Bird & Bird

UK & EU Data Protection Bulletin: September 2020

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

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

United Kingdom

ICO

UK Cases

EU and Council of Europe

EDPB

CJEU Cases

UK Enforcement

ICO Enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
July 2020	**Regulatory approach continues to evolve for COVID 19 and beyond** On 14 July 2020, the ICO released a (slightly) updated version of its document setting out the body's regulatory approach during the coronavirus public health emergency. In an accompanying blog, the Commissioner explained just a few additions had been made to policy, e.g. to reflect that the ICO may now carry out audits remotely, given contact and travel restrictions. However, it maintains the view that it will continue to exercise an "empathetic and pragmatic" approach. The ICO's original document was released in April 2020; you can read about it in our previous update here. Similar views apply to the regulation of the Freedom of Information Act and the Environmental Information Regulations although the ICO has now stated that it expects to see public authorities putting clear plans in place to get back on track with their freedom of information work. To help with this, they have launched a FOI toolkit designed to help public authorities self-assess performance in responding to FOI requests. The toolkit can be completed in stages or in full and generates a bespoke report which helps to identify areas for improvement and where action needs to be taken.
August 2020	**Guidance for teachers and schools on students' access to information about their exam results** The ICO has published guidance for teachers and schools on students' access to information about their exam results during the coronavirus pandemic. **Legal Background** Schedule 2 Part 4 Paragraph 25 of the Data Protection Act 2018 ("**DPA**") contains an exemption to the following General Data Protection Regulation 2016/679 ("**GDPR**") rights as regards personal data consisting of *information recorded by candidates* during an exam ("**Exam Script Exemption**"): • The right to be informed (Articles 13 and 14 GDPR); • The right of access (Article 15 GDPR); and • All the principles (Article 5 GDPR) insofar as they relate to the above rights, ("**Listed GDPR Provisions**"). Conversely, the Exam Script Exemption does not apply to personal data consisting of information *recorded by the data controller (e.g. the marker)* in order to determine the exam results or in consequence of that determination. Schedule 2 Part 4 Paragraph 25 DPA does,

Date	Description
	however, govern the timeframes within which a data controller must comply with a request for this information if such a request is made before the results are announced. These timeframes are: • Within five months of receiving the request; or • Within 40 days of announcing the exam results, if this is earlier. **How does the Exam Script Exemption apply to the coronavirus pandemic?** As a result of the pandemic, pupils did not sit exams at the end of the 2019/2020 academic year. Exams results were instead based on teacher assessments. The ICO has confirmed that the Exam Script Exemption *does* apply as regards requests made in respect of exam results for this academic year. Applying the exemption: (i) teachers and schools are exempt from complying with the Listed GDPR Provisions as regards personal data consisting of information recorded by pupils (e.g. mock exam answers or assignments used to assess their results); (ii) teachers and schools are not exempt from complying with the Listed GDPR Provisions as regards personal data consisting of information recorded by them (e.g. teacher assessments, rank orders and/ or email exchanges discussing the same); (iii) but if a request for such information is made before the official results were announced, teachers and schools have longer to respond. The ICO makes clear that if schools decide to take a 'proactive approach' and provide students with results or rank order information notwithstanding whether they received a request for that information, the schools should be transparent about this and provide advance notification that they are doing this and consider publishing additional information to enable pupils to understand this information and the context within which it was determined. The ICO finally briefly covers the interaction between the Exam Script Exemption and the exemption contained in Schedule 2 Part 3 Paragraph 16 (i.e. the 'third party exemption'), particularly regarding the disclosure of rank orders. After determining that a particular data subject's rank order could reveal personal data about other students; the data controller must determine whether it is reasonable to disclose the latter's personal data. Unsurprisingly, the ICO confirms that this assessment should be made on a case-by-case basis; and provides fairly common sense examples e.g. confirming that a student 'ranks top of the grade' is unlikely to reveal personal data about the rest of the cohort whereas disclosing the specific rank order of a smaller cohort (i.e. 2/3 pupils) will need more careful consideration.
August 2020	**Finalised Guidance to AI and Data Protection** As previewed in our March newsletter, the ICO has now finalised and issued its guidance on Artificial Intelligence – a comprehensive document exploring how to ensure that the design and use of artificial intelligence complies with EU and UK data protection law. This includes thoughtful guidance on core GDPR concepts like who is a controller or a processor of AI-processed data; what lawful basis to use for AI; and how to deploy AI without falling foul of GDPR and Data Protection Act 2018 rules such as those requiring data minimisation, transparency, mitigating discrimination, ensuring individual rights around potential automated decision-making, and system security. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

Date	Description
2 September 2020	**ICO's Children's Code in force** The ICO's Age Appropriate Design Code (the "Children's Code") has completed the parliamentary process and came into force on 2 September, with a 12-month transition period to give affected organisations the chance to conform. This applies to organisations providing online services and products likely to be accessed by children up to the age of 18. The Children's Code sets out 15 standards for designers of online services and products and how they should comply with data protection law. The code will require digital services to automatically provide children with a built-in baseline of data protection whenever they download a new app, game or visit a website. We will be issuing further updates on this Code in due course. The ICO has set up a new Children's Code hub to support relevant organisations and will be offering a series of webinars throughout September. The ICO is also interested in hearing from organisations who are looking at cutting edge personal data projects dealing with the issues posed by the implementation of the Children's Code and is inviting organisations to apply for places in its free regulatory Sandbox.

UK Cases

Date	Cases
4 June 2020	**ST (A Child) v L Primary School (2020) EWHC 1046 (QB)** **Compensation for misuse of private information** In this case, the High Court examined a claim brought by a child and her mother against the child's primary school, i.a. for breach of the Data Protection Act 1998 and for misuse of private information. The claim related to the school sending out - without the mother's consent- a letter to 60 parents with information about the child's condition (Down Syndrome) and her disruptive behaviour, with a view to reassuring them that the school's staff could handle the situation. The Court held that by sending the letter, the school breached the principle of fair and lawful processing; however, it did not award damages for this breach to either claimant. It held that the mother could not recover damages as under the DPA only the data subject is entitled to compensation. The Court did not award damages to the child either, as it found that there was no clear evidence that the child was informed of the sending of the letter and distressed by it. The Court further upheld the claim for misuse of private information and awarded damages to the claimants under this head. The Court held that both claimants had a reasonable expectation of privacy about the information in the letter and the school could not show that the disclosure was justified. To calculate the damages, the Court followed TLT (*TLT and others v Secretary of State for the Home Department and the Home Office [2016] EWHC 2217 (QB)*), in which damages ranging from £2,500 to £12,500 were awarded to asylum seekers whose private information had been accidentally posted on a website by the Home Office. Those damages were calculated taking into account the claimants' loss of control over their information and the impact of the data breach upon each of them; also, taking into account awards made for psychiatric or psychological injury in personal injury cases to ensure that any award would not be out of kilter with them. On this basis and in light of the limited evidence of the direct impact on the child of the sending of the letter, the child was awarded £1,500. The mother was awarded £3,000, which the Court considered that properly reflected the distress she suffered.
8 July 2020	**(1) Petr Aven (2) Mikhail Fridman (3) German Khan V Orbis Business Intelligence Ltd (2020)** **Unfair use of personal data in the Trump-Russia investigations** Orbis, an intelligence consultancy, was commissioned by a law firm to provide intelligence relating to the investigation on the links between Donald Trump and Russia. The law firm had been instructed to do this by their client, the US Democratic Party. The Orbis report was disclosed to the US consultancy Fusion and to UK politicians, as well as to the Democratic Party which has commissioned it. The claimants stated that the report contained inaccurate information about them, which has been processed unfairly or unlawfully in the

Date	Cases
	report. The claimants requested Orbis to rectify the data. The case was brought under the old Data Protection Act 1998, as the claim was brought prior to the new Act coming into force. The court considered, amongst other issues, whether the report contained personal data about the claimants and, if so, whether legal privilege could apply to the report and whether the data was inaccurate and processed unfairly. The cases raises interesting points about the definition of sensitive personal data, the application of legal privilege and how accuracy principle applies to opinions. **Implication of criminality amounts to sensitive personal data** The first issue was straightforward to establish, as the report contained biographical information on the claimants. The court held that, because the report stated that the claimants had had "illicit cash" delivered to Vladimir Putin, and therefore implied that the claimants has been involved in something criminal, the report contained sensitive personal data. The report did not refer to any specific criminal offence, but the reference to something "illicit" was enough to class this as sensitive personal data. **Legal purpose exemption** The court considered whether the content of the report could be covered by the legal purpose exemption, i.e. whether the processing was exempt from complying with the first data protection principle because it is done in the context of obtaining legal advice. Orbis had sent the report to the consultancy Fusion, who in turn had shared it with the Democratic Party's law firm. Although the Democratic Party clearly had political aims, the commissioning of the report was also for the purposes of receiving legal advice. As it was the law firm that commissioned the report, and their dominant purpose in doing so was to give legal advice to the Democrats, the fact that Orbis disclosed the report to Fusion does not defeat the legal purpose exemption, as the disclosure was still considered to be necessary to the law firm's provision of legal advice to the client. This is interesting as it provides a relatively broad interpretation of the exemption which may prove helpful in connection with the similar provisions in the Data Protection Act 2018 at Schedule 2, Part 1 (5) (although note that the exemption here is worded slightly differently). **Fairness and accuracy** The court found that the use of the claimant's data in the report was fair and lawful, as the processing was necessary for US national security. There was good legal bases for all the onward disclosures: the legitimate interest and contractual commitments of both Orbis and the Democratic party. The one point that the court found in the claimant's favour was the accuracy point. The transfer of "illicit cash" to Putin was found to be untrue, and Orbis was required to mark up the report with this finding. Although the report stated that the this information had been provided by sources, Orbis should have done more to ensure that these allegations were verified.
6 August 2020	**Johnson v Secretary of State for the Home Department [2020] EWCA Civ 1032** This Court of Appeal case concerned the lawfulness under GDPR of the transfer of personal data to the British High Commission in Kingston, Jamaica for the purposes of an out of country appeal. The appellant (the data subject) argued that such a transfer was not

Date	Cases
	permissible absent his consent and, as a consequence, the only way to ensure that he could exercise his rights was to permit him to exercise a right of appeal in the UK. The Court of Appeal dismissed the appellant's appeal. The Court considered the data subject's right to object and concluded that the exemption under paragraph 5 of Schedule 2 of the DPA 2018 applied – i.e. the transfer and disclosure of the data was necessary for the purpose of, or in connection with, legal proceedings (the appeal). Under section 92(3)(a) of the Nationality, Immigration and Asylum Act 2002, the appellant could only appeal out of country. The appellant argued that the out of country appeal need not take place if there was an in country right of appeal, and that would be a less intrusive and therefore a more proportionate way of protecting the appellant's legal rights. However, Dingemans LJ concluded that the fact that an appeal could take place in the UK "*does not mean that the out of country appeal ceases to be judicial and legal proceedings, or that it becomes disproportionate to permit the transfer of data. This is because the legal proceedings must be fair, the data is needed to ensure that*". The Court held that the transfer of data to the British High Commission amounted to a transfer to a third country for the purposes of Article 45 of the GDPR and such transfer was justifiable pursuant to Article 49(1)(e) of the GDPR (i.e. the transfer was necessary for the establishment and defence of legal claims). Interestingly, the Secretary of State advanced an argument that the transfer of personal data to Home Office officials in Jamaica was not, in reality, a transfer of personal data to a third country as it never left the control of the Home Office. This was not a determinative point in this case, so the Court said they would leave this to be resolved fully upon another occasion. Though Dingemans LJ said he saw "real difficulties" in this argument and Green LJ stated that he "*disagree[s] that one can, in effect, read into Article 46 a complex limitation based on consular and diplomatic premises and a test based upon the "sole control" of a Member State. That is simply not what the GDPR says and there is in [Green J's] view no basis upon which this can be inferred from the much broader words "transfers of personal data to third countries*".
11 August 2020	**R (Bridges) -v- Chief Constable of South Wales Police & Ors [2020] EWCA Civ 1058** On 11 August 2020, the Court of Appeal ("CA") ruled that the use of facial recognition technology ("FRT") by the South Wales Police ("SWP") was unlawful due to the lack of a sufficient legal framework that would regulate the deployment of FRT by the law enforcement bodies in public places. The CA overturned the Divisional Court's judgement which had determined that the lack of sufficiently defined legal framework could be excused by the fact that the FRT was a novel technology and that the existing primary and secondary legislation cumulatively provided a general legal framework sufficient to make the processing lawful. The CA noted that lawfulness is a binary question and there would be no exceptions made even if the law has not caught up with a new technology yet. CA was predominantly concerned by the wide and unchecked discretion left to the law enforcement officials in the absence of a clear legal framework (specifically in relation to "who can be placed on an FRT watch list" (e.g. which kind of crimes would qualify for being placed on a watch list) and "where can the FRT be deployed" with the first question often answering the latter).

Date	Cases
	The Court contended that Chapter 3, DPA 2018 did not provide a sufficient legal framework for the use of FRT by law enforcement bodies and nor was it intended to do so. It further noted that secondary legislative instruments in the form of codes of practice issued under primary legislation as well as SWP's own policies would also amount to a legal framework, however in the case at hand none of these were present and therefore the necessity test under Article 8(2) of the Human Rights Act1 was not satisfied. The ICO also welcomed the CA decision as a useful step to balance people's right to privacy against the surveillance technology that the police need to carry out their work effectively. It is important to note that whilst the CA ruled the SWP's past uses of FRT unlawful, this does not mean a ban on future uses of FRT by law enforcement bodies if a clearer legal framework is drafted. The drafting of new primary and secondary laws and law enforcement policies for this purpose was actively encouraged by the court in its ruling. However, although the case did not discuss the private sector's use of FRT, this may not be the case for the private sector's use of FRT. Where a private entity intends to deploy FRT for the purposes of detection and prevention of crime, it may need to resort to data subject's explicit consent due to their lack of power to create a legal framework. This would then bring the issues surrounding a valid consent under GDPR standards which would have to be specific, informed, freely given (i.e. without a detriment if consent is refused).

[1] Art 8(2) HRA 1998 "*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

EU and Council of Europe

EDPB

Date	Description
17 July 2020	**New EDPB Guidelines on the interplay between PSD2 and GDPR** On 17th July 2020, the European Data Protection Board ("EDPB") adopted the long-awaited Guidelines 06/2020 on the interplay between the Second Payment Services Directive and the GDPR (the "Guidelines") for public consultation. The Guidelines largely confirm the EDPB's previous views on the two laws. For example, the EDPB states consent under PSD2 is 'contractual consent' which corresponds to processing necessary for the performance of a contract under Article 6(1)(b) of the GDPR. There will be some areas in the Guidelines that payment service providers will need to consider more closely. For example, according to the EDPB any further processing of personal data beyond the provision of an AIS or PIS is automatically incompatible and can only be carried out if required by EU or Member State law or with the (GDPR) consent of the payment service user. Taking this to its logical conclusion, the Guidelines create a possible dual regime for Open Banking depending on whether the payment service user is a natural or legal person. The Guidelines also address the obligations of payment service providers when processing the personal data of individuals other than the specific payment service user — known as silent parties. The approach in the Guidelines to silent party data is not necessarily controversial but does raise concerns about how payments services providers can technically implement the EDPB's recommendations. For example, the EDPB explains that payment service providers cannot obtain the silent party's consent (in GDPR terms) for any further processing of their data but may, at the same time, be required to collect their explicit consent when processing special category data (e.g. health data). The EDPB's public consultation closes on the 16 September 2020 and feedback can be provided using the form available here.
22 July 2020	**Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA** The EDPB has adopted an information note outlining the steps that organisations which have the ICO as their BCR Lead Supervisory Authority will need to take in preparation for the end of the Brexit transition period (31 December 2020) to ensure they have identified a new BCR Lead in the EEA. The note confirms that: "For BCRs already approved under the GDPR, the new BCR Lead SA in the EEA, as the new competent Supervisory Authority ("SA") in accordance with Article 47.1 GDPR, will have to issue a new approval decision following an opinion from the EDPB before the end of the transition period".

	However for BCRS for which the ICO acted as BCR Lead Supervisory Authority under Directive 95/46/EC, no approval will have to be issued by the new BCR Lead Supervisory Authority in the EEA. Either way, it is likely that organisations having the ICO as their current lead will need to amend their BCRs with reference to the EEA legal order before the end of the Brexit transition period and to assist with this process, the note includes a checklist of elements that are likely to need amending. Most are fairly straightforward but organisations should note the need to ensure that the legal instrument used to make the BCR binding references an EEA contract law rather than the laws of England and also that under the BCRs for processors, it is necessary to ensure that the service agreement used to make the BCR-P binding towards the controllers is signed on the side of the group of undertakings/enterprises by a BCR Member in the EEA. EDPB notes that organisations should have already updated their BCRs under GDPR in accordance with the requirements in WP256 rev.01 and WP257 rev.01 but points out that a new EEA BCR Lead remains in a position to verify whether such updates have in fact been made and to request further changes if required. The ICO has also confirmed to us in recent correspondence that where BCRs continue to be relied on in the UK after the end of the transition period, this will require a separate set of documents which remove references to the EEA and focus on the UK legislative framework Note that this note is without prejudice to the EDPB's analysis on the consequences of Schrems II for BCRs as data transfer tools. For a copy of the full note, please see here.
24 July 2020	**EDPB FAQs on the Schrems II decision** On 24th July, the EDPB provided further "guidance" on the CJEU Schrems II decision. It was hoped that this would provide more clarity on how the judgment now needs to be implemented by companies that transfer personal data to countries outside the EEA. However, whilst the EDPB addresses important questions it still appears to struggle with the consequences of the Court's judgment. It is still in the process of analysing the kind of supplementary measures that may be provided in addition to SCCs or BCRs to provide a sufficient level of guarantees. For more detail on the main takeways of these FAQs, please see our separate news alert on this which we sent out over the summer. The EDPB met again on 2 September to discuss next steps and possible supplementary measures. We understand that it has set up a Supplementary Taskforce as a follow up to FAQs but no further guidance has been released at the time of writing. Further, we understand that finalising the SCCs (primarily to update for GDPR) has become a top priority for the Commission although there is no official release data yet.

<< Back to table of contents

CJEU

Date	Description
16 July 2020	**Schrems II judgment: Privacy Shield invalid, SCCs survive, but… what happens now?** Of course, one of the most significant developments over the summer months was the CJEU Schrems II decision on 16th July which invalidated the EU-US Privacy Shield Framework but also made important statements concerning the continued use of Standard Contractual Clauses for data transfers. As we reported on this in detail earlier in the summer, we have not repeated again here but here is our original news alert in case you missed it.

UK Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
02 July 2020	Decision Technologies Limited (DTL)	Monetary penalty - £90,000	DTL, a price comparison and technology company, was fined £90,000 for not checking whether the email marketing companies it used had obtained valid consents for around 16 million direct marketing emails sent on its behalf. The ICO found DTL to have instigated the transmission of these emails and was therefore in contravention of Reg.22 PECR. DTL had utilised the email marketing services of 2 Aggregators who had themselves used a series of List Owners to engage in the actual sending of the emails. DTL relied on 'indirect consent' as it was the List Owners who obtained consent and sent the direct marketing material on behalf of DTL. DTL confirmed that all due diligence on the data was to be carried out by the Aggregators and DLT had placed contractual obligations on the Aggregators to comply with all relevant legislation. However, on further investigation, the ICO found that the consents that had been obtained were not valid as they were not freely given, specific or informed enough. Furthermore the ICO also advised that DLT should have carried out additional due diligence on the List Owners: "48. Reasonable steps could have included for instance carrying out the necessary due diligence checks to ensure that DTL were specifically named within the Privacy Policy of the five List Owners as the holder of the marketing lists. That they are not, and that 'comparison websites' as a sector was listed in just one of the five List Owners' policies, should have alerted DTL that there may be issues in demonstrating that subscribers were adequately informed. Furthermore, if they had completed the customer journey it would have been apparent that, in some cases, agreement to marketing was a condition of service, and that subscribers often had no way of specifying the sectors they might wish to hear about, or the method by which they may wish to receive marketing. DTL advise that it relied wholly on a contractual agreement with the Aggregators as evidence of its due diligence, however the Commissioner is of the view that the reliance on indirect consent, and the more stringent checks that it requires of organisations, should have caused DTL to conduct its own checks into the veracity of the data being used by the List Owners, rather than to rely on assurances." This case serves as a timely reminder of the difficulties for organisations in relying on indirect consent. DTL's failure to maintain its own records of its direct marketing activities played an aggravating factor in the Commissioner's decision to issue a monetary penalty. However, DTL's change of business model

			and termination of the services provided by the Aggregators and List Owners for direct marketing, acted as a mitigating factor in the Commissioner's decision.
03 Aug 2020	Rain Trading Ltd. (RTL)	Monetary penalty - £80,000	RTL was fined £80,000 for making over 270,000 unsolicited callers to individuals on the TPS Register without the valid consents being in place in breach of Regulation 21 of PECR. RTL came to the attention of the Commissioner when a particular Caller Line Identity (CLI) was identified in the ICO's 'Monthly Threat Assessment' as being a CLI used by one of the organisations responsible for generating the most complaints that month via the TPS. The ICO subsequently discovered a number of other CLIs which had been allocated to RTL and which had generated a total of 99 complaints. In response to initial investigations by the Commissioner, RTL claimed the data it was using for direct marketing had been purchased "under contract" from two third party data providers, that consent was not recorded and it was thought that the due diligence had been carried out by the third parties and therefore there was no system in place to allow RTL to run the list against the TPS register or internal suppression lists. However, following further correspondence RTL failed to provide copies of these contracts and gave no further assurances regarding due diligence. As such, the ICO concluded that RTL was indeed in breach of Regulation 21 of PECR. Reasonable steps should have included: • Asking the third party data providers for evidence that the subscribers had consented to receiving the calls from RTL; • Screening the data against the TPS register itself regardless of any assurances given by the providers of the data; and • Ensuring that it had in place an effective and robust suppression list.

12 Aug 2020	Koypo Laboratories Ltd. (Koypo)	Monetary Penalty & Enforcement Notice	Koypo, a lead generator specialising in scientific customer acquisition, was 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, it was the "instigator" and would require explicit consent from the recipients that they want to receive the emails before they were sent. Koypo was not 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.

Schrems II

Of course, one of the most significant developments over the summer months was the invalidation of Privacy Shield in the CJEU Schrems II case. We have been reporting on this in separate news alerts but you can find the articles again here and here in case you missed them.

HR Essentials: Diversity and Inclusion

The Black Lives Matter (BLM) protests have prompted many employers to reconsider their approach to diversity across their workforce. In our recent article, we consider the implications of the BLM protests and steps that employers can and should be taking to support diversity and protect their business.