Bird & Bird

UK & EU Data Protection Bulletin: May 2020

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

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

United Kingdom

ICO

UK Cases

EU and Council of Europe

EDPB

CJEU Cases

Other EU news

UK Enforcement

ICO enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
19 March	**New CCTV Guidance and Templates** The Surveillance Camera Commissioner and the ICO have updated their CCTV DPIA guidance and template on 1 April 2020 to fully reflect the requirements under GPDPR and the Data Protection Act 2018. It has been designed for entities that have to comply with the Surveillance Camera Code of Practice under Section 33(5) of the Protection of Freedoms Act 2012 such as local authorities and police forces etc. However, it can also be used by private companies that deploy surveillance cameras in the UK. According to the explanatory notes, the SCC recommends carrying out a DPIA where: • cameras are added or removed from systems or where existing cameras are moved or their direction is changed; • whole or parts of systems are upgraded; • new systems are installed; and • where systems that include biometrics capabilities such as automatic facial recognition are put in use. The DPIA template contains 20 questions, and relevant guidance/explanatory notes have been provided within each question.
15 April	**How the ICO will regulate during the Coronavirus** The ICO has issued a short paper about how it will regulate during the pandemic in order to take account of the fact that organisations are facing staff and operating capacity shortages as well as acute financial pressures and many public bodies are facing severe front-line pressures and are redeploying resources to meet those demands. The ICO confirms that it is committed to taking an "empathetic and pragmatic approach" to enforcement, focussing on the most serious challenges and greatest threats to the public and will take firm action against those looking to exploit the public health emergency through nuisance calls or by misusing personal information. It states that when dealing with the public's complaints about organisations, its approach will take into account the impact of the crisis which may mean resolving the complaint without contacting an organisation, or that it gives it longer than usual to respond or to rectify any breaches associated with delay if it is recovering its service and gradually improving timescales. Personal breach reporting should continue, without undue delay but the ICO acknowledges that the 72hour timescale for reporting may be impacted and it will assess these reports, taking an appropriately empathetic and proportionate approach. Reassuringly, the ICO also confirms that in deciding whether to take formal regulatory action, including issuing fines, it will take into account whether the organisation's difficulties result from the crisis, and if it has plans to put things right at the end of the crisis. The ICo

Date	Description
	may give organisations longer than usual to rectify any breaches that predate the crisis, where the crisis impacts the organisation's ability to take steps to put things right. Before issuing any fines, the ICO will take to account the economic impact and affordability stating that this is likely to mean the level of fines reduces. The ICO may also decide not to enforce against organisations who fail to pay or renew their data protection fee, if they can evidence that this is specifically due to economic reasons linked to the present situation, and provided we are adequately assured as to the timescale within which payment will be made. For more detail about the ICO's regulatory approach, see here.
16 April	**Videoconferencing: ICO Tips** The ICO's Director of Assurance has released a short blog advising organisations about how to safely roll out the latest video conferencing technology to ensure that staff can communicate securely. His top tips include: • **Checking the privacy and security settings –** it is important that you check the default privacy and security settings and make use features such as restricting access to meetings using passwords, controlling when people join the meeting and controlling who is allowed to share screens and record the meeting. Check whether the meeting is covered by end to end encryption. Be careful about who and how you share the meeting ID or password. Users will need to know how their data will be processed as well as having choice and control over it. Participants should also remember to turn off their webcam when the call ends to avoid cybercriminals using spyware to watch the participants. • **Look out for phishing scams in a video chat –** the live chat feature can be used by malicious people to spread phishing messages. • **Ensure that your employees are using a video conference platform that matches your policies and procedures rather than the preferred app they might use to keep in touch with friends and family** • **Regularly update your video conferencing software – whether via an app or browser** It is also important to understand what personal data the video conferencing app is actually processing about the participants in any call and for what purpose– for instance is data being used for targeted advertising (and can users easily stop such processing) or does the app get access to all of an employee's contacts in their device?
17 April	**Using new technologies and tracking to combat the pandemic: Key Data Protection Questions to consider** Elizabeth Denham released a new blog examining some of the relevant privacy issues that organisations exploring the possibility of using contact tracing and location tracking technologies to combat the Covid-19 will need to think about. The ICO states that it is here to offer advice and guidance to organisations ahead of such projects and can provide assurance via audit once a project is up and running. This follows on from the ICO's Statement about Data Protection and Coronavirus on 12 March which confirmed that that data protection laws will not get in the way of innovative use of data in a public health emergency – as long as the principles of the law (transparency, fairness and proportionality) are applied.

Date	Description
	The key issues to consider are: • Can you demonstrate how principles of data protection by design and by default have been built into the technology –this is likely to require an initial privacy impact assessment. • Can you show that the planned collection and use of personal data is necessary and proportionate? This is particularly important in the context of "location data". • Looking at the control users have over their data and whether they can exercise their rights • Considering how much data needs to be gathered and processed centrally. The starting point should be to shift processing to the individuals' devices where possible. • What governance and accountability processes are in place for ongoing monitoring and evaluation of the data processing to ensure it remains necessary and effective and that appropriate safeguards continue to be used? • What happens when the processing is no longer necessary? The ICO notes that this point is crucial – what is appropriate and proportionate in an international health emergency will look quite different when that emergency ends. The ICO has also published an Opinion regarding Google and Apple's joint work to enable the use of Bluetooth technology to help governments and health agencies use contact tracing to reduce the spread of Covid-19 which confirms the project appears to broadly align with the principles of data protection by design and default, while being clear that app developers must still take their own measures to ensure they comply with data protection law. The Opinion is primarily aimed at organisations involved in the project but it may be of interest to those involved in other contact tracing initiatives.

UK Cases

Date	Cases
9 January	**Leighton v Information Commissioner (No.2) [2020] UKUT 23 (AAC)** This case concerns section 166 of the Data Protection Act 2018 ("**DPA**") and the jurisdiction of the First-tier Tribunal ("**FTT**"). Under section 166, a data subject can apply to the FTT where, in relation to the data subject's complaint under section 165 of the DPA or Article 77 of the GDPR, the ICO (a) fails to take appropriate steps to respond to the complaint; (b) fails to provide the complainant with information about progress on the complaint, or of the outcome of the complaint, before the end of the period of 3 months beginning when the ICO received the complaint; or (c) if the ICO's consideration of the complaint is not concluded during that period, fails to provide the data subject with such information during a subsequent period of 3 months. The FTT has powers to make an order requiring the ICO to take appropriate steps to respond to the complaint or to inform the data subject of progress on the complaint, or of the outcome of the complaint, within a period specified in the order. In response to a complaint from Mr Leighton that North Yorkshire Police had not complied with its obligations in relation to a subject access request submitted by Mr Leighton under section 45 DPA, the ICO had concluded that North Yorkshire Police had complied. Mr Leighton filed an appeal with the FTT against the ICO's decision and the FTT rejected his application. Mr Leighton then appealed the FTT'S decision with the Upper Tribunal, but this appeal was dismissed on the basis that the FTT does not have jurisdiction in relation to the enforcement of section 45. In discussing the scope of section 166 and the FTT's jurisdiction, Judge Wikeley said: "*Section 166 is directed towards providing a tribunal-based remedy where the Commissioner fails to address a section 165 complaint in a procedurally proper fashion. Thus, the mischiefs identified by section 166(1) are all procedural failings. "Appropriate steps" mean just that, and not an "appropriate outcome". Likewise, the FTT's powers include making an order that the Commissioner "take appropriate steps to respond to the complaint", and not to "take appropriate steps to resolve the complaint", least of all to resolve the matter to the satisfaction of the complainant. Furthermore, if the FTT had the jurisdiction to determine the substantive merits of the outcome of the Commissioner's investigation, the consequence would be jurisdictional confusion, given the data subject's rights to bring a civil claim in the courts under sections 167-169.*" In summary, it was held that section 166 and FTT's powers cover procedural issues with the ICO's approach to complaints rather than issues regarding the substance of the outcome of the ICO's investigation. For substantive issues, the courts have jurisdiction.
3 March	**Scott v LGBT Foundation Ltd [2020] EWHC 483 (QB)** In this judgment, Saini J in the High Court struck out claims for breach of the Data Protection Act 1998 (DPA), the law of confidence and the Human Rights Act 1998 (HRA) which stemmed from an allegedly non-consensual, verbal disclosure of information about the claimant by a charity to the claimant's GP.

Date	Cases
	In seeking counselling from the LGBT Foundation, Mr Scott had disclosed information about himself and his personal situation to the charity. Mr Scott completed various forms on self-referral, some of which stated that, "*if there is reason to be seriously concerned about your welfare, we may need to break confidentiality without your consent to help you stay safe*". The charity was of the view that Mr Scott posed a significant risk to his own health and well-being, and so orally communicated this to Mr Scott's GP. The charity informed Mr Scott (both orally and by follow-up email) that it intended to make this disclosure to his GP. Mr Scott's GP recorded the information about which it had been informed in Mr Scott's personal GP file. Mr Scott, a nuclear safety consultant, sought damages in excess of £1.8 million for breach of the DPA, the law of confidence and the HRA on the basis that the information recorded in his GP file contradicted information which he had disclosed during the background checking process for his current job role. As regards the DPA claim, Saini J found that the DPA "*does not apply to purely verbal [sic] communications*". This is on the basis that 'data', as defined by s 1 (1) DPA, must be recorded in electronic or manual form. Oral communication of information, notwithstanding any intention that this would be subsequently recorded, does not constitute data; such that, it could not constitute 'personal data', as defined by s 1 (1) DPA. Such communications are instead protected by the law of confidence. Saini J further found that, even if the disclosure had amounted to the processing of personal data, it would have been justified as necessary in order to protect the vital interests of the claimant.
1 April	**Hands down – no representative action for Equifax** Counsel for Equifax *blogged* on 1 April 2020 that a representative action brought by Richard Atkinson in the High Court of England and Wales had been withdrawn. Atkinson's claim, brought under the Data Protection Act 1998, stemmed from a large scale personal data breach at Equifax in 2017 which was the resulted from a malicious cyber-attack. One of the interesting points in the claim was Atkinson's attempt to claim damages in this scenario under the novel "loss of control" head (i.e., without proving pecuniary loss or distress). Many data elements collected by Equifax were (as expected, for a credit reference agency) not collected from data subjects directly, but from third party data controllers. It remains to be seen if and how this new "loss of control" head for damages in data protection and privacy cases will play out. Recognised, in principle, by the Court of the Appeal in Lloyd v Google LLC [2019] EWCA Civ 1599, the Supreme Court has reportedly confirmed that on 11 March 2020 it granted Google LLC leave to appeal, and a hearing is not expected (pre-Covid-19) until late 2020 or early 2021.
1 April	**Employers breathe a sigh of relief following the Supreme Court decision in Morrisons** In a unanimous decision on 1 April 2020, the Supreme Court reversed the Court of Appeal's decision that found Morrisons vicariously liable for a data breach committed by a rogue employee. The Supreme Court held that the Court of Appeal "misunderstood the principles governing vicarious liability in a number of relevant respects". Click here to read full article.

25 March

Elgizouli (Appellant) v Secretary of State for the Home Department (Respondent) [2020] UKSC 10

In its judgment on the Elgizouli case, the Supreme Court unanimously held that the Secretary of State breached the Data Protection Act 2018 by transferring personal data to US law enforcement authorities for use in capital criminal proceedings.

Background

The appellant's son is alleged to have been part of a group of terrorists involved in the murder of US and British citizens in Syria. In June 2015, the US made a request to the UK under the treaty for Mutual Legal Assistance ("MLAT") in respect of a criminal investigation into the activities of this group of terrorists, looking for material gathered by the UK police as part of a UK investigation into this group. In line with a long-standing policy, the Home Secretary initially requested, as a pre-condition to the supply of information, an assurance that the information would not be used directly or indirectly in a prosecution that could lead to the imposition of the death penalty. However, a full death penalty assurance was not provided by the US and ultimately, in June 2018, the Home Secretary decided to provide the information to the US without requiring any assurance whatsoever.

The Divisional Court dismissed the appellant's claim for a judicial review of the MLAT provision, but certified the following two question of law of public importance:

(i) Whether it is unlawful for the Secretary of State to exercise his power to provide mutual legal assistance so as to provide evidence to a foreign state that will facilitate the imposition of the death penalty in that state on the individual in respect of whom the evidence is sought; and

(ii) Whether (and if so in what circumstances) it is lawful under Part 3 of the Data Protection Act 2018 for law enforcement authorities in the UK to transfer personal data to law enforcement authorities abroad for use in capital criminal proceedings.

1. Facilitating the death penalty

The Supreme Court dismissed the first ground of the appeal and held that the common law has not developed to recognise a principle prohibiting the provision of mutual legal assistance that will facilitate the death penalty.

The majority took the view that the key legal developments in respect of the death penalty come from the European Convention on Human Rights ('ECHR') and not from domestic courts. In this respect, the law (the Crime (Overseas Production Orders) Act 2019, section 16) imposes an obligation to seek death penalty assurances; nothing in the law specifically prohibits the Home Secretary from exchanging material where he had sought *but not received* death penalty assurances. The common law cannot be construed to have evolved so as to prohibit the transfer of information in these circumstances.

A dissenting opinion supported that a common law "non-facilitation" principle should be recognised whereby it is deemed unlawful –with very limited exceptions– to facilitate the trial of any individual in a foreign country where to do so would put that person in peril of being executed. On the basis that the provision of information in these circumstances breached this common law principle, the dissenting opinion found that the processing of personal data was also for this reason unlawful. However, this view was not endorsed by the majority, which –as explained below– focussed on the absence of the necessary conditions for such data transfer.

2. Data Protection Act 2018 ('2018 Act')

On the second ground, the court unanimously held that the MLAT decision was unlawful under the 2018 Act.The processing of data by the

Secretary of State required a conscious, contemporaneous consideration of whether the criteria for such processing were met. "Substantial compliance" with those criteria, as found by the Divisional Court and as claimed by the respondent, was not enough. A direct, personal evaluation was required, which undisputedly did not occur in this case: the decision was based on political expediency, rather than strict necessity under the statutory criteria.

Part 3 of the 2018 Act, which transposed the EU Law Enforcement Directive ('LED'), makes provision for data processing by competent authorities for law enforcement purposes. Under s.73, data transfers to a third country must meet, among others, the following conditions:

a) the transfer must be *necessary* for any of the law enforcement purposes; and

b) in the absence of an adequacy decision, the transfer must be either based on there being appropriate safeguards (as set out in s. 75), or based on special circumstances (as further specified in s. 76).

The Court found that there were no appropriate safeguards and that the transfer did not meet the special circumstances criterion either. It was held that the above conditions required a strict necessity test which must include a proportionality assessment. The controller must address his mind to the proportionality of the transfer; however, this was not the case here.

In addition, in relation to safeguards, the Court quoted Recital 71 LED, pursuant to which "the controller should take into account that the personal data *will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment*". Although recitals are not binding and serve only as interpretative aid, it was held that the wording used here seems to leave little room for discretion and the expectation is that the safeguards will be designed to achieve that objective. Given that in this case the information was transferred without any safeguards at all, it transpires that the Secretary of State could not have regarded this condition as satisfied.

In respect of special circumstances, the Court identified that only two of the circumstances listed in the 2018 Act (s. 76(1)(d) & (e)) could be relevant in this case, namely, that the transfer is necessary (i) in individual cases for any of the law enforcement purposes, or (ii) in individual cases for a legal purpose. Recital 72 LED mentions that this gateway should be interpreted restrictively and be limited to data *strictly* necessary. Again, this requires a strict necessity test, where the proportionality of the transfer should be assessed. However, as the Secretary of State did not address his mind to the 2018 Act at all, such condition cannot be deemed to be met.

It is worth noting that the two circumstances above (s. 76(1)(d) & (e)) do not apply if the controller determines that "*fundamental rights and freedoms of the data subject override the public interest of the transfer*" (s. 76(2)). One of the judges found that these fundamental rights and freedoms include the rights protected by the ECHR, the most fundamental of which is the right to life and that this points towards an interpretation that s. 76(2) would not allow the transfer of personal data to facilitate a prosecution which could result in the death penalty. However, this point was not fully argued and examined by the Court.

12 March

Dawson- Damer Court of Appeal [2020] EWCA Civ 352

On 12 March the Court of Appeal handed down its second judgment in the long running case of Dawson Damer v. Taylor Wessing [2020] EWCA Civ 352.

Readers may recall the appellants were beneficiaries under a Bahamian Trust. The trustees had appointed the majority of the trust fund to new trustees to hold for the beneficiaries, excluding the appellants. The appellants challenged this arrangement. As part of this, they made a subject access request to Taylor Wessing LLP which acted for the trustees of one of the trusts.

There were two questions before the Court of Appeal, both of which pertained to the subject access request:

1. Were Taylor Wessing entitled to rely on the exemption for subject access for legal professional privilege thereby meaning the information did not have to be released as part of the access request?

2. Did Taylor Wessing's paper files, ordered chronologically, constitute a relevant filing system within section 1(1) of the Data Protection Act 1998 (DPA 1998)?

On question 1, the Court found that Taylor Wessing weren't entitled to rely on the legal professional privilege exemption - with the Court ruling that a trustee cannot withhold documents requested by a beneficiary by calling on a legal professional privilege exemption provided in the DPA 1998 because that privilege also extends to the beneficiary.

It's question 2, however, that will be of most interest to data protection practitioners. The previous trial judge had found that 35 paper files held by Taylor Wessing referred to as the 'Yullis Trusts' were a relevant filing system and ordered Taylor Wessing to search the files for the purposes of the access request.

In assessing the issue of whether the files were 'a relevant filing system' the Court had regard, among other matters to ICO Guidance, Durant v Financial Services Authority [2003] EWCA Civ 1746 and the CJEU's approach Tietosuojavatuutettu (EU:C:2018:551).

Having reviewed the authorities, the Court found the questions to be asked were the following: first, are the files a structured set of personal data? secondly is the data accessible according to specific criteria? thirdly, are these criteria 'related to individuals', and fourthly, do the specific criteria enable the data to be easily or 'readily' retrieved?

The determining factor in this case was the final criterion of ready accessibility: this the Court found was not met.

According to the Court, the files were, beyond their chronological compilation, 'completely unstructured' and the trial judge had lost sight of the need for the causative link between that criterion and the ease of retrieval of the data. It was thus misplaced for the trial judge to conclude that just because a trainee lawyer and an associate solicitor could extract personal data from the files that they were easily accessible:

'*the ready access required under the Directive and the Act must be enabled by the criteria, that is to say by the structure of the files. If access to the relevant data requires the use of trainees and skilled lawyers turning the pages of the files and retrieving the material identified that is a clear indication that the structure itself does not enable ready access to the data*'.

The Court also concluded that this was in line with ICO's 'temp test' i.e. ICO's rule of thumb of whether a reasonably competent temp would be able to extract the specific information about an individual from manual records without any particular knowledge of the type of work or the documents held. In this case, the Court found, the temp would not.

EU and Council of Europe

EDPB

Date	Description
March & April	**Data processing and Covid-19 – EDPB statement** Like many national authorities around the EU, the European Data Protection Board released a statement about data processing in the context of the current pandemic. The EDPB underlines that data protection is not a barrier to combatting the coronavirus, but that personal data must continue to be protected despite the unprecedented situation. The EDPB addressed four main areas in which issues may arise: Legal basis In an employment context, Article 9(2)(b), (c) or (i) GDPR could apply, depending on the processing and the jurisdiction. The EDPB refers to recital 46 which specifically discussed the control of epidemics. In relation to telecoms data, the ePrivacy Directive is also relevant. Generally location data can only be used with consent but Article 15 of the Directive allows member states to introduce provisions to safeguard public safety, if it necessary, appropriate and proportionate, and compatible with human rights. Such measures are also subject to judicial control from the European Court of Justice and the European Court of Human Rights. Data protection principles Transparency must be maintained to allow individuals to understand how their data is used. The security and confidentiality of data collected in the context of Covid-19, and any new processing decisions taken in light pandemic must be properly documented. Mobile location data Some countries are considering using location data to monitor and prevent the spread of coronavirus. The EDPB asks public authorities to process this in anonymous way if possible, and only introduce specific legislation to safeguard public safety if the anonymised data is not sufficient. Governments should preferentially use the least intrusive solution. Employment The EDPB has answered four employment specific questions:

	- Health information can be asked of employees or visitors, if proportionality and data minimisation are followed and where allowed by national law - Employers can only carry out medical checks on employees if required by national law - Employers can inform other staff about Covid-19 cases, if allowed by national law. Data minimisation should be followed and only the necessary data should be disclosed. - Employers are allowed to collect personal information in order to manage the current pandemic, and so far as is allowed under national law.
21 April	Following its remote plenary meeting on 3 April 2020, the EDPB has adopted further Guidance on data protection issues arising in the context of the Covid-19 crisis: 1. **The processing of health data for scientific research purposes.** The Guidance sets the scene by providing a wide interpretation of what is meant by "*data concerning health*" including information that becomes health data (i) by cross referencing with other data thus revealing the state of health or health risks or (ii) because of its usage in a specific context (such as information about a recent trip to a region affected by Covid-19). Recital 159 of GDPR also gives a wide interpretation of the term "*scientific research*" although the former Art 29 Working Party has already pointed out that this term should not be stretched beyond its common meaning and should be understood to mean " *a research project set up in accordance with relevant sector related methodological and ethical standards, in conformity with good practice.*" The Guidance focusses on the following points: **Legal Basis:** EDPB suggests that explicit consent may be a valid ground under GDPR but that Article 6(1) (e) or (f) GDPR in combination with the enacted derogations under Article 9(2)(i) or (j) can also provide a legal basis. However, the conditions and the extent for such processing will vary depending on the enacted laws of the particular Member States. The derogations and limitations in relation to the protection of data provided in Article 9(2)(j) and Article 89 must apply only in so far as is strictly necessary. **Transparency:** Individuals must be told that their health data is being processed for scientific purposes including when this has not been obtained directly from the individuals (unless an exemption applies)– in case of further processing for scientific purposes, this notice should be given to individuals within a reasonable period of time before the implementation of the new research project **Purpose Limitation:** The Guidance states that the "compatibility" presumption provided by Article 5 (1) (b) GDPR will be considered in more detail in the future given its complex nature. **Security, Retention & Data Minimisation:** Given the processing risks, high emphasis must be put on ensuring that the processing is secure. Data should be anonymised where possible and proportionate storage limits should be set. A DPIA may be required where the processing is likely to result in a "*high risk to the rights and freedoms of natural persons*" and DPOs consulted. **Individual Rights:** In principle, emergency situations like the Covid-19 outbreak do not suspend or restrict the possibility of data

subjects to exercise their rights but the restrictions of the rights may vary depending on the enacted laws of the Member States.

Data Transfers: Within the context of Covid-19 research, there is likely to be the need for international cooperation that may also require international transfers of data outside of the EEA. EDPB notes that in the absence of an adequacy decision or other appropriate safeguard that the derogation addressed in Article49(1) (d) (transfer necessary for reasons of important public interest or explicit consent may apply.

More detailed guidance on this topic is expected as part of the EDPB's annual work plan. The guidance does not address the processing of personal data for epidemiological surveillance.

2. The use of the use of location data and contact tracing tools

These Guidelines clarify the conditions and principles for the proportionate use of local data and contact tracing tools for two specific purposes:

- Using location data (e.g. collected by telcos or by information society service providers' applications offering navigation or transportation services) to support the response to Covid-19 by modelling the spread of the virus so as to assess the overall effectiveness of the confinement measures;
-
- Contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus so as to break the contamination chains as early as possible.

The overall message from this Guidance is that whilst automated data processing and digital technologies will be key in the fight against Covid-19, one should not have to choose between an efficient response to the crisis and the protection of our fundamental rights. What is important is to ensure that every measure taken in this pandemic is necessary, time limited, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation to ensure that our individuals rights and freedoms are not eroded in the process.

Location Data

The Guidelines remind us that the use of location data collected from electronic communication providers is restricted under the ePrivacy Directive and can only be transmitted to authorities or other third parties if they have been anonymised by the provider, or for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of users.

Location data (and other information) collected directly from the terminal equipment, will also require user consent under Art 5(3) of the ePrivacy Directive unless the access is strictly necessary for the information society service explicitly requested by the user (although noting that there may be further derogations when they constitute a necessary, proportionate measure within a democratic society to certain objectives). Additional conditions apply before location data collected by an information society service can be re-used for modelling purposes.

Ideally, preference should be given to the processing of anonymised data rather than personal data but the Guidelines warn against the difficulty of effectively anonymising location data. To achieve anonymization, the EDPB suggests that location data must be carefully processed in order to meet the "reasonability" test (i.e. removing the ability to link the data with an identified or identifiable natural person against any "reasonable" effort) which will include considering location datasets as a whole as well as processing data from a reasonably large set of individuals using available robust anonymization techniques

Contact Tracing

In EDPB's view, the systematic and large scale monitoring of location and/or contacts between individuals can only be legitimised by relying on voluntary adoption by the users for each of the respective purposes. In terms of how such processing can be carried out lawfully under the GDPR, EDPB recommends the following:

Accountability: The controller(s) should be clearly established at the outset and explained to users. In some instances, the national health authority might be the appropriate controller. A DPIA must also be carried out before implementing such tools.

Purpose Limitation: The purpose must be specific enough to exclude further processing for purposes unrelated to the management of the Covid-19 health crisis. Any use of data must be adequate, necessary and proportionate.

Lawful Basis of Processing: Consent will be required (under the ePrivacy rules) where the contact tracing applications involve storage/access to data stored on the user's terminal device (unless an exception applies). The EDPB notes that the mere fact that the use of contact tracing applications takes place on a voluntary basis does not mean that the processing will necessarily be based on consent – if a public authority provides a service based on a mandate assigned by and in line with the requirements laid down by law, the most relevant ground will be that set out in Article 6(1)(e) GDPR (necessity for the performance of a task in the public interest) which will be further defined by Member State laws. This will however require the incorporation of meaningful safeguards (such as the voluntary nature of the application, clear specification of purpose, and more importantly, when the application will be dismantled and who is responsible for making that decision etc). However, consent remains an option if the specific requirements under GDPR for obtaining such consent can be met.

If the application also leads to a collection of health data (ie status of an infected person), then EDPB suggests that this will be allowed under Article 9(2)(h), Article 9(2)(i) or possibly Article 9(2)(a). Article 9(2)(j) also allows for health data to be processed when necessary for scientific research or statistical purposes (see other Guidelines above).

Retention: Personal data should only be kept for the duration of the Covid-19 crisis and then erased or anonymised.

Security, Data Minimisation & Privacy by Design: Careful consideration should be given to these principles and the data processed should be reduced to the strict minimum. In particular, proximity data (rather than tracking the location of individuals users) should be used, steps should be taken to prevent re-identification of users and collected information should reside on the users' devices where possible and extracted only when absolutely necessary. State of the art cryptographic techniques must be implemented to secure the data stored in servers and applications and in the exchanges between the applications and remote servers. The Guidelines contain more detailed recommendations on these measures.

Use of AI: Any algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel

	to limit the occurrence of false positives and negatives and the task of providing advice on next steps should not be based solely on automated processing. Algorithms must be auditable and regularly reviewed by independent experts and the source code should be made publicly available for the widest scrutiny. The Guidelines end with more detailed general guidance and recommendations aimed at designers and implementers of contact tracing applications. On 14th April, the EDPB also adopted a letter concerning the European Commission's draft Guidance on apps supporting the fight against Covid-19. This Guidance on data protection and privacy implications complements the European Commission's Recommendation on apps for contact tracing, published on 8 April and setting out the process towards a common EU toolbox for the use of technology and data to combat and exit from the COVID-19 crisis. The EDPB considers that the development of the apps should be made in an accountable way, documenting with a data protection impact assessment all the implemented privacy by design and privacy by default mechanisms. In addition, the source code should be made publicly available for the widest possible scrutiny by the scientific community. The EDPB's letter is available here.
4 May	**EDPB published updated guidance on consent** On the 04 May the European Data Protection Board (EDPB) adopted a slightly updated version of its guidelines on consent under the GDPR to address implied consent and cookie walls. The opinion clarifies that cookie walls are not valid. According to the EDPB: *'In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls).'* So for example, the EDPB state it would not be valid for a website to make its content conditional on the user accepting cookies: *'since the data subject is not presented with a genuine choice, its consent is not freely given'*. The opinion further clarifies that scrolling or swiping through a webpage does not constitute a clear and affirmative action that can signify GDPR standard consent. According to the EDPB: *'Based on recital 32 [GDPR], actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.'* The legality of cookie walls is a difficult issue that often engage other rights such as freedom of expression, the right to own property and the freedom to run a business. Therefore the EDPB's opinion is unlikely to be the last we hear on the point. The EDPB's comments on scrolling and swiping may, however, push those data protection authorities which are still arguing that implied consent to cookies is valid (such as the AEPD in Spain) to re-think their position. The updated opinion is available here.

CJEU

Date	Description
5 March 2020	**Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Cases C-61/19) Advocate General's Opinion: Examining the definition of "consent"** On 5 March 2020, Advocate General (AG Szpunar) handed down his Opinion in Case C-61/19 Orange România SA, a case which could impact how companies across a wide range of sectors obtain GDPR consents, offline or online. Orange Romania has challenged a fine and a data destruction order issued to it by the Romanian Data Protection Authority (the ANSPDCP). The ANSPDCP claims that Orange Romania has failed to demonstrate that it validly obtains customer consents to its retention of copies of identity documents. When signing up for Orange Romania's mobile telecoms services, Orange Romania's practice was to take a copy of customers' identity documents, which it would then store as an attachment to the signed customer contracts. The contract wording included, inter alia, a relatively lengthy passage about this practice, including a statement that the customer had been fully informed of, and had freely and expressly consented to, the collection and storage of those copies. This consent was further demonstrated by the customer ticking boxes on the contract itself. In some cases, customers refused to tick the aforementioned box; Orange Romania's practice was to require the customer to record this refusal in writing; after which point it would then nevertheless let the new customer sign up for the service. Orange Romania further claims that the individual's freedom to refuse was explained to them orally, albeit not in writing. Despite this, the ANSPDCP claimed that Orange Romania could not demonstrate that the customers who did sign the box, had in fact been properly informed of the optionality of that consent before they gave it. AG Spzunar's opinion provides a detailed look at recent CJEU caselaw on consent, and he advises the CJEU to rule, inter alia, that: - For consent to be valid, "*[t]he data subject must be informed of all circumstances surrounding the data processing and its consequences. In particular he or she must know which data are to be processed, the duration of such processing, in what way and for which specific purpose. He or she must also know who is processing the data and whether the data are intended to be transferred to third parties. Crucially, he or she must be informed of the consequences of refusing consent: is consenting to the data processing a condition for concluding the contract or not*?" - "*The burden of proof (...) squarely lies with the entity carrying out the processing*." Therefore, *"[a]ny doubts concerning the giving of consent of the data subject are to be eliminated by evidence to be provided by the controller*." - In Orange Romania's case, AG Szpunar therefore suggests that the CJEU rule in the ANSPDCP's favour. For the AG, several points support this conclusion: - the company's confusing records of its instructions and processes for salesperson did not help it meet the evidential burden;

	○ moreover, the company's requirement that individuals take an action to refuse consent meant that the consent was not "*freely given*" (because "*the customer is put into a situation in which he or she perceptibly deviates from a regular procedure*", and will therefore "*feel that their refusal to consent (...) is not in line with regular procedures*"); and ○ finally, the company failed to make it "*crystal-clear to the customer that a refusal to the copying and storing of his or her ID card does not make the conclusion of a contract impossible*" – so the consent was not "*informed*". A final ruling in the case is expected later this year, unless delayed due to Covid-19. See here for the Opinion.

Other EU News

Date	Description
18 March	**EDPS Publishes its 2019 Annual Report** The EDPS has published its Annual Report which provides an insight into all its activities over the past year. See here for a copy of the Report.
March	**EDPS Guidance to use of Photo Booths** On a lighter note, the EDPS has just published new guidance on the use of photo booths by EU institutions recognising that these are a great way for such institutions to reach out to the public and they are frequently used during events. Given that photo booths are used publicly, with the aim of generating a positive customer experience, it would be counterproductive for EU institutions to use them in a way that could violate anyone's fundamental right to data protection. Once we are all back to work again, this guidance could be of more general interest to other organisations who hire out or use such booths at their events. Please see here for the Guidance.
25 March	**Using Telecoms Data for Covid-19 tracking – comments from the EDPS** The European Commission announced plans to monitor the spread of coronavirus using telecommunications data. The European Data Protection Supervisor (EDPS) was consulted and provided their comments in an open letter to the Commission. The EDPS confirmed that EU data protection law is flexible enough to allow some personal data to be used to combat the pandemic, and went on to clarify some of the issues that arise from using telecoms data for monitoring public health. The EDPS pointed out that anonymised data is outside the scope of data protection laws, but that this requires proper measures to be taken to make the data truly anonymous. If a third party is involved in the monitoring, the Commission will need to consider the third party's security and confidentiality, to make sure that the data is not used for other purposes. Lastly, the EDPS expressed its concerns about data retention. As this data is collected to combat the current pandemic, its processing should be temporary and the use of telecommunication data should be considered extraordinary rather than routine. The data should be deleted as soon as the current health emergency ends.

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
27 March	Black Lion Marketing Ltd.	Monetary penalty (under PECR)	Black Lion Marketing Ltd (BLM Ltd) fined £171,000 for making unsolicited direct marketing calls. This penalty has been issued in the context of a series of investigations started in 2017 into companies with links to Kurlos Sami Asaad who is a director of BLM Ltd. The ICO received a number of complaints relating to unsolicited direct marketing calls made by BLM Ltd. On 12 March 2019, the Commissioner sought and executed a search warrant. The ICO investigations established that 240,576 calls were made to subscribers who had been registered with the telephone preference service (TPS). In total 233 complaints were made regarding unsolicited marketing calls made by this company. After receiving the warrant, BLM Ltd took steps to enter voluntary liquidation to avoid regulatory actions. In light of the seriousness of the breaches and a list of aggravating factors (e.g. the use of multiple fictious company names during the course of its unsolicited direct marketing campaigns), the ICO decided to issue a penalty of £171,000. This must be paid by 1 May 2020 at the latest.

COVID-19

Please click here to view our Privacy & Data Protection COVID-19 site with regularly updated country guidance, webinars and more.