Bird & Bird

UK & EU Data Protection Bulletin: Highlights from Summer 2019

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

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

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
July	**ICO guidance on cookies** In July, the ICO published its cookie guide, accompanied by a short myth-busting article on the topic. The ICO's cookie consent banners have also been changed, to reflect the new guidance. The guidance emphasises that the user must give specific, freely given and unambiguous consent to the cookies prior to the cookie being dropped, and that consent cannot be implied from the user continuing to browse the site. Users must be given a clear option to accept or decline, and the accept button should not be given more prominence than the decline option. Pre-ticked boxes or "sliders" are also not valid forms of consent. Cookie walls, in which a user is asked to consent before they can continue to the site, are unlikely to constitute "freely given" consent. The ICO is still seeking industry views on cookie walls, so this point of the guidance may change in the future. The new guidance also emphasises that there is no exemption to the consent requirement for analytics cookies, as these are distinct from strictly necessary cookies. The interplay between the GDPR and PECR is also discussed. As consent is required under PECR, the ICO encourages organisations to also rely on consent as a legal basis under GDPR, although it does not rule out that another lawful basis may be possible. You can read more about the guidance in our article. The CNIL has also published guidance on cookies this summer – you can consult our comparison table to find out more about the differences and similarities.
16 July	**Data sharing: ICO publishes new draft code on data sharing** On 16 July 2019, the ICO published an updated draft data sharing code of practice, which explains and advises on changes to data protection legislation relevant to data sharing. It offers practical guidelines and good practice, addressing many aspects including transparency, lawful bases for processing, accountability principle and the requirement to record processing activities. The updated draft code is now out for public consultation (open until Monday 9 September 2019). Feedback can be submitted via the ICO's online survey or email. Key points from the new draft code are summarised below. **What does the code cover?** It covers personal data sharing, whether in a routine, systematic way or on a one-off basis, by organisations acting as controllers subject to the processing regimes under the GDPR and Part 2 of the UK Data Protection Act 2018 (DPA), and also the Law Enforcement (LE) regime in Part 3 of the DPA.

Date	Description
	What is the effect of the code? Under section 127 of the DPA, the ICO must take the code into account when considering whether organisations have complied with their data protection obligations in relation to data sharing. In particular, the ICO will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR or the DPA. **Misconceptions and clarification** The code clears up some common concerns about data sharing, further clarifying that: • Data protection does not prevent data sharing, nor does it present additional barriers to sharing data • Sharing data can be beneficial if "done well"; and • Data might be shared without consent or in an emergency. **What should we learn from the code?** Legal requirements and practical recommendations are detailed in the code. In addition to guidance on key data protection principles (lawfulness, fairness and transparency, accountability, security, etc.) and rights of individuals, the following points may be of particular interest: - Data pooling: The code mentions data pooling as a form of data sharing "where organisations decide together to pool information they hold and make it available to each other or to different organisations". In this scenario, organisations responsible for the data sharing would be regarded as joint controllers under Article 26 of the GDPR. - References to the Digital Economy Act 2017 (DEA): Some parts of the code also refer to the DEA, under which the Government has devised a framework for the sharing of personal data, for defined purposes across specific parts of the public sector. This aims to "improve public services through the better use of data, while ensuring privacy, and to ensure clarity and consistency in how the public sector shares data". The DEA codes, which are required to be consistent with this data sharing code, provide guidance on the proportionate exercise of the tightly-defined DEA data sharing powers, in compliance with the data protection legislation. For example: • Other than the GDPR, there are instances under the DEA where a DPIA is obligatory (e.g. information sharing pilots under the debt and fraud powers); • Specific "gateways", meaning "express statutory obligations and powers to share information", are provided under the DEA for data sharing for defined purposes between specified public authorities, for public benefit.

Date	Description
	Examples for Data Protection Impact Assessment (DPIA): In addition to examples of processing given by the GDPR where a DPIA is required, the code further provides three examples that might be relevant to data sharing, i.e.: • Data matching; • Invisible processing; and • Processing records where there is a risk of harm to individuals in the event of a data breach, such as whistleblowing or social care records. The code also provides a list of questions to help organisations to assess whether or not a DPIA is required. - Data sharing agreements: The code notes that it is a good practice to have a data sharing agreement which sets out the purpose of the data sharing, covers what is to happen to the data at each stage, sets standards and helps all parties to be clear about their respective roles. The code further provides a range of questions to explain what should be included and reviewed in a data sharing agreement. - Due diligence when sharing data following mergers and acquisitions: The code draws particular attention to the data sharing during the mergers and acquisitions and other change in an organisational structure. It addresses that due diligence in this aspect should also consider data sharing activities. Shared data management following the mergers or restructure or other change in an organisation structure must check that the data records are accurate, up to date, documented, consistently retained, and appropriately secured. However, it currently makes no reference to TUPE which we consider to be a major omission. - Sharing personal data in databases and lists: The code states that transfer of databases or lists of individuals is a form of data sharing, which may include sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies, and political parties. Organisations should make appropriate enquiries and checks for legal compliance. - Data sharing and children: The code emphasises that sharing children's personal data should be proceeded with caution. A DPIA is compulsory when such data sharing is likely to result in a high risk to children's rights and freedoms. - Data sharing in an urgent situation or in an emergency: In case of urgent or emergency situations, organisations should go ahead and share data as necessary and proportionate. Therefore, it is helpful for organisations to have procedures about the personal data they hold and whether and how they should share any of this information. - Data ethics and data trusts: The code also suggests the potential use of 'data trust' in data sharing, which is a new model to enable access to data by new technologies while protecting other interests and retaining trust and following a 'privacy by design' approach.

Date	Description
29 July	**The ICO has selected its first 10 participants (out of 64 applications) for the initial beta phase of its data protection Sandbox. The programme participants are:** • **FutureFlow:** A regtech startup designing a forensic analytics platform that monitors the flow of funds in the financial system. Its platform enables multiple financial institutions, regulators and agencies to capitalise on each other's intelligence on electronic financial crime without heavy reliance on PII. This collaborative approach to tackling financial crime opens the prospect of higher detection rates with lower false positives, while reducing the burden of scrutiny on each individual and business consumer. • **Greater London Authority:** The GLA's Violence Reduction Unit (VRU) is working to understand better how public health and social services can be managed to prevent and reduce crime, with a focus on early intervention. There is increasing interest from the VRU, the Mayor's Office of Policing and Crime (MOPAC) and the GLA for health, social and crime data to be looked at in an integrated and collaborative way. • **Heathrow Airport:** The automation of the Passenger Journey Programme aims to streamline the passenger journey by using biometrics. Facial recognition technology would be used at check-in, self-service bag drops and boarding gates to create a seamless experience for passengers travelling through the airport. Current processes require passengers to present different forms of documentation, such as boarding cards and passports, at different points in their journey to prove their identity and show they are authorised to travel. By offering passengers the option of using facial recognition technology, they would have the choice to enjoy a frictionless journey through the airport. • **Jisc:** A not-for-profit company that supports post-16 and higher education and research by providing relevant and useful advice, digital resources and network and technology services, while researching and developing new technologies and ways of working. It is developing a code of practice with universities and colleges wishing to investigate the use of student activity data to improve their provision of student support services to protect both privacy and wellbeing. • **Ministry of Housing Communities and Local Government:** A partnership with Blackpool Council and the Department for Work and Pensions seeks to match personal information controlled by multiple parties in order to create a dataset to understand more about the private rented sector in Blackpool, who lives there, and how to help improve the quality of properties. • **NHS Digital:** Is working on the design and development of a central mechanism for collecting and managing patient consents for the sharing of their healthcare data for secondary use purposes, including medical research and regulated clinical trials. • **Novartis Pharmaceuticals UK:** Is exploring the use of voice technology within healthcare. Through its Voice Enabled Solutions project, Novartis is working with healthcare professionals to design systems to make patient care easier, and addressing the data privacy challenges posed by this emerging technology. • **Onfido:** A document ID verification and facial biometrics technology firm researching how to identify and mitigate algorithmic bias in machine learning models used for remote biometric-based identity verification. • **Tonic Analytics:** The Galileo Programme was launched in 2017 and is jointly sponsored by the National Police Chiefs' Council and Highways England. Galileo's primary focus is on the ethical use of innovative data analytics technology to improve road safety while also preventing and detecting crime. • **TrustElevate:** A secure authentication and authorisation provider for under-16s is working to enable companies to comply with regulatory requirements, and to make the internet a safer environment for children, facilitating a more robust digital ecosystem and economy. The Sandbox is a new ICO service which will support organisations which are developing innovative products and services using personal data with a clear public benefit. More detail can be found here.

Date	Description
July	**ICO's Information Rights Strategic Plan: Trust and Confidence** Research issued by the ICO in July shows that top concerns from respondents are: (1) Cyber security (2) Children's privacy (3) Data sharing of data for marketing (4) Tracking of web browsing for marketing More information: https://ico.org.uk/media/about-the-ico/documents/2615515/ico-trust-and-confidence-report-20190626.pdf
9 July	**ICO published Annual Report 2018-19** The ICO has reported that last year's trends have continued, with members of the public increasingly aware of their privacy rights and an increase in complaints as a consequence of this. Despite the increase in complaints, the public's trust and confidence in organisations storing their data has also increased significantly since last year's report. In the last year, the ICO has issued a number of statutory codes (e.g. age appropriate design, data sharing and direct marketing codes) and has also launched a number or large scale industry investigations, including one on the use of live facial recognition technology. In the 2018/2019 period, the ICO received 13,840 data breach notifications, up from 3,311 in the previous period. 2018/2019 was also a record breaking year for fines, both in number and in amount. The largest fines issued in the last year are: • £500,000 fine against Equifax Ltd, relating to a cyber security incident which affected the personal data of up to 15m UK citizens and residents. • £500,000 fine against Facebook Ireland Ltd, relating to a data incident affecting the personal data users worldwide (appealed). • £385,000 fine against Uber, relating to a cyber security incident effecting the personal data of 2.7m UK Uber users and 82,000 UK Uber drivers. • £325,000 fine against the Crown Prosecution Service, for losing unencrypted DVDs containing recordings of police interviews. The full report can be found here.

7 August	**Update on Progress of the Children's Code** Since its publication in April, the ICO has received over 450 written responses and met with more than 40 key stakeholders. In her latest blog post, the Commissioner expressed optimism that the consultation has helped ensure the final Code is effective, proportionate and achievable. While recognising that the Code will present challenges to certain industries (*calling out the tech, gaming and interactive industries*), the Commissioner reiterated that protecting children's data is of paramount importance and backed by strong public support (*hinting that no substantial changes are likely*). To assist organisations implement the Code, the ICO is preparing a significant support package and will provide "*an appropriate*" implementation period, which could as long as one year. The Commissioner also confirmed that the Code will be presented to the Secretary of State ahead of the statutory deadline of 23 November, who will then lay it before Parliament "*as soon as reasonably practicable*". Once laid, unless Parliament resolves not approve the Code within 40 days, it will be issued by the Commissioner.
15 August	**ICO changes guidance on meaning of a 'month' on data request responses** The ICO has updated its guidance on the meaning of a month. Previously, the ICO had adopted the position that the calculation of a month did not include the day during which a request was received – this was based on its reading of Regulation (EEC, EURATOM) 1182/71 which includes language to this effect. As such, it had advised that organisations receiving a response on a particular day (e.g. the 1st) would have until the following day in the next month (e.g. the 2nd) unless this was not a working day, in which case the response would be due on the next working day. This position, however, neglected a case (Case C-171/03 Maatschap Toeters and M.C. Verberk v Productschap Vee en Vlees on the unlikely topic of the admissibility of applications made after the slaughter of calves) in which it held that the date that an action/event occurred must be included within a calculation. The ICO has recently announced an update to its guidance which takes the case into account. Whilst rules on working days remain (so a response that would be required on a weekend or bank holiday by a standard calculation is not required until the next working day) the rules now require the date the request was received to be included in the calculation of a month. Using our previous example, the response would now be required on the 1st, rather than the 2nd. The updated guidance can be seen here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ The ICO announcement can be seen here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/timescales-for-responding-to-a-subject-access-request/

UK Cases

Date	Description
28 June	**C v Chief Constable of the Police Service of Scotland [2019] CSOH 48; [2019] 6 WLUK 447 (OH)** In the course of a police investigation into a sexual offence, an officer seized a suspect's phone and discovered offensive Whatsapp messages between other officers unrelated to the investigation. The 10 police officers involved were seeking an order to prevent the Whatsapp conversations being used in relation to misconduct charges against them, on the basis that it would be an infringement of their common law right of privacy and incompatible with their right to respect for their private and family life under Article 8 of the ECHR . The Outer House of Scotland's Court of Session held it fair in all the circumstances for the material to be admitted for use in the disciplinary proceedings. Lord Bannatyne recognised that there is a right of privacy in terms of the common law of Scotland. However, despite the nature of Whatsapp messages, the police officers had no reasonable expectation of privacy in respect of the messages – this flows from the attributes which arise as a result of their position as constables.
18 July	**Mircom International Content Management & Consulting Ltd, Golden Eye & Ors v Virgin Media Ltd & persons unknown [2019] EWHC 1827 (Ch)** In this case, the High Court considered the correct legal approach to granting a *Norwich Pharmacal* order requiring an internet service provider (Virgin Media) to disclose the names and addresses of tens of thousands of residential broadband subscribers accused of unlawfully downloading pornographic films to the Claimants. The main Claimants here were Mircom and Golden Eye, who act on behalf of film production companies claiming copyright in such films, and who would be instructed to send out (often threatening) letters on their behalf alleging claims of internet piracy and seeking payments. This case is highlighted as one of the questions under discussion was whether the GDPR had affected the approach to be taken in such cases (Virgin Media arguing that it did) or whether previous file-sharing case law still applied (namely *Golden Eye (International) Limited v Telefonica UK Ltd [2012] EWHC 723 (Ch)* and at the Court of Appeal in *Golden Eye (International) Ltd v Telefónica UK Ltd (Open Rights Group intervening) [2012] EWCA Civ 174)*. Mr Recorder Douglas Campbell QC (sitting as High Court judge) concluded that the legal approach remained the same as under the Golden Eye cases, but refused to grant the orders sought due to defects in the fact and expert evidence. He also added that the Claimants had not shown that they harbour a "*genuine intention*" to try and obtain redress for the infringement rather than "*merely setting up a money making scheme designed to embarrass and coerce as many people as possible (regardless of whether they were actual infringers) into making the payments demanded*". Regarding the relevance of GDPR, 3 points were considered: (i) **whether the raw IP addresses (i.e. the data which the Claimants already possess) were "personal data" within the meaning of Art 4(1) GDPR?** Campbell concluded that they were. In doing so, he referred to the ECJ's decision in *Breyer v Bundesrepublik Deutschland, C-582/14* (a pre- GDPR case which looked at whether dynamic IP addresses could constitute "personal data") and decided that it was not a matter of

Date	Description
	simply importing the result into domestic law on the basis "*it would be surprising if the mere fact that a party was able to obtain a Norwich Pharmacal order to identify a natural person under the English civil system, automatically made that procedure "reasonably likely to be used' to identify the natural person, so that otherwise pseudonymous data automatically became personal data.*" However, he did conclude that the mere possibility of granting the relief sought in this case meant that the IP addresses were "personal data" in the Claimants' hands and the data would certainly become personal data in the Claimants' hands if the orders sought were granted. **(ii) whether the disclosure would make the Claimants "data controllers" within the meaning of Art 4(7) GDPR or merely "data recipients" within the meaning of Art 4(9)?** Campbell concluded that the Claimants were "data recipients". The arguments for this point were brief and mostly came from the Claimants and the logic/relevance to the overall case is not entirely clear. However, Campbell appeared to base his decision on the fact that Schedule 2, Part 1, paragraphs 5(2) and 5(3) of the DPA 2018, disapplied major parts of the GDPR where disclosure of the data was required by a court order. **(iii) did it make a difference if one of the Claimants had registered as a data controller with the ICO within 14 days of the date of the order and appointed a DPO?** Campbell concluded on the basis of the previous answer that there was no need to consider this point.
5 August	**Liberal Democrats v ICO: Information Rights Decision Notice, EA/2019/0161** This case related to an appeal against an Assessment Notice issued against the Liberal Democrats on 27 February 2019 which required the organization to give access to its premises and records during the period 10-14 June 2019 to enable the ICO to examine the processing of personal data. The main purpose of this audit was to "demonstrate to the Commissioner that the Liberal Democrats are complying with the data protection legislation, to highlight to the Liberal Democrats areas of risk to their compliance, and to make recommendations in areas that require improvement". Subsequently a date for the European Parliament Elections was announced and the Liberal Democrats raised concerns about the impact for the preparation of the audit on its election campaigning. The ICO agreed to push back the deadline slightly and issued a new Assessment Notice. The Liberal Democrats then appealed against the new Assessment Notice arguing unfairness and significant operational disruption. In resisting the appeal, the ICO argued that similar notices had been issued to 7 other political parties and confirmed that all parties were treated consistently and fairly. The audits were of pressing public importance and a part of the ICO's investigation into the use of data analytics by political actors and the impact on the political process. She also argued that she had discretion with respect to the conduct of audits but that the inconvenience of an audit was not a reason to restrict her discretion. On 24 July, the tribunal noted that the issue giving rise to the appeal no longer existed (due to the passage of time) and issued directions to the parties to agree new dates by 1 August. The parties confirmed the agreed dates for the audit and the appeal was dismissed.

Other UK News

Date	Description
23 & 24 July	**'Immigration exemption' under scrutiny** The High Court in London began hearing an application for judicial review brought in respect of the 'immigration control' exemption in Schedule 2, Part 1, paragraph 4 of the Data Protection Act 2018. The exemption dis-applies a number of data subject rights, including the right to erasure, the right to access and the right to transparent information about the use of personal data to extent that complying with these rights would prejudice the maintenance of effective immigration control, or investigation or detection of activities that would undermine the maintenance of effective immigration control. The challenge is based on the exemption's alleged incompatibility with Article 23 of the GDPR and with the rights to privacy and data protection under the European Convention on Human Rights and/or the Charter of Fundamental Rights. Article 23 allows EU Member States to restrict the application of certain GDPR provisions via local legislative measures which are made to safeguard a number of areas (such as national security, defence and for other important objectives of general public interest in that Member State or the EU overall) provided that such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society. The proceedings are brought by the Open Rights Group and, EU citizen's group, the3Million against the Secretaries of State for the Home Office, and the Department of Culture, Media and Sports.
25 July	**UK Government publishes its approach to regulating non-UK Digital Service Providers under the NIS Regulations after Brexit** The EU Security of Network and Information Systems Directive ("**NIS Directive**") aims to improve the security of network and information systems across Europe by introducing a legal framework with which Operators of Essential Services and Digital Service Providers ("**DSPs**") which offer services in the EU must comply. In the UK, this was implemented into national law via the Network and Information Systems Regulations 2018 ("**NIS Regulations**"), which will continue to apply after the UK exits the EU. DSPs must comply with the NIS Regulations where they provide online marketplace services, online search engine services and/or cloud computing services and whether they employ greater than 49 staff or a turnover than more than 10 million Euros per annum. The NIS Regulations require DSPs which aren't established in the EU, but which provide digital services within the EU to designate an EU representative and comply with the national implementation of the NIS Directive in one of the EU Member States where they offer digital services. Once the UK exits the EU, this requirement will apply to UK based DSPs. However, there is not currently a requirement in the UK NIS Regulations for non-UK based DSPs which offer digital services in the UK to appoint a UK representative and comply with the NIS Regulations. As such, the ICO (as the UK's authority for overseeing compliance with

the NIS Regulations) would be unable to enforce the NIS Regulations against non-UK based DSPs which operate in the UK post-Brexit.

The Government therefore proposed to introduce such a requirement into the NIS Regulations and sought public consultation on this proposal. Several positive responses were received and the Government has published its response to the consultation, stating that it intends to introduce a statutory instrument to amend the NIS Regulations to include this requirement.

Once the statutory instrument comes into force (20 days after the UK's departure from the EU), DSPs which are based outside the UK and provide digital services to the UK will need to appoint a UK representative and comply with the NIS Regulations within three months, therefore bringing them in scope of the ICO's enforcement powers.

Where a DSP is required to appoint a UK representative, the representative:

- can be any natural or legal person established in the United Kingdom, who is able to act on behalf of a digital service provider with regard to its obligations under the NIS Regulations;
- must be designated in writing;
- must be contactable by the Information Commissioner or GCHQ for the purposes of ensuring compliance with the NIS Regulations;
- is nominated without prejudice to any legal action which could be initiated against the nominating digital service provider; and
- must be nominated within three months of the amendment coming into force, or within three months after the date on which a digital service providers falls in scope.

DSPs which are required to appoint a UK representative must fully comply with the NIS requirements, which includes:

- meeting their legal requirements in accordance with Regulation 12 of the NIS Regulations;
- registering with the ICO;
- notifying the ICO about any security incident which has a substantial impact on the provision of digital services;
- meeting the inspection requirements; and
- complying with information, enforcement, and penalty notices issued by the ICO.

August	**Changes in Civil Procedure Rules re DP Claims** The latest round of updates to the Civil Procedure Rules come into force on 1 October 2019 and contain significant developments in how data protection claims should be brought before the English Courts. Firstly, the Media and Communications list of the Queen's Bench Division has been designated as a specialist list of the High Court, and data protection claims are included within its remit. This means data protection claims should be issued in the Queen's Bench Division at the Royal Courts of Justice in London. Any claim issued in a district registry of the High Court will be transferred to the Royal Courts of Justice unless it is straightforward and low value in nature, in which case the County Court continues to be the appropriate forum. Secondly, CPR 53 (Defamation) and the existing pre-action protocol for defamation claims have been replaced with a new CPR 53 (Media and Communications Claims) a new pre-action protocol that deal with the full remit of the Media and Communications specialist list, including data protection claims. The new pre-action protocol includes a list of specific information that must be included in a letter before action alleging breaches of data protection law (for further detail of what information must be included see paragraph 3.4 of the pre-action protocol, which can be found here). This welcome development will provide parties (particularly prospective defendants) with some certainty as to what information they will receive prior to a claim being issued.

UK Legislation

Date	Description
16 September	**The Data Protection Act 2018 (Commencement No. 2) Regulations 2019 – (in force September 16)** The Data Protection Act 2018 (Commencement No. 2) Regulations 2019 have been passed bringing the following provisions of Part 4 of the Data Protection Act 2018 (intelligence services processing), so far as not already in force, into force on 16 September: (a) section 93 (right to information); (b) section 102 (general obligations of the controller); (c) section 103 (data protection by design); (d) section 104 (joint controllers); (e) section 105 (processors); (f) section 108 (communication of a personal data breach). Part 4 of the 2018 Act was brought into force on 25th May 2018 by the Data Protection Act 2018 (Commencement No. 1 and Transitional and Saving provisions) Regulations 2018 (S.I. 2018/625), with the exception of the sections specified in regulation 2 of these Regulations. Section 212(2)(f) of the 2018 Act brought into force on 23rd May 2018 any provision of the 2018 Act so far as it conferred powers to make regulations or Tribunal Procedure Rules or it was otherwise necessary to enable the exercise of such a power.

Europe

EDPB

Date	Description
9 July	**EDPB 12th Plenary Session** On July 9th and 10th, the European Data Protection Board (EDPB) met for their twelfth plenary session. During the plenary, the following documents were adopted: (a) Draft Guidelines on video surveillance (see here). The Guidelines, which are currently open to public consultation (closes 9 September), cover among other things the lawfulness of processing, the applicability of the household exemption and the disclosure of footage to third parties. The Guidelines aim to provide for a consistent application of the GDPR when traditional video devices and 'smart' video devices are used to process personal data. Smart video devices are video devices which implement tools to exploit captured images (e.g. cameras with facial recognition functionality). The EDPB pays particular attention to the processing of biometric data. For the EDPB, such processing involves heightened risks for data subjects' rights, with a large threat posed by databases comprised of raw material (like facial images, speech signals and gait). Key risk-mitigation measures here include deleting such information and adding 'noise' to an image to render it ineffective (such as a watermark). A good proportion of the Guidelines is also dedicated to the technical and organisational measures the EDPB expects to be in place to meet GDPR security (Article 32) and data protection by design and default (Article 25) requirements. Here, the EDPB explains that measures should be in place for the entirety of a video surveillance system, encompassing the video environment (image capturing, handling and interconnections), systems management and security. (b) EDPB-EDPS joint reply to the LIBE Committee on the implications of the US CLOUD Act. The CLOUD Act allows US law enforcement authorities to require the disclosure of data by service providers in the US, regardless of where the data is stored and the joint reply emphasises the importance of a comprehensive EU-US agreement on access to electronic evidence containing sufficient data protection safeguards (see here). (c) Opinion on Standard Contractual Clauses for processors under Art.28.8. The EDPB adopted consistency Opinion 14/2019 on the draft Standard Contractual Clauses under Article 28(8) of the GDPR submitted by the Danish supervisory authority (the "Opinion"). While the Opinion specifically addresses the provisions of the Danish authority's agreement, it does contain helpful pointers as to the limits of what the EDPB considers acceptable for an Article 28 data processing agreement – which is, broadly, contractual terms which mirror the language of Article 28. The Opinion can be found here and an English-language version of the Agreement can be found here (d) Opinion on Accreditation Criteria for monitoring bodies of Codes of Conduct by the Austrian Supervisory Authority. The opinion, available here, contains recommendations of the EDPB with the view to ensuring the consistent application of the GDPR.

	(e) Opinion on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment which occurs mid-procedure. The Board opined that the competence of the lead supervisory authority (LSA) can switch to another supervisory authority as long as no final decision has been reached by the competent supervisory authority, while the cooperation procedure set forth under Art. 60 GDPR shall continue to apply. The opinion is available here. (f) EDPB-EDPS Joint Opinion on the eHealth Digital Service Infrastructure (eHDSI). eHDSI is an IT tool developed by the European Commission and the eHealth Network in the context of cross-border healthcare, in order to enhance interoperability between national digital health systems in exchanging patients' data. The opinion, available here, aligns with the Commission's position that it acts as processor for the processing of patients' data and stresses the need of setting out the Commission's obligations as processor in the relevant Implementing Act. For further detail, see below. Furthermore, the EDPB adopted an opinion on the Data Protection Impact Assessment (DPIA) list submitted by the Cypriot supervisory authority as well as opinions on the DPIA exemption lists submitted by the French, Spanish and Czech supervisory authorities respectively. Finally, the EDPB issued a recommendation to the EDPS on its DPIA list for processing operations carried out jointly by EU institutions and bodies and other controllers (available here). In addition to the above documents, this autumn the EDPB is expected to adopt final guidelines on the territorial scope of the GDPR and to update the opinion on the concept of "controller" and "processor" issued by its predecessor, Article 29 Working Party (Opinion 1/2010). Also, guidelines on the lawful basis of the performance of a contract (Art. 6.1(b) GDPR) in the context of the provision of online services are expected by the end of the year. Finally, guidance on the following topics is on the EDPB's list; however, no timeframe for such guidance has been announced yet: Codes of conduct and certifications as appropriate safeguards for the transfer of personal data to third countries, interplay between the extra-territorial scope of the GDPR and the rules on data transfers to third countries and interplay between the second Directive on Payment Services (PSD2) and the GDPR.
Summer 2019	**EDPB and EDPS: European Commission is a processor of patient data in the eHealth Digital Service Infrastructure** On 12th July 2019, the European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS") adopted *Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Services Infrastructure (eHDSI)* (the "Opinion" available here). In the Opinion, the EDPB and the EDPS addressed the questions raised by the Directorate-General for Health and Food Safety of the European Commission ("DG SANTÉ") regarding the eHDSI system, which enables the exchange of electronic health data of European patients, including e-prescriptions and summaries of patient medical records using a secure private network known as TESTA. The Opinion recognised that personal data processed in the eHDSI system are processed for two separate purposes: (1) the Commission processes personal data of individuals with access to the eHDSI system and manages their accounts; and (2) the relevant stakeholders process personal data of patients for the purposes of ensuring the continuity of cross-border healthcare. The EDPB and EDPS confirmed that: • by making data available through a private network, personal data are being processed, independently of the fact that the European Commission may or may not have access to it;

	• despite the fact that personal data are encrypted, they remain personal data; • the Commission, although involved in some of the procedures regarding the development of technical and organisational solutions in respect of the eHDSI system, including the provision of the TESTA network, does not have decision-making power in terms of defining the purpose or the essential means relating to the processing and is therefore a processor; and • the draft European Commission Implementing Decision seeking to clarify the functioning of the eHDSI system must set the Commission's processor role, including the rules set out in points (a) to (h) of Article 29(3) of Regulation 2018/1725.
Summer 2019	**EDPB's review of the Austrian requirements for code of conduct monitoring bodies** On 9th July 2019, the European Data Protection Board ("EDPB") adopted *Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR* (the "Opinion" available here) following the submission by the Austrian data protection authority of its draft decision containing the accreditation requirements for a code of conduct monitoring body (the "Draft Decision"). The Opinion was adopted in furtherance of the GDPR's consistency mechanism enshrined for present purposes in the EDPB's *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (the "Guidelines"). Article 40 of the GDPR makes provision for the approval of codes of conduct to help controllers and processors demonstrate compliance and best practice. Article 41 of the GDPR provides that the monitoring of compliance with codes of conduct must be carried out only by bodies accredited by the competent supervisory authority and meeting the criteria set out in Article 41(2) of the GDPR. The draft criteria for accreditation of such bodies must be submitted to the EDPB by the competent supervisory authority pursuant to Article 41(3) of the GDPR. In review of the Austrian data protection authority's Draft Decision, the EDPB had the following recommendations: • **Independence**: the Austrian accreditation requirements on independence need to be strengthened. • **Conflict of interest**: the Austrian accreditation requirements do not address conflict of interest. • **Expertise**: despite the Draft Decision requiring "*an excellent knowledge of data protection and either a relevant degree (or equivalent qualification), or at least five years of relevant sector experience…*" the Austrian data protection authority must take into account the additional expertise requirements set out in the Guidelines. • **Established procedures and structures**: the procedures to monitor compliance with codes of conduct are too general. Instead, such procedures must be specific enough to ensure consistent application by monitoring bodies. This can include audit procedures (with appropriate methodologies) and investigation procedures. • **Transparent complaints handling**: the specific requirement in the Austrian Draft Decision for complaints to be resolved in two months is too specific. The EDPB recommended that complaints handling process requirements should reflect the approach in Article 78(2) of the GDPR, namely notification within three months of the progress or outcome of the complaint.

	• **Communication with the Competent Supervisory Authority**: the annual reporting requirement by the monitoring body to the Austrian data protection authority is too infrequent and do not address reporting of substantial changes. • **Review mechanisms**: the requirements should address the monitoring body's obligation to contribute to any review of the code. • **Legal status**: contrary to the Draft Decision, the EDPB notes that the monitoring body should be established in the EEA so as to ensure that it can uphold data subject rights. Further, the EDPB recommends that the monitoring body should have access to adequate resources, particularly where the monitoring body is an individual, so that it can deliver the code's monitoring mechanism over a suitable period of time. Finally, the EDPB recommends that provisions are included with regard to subcontracting to clarify whether monitoring bodies may have recourse to subcontractors and on which terms and conditions.

ECJ cases

Date	Description
9 July	**Schrems II: International Transfer Methods under the magnifying glass** On 9th July, the ECJ heard arguments on whether the Standard Contractual Clauses (SCCs) are effective to provide adequate protection for personal data, both as regards transfers to the US and in general (the so-called "Schrems II" case). The High Court in Ireland, which referred the case to the ECJ, made a number of findings about US law. The ECJ was asked multiple questions about whether, in the light of these findings, transfers of personal data to the US (pursuant to the SCCs) breach the EU Charter of Fundamental Rights. The ECJ was also asked to rule on the impact of the EU-US Privacy Shield on these questions. The ECJ is expected to hand down its decision in early 2020. For further details, please see our earlier article.
29 July	**Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW C-40/17** This ECJ decision deals mainly with the issue of "joint controllership" between Facebook and website operators using Facebook's 'Like' button on their website. The highest EU court decided that the operator of the website can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of the personal data of visitors to the website, but not in respect of subsequent processing. For more detail, please see our earlier article.

CoE cases

Date	Description
2 July	**Gorlov and Other v Russia [ECtHR: 27057/06]** The ECtHR unanimously concluded that the right to respect for private life of detainees in prisons had been violated by a lack of safeguards in the national law regarding the use of CCTV in penal facilities. In the applicant's specific situation they were subject to constant CCTV monitoring in their cells that was not based on an individual decision and no process was in place to allow for regular review of whether such surveillance was appropriate. The national legislation in place only provided for general rules on the use of CCTV in prison and did not include any specifications on which areas of the facilities it was permitted to be used in, what times of day it could be used, any conditions for use or restrictions on the length of time of the monitoring. The court held that the legislation at the time lacked sufficient clarity with regards to scope and manner of exercise and did not provide adequate protection against arbitrary use. The court noted that the domestic courts had interpreted the legislation as giving such facilities "unrestricted power" to place all individuals under permanent video surveillance unconditionally for an indefinite period of time with no review. The court noted that surveillance may be necessary in certain areas or on certain persons on a permanent basis. The court concluded that the measure complained of had not been "in accordance with the law" and so did not go on to consider if it was in pursuit of legitimate interests etc. For more information, please see here .
10 July	**European Court of Human Rights Grand Chamber Hearing on UK surveillance regimes** On 10 July 2019 the Grand Chamber of the European Court of Human Rights ('ECtHR') held a hearing in the case of *Big Brother Watch and others v the United Kingdom* (58170/13). The hearing concerns three joined applications brought against the UK government by a total of 16 organisations and individuals who are journalists or actively campaign on civil liberties issues, relating to three different surveillance regimes: (i) bulk interception of communications; (ii) intelligence sharing with foreign governments; and (ii) obtaining communications data from communications service providers. The applications were lodged following Edward Snowden's revelations relating to (amongst other things) surveillance and intelligence-sharing programmes operated by the UK government. The applications assert that the UK government's activities violate certain aspects of the European Convention on Human Rights ('ECHR'). Namely, that electronic communications or communications data were likely to have been intercepted/obtained by the UK intelligence services in breach of: (i) Article 8 ECHR (right to respect for family and private life) – particularly in respect of bulk interception of communications, intelligence sharing and acquisition of data from communications service providers (all applications); (ii) Article 10 ECHR (freedom of expression) – in respect of applicants' work as journalists and non-governmental organisations (applications 2 and 3);

(iii) Article 6 (right to a fair trial) – in respect of domestic procedure for challenging surveillance measures (application 3); and

(iv) Article 14 (prohibition of discrimination) – in respect of people located outside the UK, whose communications were more likely to be intercepted in the context of bulk interception practices (and, if intercepted, selected for example) (application 3).

In an earlier hearing, the ECtHR Chamber held that the Article 8 ECHR was violated by the UK government's bulk interception regime (in light of insufficient oversight and inadequate safeguards) and by the regime for obtaining communications data from communications service providers (as it is not in accordance with the law). Both regimes were also found to be in breach of Article 10 ECHR (in light of insufficient safeguards in respect of confidential journalistic material). However, the Chamber found that intelligence sharing with foreign governments did not violate Articles 8 or 10 ECHR, and rejected complaints under Articles 6 and 14 ECHR. The Grand Chamber Panel accepted applicants' request for the case to be referred to the Grand Chamber. The case was heard by the Grand Chamber on 10 July 2019 and a judgment is expected in early 2020.

The ECtHR's press release is available here

Other EU News

Date	Description
18 July	**European Data Protection Supervisor: Guidelines for European Institutions on International Data Transfers after Brexit** The European Data Protection Supervisor ("EDPS") has issued guidelines for European Institutions on transfers to the UK following a 'hard/ no-deal Brexit' on 1 November 2019 i.e. if no withdrawal agreement is signed before this date. A withdrawal agreement would ensure the continued application of the GDPR, ePrivacy Directive and the Law Enforcement Directive in the UK until 31 December 2020 (with the possibility of a further extension, to 31 December 2022), such that, the UK would not constitute a third country before that date. The EDPS confirms that, in the event of a no-deal Brexit on 1 November 2019, the Chapter V GDPR data transfer mechanisms must be implemented to enable transfers of personal data to the UK on and from that date (as an adequacy decisions will not be given before this time). The EDPS recommends that European Institutions take the following steps to prepare for a no-deal Brexit (these steps also apply more broadly to all organisations impacted by Brexit): - Map your company's data processing/ flows - Analyse the most appropriate data transfer mechanism for your company - Implement this mechanism before 1 November 2019 - Update applicable internal documentation - Update the transfer section (and other applicable sections) of your company's privacy policy
24 July	**Blockchain and the General Data Protection Regulation – can distributed ledgers be squared with European data protection law?** On 24 July the European Parliament published a study regarding blockchain and the General Data Protection Regulation ("**GDPR**"). The study is divided into three parts and the matters discussed include: a. the tension between blockchain and the GDPR; b. how blockchain could be a suitable tool to achieve some of the GDPR's underlying objectives; and c. policy recommendations to consider going forward.

Date	Description
	One key takeaway the study emphasises is that as blockchains are a class of technology with different features and governance arrangements e.g. public and permissionless blockchains and private and permissioned blockchains. Accordingly, *"it is impossible to state that blockchains are, as a whole, [are] either completely compliant or incompliant with the GDPR."* and as such, a case-by-case assessment will be required when assessing whether a particular blockchain is GDPR complaint. Tension between blockchain and the GDPR The study recognises that a lot of the points of tension between blockchain technology and the GDPR are due to two principal factors: a. a data subject can enforce their rights under the GDPR to at least one natural person i.e. a data controller. However, blockchain technology is inherently decentralised and essentially acts as a *"shared and synchronised digital database"*, which *"makes the allocation of responsibility and accountability burdensome, particularly in the light of the uncertain contours of the notion of (joint)-controllership under the regulation."*; and b. a data subject's data can be modified or erased as set out in Article 16 (right to rectification) and 17 (right to erasure ('right to be forgotten') of the GDPR. However, blockchains are considered *'append-only data structures'*, as blocks are never removed from the blockchain, only added. This is purposeful to ensure the integrity of the data and trust in the network but this can make modification or erasure extremely burdensome. Blockchain as a means to achieve GDPR objectives The study highlights that there is room to experiment with blockchain technology to achieve objectives of the GDPR, such as article 15 (right of access) and article 20 (right to data portability). Depending on the design, *"blockchains can be designed to enable data-sharing without the need for a central trusted intermediary, they [can] offer transparency as to who has accessed data, and blockchain-based smart contracts can moreover automate the sharing of data"*. Accordingly, blockchain has the potential to give the data subject more control over their personal data. Policy options Interestingly, the study offers a number of policy options to consider going forward. The three recommendations the study outlines are: a. regulatory guidance – *"legal certainty for those wanting to use blockchain technologies… regarding how specifics concepts ought to be applied where these mechanisms are used."* Currently, certain concepts such as joint data controllers remain unsettled and more guidance is needed to apply the GDPR legal framework to blockchain technology. b. certification mechanisms and codes of conduct – the GDPR has mechanisms in the form of codes of conducts and certification mechanisms to help apply the overarching principles of the GDPR. The study recommends applying these mechanisms so the private sector can collaborate with regulators to ensure the principles of GDPR are respected appropriately in blockchain technologies. c. research funding – the study recognises there are current technical limitations with blockchain in terms of GDPR compliance e.g. the right to erase data under article 17 of the GDPR, and recommends research to see if solutions can be found. Work Program 2019/2020 The study highlighted that the European Data Protection Board ("**EDPB**") published on 12 February that blockchain may be one topic that they examine in their 2019/2020 work program, so we may see further guidance in relation to blockchain from the EDPB over the next year.

Date	Description
24 July	**EU Commission report on impact of GDPR and how implementation can be improved** To mark the one year anniversary of the GDPR coming into force (May 2018), the European Commission has published a 'reflective' report on progress made since that date. The Press Release states that, *"The report concludes that most Member States have set up the necessary legal framework, and that the new system strengthening the enforcement of the data protection rules is falling into place. Businesses are developing a compliance culture, ... At the same time, convergence towards high data protection standards is progressing at international level"*. To this, the European Commission adds that individuals are becoming more aware of their data protection rights. This is evidenced by the results of a 2013 Eurobarometer survey; 67% of survey respondents 'have heard of' the GDPR and, of that, 36% know what it is. The European Commission also identifies 'next steps' which are designed to continue improving the application of the GDPR: - *"One continent, one law"*; The European Commission is keen to ensure that Member States implement the GDPR consistently and without 'gold-plating it'. All but Greece, Portugal and Slovenia have updated their local laws in line with the GDPR. Note that the UK has enacted the Data Protection Act 2018 in this respect. - *"Businesses are adapting their practices"*: The implication here is that the European Commission has seen evidence that, in working towards GDPR compliance, businesses have improved their data security and gained *"a competitive advantage"*. The Commission commits to continuing to support SMEs in working towards that compliance. - *"Stronger role of data protection authorities"*: The European Commission notes that national supervisory authorities ("**SAs**") are using the enforcement powers bestowed upon them 'effectively'; and are collaborating and cooperating effectively with one other as intended (by end June 2019, 516 cross-border cases had been managed). The Commission seemingly 'wraps the EDPB on the knuckles' by providing that it must *"step up its leadership"*. - *"EU rules as reference for stronger data protection standards across the globe"*: The Commission proudly reports evidence of this, and commits to progressing ongoing adequacy proceedings (in particular, concluding the Korean proceedings (presumably this year (?)). The European Commission will again report on progress during 2020. This report will include a report on the review of the adequacy decisions made under Directive 95/46/EC (11 in total).

July 25	**EU Commission is asking the Court of Justice of the European Union to impose financial sanctions on Greece and Spain for failing to transpose the rules on the Data Protection Law Enforcement Directive before the 6 May 2018, deadline** The European Commission has referred Greece and Spain to the Court of Justice of the EU ("CJEU") for failing to implement Directive (EU) 2016/680 (i.e. the Law Enforcement Directive) into national law by the 6 May 2018 deadline; recommending that prescribed administrative fines (lump sum penalties and daily penalty payments) should be imposed pursuant to Article 260 (3) of the Treaty on the Functioning of the EU ("TFEU"). The Law Enforcement Directive governs the processing of personal data by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. A key consequence of Greece and Spain failing to implement the Directive is that it hampers the exchange of personal data between them, and other Member States (who have implemented the Directive), for law enforcement purposes. It clearly also impinges on the rights of applicable data subjects. The Commission has recommended that different administrative fines should be imposed on Spain and Greece for their respective failures to fulfil their obligations under the Directive (including, as a 'step one', its transposition into local law). This likely reflects the different application of the Article 260 (3) TFEU factors to consider when imposing such fines i.e.: (i) the seriousness of the infringement; (ii) the duration of the infringement; and (iii) the 'n' factor (i.e. a unique factor reflecting a Member State's GDP).

EU Enforcement

Date	Description
26 June	**Romanian DPA imposes its first GDPR fine to Unicredit Bank SA for breach of Article 25 of the GDPR (Privacy by Design) and failure to implement appropriate technical and organizational measures** For payments made via Unicredit Bank's online system as well as on bank statements, the payers' addresses and sometimes their national ID number was made accessible to the payment recipients. 337,042 individuals were affected by this breach. The Romanian DPA issued a fine of €130,000 and argued that the bank hadn't put in place sufficient technical and organizational measures and hadn't complied with Article 25 of the GDPR (Privacy by Design) as the Bank's online system was designed in a way that breached GDPR (disclosing unnecessary data). It also based its arguments on both Article 5(1)(c) and Recital (78) of the GDPR. In particular, it emphasized that this information wasn't needed for the processing activities at stake and that the controller has the obligation to process only the data that is necessary in relation the relevant purpose of processing. For more information, please see**:** https://edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_en
3 July	**Dutch DPA announces that Banks cannot use payment data for marketing purposes as both purposes of processing are not compatible** In reaction to the announcement of a major Dutch bank that that it will use payment information to send targeted offers (direct marketing) to its customers and to a several complaints, the Dutch DPA sent a letter to Dutch banks asking them to review and reconsider their marketing practices. Considering the wide range of information a bank has on an individual, the Dutch DPA stressed in its letter that financial information about data subject can reveal particularly sensitive information including medical data, political opinions, sexual orientation etc. The Dutch DPA further argued that using financial information for marketing purposes would not be compatible with the "purpose limitation" principle under Article 5 of the GDPR as this information is originally collected to enable financial transactions. It then concluded that direct marketing is simply not compatible with the purpose of enabling financial transactions as this would not fall within the reasonable expectations of a customer. The only lawful basis to process financial transactions data for direct marketing purposes would therefore be the individual's consent. Pending further guidance or clarification from the DPA on this topic, several banks have stated that they have suspended their direct marketing analysis. The original press release is available here: https://autoriteitpersoonsgegevens.nl/nl/nieuws/banken-mogen-betaalgegevens-niet-zomaar-gebruiken-voor-reclame

Date	Description
3 July	**Danish DPA confirms a decision of the Metro Service not to provide access to CCTV data of an individual** The Danish DPA upheld the decision and confirmed the company's arguments which were as follows: • The individual had not provided a concrete reason for which access to his data was needed • Granting access to the video files would endanger the public as it would reveal the positioning of the cameras and as a consequence any potential blind spots. Considering the above the Metro Service didn't give access to the data and the DPA confirmed this assessment. The original press release is available here: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/jun/ny-afgoerelse-klage-over-manglende-indsigt/
9 July	**German DPA of Hesse banns Office 365 (and others) from German public schools** The DPA of Hesse published a statement on July 9 addressing the legality of using Office 365 in German schools. The DPA argued that the use of Office 365 was not compliant with data protection regulations. It found data was stored in a datacentre to which US authorities have access to and that telemetry information (the extent of which is unclear) was sent back to the US. The DPA also stated that although the ruling is about Office 365, the same reasoning applies to other providers of similar solutions such as Google or Apple as long as their cloud solutions do not comply with German data protection legislation. In the absence of possibility to disable this and the impossibility for school children to give consent by themselves, the DPA concluded that this processing is illegal under the GDPR. For more information please see: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und
31 July	**Greek DPA fined PWC €150,000 for using the wrong legal basis to process employee personal data** In response to a complaint, the Greek DPA conducted an investigation on the lawfulness of processing of the personal data of PWC employees. PWC gave the impression that it relied on its employees' consent to process their personal data whereas, in reality, it relied on another legal basis. The Hellenic DPA found that PWC: *"i. has unlawfully processed the personal data of its employees contrary to the provisions of Article 5(1)(a) indent (a) of the GDPR since it used an inappropriate legal basis;*

Date	Description
	ii. has processed the personal data of its employees in an unfair and non-transparent manner contrary to the provisions of Article 5(1)(a) indent (b) and (c) of the GDPR giving them the false impression that it was processing their data under the legal basis of consent pursuant to Article 6(1)(a) of the GDPR, while in reality it was processing their data under a different legal basis about which the employees had never been informed; and *iii. although it was responsible in its capacity as the controller, it was not able to demonstrate compliance with Article 5(1) of the GDPR, and that it violated the principle of accountability set out in Article 5(2) of the GDPR by transferring the burden of proof of compliance to the data subjects*." The Greek DPA also ordered PWC to implement corrective measures within 3 months of the decision. These include the necessity to bring these processing activities in line with the GDPR and restoring the correct application of the principles listed under Article 5 of the GDPR For more information please see: https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_bg
22 August	**Swedish DPA issues a fine for facial recognition technology** The Swedish DPA has fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in school. A school in northern Sweden has conducted a pilot using facial recognition to keep track of students' attendance in school. The test run was conducted in one school class for a limited period of time. The Swedish DPA concluded that the test breaches several articles in GDPR and has imposed a fine of approximately 20 000 euros. In Sweden public authorities can receive a maximum fine of 10 million SEK (approximately 1 million euros). This is the first fine issued by the Swedish DPA. The school has processed sensitive biometric data unlawfully and failed to do an adequate impact assessment including seeking prior consultation with the Swedish DPA. The school has based the processing on consent but the Swedish DPA considers that consent was not a valid legal basis given the clear imbalance between the data subject and the controller. For more information, please see: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_bg

UK Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
19/07/2019	Life at Parliament View Limited	Monetary penalties	Life at Parliament View Limited (LPVL) (a London estate agency) has been fined £80,000 for leaving 18,610 customers' personal data exposed for almost two years. The security breach happened when LPVL transferred personal data from its server to a partner organisation and failed to switch off an 'Anonymous Authentication' function. This failure meant access restrictions were not implemented and allowed anyone going online to have full access to all the data stored between March 2015 and February 2017. The exposed details included personal data such as bank statements, salary details, copies of passports, dates of birth and addresses of both tenants and landlords. During its investigation, the ICO uncovered a catalogue of security errors and found that LPVL had failed to take appropriate technical and organisational measures against the unlawful processing of personal data. In addition, LPVL only alerted the ICO to the breach when it was contacted by a hacker.
02/08/2019	Making it Easy Ltd	Monetary penalties	Making it Easy Ltd (MIEL) has been fined £160,000 by the ICO for making spam calls to people registered with the Telephone Preference Service (TPS). MIEL made more than one million marketing calls between May 2018 and December 2018, with 853,769 of those calls being made to people registered with the TPS. That means that 80% of all marketing calls made by the firm during that period were unlawful. It is against the law to make marketing calls to numbers that have been registered with the TPS for more than 28 days, unless people have provided consent. The ICO and the TPS received nearly 200 complaints about the company. Whilst a valid CLI was presented, it did not allow subscribers to identify the caller, because the company name provided was not trading name of MIEL, and despite further probing, false or misleading information was provided

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			by MIEL to subscribers. MIEL told the ICO it purchased the data used to make the calls from a third party but that it did not have a contract. The company also did not screen the numbers against the TPS register nor could provide evidence of consent being given.
12/08/2019	Hudson Bay Finance Ltd	Enforcement notices	Hudson Bay Finance Ltd (HBFL) issued with an enforcement notice for failing to respond to a subject access request. The complainant failed to receive response to her subject access request in May 2018 and contacted the ICO on September 2018. The ICO wrote to HBFL to ask it to review the request in December but received no response either. The ICO telephoned HBFL in March, but HBFL refused to engage and hung up the call. Moreover, HBFL failed to answer or return the subsequent calls as requested in June 2019. The ICO subsequently issued a preliminary enforcement notice instructing the data controller to respond to the complainant's subject access request, but the HBFL did not response. The ICO therefore issued this enforcement notice.

The ICO issues its notice of intent to fine British Airways and Marriott Hotels

This July, following extensive investigations, the ICO issued a notice of its intention to fine British Airways £183.39 million and Marriott International £99.2 million for infringements of the General Data Protection Regulation (GDPR). There is limited information about the detail of these notices on the ICO website as they were issued confidentially. However, the notices of intention became public knowledge as the companies had market duties to disclose them. The ICO followed BA's and Marriott's public disclosures with a brief statement.

Commissioner Elizabeth Denham provided more insight into the ICO's motivations in an interview to the Wall Street Journal ("WSJ").

The ICO's main considerations when determining the level of fine according to the WSJ interview were:

1) **The cybersecurity gaps**

   If basic security requirements are not in place, the amount of any fine will be very high. The ICO stresses the need to have in place appropriate security measures for the type of data being processed especially if payment data is involved. However, the ICO does take the standards across the specific industry into account when issuing a fine.

2) **The severity of the attacks**

The type of data stolen and the implications it has on people's lives are relevant factors. If payment data or sensitive personal data is involved then the fine will likely be higher than if the breach only revealed ordinary personal data.

3) **The company's size**

The ICO has a larger expectation from companies with high revenues, because they have the resources to dedicate to protecting customer data and also because the volume of people affected in a data breach would likely be higher. This also translates into ICO's fines, meaning the higher the turnover of a company, the higher the fine.

4) **The number of people affected**

The higher the number of people affected, the higher the fine. The ICO does not focus on whether the compromised data has been used for fraudulent purposes or not, because this can take years to come to light. However, the ICO does have a team who looks through the dark web to check if compromised data is being used or sold there.

5) **The length of time the hackers had access to the data before it was discovered**

This emphasises the importance of ongoing security checks on IT systems to discover any breaches in a timely manner. The longer a breach goes unnoticed, the more culpable the institution is in the ICO's eyes.

6) **Due Diligence**

The GDPR makes it clear that organisations are accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place sufficient accountability measures to assess not only what personal data has been acquired, but also how it is protected.

7) **Repetitive failures**

Another relevant factor is whether there have been any complaints on the entity's data processing practices previously.

The organisations will now have time to make representations to the ICO as to the proposed findings and sanctions. The ICO also stated that it will be issuing more fines this summer. However they will be handed out confidentially.