDPB

CJEU Cases

UK Enforcement

ICO Enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
17 February 2021	**Data analytics toolkit launched** The toolkit is aimed at those using software to automatically discover patterns in data sets containing personal data – including use of AI (but not limited to this). The toolkit asks a series of questions to give guidance on lawfulness of processing; accountability and governance; data protection principles and data subject rights. The output is in the form of a report with tailored advice. ICO advises that use of the toolkit is anonymous and that ICO cannot view the information submitted to it.
9 March 2021	**New Guidance on Political Campaigning** ICO has published its final guidance on this, following a public consultation launched in October 2019. The Guidance summarises the impact of existing laws on political campaigning: it does not change the law. The guidance is aimed at those using political campaigning to engage with members of the public; it is not intended to apply to internal campaigns (for example, relating to leadership elections). The guidance contains useful commentary on who is regarded as a separate controller for data protection purposes – recapping earlier guidance which explained that – for example – elected representatives and candidates are regarded as separate controllers from the party of which they are a member. There is also useful guidance on purpose limitation – with examples looking at when petition data and constituency data can be used in national campaigns.
10 March 2021	**Digital Regulation Co-operation Forum publishes first annual plan of work** The Forum consists of the Competition and Markets Authority, ICO and Ofcom. As from April 2021, the Financial Conduct Authority will join the Forum. In the coming year, the Forum will focus on the following: - Joint projects to complex issues of relevance to multiple Forum participants. This will include looking at the impact of algorithms, service design frameworks, AI, digital advertising technologies and end to end encryption - Developing joined-up regulation – with a focus on overlaps between data protection and competition law and AADC and regulation of video-sharing platforms and Online Harms - Building shared skills and capabilities – for example, by building cross agency specialist teams

Date	Description
19 March 2021	**ICO announces plan to update anonymisation guidance** Ali Shah, the ICO's Head of Technology Policy, has blogged about the ICO's plan to update its anonymisation guidance. ICO is interested in engaging with experts ahead of public consultation. The guidance will cover: - The legal and policy issues concerning anonymisation - Identifiability – looking at how to assess and manage risk - Pseudonymisation techniques and best practices - Accountability and governance - The role of anonymisation in research - The role of PETs in data sharing - Technological solutions - Case studies Those interested in participating should contact anonymisation@ico.org.uk.

UK Cases

Date	Cases
8 January	**True Vision Productions v Information Commissioner [2021] UKFTT 2019 EA 0170** The case is useful in showing how exemptions in data protection legislation relating to processing of personal data for journalistic purposes should be applied. The First Tier Tribunal found that filming of mothers – at the moment they received a diagnosis that their unborn child had died – breached data protection legislation because the filming was carried out without notice, whereas notice could have been provided. The Tribunal imposed a reduced monetary penalty – of £20,000 instead of £120,000. It noted that mitigating factors were the fact that unused footage was only accessed with consent and was destroyed quickly. However, the filming involved highly sensitive data about women at an especially vulnerable moment, so a penalty was appropriate. The case was determined under the Data Protection Act 1998, but as the provisions in the 2018 Act relating to journalistic processing are very similar to those in the 1998 Act it is still of wider relevance. True Vision Productions Limited (TVP) had a reputation for making films about difficult issues involving matters of social justice. It determined to make a film about the impact of stillbirth – *Child of Mine* – which it considered would be in the public interest. The film company took an editorial decision that it was important to record the moment of diagnosis, in order to convey the impact of this to the public. The DPA 1998 provided for an exemption where the data controller reasonably believed that publication would be in the public interest and that complying with the certain provisions of the legislation would be incompatible with journalistic purposes. The First Tier Tribunal noted that TVP hadn't been aware that data protection legislation would apply to the filming. However, TVP had been concerned to respect the privacy of participants. The First Tier Tribunal concluded that the reasonable belief test should be substantive rather than formalistic; the fact that TVP had not considered data protection legislation did not stop them relying on the exemption; TVP had considered the public interest in broadcasting and had considered privacy more generally. The First Tier Tribunal noted that TVP could rely on an exemption not to obtain consent from participants. Consent would only have been valid if it was explicit and informed; this would have meant explaining to those filmed that there was a risk that they had suffered a stillbirth (before a diagnosis was given). The doctors at Addenbrookes hospital had refused to allow TVP to seek consent, concluding that this would be detrimental to the women's wellbeing. However, the Tribunal agreed with the Commissioner that the filming was unfair, because no effective notice was given of the filming and it would have been possible for TVP to make the filming more prominent – via use of handheld cameras -and so address fairness. While there were notices in the waiting rooms and in the clinic, the Tribunal noticed that – given the likely focus of the women – it was not reasonable to assume that they would have read them; they would likely have assumed that CCTV cameras were there for security reasons. Additional steps could and should have been taken.

Date	Cases
1 February	**Koypo Laboratories Limited v Information Commissioner [2021] UKFTT EA/2020/0263P** This case was an appeal against a monetary penalty issued by the ICO in August 2020 relating to a breach of Regulation 22 of PECR. Koypo, a lead generator specialising in scientific customer acquisition, had originally been issued with an enforcement notice and monetary penalty for £100,000 for instigating the transmission of over 21 million unsolicited direct marketing emails (linked to PPI Claims) between 1 March 2017 and 31 March 2018 without consent. Koypo was engaged in "hosted marketing" (ie where an organisation sends direct marketing to their own databases but the marketing material relates to a third party). Here, Koypo was the third party and whilst it was not the sender of the emails (these were affiliated companies), it was the "instigator" and would require explicit consent from the recipients that they want to receive the emails before they were sent. Koypo had not been able to evidence to the ICO that sufficient consents had been obtained and therefore was found to be in breach of Reg 22 of PECR. In the appeal, which was challenging the level of the fine, Koypo tried to argue that it did in fact have consent from the individuals in question (this could be shown in relation to one of the affiliated companies, WRM which had sent out over 11 million of the emails and the other affiliates had obtained consent for the marketing of financial products or similar even if Koypo had not been specifically named) and that Koypo had now stopped email marketing and would only now do so with the company name specifically mentioned. Koypo also argued that there were minimal complaints (only 11) and that it had carried out due diligence with the third party affiliates. The Tribunal concluded that the consent had not been properly obtained and was in breach of Regulation 22 of PECR; the sheer volume of emails sent was an important factor even if there had been relatively few complaints. However, the Tribunal did consider that the level of the fine could cause financial hardship to Kyopo and therefore agreed to reduce the penalty to £80,000.
2 February	**Weaver and others v British Airways plc [2021] EWHC 217 (QB)** Data protection claims are one of the driving forces behind the ongoing debate concerning the way group actions are conducted in the UK. This recent High Court decision was made after a costs and case management conference in the group litigation which follows the high-profile British Airways data breach. The claim is being conducted under a Group Litigation Order (commonly referred to as a GLO). GLOs are an 'opt in' procedure; they require each claimant to make their own claim individually, those claims are then grouped together and the Court manage all of the claims together to avoid a multitude of separate claims and the risk of inconsistent judgments. A GLO commonly provides for a cut-off date, which is effectively a deadline by which a claimant wishing to be part of the group must submit their claim. This gives the defendant a clearer idea of the size of the case they are facing, which may influence strategic decisions they take, such as their approach to settlement discussions. While claimants can still join a GLO after the expiry of the cut-off date, they will need the permission of the court to do so. The court ruled on two important issues in this case: 1. An application by the claimant to extend the cut-off date to the summer of 2022, which would have been an extension of over a year and moved the deadline to a year after the proposed trial date. The court had to consider BA's interest in having a degree of

Date	Cases
	certainty about the size of the claim against ensuring access to justice for prospective claimants who might wish to join the group. Having considered the issues, the court granted an extension of 2 months to the cut-off date, substantially shorter than the extension requested by the claimants but enough time to allow their recent advertising to come to fruition. 2. The court had to rule on the recoverability of the claimants' solicitors advertising costs which had been incurred to recruit claimants for the group litigation. £443,000 of advertising costs had been incurred and provision made for a further £557,000 of future advertising costs (taking total advertising costs to £1 million). The court agreed with BA that these costs were not recoverable as a matter of law, citing an earlier decision of the Court of Appeal which ruled that the expenses of obtaining business should be treated as part of a solicitor's general overheads and are therefore not recoverable. This decision will disappoint claimant law firms focussed on data protection litigation post-GDPR. The ability to build a large group of claimants is an expensive but essential part of any group litigation, particularly where litigation funders are involved, and inability to recover costs of doing this will make a significant dent in their margins when it comes to assessing financial viability of such actions. This decision may further encourage the shift by claimants towards 'opt out' class action devices, which appear to be possible using the representative action procedure contained in CPR 19.6. This mechanism does not require all class members to be identified and signed up to the action in advance, doing away with the need to fork out on the sort of advertising at issue in the Weaver case.
2 February	**Phones 4U LTD (In Administration) v EE Ltd & 7 ORS** After going into administration in 2014, Phones 4U brought a competition claim against a number of mobile phone companies alleging anti-competitive behaviour. It claimed that the defendants forced it into administration by colluding to terminate their contracts. It submitted that current and former employees of the defendants had used their personal devices to collude. Phones 4U submitted that the defendants had control of the relevant documents by virtue of the principle of agency and requested that the defendants request access to the personal email accounts and phones of the relevant individuals. Some of the defendants refused and so Phones4U applied to the court for an order obliging them to do so. The defendants resisted on the following grounds: the court had no jurisdiction to make an order for searches of personal email accounts and phones. The defendants submitted that Phones4U ought to apply for third party disclosure against the relevant individuals; • such an order would breach the Art 8 ECHR rights of the relevant individuals (right to privacy); and • it was unclear what Phones 4U were asking the defendants to do. • At first instance the judge granted the order, which included restrictions on what could be done with the devices; The defendants appealed to the Court of Appeal on the basis of the first ground above. They suggested alternative, less invasive, options to proceed including: • orders for specific disclosure of classes of relevant documents held on the employees' personal devices that were in the control of the defendant; • that the defendants request documents relating to their affairs from the relevant individuals;

Date	Cases
	• Phones 4U applying for third party disclosure of the relevant documents. The Court of Appeal rejected these arguments on the basis that their objection to the order was unfounded. The order required the defendants to request information from the relevant individuals. Additionally, while the alternative options were viable, they would result in additional costs and administration and were therefore less favourable. The arguments that the privacy of the relevant individuals would be infringed were dismissed. The right had to be balanced against the need for the effective administration of justice, and the first instance judge had adopted safeguards to address this. Should the relevant individuals refuse to comply, Phones4U would have to pursue an alternative approach to obtain the documents. The Court of Appeal made some helpful comments on this: • The Court of Appeal noted that the documents may be in the control of the defendants. The question is a complicated one and would involve reviewing the relevant contract of employment. (In Pipia v BGEO Group Ltd [2021] EWHC 86 (Comm), the court held that a clause which permitted the employer to access the employee's computers regardless of the personal nature of the material held on it, extended the employer's control to the personal devices of an ex-employee.) • The Court of Appeal indicated that the relevant individuals couldn't refuse to deliver the documents on the basis that they contents were 'mixed' with personal information. The judgment is an indication of pragmatic approach of the court to disclosure. You can read the decision here.
8 February	**Leave.EU Group Ltd (2) Eldon Insurance Services Ltd v Information Commissioner** The Upper Tribunal rejected all arguments by Leave.EU and Eldon Insurance Services against enforcement action taken against them in relation to newsletters about Brexit which also contained advertising material about GoSkippy insurance products. The Tribunal found that under the Privacy and Electronic Communications (EC Directive) Regulations 2002 (PECR), a mere banner, or other strap line, containing marketing material in an email could amount to an unsolicited communication; that those including such banners or strap-lines in their emails would therefore need to meet the requirements of the PECR (in this case obtain consent) and that consent to receive information "of interest to you" is too vague to be valid. Readers may also enjoy the irony that Leave.EU has been responsible for a case confirming the continued relevance of CJEU case law to UK information law post-Brexit. The Upper Tribunal referred in detail to the CJEU cases of *Planet 49* (C-673/17) and *Orange Romania* (C-61/19), considering them to be "*high authority as to the proper meaning of consent*". An appeal against enforcement action taken against newsletters sent to Brexit supporters, which advertised GoSkippy services Leave.EU is a political pressure group owned by Arron Banks, the prominent Brexiteer. Eldon Insurance Services is majority owned by Arron Banks and is the provider of "GoSkippy" insurance products. Leave.EU has sent regular email newsletters to 51,000 subscribers. 21 of these newsletters contained advertising material for GoSkippy. One newsletter focused almost exclusively on GoSkippy; the other 20 newsletters simply had a footer or banner containing offers such as "10% off GoSkippy Insurance". In total about 1,000,000 newsletters were sent which contained some marketing reference to GoSkippy. There were two complaints about this to the Information Commissioner. The Information Commissioner issued a monetary penalty notice of £45,000 against Leave.EU (for sending the communications) and of £60,000 against Eldon for instigating the sending of the communications. The Commissioner also issued

Date	Cases
	assessment notices (i.e. forced audits) against both companies. It is worth noting that other monetary penalty notices and information notices had been served on these and other associated companies, where appeals were not pursued. Leave.EU and Eldon appealed to the First Tier Tribunal and then, again, to the Upper Tribunal. They argued that the newsletters did not fall within PECR; that the criteria for the Commissioner to issue Monetary Penalty Notices had not been met; that the notices did not comply with the Commissioner's Regulatory Action Policy, were disproportionate, did not meet the statutory requirements for an assessment notice and were vitiated by procedural unfairness. The Upper Tribunal rejected all of these arguments. The PECR restrict sending any kind of unsolicited direct marketing communication – even just a banner or footer containing advertising The PECR provide that a personal "*shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail…"*. Leave.EU and Eldon argued that the PECR should be restricted to cases of bulk spamming and that incidental advertising in solicited newsletters should not be covered. The Upper Tribunal disagreed. It held that there was no such limit to the scope of the PECR. The Upper Tribunal specifically noted that the inclusion of a banner or other advertising content in a newsletter would amount to an unsolicited communication. It also rejected arguments that the PECR should only apply where the primary purpose of the newsletter was for direct marketing. Instead, the Tribunal suggested, the answer to these points should be for the sender of the newsletter to obtain appropriate consent [61]. Consent to send information "that we feel may interest you" is vague and invalid Leave.EU and Eldon argued that – in any case – they had consent to send this material. The Upper Tribunal disagreed. The relevant privacy notice referred to the provision of "*information, products or services that you request from us or that we feel may interest you…*". There was no doubt that subscribers had agreed to received political campaign information. However, the broad wording "was so all-encompassing as to fail to meet the necessary standard of consent" [45]. The Upper Tribunal approvingly quoted arguments from counsel for the Information Commissioner, Christophe Knight, that that "*the very loosely drafted privacy policy amounted to signing a blank cheque*". Confirmation that PECR covers "instigation" as well as transmission The Upper Tribunal cited *Microsoft v McDonald* noting that the PECR also apply to the person who instigates transmission – which includes urging, or inducing, or some form of positive encouragement to do something. In this case, Eldon had instigated the transmission of the marketing communications. Grounds for taking enforcement action The Commissioner can issue a monetary penalty notice for breach of the PECR were there is a "serious" contravention of the PECR. The Upper Tribunal noted that there is no requirement that there be a *"serious intrusion of individuals' privacy rights – rather, they require a serious contravention of PECR"*. The volume of emails sent was relevant – and the First Tier Tribunal was entitled to conclude that sending 1,000,000 emails was a serious breach of the PECR. A monetary penalty can be issued where the breach is deliberate (not the case here) or where the wrongdoer knew, or ought to have known, that there was a risk of contravention and failed to take steps to prevent it. In this case, the associated notices were relevant: the businesses

Date	Cases
	here knew, or ought to have known, of the risks associated with the PECR and should have put in place more steps to mitigate against breaches. The Tribunal noted that knowledge of a risk of breach was "hardly a high threshold". On the assessment notice, the Upper Tribunal confirmed that the DPA 2018 allows the Commissioner to issue these without any particular minimum threshold or specific prior procedural requirements. The Upper Tribunal rejected arguments by Leave.EU and Eldon that the enforcement action was unlawful because it was not in line with the Commissioner's Regulatory Action Policy – in that the RAP gave examples of when the Commissioner would take action and the circumstances in this case were different to the examples cited. The Upper Tribunal held that these were purely illustrative examples, that this was sufficiently clear from the RAP and that the fact that the RAP does not anticipate a particular scenario does not preclude the Commissioner from taking action in that situation. The Tribunal also rejected arguments by Leave.EU and Eldon that the Commissioner's actions were procedurally unfair.
11 February	**HRH Duchess of Sussex v Associated Newspapers [2021] EWHC 273 (Ch)** This High Court judgment relates to a letter sent by the Duchess of Sussex to her father which was reproduced in large parts in articles published by the Associated Newspapers in the Mail on Sunday and MailOnline. The Duchess of Sussex claimed that Associated Newspapers had misused her private information, had breached data protection legislation and infringed her copyright – this judgment was concerned only with the claims in privacy and copyright (and not the data protection claim). We have focused on the privacy claim below. The Duchess of Sussex applied to strike out the defences to the claim of misuse of private information and/or for summary judgment on that claim. A two-stage test was applied to the question of liability for misuse of private information: (1) Did the claimant enjoy a reasonable expectation of privacy in respect of the information in question? (2) In all the circumstances, should the privacy rights of the claimant yield to the imperatives of the freedom of expression enjoyed by publishers and their audiences? The High Court applied the factors set out in ***Murray v Express Newspapers plc*** [2008] EWCA Civ 446, [2009] Ch 481 [36] at stage 1 and commented that there was no room for serious debate in relation to some of the factors. After looking at some particular issues in detail (including the status and role of the Duchess of Sussex, whether the contents of the letter were private in nature, the character of the recipient, whether information was already in the public domain and the Duchess of Sussex's intentions regarding the letter), Mr Justice Warby concluded that the Duchess of Sussex would be bound to win at trial on the issue of whether she had a reasonable expectation of privacy and it would be fanciful to think otherwise. On stage 2, it was determined that the only tenable justification for the interference with the Duchess of Sussex's reasonable expectation of privacy would be to correct inaccuracies about the letter contained in an earlier article about the letter in People Magazine. However, the High Court held that "*the disclosures made were not a necessary or proportionate means of serving that purpose and for the most part*

Date	Cases
	they did not serve that purpose at all. Taken as a whole the disclosures were manifestly excessive and hence unlawful. There is no prospect that a different judgment would be reached after a trial. The interference with freedom of expression which those conclusions represent is a necessary and proportionate means of pursuing the legitimate aim of protecting the claimant's privacy." Having reached these conclusions, the High Court saw no useful purpose in striking out any of the defence. It was considered that there were parts of it that might be relevant to damages, and the work involved in filleting would be disproportionate to the gains. The High Court saw no good reason not to enter summary judgment on liability (with damages and other remedies to be decided later) and it was held that there were compelling reasons not to allow this aspect of the case to go to trial. For a copy of the case see here.
16 February	**Collette Lloyd v Information Commissioner** Collette Lloyd made a Freedom of Information request to Airedale NHS Foundation Trust i.a. for the numbers of live births per year of children with Down Syndrome. The Trust explained that it was a small NHS Trust and that numbers would be below 5 per year. Accordingly, it concluded that release of the data would amount to disclosure of personal data and that this meant that it should not provide the information. The Information Commissioner agreed with the Trust. Ms Lloyd appealed against this decision. The First Tier Tribunal agreed with the Information Commissioner that this would amount to disclosure of personal data. The Tribunal applied earlier case law to reach this conclusion – especially *Information Commissioner v Miller [2018] UKUT229 (AAC)* and R v *Department of Health v Information Commissioner [2011] EWHC 1430 (Admin)*. It noted that in cases relating to the disclosure of personal data by a controller to someone else the relevant question was whether it was reasonably likely that an individual could be identified by someone other than the controller. Ms Lloyd requested the information in order to undertake planning relating to non-invasive pre-natal testing and offered to enter into a confidentiality undertaking relating to the information received. The Tribunal concluded that this did not assist – finding that neither the Information Commissioner nor the Tribunal had powers to ask for or to enforce an undertaking.

UK Law

Date	Law
23 February	**Update on S189 DPA: Representative Actions** The UK Government recently undertook a review of the representative action provisions of the DPA 2018. Currently, the UK DPA 2018 (section 187) provides that data subjects can authorise a representative body to, on their behalf, (1) lodge a complaint with the ICO (2) obtain an effective judicial remedy in respect of a decision made by the ICO which impacts that data subject; (3) obtain an effective judicial remedy (non-financial) against a data controller or processor for an infringement; and (4) receive compensation for damage suffered by the data subject as a result of an infringement. In its drafting of the DPA 2018, the UK refrained from exercising its discretion, under Article 80(2) GDPR, to permit representative bodies to carry out the first 3 actions in the above list without authority from data subjects (a discretion that currently only 3 EU Member States (Belgium, France and Denmark) have chosen to exercise). However, section 189 DPA obliged the government to review this by October 2020. There was scope, under the review, for the UK to go further than Article 80(2) GDPR, in that the government was also obliged to consider whether or not to introduce a right for representative bodies to sue for monetary compensation on behalf of data subjects without their mandate – which would, in essence, have created a right of action akin to an opt-out class action for UK data protection claims. Section 189 also obliged the government to consider whether it should specifically provide for children's rights organisations to bring representative actions on behalf of child data subjects, either with or without their mandate. Many organisations responded to the government's call for views on this subject, among them not-for-profits, private businesses, the ICO and the UK courts. The results of the review were not ground-breaking. The conclusions reached were that there is currently no need to make (any) representative action permissible without requiring authority from data subjects. The reasoning for this was based partially upon a perceived lack of need. The government asserted that evidence showed that the ICO can and does take action in response to complaints received from privacy organisations, even without named representees. It also made reference to existing civil procedural remedies (namely Group Litigation Orders, and the representative action mechanism under Civil Procedure Rule 19.6 which has been employed in the well-publicised Lloyd v Google case) to demonstrate that data subjects have sufficient collective recourse to judicial remedies as things currently stand. The other driver behind the conclusion that no change was required appeared to be a fear of unintended consequences. The government seemed persuaded by the concern raised by businesses that insurance costs would rise if opt-out representative action was permitted, and by arguments any change could lead to a compensation culture in the UK which was not to be encouraged. Concern was also expressed about a potential increase in burden upon the courts and the ICO. The review did conclude that further work was required to increase data subject awareness of rights and redress mechanisms and the government undertook to address this going forward. It also undertook to take action to improve existing opt-in mechanisms, especially for children (although concluded that there was no need to specifically permit children's rights organisations to bring representative action, on the basis the existing conditions to be fulfilled by any representative body could already be met by a number of children-specific organisations). What the review omitted to grapple with in any detail is the question of whether the existing civil procedural mechanisms for collective redress really are sufficient, or whether there is in fact a remedy gap in UK data protection law. As a number of respondents to the review pointed out, neither of the existing mechanisms is totally fit-for purpose. GLOs are not "true" collective actions (in that each claimant still

Date	Law
	has to file an individual claim and bear the costs risks associated with that). CPR 19.6 requires there to be a named class representative, who has the "same interest" as all those they represent; this does not provide a free-standing right of action for a representative body, but instead requires them to shoe-horn their way into the procedural requirements. For example, in the recent claim brought using CPR 19.6 by The Privacy Collective against Oracle and Salesforce, a Privacy Collective director had to front the action - luckily, in this case, she has the "same" interest as those her organisation represents, but in other cases, ones involving children for example, this is highly unlikely to be the case. What's more, neither of these mechanisms has any process built in for examination of the suitability of the representative body (i.e. fulfilment of the conditions laid down in Section 187 DPA), something that was clearly intended to feature in any representative action under GDPR. As a result, it is difficult to ignore a suspicion that the government has, by accident or perhaps by design, shied away from addressing this face on and is instead banking on the judiciary finding a way to do the hard work for them in filling this gap. Indeed, the review, when discussing the Lloyd v Google case (on its way to the Supreme Court shortly), contained a cryptic comment about monitoring developments in this area closely – leaving the reader wondering whether, should Google prevail in that case, the government will have to revisit this issue sooner rather than later.

EU

EDPB

Date	Description
10 March	On 10th of March, the EDPS and the EDPB published a joint opinion on the EU Commission Proposal for a Data Governance Act (DGA) here. To recall, the European Commission published its proposal for a Data Governance Act ("the Act") on 25 November 2020. The proposal is the first in a set of measures announced as part of the European Data Strategy, which aims to make the EU a leader in a data-driven society by allowing data to move freely within the EU to the benefit of businesses, researchers and public administration. The Act, which takes the form of a Regulation, aims to build trust for the purposes of facilitating access to data which would not otherwise have been shared due to protected characteristics. For further more detail on the content of the Act, see a previous Bird & Bird article on this topic here. The joint opinion is rather critical of the DGA and stressed that the General Data Protection Regulation (GDPR) should not be affected by the DGA. The EDPB and EDPS see a fundamental conflict in the policy trend towards a data-driven economy and the need to ensure data protection, a fundamental right. Particular points of criticism made in the opinion are: • the missing definition of the roles in terms of data protection • the unclear definition of "data user" in terms of GDPR definitions, as well as the mixing of "permission" under DGA and legal basis under Article 6(1) GDPR • a potential blurring of the treatment of non-personal data and personal data • the complexity introduced by new competent supervisory bodies and designated authorities Overall, the EDPS/EDPB found that the proposal by the Commission did not include sufficient safeguards for individuals. The opinion shows the inherent conflict between the established institutional players in data protection and a Commission eager to put the European Data Strategy in practice. The two organizations also asked for an increase in DPA resources as the DGA would bring a number of challenges that required technical expertise and new capabilities. The proposal for the Act is due to be adopted by the European Parliament's Industry Committee on 15 July 2021, with a plenary vote scheduled for December 2021.

CJEU

Date	Description
2 March	**CJEU clarifies limits on public authority access to retained traffic and location data** *H.K. v Prokuratuur* Case C-746/18 (Grand Chamber, 2 March 2021) *Prokuratuur* is the latest in a series of CJEU judgments on the ability of public authorities to access communications data retained by communications service providers. In October 2020, in its *Privacy International/La Quadrature* judgments, the Court reinforced its generally strict approach. However, it also identified some limited permissible exceptions to the prohibition on mandatory generalised retention. This new judgment considers the constraints on targeted access to retained traffic and location data. Specifically, the court has now held that: - The previously established criterion, that access to traffic and location data must be restricted to serious crime or serious threats to public security, applies regardless of the length of period over which access is sought and the quantity or nature of the data available in respect of such period. - The independence requirement for prior review of an application to access traffic or location data would not be satisfied by a public prosecutor whose task is to direct the criminal pre-trial procedure and to bring a subsequent public prosecution. The background of the case is use made against a defendant in Estonian criminal proceedings of traffic and location data obtained from a telecommunications service provider. The data had been retained under an Estonian blanket mandatory data retention law of the kind that that CJEU had held in *Tele2* (C-203/15) and *La Quadrature* (C-511/18) to be contrary to EU law. Specifically, that was not permitted by Article 15(1) of the ePrivacy Directive 2002/58. The defendant argued in the Estonian Supreme Court that the data should have been excluded from the trial as inadmissible. Although in *Prokuratuur* no question was referred to the CJEU about the EU law compatibility of the Estonian data retention law, that was the background against which the CJEU applied its previous caselaw on Article 15(1). The Estonian Supreme Court asked whether, on the basis of the CJEU's previous decision in *Ministerio Fiscal* (C-207/16), an individual proportionality assessment could be applied to the legality of access by the authorities. That would mean that if the amount of data to which the authorities had access was not large (in terms of type of data and period of time), then the interference with fundamental rights was not serious and could be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences generally. Conversely the more data to which the authorities had access, the more serious the offence had to be. The CJEU rejected this analysis. It accepted that, in principle, the longer the period for which access is sought and the broader the categories of data sought, the greater the quantity of data liable to be retained by communications providers and the greater the interference with privacy. Competent national authorities therefore have to ensure that in each individual case the period and categories sought are limited to those strictly necessary for the purposes of the investigation in question.

However, that did not detract from the overriding rule that access to traffic data and location data was regarded as a serious interference with fundamental rights, regardless of the period for which the data was sought or its quantity or nature, when the set of data was liable to allow precise conclusions to be drawn about concerning the private life of the person concerned. Moreover, since the quantity of data and specific information resulting could only be assessed after the data had been accessed, assessment of seriousness can only be carried out on the basis of the general risk pertaining to the categories of data in question.

The Court observed that the question of admissibility in evidence of communications data obtained by general and indiscriminate retention or access contrary to EU law is, in principle, a matter for national, not EU, law. However, it went on to reiterate its holding in *La Quadrature*: the principle of effective exercise of rights conferred by EU law means that where defendants are not in a position to comment effectively on the information and evidence obtained, and they pertain to a field of which judges have no knowledge and are likely to have a preponderant influence on the findings of fact, then even though there are no EU rules on the matter national criminal courts are required to disregard information and evidence obtained by means of general and indiscriminate retention of, or access to, traffic and location data in breach of EU law.

As to the question of independence of review, the Court repeated its previous caselaw that in order to ensure that conditions for access to the data in question are fully observed, it is essential that access be subject to a prior review by a court or independent administrative body, or within a short time in cases of duly justified urgency. The court or body must be able to strike a fair balance between the interests relating to the needs of the investigation and the fundamental rights to privacy and personal data protection of the persons whose data are concerned by the access.

It went on to hold that an independent administrative body must have a status enabling it to act objectively and impartially and must be free from any external influence. The authority must therefore be a third party in relating to the authority requesting access to the data, must not be involved in the conduct of the criminal investigation, and must have a neutral stance vias a vis the parties to the criminal proceedings. That is not the case for a public prosecutor. That cannot be made up for by subsequent review by the court.

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
27 January	Rancom Security Limited	Monetary penalty of £110,000	The ICO has fined Rancom Security Limited ("Rancom") £110,000 for making more than 850,000 unsolicited direct marketing calls to promote and sell their security services. The ICO and TPS received 94 complaints, and of the 851,392 calls made, 565,344 were to TPS registered users. Rancom explained that it had purchased TPS screened data from third parties and had acquired data from other security companies it had taken over. Rancom advised that no further due diligence or screening of the data was carried out. However, the ICO found that Rancom did not take reasonable steps to prevent contravention with PECR. Rancom could not provide evidence of consents, nor of screening against the TPS register. Rancom also claimed it operated an internal suppression list, however complaints alluded to multiple calls to the same number despite suppression requests, and therefore any such system was ineffective. Rancom believed the data was TPS screened and used third party contracts as evidence. However, this did not absolve Rancom of its responsibilities to ensure that the data they used was compliant. The contracts: (i) contained non-liability clauses stating the data provided may not be accurate, and (ii) were not dated or signed. Rancom also allowed other organisations to use its telephone lines and did not record the number of calls made by these organisations. Overall, the ICO stated that Rancom exhibited poor business practice.
27 January	Solar Style Solutions Limited	Monetary penalty of £90,000	The ICO has fined Solar Style Solutions Limited ("SSSL") £90,000 for making 188,665 unsolicited calls for direct marketing purposes. 126,019 were to TPS registered users, generating 29 complaints. SSSL did not screen the data against the TPS register, nor was there evidence of consent being obtained. There was no evidence of contractual provisions between SSSL and its data providers, or of due diligence checks being carried out to ensure the veracity of the data being obtained. The ICO referred to its direct marketing guidance, which states that organisations acquiring marketing lists from third parties must undertake rigorous checks to satisfy themselves that the personal data was obtained fairly and lawfully. Further, organisations must ensure that appropriate consent is obtained for passing details along for direct marketing purposes. SSSL did not undertake such checks.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			By its own admission, SSSL did not undertake steps to ensure the integrity of the data it was purchasing and did not provide evidence that the protection and privacy of subscribers was factored into the purchase of data with its providers.
27 January	Chameleon Marketing (H.I) Ltd	Monetary penalty of £100,000	The ICO has fined Chameleon Marketing (H.I) Ltd ("CML") £100,000 because CML made 617,323 direct marketing calls to people registered with TPS between 17 March and 2 July 2019. The calls promoted boiler replacements and resulted in 52 complaints from the public. CML first came to the attention of the ICO when multiple complaints about CML were identified within the monthly TPS reports. The organisation identified within the complaints was the "Home Heating Service", confirmed later to be CML using "Home Heating Centre" and "payasyousaveboilers.co.uk" as trading names. CML informed the ICO that there was a period of approximately 5 weeks when CML's director delegated telesales operations to another individual. CML did not know that the individual had bought data that was not GDPR or TPS screened. Whilst there was a spike in both complaints and calls to TPS registered numbers corresponding to the period in which CML's director had delegated the telesales operations, there were a substantial number of calls outside this period. In particular, CML continually called subscribers who had asked for their details to be supressed. The ICO was satisfied that CML had failed to take reasonable steps to prevent contravention with PECR.
27 January	Repair & Assure Ltd	Monetary penalty of £180,000 Enforcement Notice	The ICO has fined Repair & Assure Ltd ("RAL") £180,000 for making over a million nuisance calls between 2 January and 11 June 2019. The ICO and TPS received 88 complaints about the calls, which all related to washing machine warranties. RAL initially advised the ICO that its "opt in" data was obtained from 12 third party suppliers and it did not screen against the TPS register. It was subsequently found that all the data was collected via telephone marketing surveys. The ICO stated that its direct marketing guidance is clear; informed consent cannot be established when an individual has been asked to agree to third party marketing prior to being informed who the third-party organisations actually are (as occurred in this case). Organisations buying marketing lists from third parties must conduct rigorous due diligence, including ensuring they have the necessary consent. The ICO also issued an enforcement notice requiring RAL to comply with Regulation 21 of PECR within 30 days of the notice.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
28 January	Seafish Importers Limited	Monetary penalty of £10,000	Between 23 August 2019 and 7 April 2020, 491,995 direct marketing messages were sent by Seafish Importers Limited ("Seafish"). Of those messages, 276,866 were sent during the height of the Covid-19 pandemic and related to the sale of face masks. These messages contained direct marketing material for which subscribers had not provided valid consent. The data of these recipients had been obtained by a sticker manufacturer when purchasing stickers. These individuals cannot have expected to receive unsolicited direct marketing in relation to face masks. This resulted in the ICO fining Seafish £10,000.
12 February	House Guard UK Limited	Monetary penalty of £150,000	In this case, House Guard UK Limited made 699,996 nuisance calls between 8 May and 31 December 2018. Almost half of these calls were made to TPS registered numbers, without House Guard conducting any due diligence on the data provided to them. The marketing calls were made to numbers registered with the TPS for more than 28 days, without consent being provided. The ICO received 91 complaints from TPS subscribers about unsolicited direct markings calls made by the House Guard. The monetary penalty notice has been given for a serious breach of Regulation 21 of PECR, which applies to the making of unsolicited calls for direct marketing purposes.
12 February	Call Centre Ops Limited	Monetary penalty of £120,000	The ICO issued a fine of £120,000 for making unlawful marketing calls to numbers registered with the Telephone Preference Service (TPS). The ICO's investigation found that Call Centre Ops made 159,461 unsolicited direct marketing calls to TPS registered numbers between 1 May and 30 October 2019. Furthermore, Call Centre Ops was unable to demonstrate that it held valid consent from the individuals to make the direct marketing calls. Several complaints regarding the calls were received via the ICO reporting tool and the TPS. The monetary penalty notice was given for a serious contravention of Regulation 21 of PECR, which applies to the making of unsolicited calls for direct marketing purposes.
18 February	Just Hype Ltd	Monetary penalty of £48,000	Just Hype sent over 2 million unsolicited text messages about free face masks between 1 June 2019 and 12 June 2020 through a third-party SMS messaging platform provider. Individual complaints about Just Hype's direct marketing campaign were brought to the attention of ICO via ICO's online reporting tool or via the GSMA's Spam Reporting Service. The contact details had been sourced from Just Hype's own customers during the checkout process when purchasing items on Just Hype's website. Just Hype did not make clear to customers about how

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			their data would be used and how they could opt out of receiving marketing messages. Individuals were not given, at the point of their data collection, the means of refusing the use of their contact details for direct marketing. In addition, after an internal investigation into the complaints, Just Hype informed the ICO that its SMS platform provider combined distribution lists belonging to multiple companies, including Just Hype, resulting in messages being also sent to subscribers who were not Just Hype customers. The ICO found that Just Hype had not meet the requirements to be able to rely on the soft opt in requirement and was therefore in breach of Regulation 22(3) of PECR.
25 February	Valca Vehicle and Life Cover Agency Ltd	Monetary penalty for £80,000 Enforcement Notice	The ICO has fined Valca Vehicle and Life Cover Ageny Ltd (Valca) £80,000 for sending unsolicited marketing messages during the pandemic. Valca specialises in lead generation for financial products. Following 114 complaints from the public to the ICO, the company was found to have sent more than 95,000 unsolicited direct marketing messages from 15 June to 20 July 2020 without the recipients' consent. The messages referenced the pandemic and were designed to appeal to individuals whose finances have been adversely affected. This, in the ICO's view, was a clear attempt to profiteer from the health crisis. The ICO outlined that, among other things, Valca had failed to include an opt-out in its unsolicited direct marketing messages until the ICO's initial investigation letter, which was in contravention of Regulation 23 of PECR. Furthermore, the ICO noted that, despite being under investigation, and even though it had been notified that a number of complaints had already been received, Valca continued to send unsolicited messages to its database. The ICO also issued an enforcement notice requiring Valca to comply with Regulation 22(3) PECR within 30 days of the notice.
3 March	Muscle Foods Limited	Monetary penalty of £50 000 Enforcement Notice	Muscle Foods Limited (MFL) sent over 1 million unsolicited marketing emails and over 6 million unsolicited marketing SMS messages to individuals without their consent. The ICO received 27 complaints about the emails and 7 complaints about the SMS messages. MFL customers that placed an order were automatically opted in to receive marketing and could only update their marketing preferences, including opting out, after an order had been placed. Thus, the individuals were not given a simple means of refusing the use of their contact details for direct marketing purposes at the time the details were initially collected (as required by the soft opt in requirements).

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			In deciding the severity of the contravention, the ICO took into account that MFL had continued to send direct marketing emails to individuals without apparent remedial measures to prevent further breaches of Regulation 22 of PECR in the time since the ICO's investigation had begun up to the date of the monetary penalty notice. The ICO also issued an enforcement notice requiring MFL to comply with the soft opt in rules under Regulation 22(3) within 35 days of the notice.
5 March	Leads Work Limited	Monetary penalty of £250,000 Enforcement Notice	Between 16 May and 26 June 2020, Leads Work Limited sent 2,670,140 marketing text messages to individuals without their consent, in breach of Regulation 22 of the PECR. The text messages had the following content: "In lockdown and want to earn extra cash? Avon is now FULLY ONLINE, FREE to do and paid weekly. Reply with your name for info. 18+ only. Text STOP to opt out." The 7726 SPAM reporting tool received 12,281 complaints about these texts, over a period of 41 days, which were then brought to the attention of the ICO. The ICO outlined that the largest data suppliers of Leads Work Limited shared vague consent statements which did not constitute informed and specific consent to send direct marketing texts to individuals. Moreover, from reading these consent statements, individuals could not have reasonably be expected to know that Leads Work Limited were linked to Avon. The text messages appeared to be sent by Avon Cosmetics Limited as Leads Work Limited had deliberately not identified itself in the body of the texts as the sender, to avoid confusing recipients. Furthermore, the ICO took into consideration, when deciding to impose the monetary penalty, that Leads Work had continued to run the marketing campaign both during, and since the ICO's investigation, without attempting to amend or review its practices. Moreover, the ICO found that Leads Work failed to inform the ICO of its marketing methods, including email marketing. The ICO also found that there were no mitigating factors to be considered. In addition, the ICO issued an enforcement notice requiring Leads Work Limited to comply with Regulation 22(3) PECR within 30 days of the notice.

Other recent articles

Connected vehicles – Finalised guidelines from the EDPB

HR Essentials

Governments around the world are now racing to approve and roll out various vaccines in an attempt to gain control over the spread of the virus. There are pressing employment and data protection issues around this in relation to the workplace and more broadly, including around requesting and handling information regarding employee vaccine status, mandating vaccination for access to workplaces, and more. To address this, we have updated our COVID-19 chart which has been developed to help employers prioritise and understand these questions through a traffic light system, as well as detailed responses to some pressing questions.

For any organisation, equality, diversity and inclusivity are key cornerstones to building a strong, engaged and open workforce. Often, the first step for many employers is to collect data from their employees and other members of staff on a range of matters in this area. Bird & Bird has produced guidance to help you.