

Bird & Bird

UK & EU Data Protection Bulletin: November 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](#)

[Other UK News](#)

EU and Council of Europe

[EDPB](#)

[CJEU Cases](#)

[Other EU news](#)

UK Enforcement

[ICO Enforcement](#)



United Kingdom

Information Commissioner's Office (ICO)

Date	Description
1 October	<p>ICO consults on draft statutory guidance on regulatory action</p> <p>The ICO has launched a public consultation on its draft statutory guidance on regulatory action. The guidance sets out how the ICO will regulate and enforce data protection legislation in the UK following the end of the transition period.</p> <p>The guidance, which the ICO is required to publish under the Data Protection Act 2018, aims to raise awareness and provide transparency around the ICO's powers for both organisations subject to its regulation under that Act and the GDPR, and the wider public who benefit from its enforcement. It will ultimately sit alongside the ICO's wider Regulatory Action Policy, which is currently under review. Together these documents will provide a comprehensive view of the ICO's regulatory approach and powers.</p> <p>The guidance specifically provides a guide to the powers the ICO has been granted under the Act, in particular:</p> <ul style="list-style-type: none">• Information notices;• Assessment notices, including urgent and “no-notice” assessment notices;• Enforcement notices;• Penalty notices; and• Fixed penalties <p>The draft guidance examines, at a high level, the types of scope of these powers and the considerations the ICO will take into account in their use. For example, it sets out a nine-step process for the consideration of an administrative penalty, and the considerations at each stage of this assessment, including a “penalty starting point” based on seriousness and degree of culpability.</p> <p>The consultation closed on 12 November.</p>
21 October	<p>New Guidance on Subject Access Rights</p> <p>The ICO has now issued the finalised version of its detailed Rights of Access Guidance. This is the finalised version of the Guidance that went out for consultation back in December 2019. There are some clarifications from the original draft guidance including on when the clock can be stopped whilst waiting for the requester to clarify their request and on what constitutes a “complex” request for the purposes of extending the 1 month response time limit, examples on what might constitute a manifestly unfounded or excessive request which does not need to be dealt with under Article 12(5) and what can be included when charging a fee for excessive, unfounded or repeat requests.</p> <p>In terms of the efforts that the data controller needs to go to when trying to search for the relevant information, the ICO states that it must make “reasonable efforts to find and retrieve the requested information. However you are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information. The burden of proof as to why a search is unreasonable or disproportionate will fall on the controller and will depend on the circumstances of the request, any difficulties involved in finding the information and the fundamental nature of the right of access.</p>

UK Cases

Date	Cases
24 August	<p data-bbox="443 339 1093 368">Lees v Lloyds Bank plc [2020] EWHC 2249 (Ch)</p> <p data-bbox="443 387 2063 475">The claimant had sent Lloyds three data subject access requests (DSARs) to which Lloyds had replied. These were made alongside the claimant’s ongoing litigation against Lloyds in relation to claims for possession it was pursuing in respect of the three properties with buy-to-let mortgages granted to the claimant.</p> <p data-bbox="443 494 2063 582">In this claim, the claimant asserted that Lloyds had failed to provide his personal data contrary to the Data Protection Act 2018 and the GDPR. The Court noted that given the dates of the three DSARs, the Data Protection Act 1998 was the applicable law. The Court dismissed the claim on the basis that Lloyds had provided the claimant with an adequate response to each of the DSARs.</p> <p data-bbox="443 601 1995 660">Interestingly, the Court, in obiter, went on to consider whether an order would have been made even if Lloyds had failed to provide a proper response to a DSAR. The Court noted that a court would have discretion as to whether or not to make an order.</p> <p data-bbox="443 679 2063 738">It was stated that there seemed to be “<i>good reasons in this case for declining to exercise the discretion in favour of [the claimant]</i>” in light of the following factors:</p> <ul data-bbox="443 758 2063 1153" style="list-style-type: none"><li data-bbox="443 758 1227 786">“(1) <i>The issue of numerous and repetitive DSARs which is abusive;</i><li data-bbox="443 805 1547 834">“(2) <i>The real purpose of the DSARs being to obtain documents rather than personal data; and</i><li data-bbox="443 853 2063 999">“(3) <i>There being a collateral purpose that lay behind the requests which was to obtain assistance in preventing Lloyds bringing claims for possession. As Lewison LJ points out in Ittihadieh a collateral purpose of assisting in litigation is not an absolute answer to there being an obligation to answer a DSAR, but it is a relevant factor in the exercise of the court’s discretion. In this case [the claimant] has formed, so it appears, a fixed view that the benefit of loans made to him have been the subject of securitisation without having any evidence to support that belief.</i><li data-bbox="443 1018 1995 1077">“(4) <i>The fact that the data sought will be of no benefit to [the claimant]. The decision of the Court of Appeal in Paragon Finance plc v Pender provides a complete answer to the defence he wished to pursue.</i><li data-bbox="443 1096 1995 1153">“(5) <i>The claims for possession have been the subject of final determinations in the County Court from which all available avenues of appeal have been exhausted.</i>” <p data-bbox="443 1173 2018 1232">This commentary is interesting, given it shows an apparent readiness of the Court to refuse to impose an order when an individual uses DSARs as a litigation tool.</p> <p data-bbox="443 1251 2063 1426">For data controllers considering their obligations in relation to DSARs, the ICO’s guidance should be considered, as enforcement will more frequently be taken through the ICO than through the courts. In previous guidance on DSARs, the ICO said that a data subject’s ‘collateral purpose’ (i.e. other than seeking to check or correct their personal data) is not relevant and that simply because a court may choose not to order the disclosure does not mean that, in the absence of a relevant exemption, the law does not require data controllers to disclose it. In its latest guidance, discussed in more detail earlier in this newsletter the ICO has said that data controllers can refuse to comply with a DSAR if it is “manifestly unfounded”, but the guidance only talks about situations where the individual clearly has no intention to exercise</p>

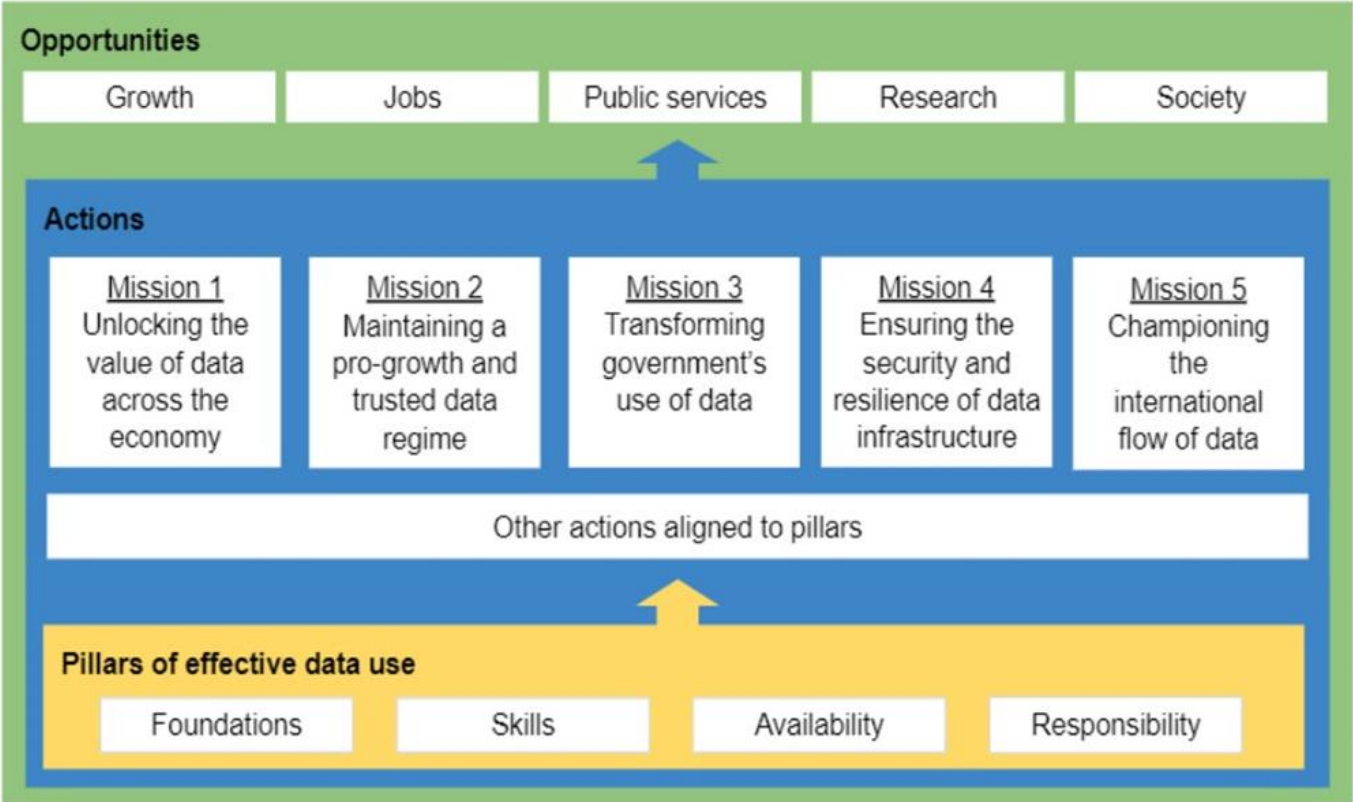
Date	Cases
	<p>their right of access (e.g. an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation) or the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption.</p> <p>Arguments on collateral purpose will only potentially assist, therefore, on a judicial hearing of the case – there is no guarantee or likelihood that the ICO will take this into account in assessing its enforcement action over a DSAR.</p>
<p>1 September</p>	<p>Kathryn Hopkins v Revenue & Customs Commissioners [2020] 8 WLUK 232</p> <p>The court struck out a claim by an HMRC employee who argued that the use of her criminal record information by her employer in disciplinary proceedings was unlawful under the GDPR and the DPA 2018.</p> <p>The Claimant, who was arrested by Merseyside Police on 4 accounts in 2018 (some of which included serious sexual offenses), informed her manager of her arrest due to her contractual obligations. Her manager then escalated the matter to the HMRC’s internal investigations team who suspended the Claimant on full pay during the disciplinary investigation.</p> <p>The Claimant attempted to suspend the investigation by arguing that the further dissemination of her arrest information within the HMRC was a breach of the GDPR and the DPA 2018 because it was a special category data under Article 10 GDPR and the HMRC did not have a lawful basis as required by Article 5 GDPR. The Claimant had in total 20 allegations of breaches of GDPR and the DPA including that her contractual requirement to notify HMRC in relation to her arrest being a breach of Article 7 GDPR and that HMRC was a processor rather than a controller of her arrest data and the Merseyside Police was the controller.</p> <p>The court contended that it was clear that the HMRC was the controller of the Claimant’s personal data when instituting the disciplinary proceedings, suspending the Claimant, handling her grievances and responding to her complaint to the ICO and this claim as it has processed the data on its own behalf rather than Merseyside Police or anyone else.</p> <p>The judgement also clearly set out that the processing of criminal record data was necessary for the performance of the employment contract between the Claimant and the HMRC and it met the requirements of Article 10 and paragraph 1 of Schedule 1 to the DPA and the HMRC did have an appropriate policy document in place. It was further found that the sharing of the Claimant’s criminal record information was necessary for:</p> <ol style="list-style-type: none"> 1) Compliance with a legal obligation to which the HMRC is subject under Revenue and Customs (Complaints and Misconduct) Regulations (Article 6(a)(c) GDPR); 2) The performance of a task carried out in the public interest (Art 6(1)(e) GDPR); and 3) Reasons of substantial public interest and necessary in the exercise of a function on HMRC by an enactment, in accordance with s.10(5) of, and paragraph 6 of Schedule 1 to, the DPA and so met the requirements of Art.10. <p>The court also clarified that the Claimant’s reliance on Article 7 GDPR was misplaced as the HMRC did not rely on the Claimant’s consent to process her arrest data. All in all, the claimant’s unlawfulness arguments under the GDPR and the DPA were dismissed due to having no realistic prospect of success.</p>

Date	Cases
22 September	<p data-bbox="443 220 1816 252">R (on the application of Maha Elgizouli) v SoS for the Home Department & DPP EWHC 2516 (Admin)</p> <p data-bbox="443 268 1368 300">Elgizouli challenge to fresh mutual legal assistance decision refused</p> <p data-bbox="443 316 2040 443">The Divisional Court refused an urgent application from Maha Elgizouli for a judicial review of the Home Secretary’s 24 August 2020 decision to accede to a request for mutual legal assistance (“MLA”) from the United States’ Government under the US-US MLA Treaty, which would involve the transfer of personal data relating to Ms Elgizouli’s son (Mr El Sheikh) to the United States for the purpose of his possible prosecution there for alleged terrorist activities (the “August 2020 Decision”).</p> <p data-bbox="443 459 2063 722">Counsel for Ms Elgizouli argued that a transfer of Mr El Sheikh’s personal data did not comply with Part 3 of the Data Protection Act 2018. Counsel submitted that, on the objective and particular facts of the present case, the Home Secretary could not demonstrate that it was strictly necessary and proportionate to transfer data to the US for the relevant law enforcement purpose (i.e. prosecution) in accordance with ss.35 and 73 DPA 2018. Central to Counsel’s argument was the fact that the Crown Prosecution Service had recently sought consent from the Attorney General to prosecute Mr El Sheikh domestically for serious terrorist offences, and that disclosure was not necessary or proportionate in the circumstances. Counsel for the Home Secretary argued that disclosure was essential, that the Claimant’s argument speculated on future decisions in Mr El Sheikh’s case and that there was no proper basis for an argument that the Home Secretary could not lawfully accede to an MLA request because there was a possibility of prosecuting the person concerned in England.</p> <p data-bbox="443 738 808 770">Divisional Court judgment</p> <p data-bbox="443 786 1115 818">Having considered the above, the Divisional Court found:</p> <ul data-bbox="488 834 1995 1209" style="list-style-type: none"> • the proposed transfer to the United States further to the MLA is for a valid law enforcement purpose – the investigation and prosecution of Mr El Sheikh in the US; • on a proper reading of the Law Enforcement Directive and Data Protection Act 2018, whether processing for the specified law enforcement purpose is strictly necessary or proportionate is a question to be answered by reference to that particular task (the investigation and prosecution of Mr El Sheikh by US authorities) and not by reference to an “inchoate or generalised objective” (for example, of prosecution of Mr El Sheikh generally); • it follows that there is no scope to argue that the processing is not necessary (or is disproportionate) on the basis that the relevant objective is “prosecution” and Mr El Sheikh might be prosecuted domestically; and for the task of prosecution by the US authorities, disclosure of the requested material is strictly necessary and proportionate – on necessity, the evidence is that with the material requested the US authorities would prosecute, and without it they cannot prosecute; on proportionality, the objective of facilitating a prosecution in the requesting state can only be achieved by disclosure of the material. (paras. 58 and 59). <p data-bbox="443 1225 1099 1257">Previous proceedings before the Supreme Court</p> <p data-bbox="443 1273 2063 1431">Earlier this year, Ms Elgizouli succeeded before the Supreme Court in similar proceedings concerning a decision made by the then Home Secretary in June 2018 to provide MLA to the US Govt. Here, the Supreme Court held that the Home Secretary’s June 2018 decision to the US Govt was unlawful under the DPA 2018 because, amongst other things, that June 2018 decision was based on political expediency, rather than strict necessity as required by the DPA 2018. Those proceedings related to materially different facts, including a lack of contemporaneous consideration by the then Home Secretary of whether the Part 3 DPA 2018 criteria were met and the absence of a death</p>

Date	Cases
	<p>penalty assurance from the US Govt. In the present action, the US Govt had provided a death penalty assurance and the Home Secretary had contemporaneously considered the requisite parts of Part 3 of the DPA 2018 when taking the August 2020 Decision. As Counsel for the Home Secretary put, and the Divisional Court agreed: “given that the death penalty assurance had now been provided, this was a very different case from that considered by the Supreme Court; in fact, it was now a “run of the mill case”” (paras.45 and 70).See our update here for more details on the previous proceedings.</p>

Other UK News

Date	Cases
9 September	<p data-bbox="443 400 1173 427">UK National Data Strategy published for consultation</p> <p data-bbox="443 448 2047 592">On 9 September 2020 the Department for Digital, Culture, Media & Sport (“DCMS”) published a consultation on its Policy Paper on the UK National Data Strategy (“NDS”). According to the DCMS, the intention behind the NDS is to produce a forward-looking strategy that “<i>takes into account public opinion and delivers real change in the way that data is used and shared in the United Kingdom</i>” in order to unlock the value such data can bring. The focus is very clearly placed on freeing up the use of all data and is not just focused on personal data.</p> <p data-bbox="443 616 2063 671">Under the framework of the GDPR, adequacy decisions are based on assessments performed by the EU Commission to determine whether the third country in question (here the UK) guarantees a level of protection “essentially equivalent” to that ensured within the EU.</p> <p data-bbox="443 715 2069 954">Currently in the UK, the data protection regime is based on the GDPR and the ePrivacy regime together with protections enshrined in human rights laws. There is therefore currently close alignment between the UK and EU positions and in principle there should already be an essentially equivalent level of protection (subject to any current potential non-compliance, see for example the recent Quadrature and Privacy International cases). However, many of the aims of the NDS could be seen to limit the protections contained in the UK implementation in the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Investigatory Powers Act 2016 (and associated legislation) in the UK post-Brexit. This could lead to implications for any adequacy decision being made or, depending on the timing, could lead to a decision that it is later invalidated, as has recently occurred with the Privacy Shield.</p> <p data-bbox="443 999 667 1026">Aims of the NDS</p> <p data-bbox="443 1046 2040 1134">The NDS builds upon initiatives such as the Industrial Strategy, the AI Review, the AI Sector Deal and the Research and Development Roadmap and brings all of these inputs together for the NDS. The DCMS has produced a diagram below of the NDS pillars, missions and opportunities that it has identified as important for the UK’s data strategy going forward.</p>

Date	Cases
	 <p>The diagram illustrates a three-tiered structure for data use. At the base is a yellow box labeled 'Pillars of effective data use' containing four categories: Foundations, Skills, Availability, and Responsibility. Above this is a blue box labeled 'Actions', which includes five missions: Mission 1 (Unlocking the value of data across the economy), Mission 2 (Maintaining a pro-growth and trusted data regime), Mission 3 (Transforming government's use of data), Mission 4 (Ensuring the security and resilience of data infrastructure), and Mission 5 (Championing the international flow of data). Below the missions is a white box for 'Other actions aligned to pillars'. At the top is a green box labeled 'Opportunities', containing five categories: Growth, Jobs, Public services, Research, and Society. Arrows indicate a bottom-up flow from Pillars to Actions, and from Actions to Opportunities.</p>
	<p>Whilst the precise steps that will result from the NDS are unclear at this stage, including any legislative amendments, it will be important to keep track of the outcomes of this consultation and whether the rules affecting the processing of personal data will have an impact on any adequacy process.</p> <p><u>Next Steps</u></p> <p>The Government's response to this consultation will be published following the deadline (2 December 2020), after which the UK Government will put together a response.</p>

Date	Cases
14 October	<p data-bbox="443 220 1301 252">Government publishes latest draft Brexit Statutory Instrument</p> <p data-bbox="443 268 2040 387">The Government has laid its latest statutory instrument related to the UK’s data protection framework following Brexit. Once in force, it will revise the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, which can be found here. It will also repeal the previous statutory instrument, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019.</p> <p data-bbox="443 419 1861 451">Relatively little is set to be amended through the new draft regulations (which can be found here). The main changes are:</p> <ul data-bbox="443 467 2063 683" style="list-style-type: none"> • all references to ‘exit day’ will be changed to ‘IP completion day’, reflecting the term of the withdrawal agreement and the position under the European Union (Withdrawal Agreement) Act 2020; • references to recognised adequate countries and EU adequacy decisions have been amended, to remove Privacy Shield and add Switzerland and Japan; • the recognition of Binding Corporate Rules approved by a supervisory authority in the EU, rather than the ICO, will now only be assured once the ICO has been notified of the BCRs and has itself approved of the rules. <p data-bbox="443 699 2063 762">This last update is the one likeliest to cause upheaval. Organisations reliant on BCRs approved outside the UK should take steps to engage with the ICO on seeking approval of their existing frameworks, given the ever-approaching deadline of 11pm of 31 December 2020.</p>

EDPB

Date	Description
2 September	<p>EDPB publishes draft guidelines on controllers and processors</p> <p>The EDPB has released its draft guidelines on the concepts of controllers and processors, an area that the body has not reviewed in detail since the Article 29 Working Party produced its longstanding 2010 opinion, WP 169. The draft guidance, which was subject to public consultation until 19 October 2020, includes detailed assessment of the principled differences between controllers and processors, whilst also addressing the concept of joint controllership, as notably explored in a series of CJEU judgments in recent years.</p> <p>Our full article on these guidelines can be found here.</p>
2 September	<p>EDPB publishes draft guidelines on the targeting of social media users</p> <p>Alongside its draft guidance on controllers and processors, the EDPB has also released draft guidance on the targeting of social media users. This guidance examines the various methods used by advertisers and social media platforms to collaborate and market products to social media users, and sets out the EDPB's position on legal basis, joint controllership and other necessary compliance steps required to carry out certain types of marketing activity on such platforms.</p> <p>Our full article on these draft guidelines can be found here.</p>
13 October	<p>Draft Guidelines on “relevant and reasoned objection” under the cooperation mechanism (Art 60 GDPR)</p> <p>On 13th October, the EDPB issued its draft Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679. These Guidelines look at certain aspects of the cooperation mechanism between the lead supervisory authority (LSA) and other competent supervisory authorities (CSAs) in connection with Article 60 GDPR. Under this process, the LSA shall cooperate with the CSAs concerned in an endeavour to reach a consensus. The LSA is required to submit a draft decision to the CSAs to which they can raise a “relevant and reasoned objection” within a specified timeframe.</p> <p>Upon receipt of such an objection, the LSA has two options: (i) if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not reasoned or relevant, it shall submit the matter to the EDPB within the consistency mechanism; or (ii) if the LSA, on the other hand, follows the objection and issues the revised draft decision, the CSAs may express a relevant and reasoned objection on the revised draft decision within a period of two weeks.</p> <p>When the LSA follows option 1, it then becomes incumbent upon the EDPB to adopt a binding decision on whether the objection is “relevant and reasoned” and if so, on all the matters which are the subject of the objection. Therefore, one of the key elements signifying the absence of consensus between the LSA and the CSAs, is the concept of “relevant and reasoned objection”. The draft Guidelines seek to provide guidance on this concept.</p>

20 October

Data Protection by Design and by Default

On 20th October, the EDPB issued its final Guidelines on [Data Protection by Design and by Default](#). These Guidelines were first issued in draft in November 2019 (a summary of which is contained [here](#)) and give general guidance and examples on the interpretation of the obligations of data protection by design and by default. In addition to covering these principles, the Guidelines also cover certification mechanisms for demonstrating compliance with Article 25 GDPR and enforcement by supervisory authorities.

Date	Description
6 October	<p data-bbox="427 368 1843 400"><u>C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others</u></p> <p data-bbox="427 432 1272 464">EU e-privacy laws apply to state communications surveillance</p> <p data-bbox="427 496 1968 560">Hard on the heels of <i>Schrems 2</i> came the 6 October 2020 CJEU judgments in C-623/17 <i>Privacy International</i> and C-511-512/18 <i>La Quadrature du Net</i> (the latter joined with C-520/18 <i>Ordre des barreaux francophones et Germanophone</i>).</p> <p data-bbox="427 576 2067 727">The twin streams of third country data protection adequacy and Member State compliance with EU law meet and merge in this series of judgments. Their origins are found in the 2014 <i>Digital Rights Ireland</i> judgment (C-293/12) striking down the EU Data Retention Directive, and the 2016 <i>Tele2/Watson</i> judgment (C-203/15 and C-698/15), which held the blanket Swedish data retention legislation to be contrary to EU law. A tributary, the 2017 CJEU Opinion on the proposed EU-Canada Passenger Names Record Data Agreement (Opinion 1/15), also flows in.</p> <p data-bbox="427 743 2067 895">The judgments address a variety of bulk communications surveillance activities that one or other of the referring countries (UK, France and Belgium) had imposed on service providers: data retention, computerised analysis of retained data, and transmission to the authorities. The outcomes are more nuanced than the previous judgments, but reiterate that for most kinds of data, in most situations, general and indiscriminate data retention cannot be required. A requirement for general and indiscriminate data transmission to the authorities is never permissible.</p> <p data-bbox="427 911 2067 1031">The judgments all concerned communications data: contextual ‘who, when, where, how’ data surrounding communications as opposed to their content. Whilst in the past content may have been regarded as more sensitive than communications data, the CJEU in these cases stated emphatically that information that may be provided by profiling using traffic and location data is no less sensitive than the content of communications.</p> <p data-bbox="427 1046 2045 1142">The CJEU held that requirements imposed on service providers for national security purposes were within the scope of EU law. That contrasted with the activities of member state national security agencies themselves, which fall outside the scope of EU law so long as they do not impose processing obligations on service providers.</p> <p data-bbox="427 1158 2067 1254">However that distinction, although critical for the scope of EU law applicable to Member States, has no relevance to a European Commission determination of a third country’s data protection adequacy, such as the EU-US Privacy shield that was invalidated in <i>Schrems 2</i>. For an adequacy determination there is no national security exclusion.</p> <p data-bbox="427 1270 2000 1334">Although third country adequacy does not require protection of personal data identical to EU law, the protection has to be “essentially equivalent”.</p> <p data-bbox="427 1350 1906 1374">In summary, the CJEU’s main specific conclusions regarding different kinds of processing imposed on service providers were:</p>

- **Obligations requiring general and indiscriminate data retention** remain impermissible as a rule, but now with some exceptions.

Source IP addresses. Legislation requiring general and indiscriminate retention of source IP addresses is permissible for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security. Retention must be limited to a strictly necessary period, although extensible.

Civil identity of users. Legislation requiring general and indiscriminate retention of civil identity data is permissible for the purposes of safeguarding national security, combating crime and safeguarding public security.

Situation presenting a genuine and present or foreseeable serious threat to national security. An instruction to retain traffic and location data generally and indiscriminately is permissible if such a situation exists. It must be limited to a strictly necessary period, although extensible if the threat persists. The decision imposing the instruction must be subject to effective review, either by a court or binding decision of an independent administrative body. The aim of the review is to verify that a situation justifying such a measure exists and that the necessary conditions and safeguards are observed.

The French and Belgian mandatory retention regimes were similar to the Swedish regime considered in *Tele2/Watson*, in that the legislation directly imposed a mandatory retention obligation on all service providers, covering a wide range of communications data. The CJEU had no difficulty in holding all of those regimes contrary to EU law, as mandating illegitimate general and indiscriminate retention.

- **Obligations requiring general and indiscriminate automated analysis of traffic data and location data** retained by a service provider are permissible where a situation exists presenting a genuine and present or foreseeable serious threat to national security; and on condition that recourse to automated analysis may be subject to effective review, either by a court or binding decision of an independent administrative body. Again, the aim of the review is to verify that a situation justifying such a measure exists and that the necessary conditions and safeguards are observed.

The CJEU also emphasised the care that should be taken to ensure that pre-established models, criteria and databases are specific, reliable, non-discriminatory, not based on sensitive personal data in isolation, and subject to regular re-examination; and that any positive result should be subject to individual manual re-examination before being acted upon.

- **Obligations requiring general and indiscriminate transmission of traffic and location data** to the security and intelligence agencies for the purpose of safeguarding national security are impermissible. (It follows that the same would apply to such transmission for less weighty purposes.)
- **Targeted real-time access to retained traffic and location data** (which would enable real-time tracking of online activity and physical movements) is not precluded for persons in respect of whom there is a valid to suspect that they involved in one way or another in terrorist activities. Such access must be subject to prior review either by a court or binding decision of an independent administrative body, or within a short time afterwards in the case of duly justified urgency. The aim of the review is to ensure that real-time collection is authorised only within the limits of what is strictly necessary.

The CJEU drew a distinction between a threat to national security (activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the

State itself, such as terrorist activities) and a threat to public security (the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise).

Throughout the judgments the CJEU emphasised the need for clear and precise rules laying down the substantive and procedural conditions governing the use of the data, thereby ensuring that the interference is limited to what is strictly necessary. It repeated its statement in *Schrems 2* that the legal basis which permits the interference with fundamental EU Charter rights must itself define the scope of the limitation on the exercise of the right concerned.

From a UK perspective, the judgments have implications for any contemplated adequacy determination by the European Commission once the UK becomes a third country. The UK legislation considered by the CJEU (Section 94 Telecommunications Act 1984) has now been superseded, as far as bulk transmission of communications data to intelligence agencies is concerned, by the bulk communications data acquisition warrant under the Investigatory Powers Act 2016. The 2016 Act also contains the UK's mandatory communications data retention regime, superseding the DRIPA powers that were the subject of the CJEU reference in *Tele2/Watson*. Under the 2016 Act the Secretary of State can issue retention notices to individual service providers or categories of service providers.

Both these provisions, and similarly other bulk powers in the 2016 Act such as interception and equipment interference (which cover both content and communications data), are hedged around with more safeguards than was Section 94. Most notably, they are all subject to the 'double-lock' of prior approval by an independent Judicial Commissioner. The UK can be expected to rely heavily on that as a sufficient safeguard; and on the fact that the Secretary of State issuing the warrant is required to consider that the notice or warrant is necessary and proportionate.

However, the question now is whether safeguards around broadly drawn discretionary powers are enough. The CJEU repeatedly referred to substantive conditions and limitations as well as safeguards. It has also now drawn lines demarcating when, and for what purposes, different kinds of communications surveillance technique may be utilised. These judgments may be leaning towards an expectation that hard limits will be set out in legislative instruments, rather than being left to soft limits such as factors to be taken into account and case by case assessments of necessity and proportionality by the authorities, combined with the safeguards of independent approval and oversight mechanisms.

The distinction between hard and soft limits is well illustrated by the April 2018 decision of the English High Court, in the case brought by Liberty challenging (among other things) the 2016 Act mandatory retention powers. On the court's reading of the *Tele2/Watson* decision it was sufficient if the legislation permitted decisions to be taken that were (a) sufficiently connected with the objective being pursued (b) strictly necessary and (c) proportionate, coupled with safeguards so as to achieve effective protection against the risk of misuse of personal data.

The court commented that the obligation on the Secretary of State to exercise the power only if she considered it both necessary and proportionate for one or more of the purposes listed in the Act "enshrines in the statute the essence of the tests propounded in *Watson*".

That decision may end up being considered in the Court of Appeal. The question of how far legislation must contain substantive limits is likely to come under scrutiny not only in that context, but also – as it did in *Schrems 2* for the USA – in the context of a European Commission decision on the adequacy of UK protection of personal data.

Other EU News

Date	Description
29 October	<p data-bbox="427 320 1227 351">EDPS: Strategy Document for Compliance with Schrems II</p> <p data-bbox="427 384 1702 411">The EDPS has published its strategy for compliance of EU Institutions (EUIs) with the Schrems II judgment.</p> <p data-bbox="427 448 2072 536">The strategy contains short- and medium-term compliance actions, including carrying out Transfer Impact Assessments. Interestingly, as a short term action, the EDPS strongly encourages EUIs to avoid any new processing operations or contracts that involve data transfers to the US. The EDPS is working with the EDPB & EEA DPAs on developing further guidance & recommendations.</p> <p data-bbox="427 571 1982 598">Although this strategy is applicable to EUIs only, it may give some insight into what to expect from the EDPB guidance on this point.</p>

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
10 September	CPS Advisory Limited	Monetary penalty - £130,000	<p>A report from Aviva flagged CPS Advisory Limited (CPSAL) in relation to an unsolicited live pension call. The communications service provider confirmed that the line from which these calls were made belonged to CPSAL (the account holder). CPSAL however, was unable to provide evidence of the specific consent it claimed to hold for making these calls. The ICO consequently conducted research into the websites from which CPSAL would have obtained this consent and it was clear that these sites did not allow for consent to be freely given, specific or informed. The ICO found that CPSAL had contravened Reg. 21B of PECR. As an amendment to PECR, Reg. 21B “restricts calls made for the purposes of direct marketing in relation to occupational pension schemes or personal pension schemes.” Another requirement of Reg. 21B is that to engage in such calls the caller must be an “authorised person” under the meaning given in S.31 of the Financial Services and Markets Act 2000. The ICO concluded that CPSAL was not operating from such a position, therefore could not have made these calls lawfully. The facts, such as the calls being pension calls and that the purpose of these calls was to generate further leads for a financial services provider (a form of financial gain), contributed as aggravating factors to the Commissioner’s decision of a monetary penalty. Consequently, CPSAL was fined £130,000.</p>
24 September	Digital Growth Experts Limited	Monetary penalty - £60,000 and enforcement notice	<p>Digital Growth Experts (DGE) had multiple complaints issued against it via the SPAM tool – a tool that allows mobile phone users to report unsolicited marketing text messages. Between February and April 2020, DGE sent approximately 1,076 messages. Although DGE claimed that the data used to send the messages had been collated via “website lead capture” and a list of telephone numbers collated in through interactions with the company’s online sales page, DGE was unable to provide evidence of that it had obtained consent from those individuals that had made the complaints.</p> <p>The ICO found DGE had contravened Reg. 22 PECR by transmitting electronic marketing messages without consent. The evidence provided did not suggest that individuals were aware their data would be used for purposes of direct marketing or that consent had been obtained. DGE claimed that some of the marketing texts had been sent to individuals who had previously expressed an interest in eBay offers. However, the ICO held that such interest cannot be relevant, as it is unlikely that these individuals had envisaged receiving marketing from DGE at the time of expressing interest in an eBay offer, or that they</p>

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			<p>should be considered to reasonably expect marketing from DGE in relation to hand sanitiser many years later. Therefore, the ICO was satisfied the soft opt-in exemption would not apply.</p> <p>The ICO also noted that offering products as samples could not be held as a ‘sale’ or ‘negotiation of sale’, therefore could not be relied on for the soft opt in exemption. DGE was issued with an enforcement notice and a monetary penalty of £60,000.</p>
08 October	Studios MG Limited	Monetary penalty - £40,000 and enforcement notice	<p>A complaint was made against Studios MG (SMG) in relation to an unsolicited email received by a subscriber, directing the subscriber to a website selling surgical masks. Upon investigation by the ICO, SMG stated that the subscriber’s data had been obtained via a different campaign relating to tennis. When requested for full details of the direct marketing campaign, SMG estimated the email had been sent to approximately 8,000 people, but as the data had been deleted at the point of investigation it was not able to confirm this number with accuracy. However, SMG was able to confirm it had no evidence of consent. When the ICO investigated further to identify the source of SMG’s data, SMG confirmed that it did not know how it came to have the original complainant’s email address. Furthermore, SMG stated that many of the email addresses, to which the direct marketing was targeted, “were out of date and bounced”. The ICO concluded that SMG had contravened Reg. 22 of PECR. Reg. 22 refers to the “transmission of unsolicited communications by means of electronic mail to individual subscribers”. SMG confirmed that it had sent between 8000 and 9000 direct emails for marketing purposes. However, SMG was not able to evidence any consent it had collected for the individuals that received the emails. Instead, SMG stated that it had used data that had been gathered over several years from various, vaguely described, sources. Consequently, the ICO was satisfied that SMG could not rely on the soft opt in exemption provided by Reg. 22(3) PECR as the purpose for the emails (selling personal protective equipment) had no relation to SMG’s actual purpose as a business - a “software design and build consultancy”. As a result, the Commissioner issued a monetary penalty of £40,000 and an enforcement notice against SMG.</p>
16 October	British Airways	Monetary Penalty - £20 million	<p>The ICO finally issued British Airways with a monetary penalty of £20 million on 16 Oct 2020. This was a final penalty imposed following the ICO’s original announcement last summer of its intention to impose a £183 million fine on BA for failures connected with a data breach that took place in 2018., which affected more than 400,000 customers. BA was ultimately found to have “failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Art. 5(1)(f) and Art. 32 of GDPR”. Some of the measures suggested by the ICO, as options for data controllers to follow, included the implementation of application</p>

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			whitelisting (configuring networks to ensure only certain programs/applications can be utilised by individuals that gain access to the network via a specific route), and “blacklists” which would block certain applications. The full decision explaining the ICO’s reasons can be found here. For more detail on this decision, please see our news alert .
12 October	Experian	Enforcement Notice	<p>On 27th October 2020, the ICO published a report on its investigation into data protection compliance in the direct marketing data broking sector. The ICO’s investigation focussed on offline marketing services offered by the three largest credit reference agencies (CRAs) in the UK. The investigation covered only direct marketing services and did not extend to the core credit referencing function of these companies. Also, it did not involve data collected about individuals’ online behaviour. On 12th October 2020, in connection with this investigation, the Information Commissioner published an enforcement notice on Experian, requiring it to make certain changes to its privacy notice and processing of personal data.</p> <p>The report and the enforcement notice, together, set out strict requirements in relation to: transparency and privacy notices; further processing/purpose limitation; lawful basis; and sourcing personal data from third party suppliers. For more detail on these points, please see our news alert.</p>
29 October	Reliance Advisory Limited	Monetary Penalty Notice -£250,000	<p>The ICO has fined Reliance Advisory Limited (a lead generation company for claims management services) £250,000 for making millions of unsolicited calls for the purposes of direct marketing in relation to claims management services contrary to regulation 21A of PECR (which requires prior consent). The ICO received 85 complaints from members of the public about the persistent calls they were receiving multiple times a day, often with rude and aggressive callers.</p> <p>During the ICO’s investigation, the company was unable to provide evidence for the majority of calls it made and where it did provide evidence, the consent was not found to meet relevant GDPR standards.</p> <p>The law prohibiting unsolicited calls for direct marketing purposes in relation to claims management services came into force on 8 September 2018.</p>
30 October	Marriott	Monetary Penalty Notice - £18.4million	<p>The ICO finally issued Marriott with a monetary penalty of £18.4 million for failing to keep millions of guest records secure following a cyberattack in 2014 on Starwood Hotels and Resorts which wasn’t discovered until September 2018 by which time the company had been acquired by Marriott. This penalty took into account various mitigating factors and the impact of the pandemic but was very much reduced from the £99.2million fine which had been initially proposed by the ICO in its Notice of Intent to fine. Although the security breach is thought to have lasted from 2014 to 2018, the fine was specific</p>

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			to the period after the GDPR became fully applicable – that is, from May 2018 to September 2018. The breach affected 30.1 million EEA records. The full penalty notice can be found here . For more discussion, please see our recent news alert .

Other recent articles

[The EU's Approach to AI – Recent Regulatory Developments](#)

[Cookies and other tracking devices: CNIL new guidelines](#)

HR Essentials

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

For information on the international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses, our offices, our members and partners, regulatory information, privacy, complaints procedure and the use of e-mail see www.twobirds.com/LN . Bird & Bird LLP, a limited liability partnership, registered in England and Wales with registered number OC340318, with its registered office and principal place of business at 12 New Fetter Lane, London EC4A 1JP, is authorised and regulated by the Solicitors Regulation Authority, whose professional rules and code may be found at www.sra.org.uk/handbook/ . A list of members of Bird & Bird LLP and of any non-members who are designated as partners, being lawyers or other professionals with equivalent standing and qualifications, and of their respective professional qualifications, is open to inspection at its registered office. References in this document to “Bird & Bird”, the “firm”, “we” or “our” mean Bird & Bird LLP and the other affiliated and associated businesses authorised to carry the name “Bird & Bird” or one or more of Bird & Bird LLP and those affiliated or associated businesses as the context requires.

twobirds.com

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

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.