Bird & Bird

UK & EU Data Protection Bulletin: June 2019 Highlights

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

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

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
30 May	**"GDPR: One year on" report** On 30 May 2019, the ICO published its "GDPR: One year on" paper to share its reflections and learnings on the 1st year of GDPR implementation, along with a blog post by the Information Commissioner, Elizabeth Denham. The paper outlines ICO's work on providing support, taking action, fostering innovation and growing its function and sets out key numbers providing a useful insight into ICO's role. Highlights of the paper include: • Public awareness, especially in respect of data rights and the ICO's role, has increased - this has also resulted in an increase in data rights requests since 25 May 2018, a 66% increase in traffic to the ICO's helpline, live chat and written advice services (amounting to 470,000 communications in 2018/2019) and 16.6 million views of the ICO's online GDPR guide. • Supporting organisations has been key to ICO's function - the ICO will be soon establishing a one-stop-shop for SMEs (along with the already established dedicated helpline, live chat and SME sessions) and is in the process of creating four statutory codes on data sharing, direct marketing, age-appropriate design and data protection and journalism. In addition, it has called on the Government to legislate on the use of personal data in political campaigns. • In terms of enforcement, the ICO is increasingly using its powers to change behaviours. 15 assessment notices have been issued under the new legislation among others in conjunction with ICO's investigations into data analytics for political purposes, political parties, data brokers and credit reference agencies. • From 25 May 2018 to 1 May 2019, 14,000 data breaches were reported - a significant increase compared to the 3,300 notifications received the year before- although only a very small number of these resulted in an improvement plan or a monetary penalty. Also, 41,000 data protection concerns were submitted to the ICO (nearly double compared to 2017/2018), with the health sector, local government and lenders being amongst the most exposed sectors. • The ICO has been involved in around 23% of the cases with EU-wide implications and aims to strengthen its links with EU authorities and continue having a leading role within the global privacy community. • Highlights of its work on enabling innovation include the ICO Sandbox and its Research Grant Programme to support innovative privacy initiatives. • In terms of resources, the ICO's workforce has grown to 700 and will continue to grow to meet the increased demand of ICO services. Also, the ICO has secured more funding by increasing its fee income by 86% compared to last year and by issuing penalties for non-payment of fees which amounted to nearly £100,000.

Date	Description
	As the Information Commissioner confirmed, the ICO will be taking "robust action" against non-compliance. Many of the ICO investigations launched under the GDPR are nearing completion and the outcome - to be expected soon - will demonstrate ICO's actions to protect the public. Organisations are expected to go beyond baseline compliance during the second year of the GDPR and to focus on accountability and real evidenced understanding of risks. During the next period, ICO's regulatory priorities will focus on data broking, use of data in political campaigning, children's privacy, cyber security, AI, big data and machine learning, web and cross-device tracking for marketing, use of surveillance and facial recognition technology and freedom of information compliance.
3 June	**Project expl*AI*n interim report** The ICO and the Alan Turing Institute released their interim report on project expl*AI*n. This collaboration aims at creating practical guidance to assist organisations with explaining artificial intelligence ("AI") decisions to affected individuals. The report highlights three main findings: 1. **Context is key when providing explanations**. The report finds that in some areas, such as recruitment and criminal justice, the expectation for explanations regarding the decision making process is much higher than in others such as healthcare. Participants also stated that the importance and the purpose of the explanation should also vary depending on who it is addressed to and their level of understanding of a particular topic (e.g. in the healthcare context the explanation shouldn't be the same for a doctor as for a patient). 2. **There is a clear need for improved education and awareness around AI.** 40% of the suggestions made by participants around how to build confidence in AI were around awareness building or education related activities. The report doesn't show who should take responsibility for this but argues that information on AI should come through various means (e.g. schools, social medias, broadcast medias, individual involvement etc.). 3. **There are a number of hurdles to overcome to deploy explainable AI.** Most participants were confident regarding the possibility to technically explain the decision process. One of the main issues highlighted by the industry consultation is around internal accountability and the lack of a standard approach in assigning responsibility and ownership around AI explanation in the company. Other issues include the difficulty to keep up with innovation, cost, resources, complexity of the explanations, commercial sensitivity or disclosure of third party personal data. According to the report, the main consequence of these findings is that there is no "one size fits all" approach. The right explanation will very much depend on the context considered. The report perceives this as the strongest message that emerged from the discussions with juries and the roundtables. The full report is available here.

Date	Description
20 June	**ICO Update Report On Adtech And Real Time Bidding – Adtech Industry On Notice** On 20 June 2019, the Information Commissioner published an update report on her office's review of adtech and real time bidding ('RTB') which is a form of auctioned online advertising. The report - which is a progress update rather than formal guidance - raises very significant concerns about the compliance of the adtech industry with the General Data Protection Regulation ('GDPR') and the Privacy and Electronic Communications Regulations ('PECR'). Headline points include: 1. Special category data is being unlawfully collected in the adtech industry, as explicit consent - the only valid lawful basis for such processing - is not being obtained. 2. Personal Data is unlawfully collected in the adtech industry due to the mistaken understanding that legitimate interests is a valid lawful basis for the placing and/or reading of cookies. According to ICO, legitimate interest has a limited role in this context, and in the Commissioner's view consent is the appropriate lawful basis for RTB. 3. Industry initiatives such as the IAB Transparency and Consent Framework ('IAB TCF') do not currently address ICO's concerns. 4. Privacy Notices do not currently go far enough in explaining to individuals what happens to their data. The Commissioner is asking controllers to re-evaluate their practices. But while the report outlines deficiencies, it does not provide any clear solutions. Please find our full analysis of this report here.

<< Back to table of contents

UK Cases

Date	Description
17 April	**Green v Group Ltd & others [2019] EWHC 954 (Ch)** This case relates to a claim arising from the processing of data by the group of companies informally known as 'Cambridge Analytica'. The High Court considered whether to appoint the incumbent joint administrators of the Cambridge Analytica companies as liquidators, despite objections about their conduct being raised by a contingent creditor. The creditor asserted on numerous grounds that the administration had not been conducted properly by the administrators, including on grounds of data protection law. This case summary considers limited aspects of the facts and judgment. **Facts** Cambridge Analytica companies combined data collection and analysis with strategic communications to create targeted advertisements for various political parties and campaign groups. Following the high-profile scandal centered around the group's harvesting of personal data from Facebook profiles without consent, the group faced financial difficulties and upon taking insolvency advice, asked the court to place them into administration. Despite the negative press surrounding the Cambridge Analytica companies and their activities, the proposed administrators asserted that they considered it reasonably likely for the objective of the administration (i.e. the sale of the companies) to be achieved, and the court granted the administration order on 3 May 2018. It soon transpired that the companies could not, in fact, continue to trade as the Information Commissioner's Office (ICO) held the companies' laptops and servers. The administrators attempted to market the business anyway, but no substantial offers to purchase the companies were put forward so the administrators sought to place the company into compulsory liquidation and to be appointed liquidators. The majority of creditors approved the administrators' proposal but one contingent creditor objected to the appointment of the incumbent administrators as liquidators on multiple grounds in the fact that that, prior to the administration order, the creditor had issued proceedings against two of the Cambridge Analytica companies for satisfaction of a data subject access request and pre-action disclosure. **The Subject Access Request** The creditor in question, a US academic, had submitted a subject access request to one of the Cambridge Analytica companies in January 2017. He did not receive a satisfactory reply from the company and instructed solicitors to draft a letter before action requesting a full response and outlining a claim for compensation for distress caused by the breach of the DPA 1998, and the torts of misuse of private information and breach of confidence. No response that could be put before the Court was received. On 16 March 2018 the creditor issued proceedings against several of the Cambridge Analytica companies which was based on s. 7 DPA 1998 and sought an order that the subject

Date	Description
	access request was complied with by a specified date, along with an application for pre-action disclosure of particular documents before pursuit of the s.7 DPA 1998 claim. On 4 May, the day after the Cambridge Analytica companies entered administration, the ICO sent an Enforcement Notice addressed to one of the companies, SCL Elections Limited ('Elections'), requiring it to provide a more satisfactory response to the creditor's SAR. The administrators took no steps to comply with the Enforcement Notice and did not seek to appeal the Enforcement Notice under s.48 DPA 1998, given that (i) the Enforcement Notice was addressed to Elections, (ii) the administrators were not the data controller, (iii) the servers on which the personal data was stored were in the ICO's custody and control with Elections having no access; and (iv) Elections had no staff as of 22 May 2018. The ICO sought to commence criminal proceedings against Elections, which entered a plea and received a £15,000 fine and had to pay a £170 victim surcharge and £6,000 costs as a consequence. **Decision** The court determined that the appointment of the administrators as liquidators was "*conducive to the proper operation of the liquidation*". In respect of the data protection issues raised by the creditor: Failure to comply with the Enforcement Notice did not amount to misconduct The High Court's view supported the generally held view that the *Southern Pacific Personal Loans* decision (that a liquidator will not be considered a data controller in respect of data processed by the insolvent company) also applies to administrators. Administrators act as the company's agent, and will only be considered a data controller where they take decisions about the processing of data as principle, not as an agent. Therefore, in this case, the administrators were not personally responsible for compliance with the provisions of the Data Protection Act 1998 in respect of the data processed by the company, including but not limited to data subject access requests. Mr Justice Norris did not find that the administrators were guilty of any misconduct in relation to the Enforcement Notice. The judgment noted that the questions to be considered by the administrators were: (i) whether it is in the interests of the general body of creditors or a necessary part of discharging statutory duties to help the creditor pursue his data rights; and (ii) whether choosing not to help the creditor would cause unfair harm to the interests of the credit (limited to interests as a *creditor*, not as an academic or campaigner). Mr Justice Norris agreed with the administrators that compliance with the Enforcement Notice would have been disproportionately costly, as it would have required the administrators to search for the creditor's data among 700 terabytes of data in the custody of the ICO. It was held that compliance with the request would have been detrimental to the body of creditors as a whole, and that the decision not to search for the creditor's data was one a competent administrator could properly make. No duty to investigate previous data protection issues The High Court found that implicit in the creditor's complaint was an assumption that the administrators were under a general duty to investigate data breaches which took place before the administrators were appointed. Mr Justice Norris confirmed that investigations into data protection infringements are not for administrators or liquidators to conduct – these should remain the responsibility of external

Date	Description
	regulators, not conducted by insolvency office holders at creditors' expense. The duty of administrators and liquidators is only to investigate breaches of directors' duties to the company and creditors. The full judgment is available here.
17 May	**Mrs Ashley Judith Dawson- Damer, Mr Piers Dawson Damer, Ms Adelicia Dawson Damer v Talyor Wessing LLP (& Others) [2019] EWHC 1258** On 17 May, the High Court handed down the third decision on this case and provided some important clarifications on the definition of a relevant filing system, the legal professional privilege exemption and what constitutes a reasonable and proportionate search. **Background** Taylor Wessing (TW), acted as the English solicitor to a trustee of Bahamian family trusts (Yuills Trusts) which included the Glenfinnan Settlement .The First Claimant, Mrs Dawson Damer, was a discretionary beneficiary of the Glenfinnan Settlement and she had challenged the validity of the appointments made out of that settlement. Back in 2014, together with her adult children, she served subject access requests on Taylor Wessing under the Data Protection Act 1998. TW refused to provide the information requested in the SARs, relying on the legal professional privilege exemption in paragraph 10 of Schedule 7 to the Data Protection Act 1998 (DPA 1998) (the" LPP Exemption"). The Claimants challenged this and TW was successful at first instance. The Claimants then appealed. In March 2015, the First Claimant also commenced proceedings in the Bahamas against the trustee of the Glenfinnan Settlement and that litigation is ongoing. It is an important part of the background that under S839(8) of the Bahamian Trustee Act 1998 (the "BTA") trustees cannot be compelled to disclose to any beneficiary or other person certain documents relating to any letter of wishes, deliberations of trustees or other documents relating to the trustees' exercise of discretion and the Bahamian court would similarly not be able to order such disclosure. In February 2017, the Court of Appeal held that the LPP Exemption only applies to information which would attract LPP as a matter of English law (and the judge at first instance was wrong to suggest that it also exempted information which would be protected from disclosure under Bahamian law). Further, TW could not refuse to provide information on the basis that any search for non-LPP material would require disproportionate effort. Whilst a search does not need to be exhaustive, solicitors relying on the LPP Exemption must evidence that they have carried out a reasonable and proportionate search of their files. Finally the Court of Appeal held that the first instance judge was also wrong to decline to enforce the subject access request because the Claimants intended to use the information in their ongoing Bahamian litigation. An application by TW to appeal to the Supreme Court was refused. The Court of Appeal however remitted a number of issues back to the High Court for further determination. Out of these, the points below are worth noting.

Date	Description
	Decision ***Relevant Filing System*** Firstly the Court had to consider whether the paper files maintained by TW before it moved to electronic files were a "relevant filing system" as defined under the DPA 1998 because if so, TW would be required to search them. The Court concluded that TW's paper files held on under the client description "Yuills Trusts" and arranged in chronological order, are a 'relevant filing system' for the purpose of the DPA 1998 and TW was required to further search these files. In doing so, the Court departed from the restrictive interpretation of a "relevant filing system" in the Court of Appeal's decision in *Durant v Financial Services Authority [2004] FSR 573* and instead concluded that the approach of the CJEU in *re Tietosuojavaltuutettu (*Case C-25/17*)* must now be followed. This was on the basis that Durant had been decided before the right to the protection of personal data was enshrined as a fundamental EU right by Article 8 of the Charter of Fundamental Rights and that since then, the perspective has changed and the focus is on the need for protection of the data subject, as opposed to the burden on the data controller. The Deputy Judge found that the requirement in *Durant* that there must be a structured referencing mechanism containing a sufficiently sophisticated and detailed means of readily indicating whether and where an individual file specific criteria or information about the applicant can be readily located is inconsistent with *re Tietosuojavaltuutettu*. However, he rejected the argument that the sole criterion is whether the personal data can be "easily retrieved". Instead he determined that 3 elements were needed: (i) The data must be structured by reference to specific criteria. (ii) The criteria must be "related to individuals". (iii) The specific criteria must enable the data to be easily retrieved. However, permission to appeal on this issue has already been granted. ***Legal Professional Privilege*** Secondly, the Court had to relook at the LPP Exemption and in particular whether there was scope to rely on legal advice privilege as well as litigation privilege. The Court found that TW was entitled to claim LPP over documents on this basis. This is now clearly stated in the Data Protection Act 2018 (Schedule 2, Part 4, Para 19). Mrs Dawson Damer tried to argue that such privilege was a joint privilege between a beneficiary and trustee under English law. Whilst the Deputy Judge agreed with this point under English trust law, he went on to question the effect of the Bahamian Trustee Act on this. In his view, given that Bahamian law governed the Glenfinnan Settlement, this should be the relevant law upon which to consider whether the Claimant has a "joint privilege". In this case, the relevant provisions under the BTA state that where Bahamian law applies to a trust, a beneficiary has no automatic right to see the legal advice to a trustee prior to any threatened litigation and no proprietary rights to

Date	Description
	documents containing that advice and so no "joint privilege" can exist under that law. Consequently, the beneficiary cannot prevent reliance on the relief provided for by the LPP Exemption. ***Reasonable and Proportionate Searches*** The Deputy Judge made a number of findings specific to the facts and held that further searches needed to be carried out to discharge TW obligations under the DPA 1998 and certain searches did not. In particular, the Deputy Judge held that searching a backup system would be disproportionate and would run the risk of disclosing confidential data about the law firm's clients or employees. Also it would also be disproportionate to search ex-employees personal spaces but not those of current employees. **Implications** This decision should be positive news for trustees who had been concerned about the potential for subject access requests to be used by litigious beneficiaries. This case was decided under the DPA 1998 which has now been replaced by the GDPR and the Data Protection Act 2018. However, the LPP Exemption remains in the DPA 2018 in Schedule 2, Part 4, Para 19 and it is now clearly states that it covers personal data to which a claim to legal professional privilege (or confidentiality of communications in Scotland) could be maintained in legal proceedings; or in respect of which a duty of confidentiality is owed by a professional legal adviser to his client. The GDPR also contemplates certain additional grounds upon which trustees might be justified in withholding disclosure – for example, on the basis of conflicting duties of confidentiality or where such disclosure would "adversely affect the rights and freedoms of others" (Article 15(4) GDPR).
11 June	**Advertising Standards Authority Limited v Robert Neil Whyte Mitchell [2019] EWHC 1469** This case relates to an application by the ASA for an injunction to prevent an unintended recipient of an email from using, publishing, communicating or disclosing any part of the email or its attachments on the grounds that the contents were confidential and in part legally privileged. As Mr Justice Warby puts it "*just about everyone who uses email will have had an experience similar to the one that led to this application*". **Facts** In this case, an investigating officer at the ASA who had been looking at a complaint about a billboard advert criticizing the Royal Bank of Scotland, apparently funded by Mr Mitchell (the person under investigation), accidentally sent an email and a number of attachments to Mr Mitchell instead of the ASA's lawyers. The attachments included details of the complaint, photo of the billboard, correspondence exchanged with Mr Mitchell, draft recommendations for a complaint, emails containing legal advice and a written opinion from Counsel from 2009. Once the office realised his mistake, he promptly tried to recall the message and emailed Mr Mitchell asserting that the email was

Date	Description
	confidential and should be deleted. This was later followed up with letters, voicemails and texts including a letter stating that an injunction would be sought in the absence of suitable undertakings from Mr Mitchell. Mr Mitchell had evidently been aware of these communications from an early stage as he started posting on Twitter but he did not reply under 5 days later and made it clear that no undertakings would be forthcoming. It was against this background that the ASA issued an application for an injunction. **Decision** The Court decided the case in favour of the ASA and ordered the injunction. Where an application for an injunction is to restrain an alleged breach of confidence, the Court must be persuaded that the claimant is likely to establish that the information has the quality of confidence, that the information has been imparted to or acquired by the defendant in circumstances importing an obligation of confidence and the defendant threatens or intends to misuse the information. With respect to the documents which were legally privileged, the established principles are that where the disclosure is as the result of an obvious mistake, the Court should ordinarily intervene. Although there may be exceptions where the Court could properly refuse relief on other grounds, the law does not require the Court to engage in the balancing of the public interest in upholding the privilege as against the public interest in allowing the documents to be used in litigation. Mr Justice Warby also stated that when it comes to the imposition of a duty of confidence, there is no special treatment for privileged information and it would be treated in the same manner as any other confidential information. In granting the injunction, the Court found that apart from the photograph, the email and the attachments were confidential in nature and Mr Justice Warby was satisfied that there was a threat or a risk that if not restrained, Mr Mitchell would publish the information – this was based on some of his previous tweets and emails sent to the ASA and also based on his past behaviour.

<< Back to table of contents

Other UK News

Date	Description
10 June	**DMCS consultation about public concerns around data protection (deadline 14 July):** On 10 June 2019, the Department for Digital, Culture, Media and Sport (DCMS) *announced* an open call for evidence for the government's intended National Data Strategy (NDS). The stated aims of the NDS are that it will empower government and the economy through the use of data, and ensure public trust in its use. The call for evidence is structured according to three key areas: people, economy and government. The DCMS has set out objectives and several questions specific to each area. The DCMS has invited submissions on the following issues specific to data protection: • Are organisations (private, public or third sector) using personal data in ways that may damage trust? • Do people know how information provided to, or inferred about them by, an organisation (private, public or third sector) is being used, stored and shared? • Are people aware of how to manage personal data about them? Do they know about tools to control access? • Have the General Data Protection Regulation and Data Protection Act 2018 made people more concerned about how personal data is managed? How has it influenced their behaviour? The DCMS has stated that it will use the evidence it receives to formulate the draft NDS, which it will consult on later in 2019.
11 June	**BEIS consultation about going beyond GDPR data portability (deadline 6 August 2019):** On 11 June 2019, the Department for Business, Energy and Industrial Strategy (BEIS) published a consultation on proposals following its Smart Data Review. The Smart Data Review has explored how government can accelerate the development and use of new data-driven technologies and services to improve consumer outcomes. In particular, it considered how such technologies can foster innovation and facilitate switching and data portability in regulated and digital markets. BEIS is consulting on a proposal to establish a new cross-sectoral Smart Data Function to oversee the delivery of smart data initiatives across multiple markets. It is also proposing to legislate to introduce an Open Communications initiative with the objective to stimulate innovation and promote the development of new services that improve outcomes for consumers in the communications market.

The consultation also considers proposals for using data and technology to help vulnerable consumers (including exploring ways regulators can utilise consumer data to support vulnerable consumers). Further, BEIS is consulting on proposals to protect consumer data, including by introducing strong data protection requirements on Third Party Providers (TPPs) accessing consumer data and a possible cross-sectoral approach to the regulation of TPPs.

The consultation document notes that the government agrees with the recommendation of the Digital Competition Expert Panel that there is a strong case for establishing a pro-competition Digital Markets Unit, tasked with securing competition, innovation and beneficial outcomes for consumers and businesses in the digital economy. The government will be consulting later in the year, as part of a broader Competition Green Paper, on extending Smart Data to digital markets in its response to the recommendations of the Digital Competition Expert Panel.

Together with this consultation, BEIS has also published a White Paper "*Regulation for the Fourth Industrial Revolution*" setting out proposed reforms to ensure an agile and flexible approach to regulation in the UK at a time of rapid technological change. This recognises that new products, services and business models are emerging which do not fit with existing regulatory systems.

The government's proposals are intended to allow entrepreneurs and business to embrace innovation, seize the opportunities of cutting-edge technology and bring transformative products to market to benefit consumers and other businesses. These measures being proposed include:

- A new Regulatory Horizons Council to advise government on rules and regulations that may need to evolve and adapt to keep pace with technology.
- Piloting an innovation test so that the impact of legislation on innovation is considered during the development of policy, introduction and implementation of legislation and its evaluation and review.
- Developing a digital Regulation Navigator – a new digital interface to help businesses ease their way through the regulatory landscape and bring their ideas to market quickly.
- A partnership with the World Economic Forum to share best practice on getting innovative products and services to market.
- A review of the Regulators' Pioneer Fund, which backs projects that are testing new technology in partnership with the regulators in a safe but innovative environment.

The government has consulted separately on how the economic regulators Ofwat, Ofgem and Ofcom could drive greater innovation in the sectors they regulate, including whether there was a case for introducing an innovation duty. The government will announce how to take these findings forward later this year (see *Legal update, Government consults on encouraging innovation in regulated utilities*).

This White Paper on regulation notes that it will be will be matched later this year with papers describing how the government will modernise consumer and competition regulation in response to the transformation in the economy. More details here.

Europe

EDPB

Date	Description
4 June 2019	**EDPB holds 11th plenary session; adopts new guidance** On 4th June 2019, the European Data Protection Board (EDPB) held its most recent plenary meeting, adopting new guidance that will be of interest to organisations looking to benefit from the GDPR's provisions on Codes of Conduct and Certification schemes. Other agenda items included discussion of the U.S. CLOUD Act (concerning U.S. law enforcement access to data stored outside U.S.), governance of social media, and common strategic priorities for the GDPR's national supervisory authorities. **The EDPB's agenda for the 11th plenary of the EDPB can be found here; the finalised guidance on code of conduct, certification and accreditation schemes can be found here.**

<< Back to table of contents

EU Cases

Date	Description
13 June 2019	**On June 13, the ECJ confirmed in the Gmail case that email services like Gmail do not fall under the definition of an "electronic communications service pursuant to Framework Directive 2002/21/EC as modified by Directive 2009/140/EC. The judgment provides the ECJ's view on a question that has been subject of a dispute with the German national regulator which originated back in 2012.** After the judgment in the preceding week concerning SkypeOut, this is the second decision of the ECJ concerning the application of the current European regulatory framework for electronic communications services on so-called over-the-top (OTT) services, i.e. services for personal communication delivered on the basis of Internet access services provided by different parties. Unlike the judgment in the SkypeOut case, this latest judgment finds that the relevant service is not a regulated electronic communications service. This means that Gmail and similar OTT services are excluded from the scope of application of the current ePrivacy Directive (in particular the restrictions on use of traffic and location data) since this relies on the definitions in Directive 2002/21/EC. However, it is worth noting that in any event, the definition of electronic communications services was expanded to cover OTTs by the Electronic Communications Code, which was adopted last year, which will repeal Directive 2002/21, and will become applicable on December 21, 2020. Please find our full article on this case here.

<< Back to table of contents

Other EU News

Date	Description
14 November 2018 (applicable as of 28 May 2019)	**New EU Regulation on non-personal data.** EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union (the "Non-personal Data Regulation" or "FFD") became directly applicable in all EU Member States on 29 May 2019. The main purpose of the FFD Regulation is to allow mobility of non-personal data across borders and ensure the freedom to provide data processing services within the EU, which are sometimes restricted by national legal requirements to locate data in a specific territory. "Non-personal data" is defined as all data which in not covered by Art 4(1) GDPR's definition of "personal data". This type of data can be categorized depending on its source: (1) data which originally did not relate to an identified or identifiable individual, such as data on weather conditions generated by sensors of wind turbines, and (2) data that was originally personal data but that has been anonymized to the point that it "cannot be attributed to a specific person". For example, non-personal data can be "data which are aggregated to the extent that individual events, such as a person's individual trips abroad or travel patterns which could constitute personal data are no longer identifiable". This is intended to encourage competition and quality of services for companies looking, for example, to outsource their data storage and processing activities to a service provider located in another Member State. The territorial scope of the FDD is different to that of the GDPR: the FDD applies to the processing of electronic data other than personal data in the EU which is: • Provided as a service to users residing or having an establishment in the EU, regardless of whether the service provider is established in the EU or not; or • Carried out by a person (legal or natural) residing or having an establishment in the EU for its own needs. The new Regulation forbids any data localisation requirements in the EU, whether direct (eg obligation to store data in a specific geographic location) or indirect (e.g requirements to use technological facilities that are certified or approved within a specific Member State that have the effect of making it more difficult to process data outside of a specific area/territory) unless these are justified on grounds of public security in compliance with the principle of proportionality. The Regulation also aims to improve the ease with which data can be ported from one processor to another. In this regard, the FFD will rely on self-regulation, by encouraging stakeholders to develop industry codes of conduct. Two such codes of conduct are already in the pipeline: the SWIPO working group is developing a code for porting/switching between Cloud service providers and the CSCERT working group is working on cloud security certification. The intention is that more will follow, and the process is expected to be finished by November 2019. Once codes of conduct are in place, it is expected that these industry working groups will develop model contractual clauses to be used in data storage and processing contracts, to give technical effect to the codes of conduct. Contracts will then need to be updated to incorporate these new clauses. On 29 May 2019, the European Commission published guidance on the new regulation and on how it interacts with the GDPR. The guidance is keen to stress that there are no contradictory provisions between the GDPR and the FFD. The guidance also clarifies how organisations should deal with "mixed datasets", i.e. datasets made up of both personal data and non-personal data. There is no requirement on data processors to store personal data separately to non-personal data. Generally, the FFD will apply to non-personal data and the GDPR will apply to personal data, but when the two types of data are "inextricably linked", the GDPR will "fully apply" to the whole dataset. The FFD's definition of "inextricably linked" is very wide, and is likely to apply to most data sets.

Date	Description
28 May 2019	**CNIL fine to real estate company amounts to 1% of its annual turnover.** Sergic, a real estate company allowing individuals to upload any supporting documentation through their website was fined €400,000 by the CNIL (the French data protection authority) on 28 May for (i) failure to implement appropriate security measures and (ii) retention of personal data for longer than is necessary. **Background** The CNIL received a complaint in August 2018 from an individual saying that when logged into their account, slightly changing the URL allowed them to have access to the documentation of other individuals. This included documents such as ID cards, social security cards, account statement, tax notices and other information. The CNIL's investigation showed that Sergic had known about this vulnerability since March 2018 and did not fix it until September of the same year. In addition, all documents were kept indefinitely in an active database. **Decision** The CNIL found that Sergic failed to comply with Article 32 of the GDPR as it lacked basic security measures such as an authentication procedure to access documents uploaded to their website by candidates. The CNIL also argued that the categories of data involved and the lack of diligence of the company were aggravating factors. On the violation of Article 5(e) of the GDPR the CNIL highlighted that retention of the personal data of unsuccessful candidates was unjustified. It stated that it could have been kept for longer than 3 months only if it had been archived on a separate database. The fine imposed by the CNIL took into account the seriousness of the violations and the lack of diligence of the company in fixing the issues as well as the size and the financial capacity of the company. It must be noted that although the face value of the fine appear relatively low, it amounts to 1% of Sergic's annual turnover.

International News

Date	Description
24 May 2019	**Tunisia becomes the 30th signatory to the Council of Europe's Protocol amending Convention 108[1] ("Convention 108+").** Convention 108+ aims to modernise and improve Convention 108. Many of the changes correspond to changes to the EU's data protection regime brought in by the GDPR, e.g. with Convention 108+ providing for (amongst other things): • stronger accountability of data controllers • an obligation to declare data breaches • sensitive data to include genetic and biometric data, trade union membership and ethnic origin and • individuals to have the right to challenge purely automated decisions. In addition to the above, Convention 108+ transforms the former 'Consultative Committee', a body composed of representatives from each party's government or national supervisory authorities, into a 'Convention Committee'. The new Convention Committee has the power to review the level of personal data protection a party provides against Convention 108+'s requirements either at the point of accession or on a periodic review; the Convention Committee may also make recommendations where it finds non-compliance. Convention 108+ opened for signature on 10 October 2018. It is pending ratification by Tunisia and its 29 other signatories.
28 May 2019	**Morocco is the sixth country in the African region and 55th State party to accede to Convention 108.** Morocco also signed-up to the Council of Europe's Additional Protocol to Convention 108. The Additional Protocol sets out requirements relating to supervisory authorities and transborder flows of personal data to recipients which are not party to Convention 108 (the "Additional Protocol"). Convention 108 is the only legally binding international treaty for data protection and it was significantly revised in October 2018. It remains to be seen whether Morocco will also sign-up to the modernised version of Convention 108, referred to as "Convention 108+" - though signing up to Convention 108 is a perquisite for becoming party to Convention 108+. Convention 108 and the Additional Protocol will enter into force in for Morocco on 1 September 2019.

UK Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
06/06/2019	Jeannette Baines	Prosecution	A caseworker has been prosecuted for sending sensitive personal data to her own personal email account without authorisation. Jeannette Baines had worked at victim support and had sent spreadsheets containing a combination of victim and offender data from her work email address to her personal email address during her last week of employment. Mrs Baines appeared before Blackpool Magistrates' Court and was found guilty of obtaining personal data in breach of s55 of the data Protection Act 1998. She was sentenced to a 3 year conditional discharge, ordered to pay £600 in costs and a victim surcharge of £20.
07/06/2019	Wendy Masterson	Prosecution	A former customer service advisor at Stockport Homes has been prosecuted for accessing records relating to anti-social behaviour without authorisation. The offenses came to light after an audit of Ms Masterson's access to SHL's case management system, after concerns surrounding her performance. An internal company investigation found that Wendy had inappropriately accessed the system 67 times between January and December 2017 without any legitimate reason to do so. The records in question related to victims, witnesses and perpetrators of anti-social behaviours. Ms Masterson appeared before Stockport Magistrates' Court and pleaded guilty to the offence of unlawfully obtaining personal data, in breach of s55 of the DPA 1998. She was fined £300, ordered to pay £364.08 in costs and a Victim surcharge of £30.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
13/06/2019	Smart Home Protection	Monetary Penalty	The Information Commissioner's Office (ICO) has fined Smart Home Protection Ltd £90,000 for making nuisance calls to people registered with the Telephone Preference Service (TPS). The ICO decided to issue the company with a monetary penalty under section 55A of the DPA 1998 after making unsolicited calls to people who had not given consent to receive such calls, for the purpose of direct marketing contrary to regulation 21 of PECR. Between 10 January 2017 and 24 September 2018, the Commissioner received 125 complaints about the unsolicited direct marketing calls made by Smart Home Protection Ltd. The Commissioner also commented that it was reasonable to suppose that considerably more calls had been made as those that complained were likely to represent a small proportion of those who actually received the calls. The Commissioner decided to issue a monetary penalty of £90,000 to encourage other businesses currently engaging in these practices to comply with PECR and reinforce the need for businesses to ensure they are only contacting customers who want to receive these calls.
21/06/2019	Met Police	Enforcement Notice	Two Enforcement Notices have been issued against the Metropolitan Police Service for sustained failure to respond to subject access requests submitted before and after the GDPR came into force. The Met Police had 8 outstanding subject access requests which had been submitted before 25 May 2018, but also had, as of 13 June, 1,727 open subject access requests received since 25 May 2018 (with 1,169 of those overdue). The Enforcement Notices require the Met Police to have complied with all outstanding subject access requests by 30 September 2019. Additionally, the Enforcement Notice relating to the GDPR subject access requests also requires the Met Police to have made system and policy changes by 30 September 2019 to ensure that future subject access requests can be handled in accordance with GDPR requirements.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
24/06/2019	David Cullen	Prosecution Disqualification Confiscation Order	A former company director found guilty of illegally obtaining people's personal data and selling it to solicitors chasing personal injury claims, has been fined for breaches of data protection and issued with a confiscation order under the Proceeds of Crime Act 2002. David Cullen was the managing director of No1 Accident Claims Limited until 20 December 2012 when the company was liquidated. The business profited from selling illegally obtained personal data to solicitors. Appearing before Manchester Crown Court on 24 June 2019, Cullen was fined £1,050 and ordered to pay £250 costs for unlawfully obtaining and selling personal data in breach of s55 of the Data Protection Act 1998. He was disqualified from being a company director for five years and an order was made for the forfeiture and destruction of items which were seized as part of a search warrant in 2012. Following sentencing, confiscation under the Proceeds of Crime Act 2002 commenced. The exact figure which Cullen is believed to have benefited from during his illegal activities is £1,434,679.60. Due to a lack of assets, the Court proceeded by making a £1 nominal order. Cullen's financial circumstances will be regularly reviewed, and should they improve, the amount of the confiscation order can be increased.
26/06/2019	EE	Monetary Penalty (PECR)	The ICO has fined EE £100,000 for sending text messages to customers without their consent, in breach of the Privacy and Electronic Communications Regulations 200. The messages, sent in early 2018, encouraged customers to access and use the 'My EE' app to manage their account and also to upgrade their phone; a second batch of messages was sent to customers who had not engaged with the first. During the ICO investigation EE stated the texts were sent as service messages and were therefore not covered by electronic marketing rules. However the ICO found the messages contained direct marketing and that the company sent them deliberately, although acknowledges that EE Limited did not deliberately set out to breach electronic marketing laws.