Bird & Bird

UK & EU Data Protection Bulletin: November 2019

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

Information Commissioner's Office (ICO)

Date	Description
	ICO – DSARs for the Public The ICO has published new guidance on subject access requests but this time from the point of view of the data subject. The guidance explains briefly what a SAR is, how to make a SAR (including a template), what companies have to do and how a data subject can complain if they're not satisfied with the outcome. The ICO's guidance on submitting a request aims to limit the amount of back and forth with a data subject by focussing the letter on the SAR and providing helpful and relevant information up front such as a list of the data being requested, information used by the organisation to distinguish the individual from others, search criteria, etc. The ICO suggests clearly labelling the request as a SAR which will help organisations to identify SARs. The ICO provides a template letter demonstrating its recommendations. The template limits the requested data but this is not to say that a request for "all personal data" is not still valid. The new guidance reiterates previous guidance for organisations that requests can be made orally and that data subjects can't be forced to use the organisation's standard form. Finally within this section, the ICO strongly recommends keeping a copy and proof of postage/delivery of a request for use when making a complaint etc. The guidance then answers a number of questions regarding the obligations on organisations to comply and what the data subject can expect to receive. The guidance is clear that a data subject is not entitled to receive full copies of original documents which is a misconception many data subjects have at the outset of the process. The guidance briefly mentions exemptions but does not go into detail on this, instead referring to the guidance for organisations. Finally the ICO recommends that when a data subject is not satisfied with the response (or lack of response) to their SAR they should first complain to the organisation before reporting the matter to the ICO. Again the ICO provides a template letter that can be sent to organisations.
	Agreement reached between ICO and Facebook The ICO and Facebook have reached an agreement over the ICO's investigation into Facebook over Cambridge Analytica. On 24th October 2018, the ICO issued a monetary penalty notice of £500,000 against Facebook following the ICO's Cambridge Analytica investigation. Facebook appealed the notice – alleging bias on the part of the ICO, due to comments in the press by the Commissioner, and that the ICO's enforcement process was procedurally unfair. An interim decision was issued in June 2019, confirming that these allegations could form part of the appeal and requiring the ICO to disclose relevant materials. The ICO appealed this decision. The ICO and Facebook have now reached an agreement on the matter: each of the ICO and Facebook will withdraw their appeals and Facebook will pay the £500,000 (but on the basis that this is without any admission of liability). The ICO and Facebook have also agreed a joint statement in which Facebook notes that the ICO has found no evidence that data of European users had been disclosed to Cambridge Analytica. See here for more.

<< Back to table of contents

UK Cases

Date	Description
4 September	**R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341** The Divisional Court has dismissed a challenge against use of Automated Facial Recognition technology ('AFR') by South Wales police ('SWP') which was brought on the basis of interference with the right to privacy and breaches of data protection and equality laws. The Court found that SWP's use of AFR was intrusive, but lawful and justified. However, this should not be interpreted as a 'green light' for controllers considering use of facial recognition technologies in all contexts – in the August edition of our Data Protection Bulletin (available here) we reported on a SEK 200,000 fine imposed by the Swedish Supervisory Authority on a municipality using facial recognition to pilot an initiative for monitoring student attendance at a school without an appropriate lawful basis (amongst other issues). **Background** The challenge was brought by Edward Bridges (supported by Liberty), a civil liberties campaigner living in Cardiff. SWP is the national lead on use of AFR in policing in the UK and has been conducting trials of AFR technology since 2017. The challenge brought by Mr Bridges related to a particular, ongoing, trial known as "AFR Locate", which involves deployment of surveillance cameras to capture digital images of members of the public. The images captured are subsequently processed to extract biometric information (i.e. measurements of facial features) and compared with biometric information about individuals on various 'watchlists' compiled by SWP. Where there is a biometric match between an image captured and the watchlist, SWP determines the appropriate action to take. Where there is no match, the biometric data is deleted immediately and the underlying CCTV deleted in accordance SWP's standard 31 day retention period. Mr Bridges did not appear on any of the SWP's watchlists, but Mr Bridges put forward (and SWP accepted) that his image would have been recorded on two particular occasions in 2018 on which the AFR technology was deployed in Cardiff. **The Grounds of Challenge** Mr Bridges brought a judicial review proceedings on the basis that SWP's deployment of AFR Locate was contrary to: • The Article 8 European Convention of Human Rights ('ECHR') right to respect for private and family life, home and correspondence ('right to privacy'); • The Data Protection Act 1998 ('DPA 1998') requirement to comply with data protection principles; • The Data Protection Act 2018 ('DPA 2018') requirements relating to law enforcement processing, namely the requirement that processing for law enforcement purposes is lawful and fair (and requirements to demonstrate such compliance) and the requirement to complete a data protection impact assessment where required; and

Date	Description
	• The Equality Act 2010 ('EA 2010') requirement that SWP, as a public authority, has 'due regard' to the need to eliminate conduct prohibited under the EA 2010 (e.g. discrimination), advance equality of opportunity and when exercising its functions. As this ground does not have significant privacy and data protection implications, we discuss this aspect of the case only briefly in this article. **Article 8 ECHR** The Court dismissed this aspect of the claim. The court found that there was there an interference with Mr Bridges right to privacy (Article 8(1) ECHR), but the interference was justified by the public interest, was conducted in accordance with the law and was proportionate (Article 8(2) ECHR). In reaching its conclusions, the Court found that: • biometric data has 'intrinsically private' character, and the fact that the biometric data is derived from individuals' faces (which are 'manifest' in public) does not undermine this; • 'immediate' deletion of biometric data does not prevent a finding of interference with the right to privacy; • AFR is intrusive, irrespective of the fact that individuals are in a public space when images are collected; • The interference with the right to privacy was in accordance with the law (given SWP's common law powers to prevent and detect crime); and • SWP's use of AFR was proportionate, given that (i.a.) the deployment was transparent, limited (in terms of geography and time), used for specific and limited purposes and involved human review (i.e. before action was taken in the event of a match), and involved 'near instantaneous' deletion of biometric data. **DPA 1998 and DPA 2018** The Court dismissed this aspect of the claim. Biometric data relating to individuals who did not 'match' any individuals on the watchlist was "personal data" (and the activity amounted to "sensitive processing" under the Law Enforcement provisions of DPA 2018), but SWP satisfied the data protection principle requiring fair and lawful processing and had complied with its DPA 2018 obligation to conduct a data protection impact assessment for the processing. The Court determined that: • where there was no match with individuals on a watchlist, the biometric data derived from the CCTV footage still amounted to personal data given that the data could be used to distinguish an individual from all others ('individuation'); • the processing of biometric data didn't breach the first data protection principle under DPA 1998 (requiring fair and lawful processing of personal data) on the basis of the same considerations that were relevant to the Article 8 ECHR claim (above) and concluded that legitimate interests would be the appropriate condition of processing under Schedule 2 DPA 1998; • the processing is 'sensitive processing' as per Article 35(8) DPA 2018 (this is a Law Enforcement provision of the DPA 2018 – this effectively means that under the Law Enforcement provisions, SWP was processing 'special category' type data);

Date	Description
	• the processing satisfied section 35 DPA 2018 requiring fair and lawful processing. As the processing was 'strictly necessary' for law enforcement purposes, it satisfied a Schedule 8 DPA 2018 condition and an adequate (although not optimal) appropriate policy document had been put in place by SWP. • SWP's obligation to undertake a Data Protection Impact assessment ('DPIA') was considered satisfied. The court felt that trying to 'second-guess' the findings of a DPIA undertaken by a controller would be to 'overstep the mark', but where it was 'apparent that a data controller has approached its task on a footing that is demonstrably false, or in a manner that is clearly lacking' then the conclusion would be that the DPIA obligation has not been satisfied. **Equality Act 2010** The Court dismissed this aspect of the claim. The Court found that there was no firm evidence that the AFR technology produced discriminatory results. Mr Bridges had argued that SWP was in breach of EA 2010 requirements on the basis that it failed to have regard to the possibility that use of AFR would produce a disproportionately higher rate of false positive matches for those who are women or from minority ethnic groups, resulting in AFR indirectly discriminating against those groups. The Court found that there was no firm evidence (at the time that the pilot commenced, or now) that AFR in fact produced such results which were discriminatory in this way. The full judgment is available here.
13 September	**(1) Al-Ko Kober Ltd (2) Paul Jones v Balvinder Sambhui [2019] 9 WLUK 139** This case examined a claim for unlawful processing of personal data alongside defamation and malicious falsehood claims made in relation to publishing videos with derogatory content on YouTube. **Background** A stabiliser manufacturing company and its marketing manager brought claims for defamation and malicious falsehood against a competitor who posted on YouTube videos relating to the claimants and their product, a caravan stabiliser. The marketing manager also brought a claim for breach of sections 10 and 13 of the Data Protection Act 1998. The videos published by the defendant showed footage of caravan accidents and footage of the marketing manager speaking about the product in trade shows. The videos contained derogatory comments about the claimants, stating among other things that they were knowingly risking lives and indicating they were lying about their product. Following a successful application for an interim injunction, the defendant was ordered not to publish untrue statements about the claimants and their product and to stop processing the marketing manager's personal data. The defendant failed to comply with the order and the claimants applied for a summary judgment on their claims for defamation, malicious falsehood and breach of data protection legislation.

Date	Description
	Summary judgment: An order for summary judgement was made in the claimants' favour both for the defamation and malicious falsehood claims. In relation to the data protection claims, the judge approved the summary judgment on the claim made under section 10 of the DPA 1998 pursuant to which the claim was contrary to the principle of fair and lawful processing of personal data: the judge did not find there to be a realistic scope for the conclusion that the publication of the marketing manager's personal data in the videos was consistent with any of the lawful grounds of processing set out in Schedule 2 of the DPA 1998. The judge clarified that he did not reach any conclusion on the argument that the processing was in breach of the first data protection principle as being unlawful; any such submission would mean that any act of defamation involving personal data is contrary to the requirements of the DPA 1998, and the judge did not have the authority for that proposition. The judge also considered that he did not have sufficient information and thus did not reach any conclusion on the claim for damages under section 13 of the DPA 1998. In this respect, the judge concluded that the claimant would need to make a further application providing evidence in support of his claims for damages if he wished to pursue this claim for compensation.
1 October	**Automotive Software Solutions Ltd v The Information Commissioner [EA/2019/0083]** In a recent case on the Freedom of Information Act and the disclosure of personal data, the first tier Tribunal held that a local authority could withhold disclosing Vehicle Registration Marks (VRMs) where such disclosure would prejudice the prevention or detection of crime. The case also confirmed that vehicle registration numbers would be personal data, on the basis that they could indirectly identify an individual by querying the owner through the Driver and Vehicle Licensing Agency. The case concerned Mr Hudson (director of Automotive Software Solutions), who requested VRMs from all vehicle licensing authorities under the Freedom of Information Act 2000 (FOIA) in order to create a database of vehicles that had previously been used for private hire or as taxis and were subsequently listed for sale. He did so with a view to publish it in a database that would inform potential buyers on the vehicle's history and consider it when negotiating the purchase price. A number of local authorities provided him with the information he requested. However, Tandridge District Council refused his request on the grounds that car registration numbers were personal data that could identify an individual indirectly and could be withheld under S40(2) and 40(3A) of FOIA. When Mr Hudson subsequently appealed, the ICO also concluded that a VRM, where the vehicle was owned by a living person, was personal data. The ICO added that the Appellant did have a legitimate interest in obtaining the VRM numbers to produce the database. However, his legitimate interest was outweighed by the vehicle owner's right to private life, particularly where the owner had not used their vehicle for private hire or as a taxi. Furthermore, the disclosure could facilitate the commission of crimes through vehicle cloning. Automotive Software Solutions then took the decision to the Tribunal. The Tribunal hesitantly agreed with ICO's conclusion that the interests of the existing owner outweigh the general interest in disclosure. The Tribunal highlighted the difficulty in demonstrating the lawfulness of disclosure. However, it highlighted that if the disclosure was lawful, it would certainly contribute to the fairness and transparency of the sale as the potential buyers would be informed about the history of the vehicle (i.e whether it was previously used for private hire or not) without having to rely on the seller's word. The Tribunal concluded by referencing s.31 FOIA which exempts disclosure of information where the disclosure would, or would be likely to, prejudice- "(a) the prevention or detection of crime..." It noted that .."for a range of criminal endeavours it is clear that make, model and registration number is more than sufficient to be effective, and the provision

Date	Description
	of a structured list would facilitate the finding of an existing registration number suitable for cloning." As the Tribunal attaches significant weight to prevention of crime, it was satisfied that the Information Commissioner's decision was correct and that withholding of information was justified by s.31 FOIA.
2 October	**Lloyd v Google LLC [2019] EWCA Civ 1599** Keen readers of this bulletin will recall the High Court decision in this case, where Richard Lloyd failed in his attempt to serve Google LLC out of jurisdiction with a representative action (under CPR 19.6) seeking compensation under s.13 of the Data Protection Act 1998. The breach behind this claim is the 'Safari workaround' deployed by Google between 2011 – 2012 (the same workaround cited by several claimants as part of the ultimately-settled *Vidal-Hall* cases in 2014-2016). At first instance, Warby J dismissed the action on the grounds that: (a) that the claimant had not demonstrated that damage (as he interpreted it) had been suffered by him or the other claimants; and (b) the members of the class did not have "the same" interest to justify a representative action. As a result of these conclusions, he withheld his discretion to permit service out of jurisdiction. The Court of Appeal has now overturned this decision. **Damage – a '*loss of control…or autonomy*' caused by breach of data protection law sufficient to mount a claim, without demonstrating distress or pecuniary loss.** Although Warby J had quite bluntly disagreed with the claimant's view that having suffered a breach might of itself be worthy of compensation, the Court of Appeal was open to this argument. In permitting the claim to be served, the Court has effectively imported from *Gulati* [2015] EWCA Civ 1291 the principle that loss of control of data through breach of data protection obligations can of itself be sufficient to lead to damages being awarded without pecuniary or distress being proven. As set out by Sir Geoffrey Vos C: "*a person's control over data or over their browser generated information does have a value, so that the loss of that control must also have a value*" This is seemingly already recognised under the GDPR – loss of control is cited as an example of *"physical, material or non-material damage"* that might lead to a need to report a breach in Recital 85 – but as this case was brought under the Data Protection Act 1998 this reclassification of recoverable damage could lead to an increase in retrospective claims for compensation. It is perhaps worth noting that the Court of Appeal envisage there to be some limits to this type of claim – Vos C specifically considered the potential financial value of browser generated information, noting that it was something that a controller might pay to access or a data subject might pay to withhold, and emphasised that *Gulati's* "*seriousness threshold*" should also apply in relation to a claim under s.13 of the 1998 Act. "*Accidental one-off*" breaches that are "*quickly remedied*" should not be subject to this type of damages claim – although the depths of what is "*de minimis*" may be an area for further judicial elucidation in time. **Same interest – if no particular circumstances are claimed, uniformity can be found to allow a (large) representative claim** Warby J's conclusions on 'same interest' were founded in substance on his findings on damage – if limited to distress or pecuniary loss, then his conclusion was that different types of individuals might suffer different financial results or different levels of distress, perhaps dependent on their usage of the Safari browser, precluding an identical class to found the basis of a representative claim. As summarised by

Date	Description
	Vos C, having come to a conclusion that the loss of control is of itself a compensable damage, *"the matter looks more straightforward". This does not mean that every such claimant would be inherently better off* as a result of this representative claim in normal circumstances. For claimants that have suffered financial loss or distress, this is excluded from the basis of the group claim, which is in effect reduced to the "*lowest common denominator*" of the fact of loss of control of data of inherent value. However, Vos C emphasised that in this case any injustice in allowing such a class to be formed on such limited damages could be countered by the fact that in this case the limitation period had closed and, theoretically at least, those suffering more substantial losses could seek to be joined as parties to the representative litigation. This interpretation opens up the potential for very large groups to be identified – even if damages for loss of control may be more restricted than if individual circumstances could be pleaded, they will "*not be nothing*". A high volume of large claims could be extremely costly. In this case, Lloyd estimated at the High Court that the class could number 4.4 million individuals. Although inevitably there is concern this will lead to additional representative action, it is highly likely that we will see this case resurface in the Supreme Court given the implications for controllers.
3 October	**R (on the application of (1) Open Rights Group (2) The3Million) (Claimants) v (1) Secretary of State for the Home Department (2) Secretary of State for Digital, Culture, Media & Sport (Defendants) & (1) Liberty (2) Information Commissioner (Interveners) [2019] EWHC 2562 (Admin)** Mr Justice Supperstone found against The3Million and Open Rights Group (the "Claimants") in his judgment on 3 October 2019 concerning the Claimants' judicial review of the "Immigration Exemption" in Schedule 2, Part 1, paragraph 4 of the Data Protection Act 2018 ("DPA 2018"). The Immigration Exemption, which was introduced for the first time by the DPA 2018, dis-applies a number of data subject rights, (including the right to erasure, the right to access and the right to transparent information about the use of personal data) to the extent that complying with these rights would prejudice either the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control. The Claimants challenged the lawfulness of the Immigration Exemption on the basis that it is incompatible with Article 23 of the GDPR and with the rights to privacy and data protection under the European Convention on Human Rights and/or the Charter of Fundamental Rights. Article 23 allows EU Member States to restrict the application of certain GDPR provisions via local legislative measures which are made to safeguard a number of areas (such as national security, defence and for other important objectives of general public interest in that Member State or the EU overall) provided that such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society. Finding that the Immigration Exemption "*is plainly a matter of "important public interest" and pursues a legitimate aim*" (para 30), Supperstone J considered: • the Immigration Exemption is comprehensible, and does not suffer from such a lack of clarity or foreseeability which would render it 'not in accordance with the law'; • since established case law and the GDPR sets out the requirement of proportionality and the DPA 2018"*supplements, and must be read with, the GDPR" (*section 4(2)(b) of the DPA 2018), the DPA 2018 does not need to expressly require that the Immigration Exemption

Date	Description
	may be relied upon only where it was proportionate to do so; • overall safeguards providing individuals with a legal remedy are in place by virtue of the enforcement regime in the DPA 2018 and GDPR, with recourse to the ICO, the First-tier Tribunal (Information Rights) and the courts; and • statutory guidance as to the meaning and application of the Immigration Exemption is not required for the exemption to be a proportionate implementation of Article 23(1) of the GDPR (contrary to the submission made by the ICO as an intervener in the matter). On this final point, the ICO submitted that it is finalising guidance on the Immigration Exemption, which it will issue further to its powers under Article 57(1) of the GDPR. The High Court's ruling is not the end of this matter; the Claimants applied to appeal the judgment on the same day it was handed down.
15 October	**Mustard v Flower and Others [2019] EWHC 2623 (QB)** This case related to Ms Mustard who was injured in a traffic accident and wanted to claim compensation. She was examined by medical experts appointed by the insurer and was advised by her solicitor to record the examinations. She covertly recorded two of the examinations and wished to use those recordings in evidence in support of her claim. The insurer objected, arguing that the recordings constituted unlawful processing contrary to the GDPR and the DPA 2018. Evidence which has been unlawfully or improperly can still in certain circumstances be admissible, but the insurer argued that the data protection contraventions in this case should tip the scales in favour of inadmissibility. Master Davison however disagreed and rejected the proposition that the recordings were a breach of the Data Protection Act or the GPDR. In reaching this decision he concluded: • Recording a consultation with a doctor constitutes processing of personal data "*by a natural person in the course of a purely personal…activity*" and therefore outside of the scope of GDPR. Further, the fact that Ms Mustard was going to supply the recordings to her advisors did not take this out of this category either. The data relate to the claimant and not the doctor; • Master Davison also concluded that the 'legal proceedings' exemption under para 5 of Schedule 2 to the DPA 2018 applied here although this line of argument is hard to follow. • Master Davison distinguished the CJEU case of *Buivids* C-345/17 which related to the recording and publication of a You Tube video of Latvian Police Officers performing their duties in a police station. • Finally whilst the recordings were considered "reprehensible" Master Davison concluded that they were not unlawful:" *The claimant acted on the advice of her solicitor and her motives were, in the context of adversarial litigation, understandable. Whilst her actions lacked courtesy and transparency, covert recording has become a fact of professional life*."

UK legislation

Date	Description
30October	The Data Protection Act 2018 (Commencement No. 3) Regulations 2019 have been enacted and will bring into force para 211 and 227 of Schedule 19 of the Data Protection Act 2018 on 2 December 2019. These paragraphs make amendments to the Children and Social Work Act 2017.

Other UK News

Date	Description
4 October	**UK-US agreement facilitates reciprocal gathering of overseas evidence for criminal investigations** On 4th October 2019, the UK and US governments announced the signing of an agreement that will facilitate the ability of UK and US authorities to demand certain documents or other data from companies and individuals, if they are based or operating in the US and UK, respectively. The agreement gives UK and US law enforcement authorities an alternative to traditional mutual legal assistance channels, and applies regardless of where in the world the data is actually located – leaving open the possibility of conflicts with non-UK and non-US laws. The new bilateral treaty comes after unilateral moves by the UK and US to expand the international reach of their investigatory and intelligence-gathering powers, including the US CLOUD Act 2018 and the UK Investigatory Powers Act 2016. The new treaty's signature will also prompt the UK to bring into force the UK Crime (Overseas Production Orders) Act 2019 ("COPO"), which became UK law earlier this year. COPO will enable UK authorities to seek a local court order compelling companies or individuals in the US to turn over data, under the terms of the new treaty. Subject to complying with the conditions set out in COPO, UK data protection legislation, and the UK-US treaty, COPOs will need to be complied with "in spite of any restriction on the disclosure of information (however imposed)". The new treaty also has other important effects for companies exposed to UK and US investigations. In particular, once the treaty is formally 'designated' by UK and US authorities, it will likely mean that: • US-based tech companies will no longer be outright barred by the US Stored Communications Act from disclosing data directly to UK authorities; • Reciprocally, tech companies may be able to lawfully comply directly with certain US demands for communications data, including wiretaps, without breaching interception provisions in the UK Investigatory Powers Act 2016; and • Tech companies may now be able invoke conflicting UK laws as a defence to US authorities' requests, pursuant to the US CLOUD ACT. The new treaty's announcement can be found here, and its full text is here; see also the US CLOUD Act, the UK COPO Act 2019, and s52 of the UK Investigatory Powers Act 2016.

Date	Description
25 October	**EU: What a difference a Brexit deal makes** The European Commission's ('the Commission') Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 of the Treaty on European Union released, on 17 October 2019, a revised text of the Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom as agreed at negotiators' level ('the Revised Political Declaration'). Emma Drake, Senior Associate at Bird & Bird LLP, provides insight into how Brexit may affect data privacy in the UK, and what companies may want to plan for if the UK enters into a 'transition period.' **What is the current situation?** For many organisations, the focus of data protection preparation ahead of each delayed Brexit deadline has been on no-deal planning. This approach has been supported not only by the general pessimism that any deal could be reached, but also by official guidance from governments and supervisory authorities, such as the Information Commissioner's Office ('ICO') and the French data protection authority ('CNIL'). Now, following a promise made by UK Prime Minister, Boris Johnson, to Parliament that, 'one way or another, we will leave the EU with this deal,' many will need to refresh their memories of how the proposed withdrawal agreement ('the Revised Withdrawal Agreement') will affect data processing and data flows. **What has changed on data protection?** Since the former Prime Minister Theresa May's deal, in short, nothing has changed. The Revised Political Declaration and Withdrawal Agreement repeat word-for-word the commitments on personal data proposed in late 2018. Any previous planning done by your organisation for a Brexit based on the former withdrawal agreement can be dusted off and resurrected. **What do we need to do if the deal is agreed?** If a deal is formally approved, the UK will initially leave the EU once this is ratified and enter into a transition period. During this transition, the UK would be required to directly apply Union law, including the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the Law No. 363/2018 transposing the EU Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) ('Law Enforcement Directive'), and the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) ('the ePrivacy Directive'), unless and until an adequacy decision is put in place by the Commission. The Revised Withdrawal Agreement also ensures that the UK will be treated as a Member State under EU law for the same period. This is with one substantial exception: the UK will be treated as a third country for the purposes of the GDPR's cooperation and consistency mechanisms during the transition period. This means that the UK will no longer be a member of the European Data Protection Board, and will no longer benefit from any one-stop shop arrangements. Potentially, organisations could see themselves subject to simultaneous action from both the ICO and EU supervisory authorities during transition.

Date	Description
	More positively, the effect of this transition is that: • for the purposes of international transfers, the UK will be considered as a Member State until the end of transition or the implementation of an adequacy decision; • UK organisations will not need to consider extra-territorial application of the GDPR until this no longer directly applies, including any requirement to appoint their own EU representative; and • the GDPR remains the applicable law for UK organisations for this period, and there is a commitment that it will remain the applicable law for any data processed prior to the end of transition, unless and until an adequacy decision is in place. Perhaps the major 'change' as compared to the position of last year is the length of transition will apply for. Despite nearly a year's worth of delay, transition remains set to end on 31 December 2020. This can be extended, but only with the consent of both parties, including parliamentary approval. **Is our no-deal data transfer planning wasted?** If your organisation has taken any steps to prepare for a no-deal, this is not wasted effort. Even if the deal is ratified and implemented promptly, this is not the end of the road for an effective no-deal. The Revised Political Declaration sets out a commitment from the EU to 'endeavour to adopt' an adequacy decision by the end of 2020, but there is no guarantee that this will be achieved in time for the UK's formal and final exit. Similarly, other no-deal planning, such as revising contract precedents to anticipate the 'UK GDPR', moving representatives to other Member States, and inserting references to the UK in privacy notices, will remain useful for a final UK exit, even if the urgency of this may have seemingly reduced. In any event, whilst at the time of publication a sudden no-deal seems unlikely, this could yet be out of date soon. A weekend is a long time in Brexit planning.

Europe

EDPB

Date	Description
October 8 & 9	**EDPB 14th Plenary Session** On 8 and 9 October, the European Data Protection Board (EDPB) met for its fourteenth plenary session. During the plenary, the following topics were discussed, amongst others: • The 3rd annual review of the Privacy Shield • The guidelines on processing necessary for the performance of a contract, in the context of the provision of online services. The EDPB adopted a final version of these guidelines, which have been amended slightly to take into account points raised during the public consultation. • The interplay between data protection and competition – there was an exchange of views on this topic • First BCRs approved under the GDPR- the EDPB adopted an Article 64 decision, marking the first Binding Corporate Rules to be approved under the GDPR. The BCRs were submitted by the UK's ICO and relate to the company Equinix. • Response to World Anti-Doping Agency (WADA)- the EDPB adopted a response regarding the ongoing review of WADA's Code and Standards. The guidelines on territorial scope have not yet been adopted, and the timeline for this happening is still unclear. The next EDPB plenary will take place on the 12 & 13 November 2019.

<< Back to table of contents

CJEU cases

Date	Description
September 24	**Should search engines implement de-listing requests globally? And do they have to remove sensitive data as a matter of course?** The CJEU has considered two further right to be forgotten cases. The first is on territorial scope of the right to be forgotten. Here, the CJEU concluded that de-listing requests should be implemented across the EU, not just in the member state applicable to the relevant data subject. It also determined that there is no general requirement under the Directive or the GDPR for a search engine to apply delisting globally. However, the CJEU specifically upheld the right of a supervisory authority or member state court to require global delisting in a particular case, if this would be required under national standards in that member state. The second case considers how search engines should deal with de-listing requests involving special category data (for example, information about religious belief) and information relating to criminal offences and convictions. The CJEU confirmed that reports of court proceedings and investigations would fall into this category – even if there is no subsequent conviction. The CJEU noted that, while the interests of data subjects would ordinarily outweigh the interests of internet users in accessing information, search engines do have an obligation to consider the interests of freedom of information. In specific cases, these interests may justify a refusal to de-list. If a search engine considers that de-listing is not appropriate then, search engines must ensure that any articles about criminal offences and convictions display current information first. Our full article on this topic is available here.
October 1	**Planet49: CJEU Rules on Cookie Consent** On 1 October 2019 the Court of Justice of the European Union (the 'CJEU') delivered its judgment in Planet49, a case analysing the standard of transparency and consent for the use of cookies and similar technologies. On the whole the findings of the CJEU were unsurprising and largely in line with recent regulatory guidance on the use of cookies and similar technologies. Key points to note from the judgment include: 1. Pre-ticked check-boxes authorising the use of cookies and similar technologies do not constitute valid consent under the e-Privacy Directive.

Date	Description
	2. Where consent is required for cookies under the e-Privacy Directive, the GDPR standard of consent applies. 3. It does not matter whether the cookies constitute personal data or not - Article 5(3) of the e-Privacy Directive (i.e. the cookie consent rule) applies to any information installed or accessed from an individual's device. 4. Website users must be provided with information on the duration of the cookies, and whether third parties will have access to the cookies. Our full article on this topic is available here.
21 October	**Are You Inadvertently Processing European Criminal Conviction Data? The Overlooked Impact of GC v CNIL** Google continues to drive the development in case law of the Court of Justice of the European Union (CJEU) on the right to be forgotten in two recent cases. A lot of the media attention in Europe has focused on Google's 'major victory' in *Google v CNIL* (Case C-507/17), according to which the EU General Data Protection Regulation (GDPR) did not require Google to de-list search engine results globally following a successful de-listing request in the EU. The CJEU noted, however, that while the GDPR did not require global de-listing, it did not prohibit it. Therefore, EU member states' courts and data protection authorities would have jurisdiction to determine whether, in light of national standards, a search engine operator would also need to de-list globally. The CJEU's decision in *Google v CNIL* is of limited importance to U.S. companies who do not operate search engines. By contrast, the other right to be forgotten case concerning the tech giant in *GC v CNIL* (Case C-136/17) may be far more significant for U.S. companies. This case concerning sensitive personal data and criminal conviction data has not received much attention outside of specialist legal and regulatory circles but may in fact have a real impact on companies which may be inadvertently processing European criminal conviction data and may be doing so in violation of EU law. **Background** Two of the claimants in *GC v CNIL* requested the de-listing of Google results linking to articles published in the French press concerning criminal proceedings brought against them. Having assessed the requests, Google determined that the public's right to the information prevailed and this determination was upheld by the CNIL following the claimants' complaints to the French supervisory authority. The CJEU held that the information about proceedings brought against an individual, even absent a conviction, constitutes data relating to 'offences' and 'criminal convictions' within the meaning of Article 10 of the GDPR and therefore were subject to conditions and protections set out in that provision. The CJEU also noted that with the passage of time and in accordance with the principles of data minimisation, accuracy and storage limitation, the processing of such information may no longer comply with the GDPR.

Date	Description

Finally, the CJEU held that search engine operators must assess whether published information relating to earlier stages of criminal proceedings that did not reflect the current situation and "*whether, in the light of all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by the data subject in public life and his past conduct, the public's interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject*" the search results should be delisted or otherwise reordered to reflect the " current legal position".

Analysis

The CJEU's decision in *GC v CNIL* can be problematic, not because the decision is unsound (in fact, the decision is well reasoned and to that extent unexceptional) but because it significantly broadens what is meant by criminal conviction data.

Article 10 of the GDPR provides the following:

"Processing of personal data relating to criminal convictions and offences or relating to security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

The drafting in Article 10 GDPR is almost identical to that of its predecessor, the Data Protection Directive, and sets out the following three cardinal rules for the processing of criminal conviction data:

- The processing criminal conviction data can only be carried out by official authorities; or
- The processing of criminal conviction data must be authorized by EU or member state law; and
- Only authorities can maintain a comprehensive register of criminal convictions.

But what is criminal conviction data? Is it just a recorded criminal offence or something much broader? The GDPR does not provide a definition and neither did the Data Protection Directive. Moreover, Article 10 is one of the few articles in the GDPR that does not have a corresponding recital to aid in its interpretation.

According to Advocate General Szpunar and the CJEU, information about proceedings brought against an individual even absent a conviction constitutes data relating to 'offences' and 'criminal convictions'. This broad definition should come as no surprise to data protection practitioners familiar with UK law as the Data Protection Act 2018 (and its predecessor, the Data Protection Act 1998) broadly defines criminal conviction data as the commission or "*the alleged commission of offences by the data subject*" and " *proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing*". A similar view was adopted by pre-GDPR guidance by the CNIL in France. However, this broader definition is likely to have significant impact in other member states and for U.S. companies operating across the EU where national laws do not contain a similar definition. For example, in Germany the prevailing view before the CJEU's decision was that allegations of criminal offences, absent an actual conviction, would not be subject to Article 10 GDPR. Similarly in the Netherlands, suspected criminal activity may have been caught by Article 10 GDPR

Date	Description
	if there are concrete and well-founded indications that an individual has committed a criminal offence. Each EU member state has its own laws concerning the recording of criminal convictions and the processing of criminal conviction data by public authorities and private organisations. Some EU member states only permit the processing of criminal conviction data by private organisations to a very limited extent, such as in respect of individuals working with children or vulnerable adults (Ireland, Poland and Sweden), whereas others only allow the data subject rather than private organisations to access the data directly (France, Germany and Spain). By contrast, other member states have established comprehensive processes for private organisations to access criminal record data whether for background checks or for other purposes (United Kingdom), with additional requirements regarding the retention and use of such data. The variability across the EU represents a hurdle for U.S. companies seeking a consistent approach regarding their European operations. For example, many U.S. companies have access to or would otherwise process data concerning the background of EU-based employees and contingent workers, which may now constitute criminal conviction data following the CJEU's decision. Consequently U.S. companies must consider applicable national variations, as enshrined in cardinal rule (2). Although the CJEU's decision goes some way to provide some consistency, albeit by bringing more data into scope, it would still defer to national law as regards what is permitted. It is important for U.S. companies that are subject to the GDPR and that may process data that would now constitute 'criminal conviction' data to review this data and determine if it is being lawfully processed whether by them or their European subsidiaries. In making that determination it is useful to refer back to the CJEU's decision that requires taking into account "*all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, [and] the time elapsed*." That assessment will necessarily require companies to research and record the development and outcome of legal proceedings, as well as recording possible convictions. It is unlikely that the recording of the assessment would generally amount to a 'comprehensive register of criminal convictions' in violation of cardinal rule (3).

Other EU News

Date	Description
9 October	The Council of European Union has set out its position and findings on the application of the GDPR from 19 Member States in preparation for its 2020 review of GDPR. See here.
17 October	**ePrivacy Regulation update** On 17 October, the Council of the European Union (the 'Council') published its latest draft of the proposed e-Privacy Regulation. [*Note that this since this article was written the Council issued a further draft on 30 October – further updates will follow*]. Originally scheduled to be introduced in parallel with GDPR, progress on the e-privacy regulation has been slow - and 18 months on - the exact timeline remains unclear. **What does the latest draft propose?** ***Making website access conditional on cookie consent*** According to the Council's latest draft, making end-user access to a website conditional on the user's consent to the use of cookies is generally permitted (and not disproportionate), particularly where the user can choose between a version of the website which includes the cookies and an equivalent version without cookies. However, the draft reflects the fact while in most cases such conditionality is permissible, there may be extreme cases where this could be disproportionate, notably where the user does not have a real choice about using the website e.g. public authorities' websites. More generally, the UK Information Commissioner in her updated cookie guidance noted that full cookie walls are unlikely to be valid. While the CNIL in its revised guidance on cookies is more definitive still and states that cookie walls are invalid. This is a contentious issue, that affects other rights such as freedom of expression and the right to carry on a business - therefore the Council's proposal is unlikely to be the last word on this point. ***Cookie consent - consent via privacy by design settings on installation not mandated*** Privacy by Design: The Council has removed the privacy by design rules for cookies and similar technologies that had required software providers to obtain consent for cookies on installation. However, elsewhere the draft provides that where 'available and technically feasible', users 'may' be granted cookie choices in the software settings. Therefore the Council draft no longer makes provision of such settings mandatory. The Council's position on this is at odds with the Commission and Parliament proposals which mandated privacy by design rules whereby the technology provider (for example the web browser) must inform the user about the cookie settings and to continue with the installation

Date	Description
	the end-user must set their preferences). Who gives consent: According to the Council, when consent is required, the consent should be given by the end-user who requested the service from the provider of the service (i.e., in the case of connected devices – no consent needed from end-users who have not requested the service but whose data is processed). This is narrower than the current e-Privacy Directive which states the 'subscriber or user concerned has given his or her consent', however the position from the Council reflects the fact that in the IoT environment obtaining consent from all individuals whose data is processed by the connected device poses significant difficulties in practice. ***Exemptions from cookie consent*** The exemptions to cookie consent have been amended and expanded to cover: • third parties carrying out audience measurement on behalf of the controller. The exemption here has been widened from 'web audience measurement' to 'audience measurement'. The Council draft also clarifies that this measurement may be carried out by a third party on behalf of one or more providers so long as the requirements in Article 28 GDPR (processor requirements) or Article 26 GDPR (joint controller requirements) , as applicable, are met; • maintenance/restoring security of web services; • where necessary for a software security update (updates to add new features or improve performance would not fall within the exemption); • where necessary to locate terminal equipment when the end-user makes an emergency communication; • It is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number; • end-user has consented These exemptions will be helpful for many organisations, in particular the security exceptions, and the widening of the analytics exemption by making clear the audience measurement can be provided by a third party. It is also interesting to note that the direction of travel in the e-privacy regulation on analytics is more permissive than the position adopted by the UK Information Commissioner in her updated guidance on Cookies and Similar Technologies which holds that analytic cookies were not exempt from the cookie consent requirements under Article 5(3) of the e-Privacy Directive. ***e-Privacy rules on direct marketing*** According to the Council draft, ePrivacy rules on direct marketing apply only to marketing which is sent to the end-user's contact details. The Council draft specifically notes that these rules do not apply to ads on websites or banner ads.

Date	Description
	Soft opt-in exemption The draft specifically provides that Member States can legislate on how long organisations can use end-user contact details for the purposes of the soft opt-in exemption (as opposed to fixing this at 12 months as had been previously proposed in some of the earlier drafts of the regulation). ***Electronic Communications Content*** The Council have amended the grounds for processing communications content data. According to this draft of the regulation communication content data may be processed 'for the purpose of the provision of a service requested by an end-user for individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned'. ***Electronic Communications Data*** • According to the Council providers of electronic communication networks and services are permitted to process the electronic communications data only if necessary to: • achieve transmission of the communication; • detect/prevent security risks and/or attacks on end users terminal equipment; or • comply with a legal obligation. ***Processing of electronic communications data for the purpose of detecting, deleting and reporting material constituting child pornography*** The Council have proposed new grounds for the purposes of processing electronic communications data for the detection, reporting and deleting material constituting child pornography. The processing of electronic communications data for these purposes only covers providers of *number-independent interpersonal communications services* (as defined in the Directive establishing the European Electronic Communications Code) and such processing is only permitted where: (i) a unique hash of material is created for the sole purpose of comparing against a hashed database of material previously reliably identified as child pornography; (ii) the data is deleted immediately after comparison with the database, except in the cases where material constituting child pornography has been detected by virtue of a hash; and (iii) the system limits the probability of mistaken detection of child pornography to at most 1 in 50 billion. In addition, prior to such processing being carried out, a Data Protection Impact Assessment needs to be completed including supervisory authority consultation on that assessment, in accordance with Articles 35 and 36 GDPR.

EU Enforcement

Date	Description
19 September	**Belgian DPA imposes €10,000 fine on a merchant for its disproportionate use of the Belgian electronic ID card.** This merchant offered the possibility to create a loyalty card but required to have access to the Belgian electronic ID card (eID) to do so. This card contains more information that the merchant needs to create a loyalty card such as the national identification number. The Belgian supervisory authority (APD) investigated this company as a result of a complaint from a data subject. This person wanted to create an account but refused to communicate their eID card details. They offered to send the necessary information via mail instead, which was refused by the merchant. Th APD found that the merchant breached the principle of minimisation of personal data as set out in the GDPR as it did not need to have access to all of the information included in the eID for the purpose of creating a loyalty account. This resulted in a disproportionate use of the eID data. Furthermore, the APD found that the merchant did not have a valid legal basis for this processing. The merchant argued that it relied on the individuals' consent to process such data. However, the authority found that consent was not freely given in this instance as individuals didn't have any other choice than to accept the processing of their eID data if they wanted to create an account.
20 September	**Polish DPA fines morele.net €645,000 (PLN 2.8 million) for insufficient organisational and technical safeguards** The company's lack of appropriate organisational and technical measures resulted in a data breach affecting of 2.2 million people. In particular, the Polish DPA outlined the presence of insufficient safeguards for data authentication and the lack of monitoring of potential risks in relation with atypical online behavior. The Polish DPA found that the failure to implement the required technical and organisational measure resulted in a breach of the principle of confidentiality, as set out in Article 5 (1)(f) of the GDPR as customer data was obtained and accessed without authorization. In addition, the Polish DPA found that the company didn't have appropriate response procedures to deal with such a situation. For most of the people affected ,the data concerned was simply contact details data (i.e. name and surname, phone number, email, delivery address). However for about 35,000 individuals, the data was leaked from a loan application and included, inter alia, a personal ID number, details about ID documents, salary information, marital status, existence and amount of credit commitments. The DPA concluded that this breach was of serious character, considerable importance and affected a large number of individuals. It added that there was a high risk of adverse effect for the people affected (e.g. identity theft). This was taken into account by the DPA when determining the amount of the fine as well as mitigating circumstances such as the actions taken to put an end to the breach, the absence of past infringements and good cooperation with the DPA during the investigations.

Date	Description
7 October	**Greek DPA fines a Greek telecommunications provider €400,000 for breaches of the accuracy principle and data protection by design and also for a failure to satisfy the right to object** The Greek DPA received complaints from telephone subscribers of the Hellenic Telecommunications Organisation ("OTE") who received unsolicited direct marketing calls despite being registered on OTE's do-not-call register. The investigation showed that those subscribers had submitted a portability request for the transfer of their subscription to another provider but as a consequence, OTE had deleted their entries from the do-not-call register. However, when those subscribers cancelled their portability request, there was no proper procedure to cancel their removal from the register. In addition when subscribers received advertising messages from OTE, they were not able to unsubscribe properly due to a technical error which had been in place from 2013 onwards.
17 October	**Spanish DPA fines Vueling €30,000 for the cookie policy used on its website** In this recent decision, the Spanish DPA states that when accessing the airline's website, a banner with information on the use of cookies is shown to the user. However the user is not offered a tool aimed at managing cookies. Instead the user is informed that cookies have to be managed by means of the web browser settings which the Spanish DPA held was invalid. For more detail on this decision, click here.

UK Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
17/09/2019	Superior Style Home Improvements Ltd	Enforcement notices & Monetary penalties	Superior Style Home Improvements Ltd ('SSHI') was issued with a monetary penalty notice of £150,000 after making unsolicited marketing calls over an 11 month period to individuals whose numbers were registered with the Telephone Preference Service ('TPS') and who had not given their consent to receive them. The ICO also issued an enforcement notice warning them to stop making the calls. **A serious contravention** • The 11-month period led to a significant number of complaints about unsolicited direct marketing calls to the TPS and the ICO. • It is reasonable to suppose that the contravention could have been far higher because those who went to the trouble to complain represent only a proportion of those who actually received calls. • Repeat calls were made even though some complainants alleged to have requested that their number be suppressed. **Deliberate actions** • SSHI relied heavily on direct marketing due to the nature of its business (double glazing company) • The issue of unsolicited calls has been widely publicised by the media as being a problem **Failed to take reasonable steps to prevent the contravention** • The investigation result showed a lack of care and attention in relation to how SSHI was operating, suggesting they failed to take action and repeatedly failed to acknowledge the convention.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
04/10/2019	Update on the British Airways data breach		**British Airways: Customers have been given the green light to bring compensation claims** Further to our prior newsletter regarding ICO's intention to fine British Airways ('BA') £183.39M under GDPR in July, Mr Justice Warby granted a group litigation order at a hearing at the High Court in London on 4 October 2019. The judge granted a window of 15 months for people to come forward and join the group litigation