Bird & Bird

UK & EU Data Protection Bulletin: March 2020

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

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

United Kingdom

ICO

UK Legislation

EU and Council of Europe

EDPB

Council of Europe cases

EU Legislation

Other EU news

UK Enforcement

ICO enforcement

First Tier Tribunal

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
7 February 2020	**ICO warns Insolvency Practitioners on data sharing with claims companies** The ICO, the Financial Conduct Authority ("FCA") and the Financial Services Compensation Scheme ("FSCS") warned Insolvency Practitioners ("IPs") against unlawful data sharing with (FCA-regulated) Claims Management Companies ("CMCs") in a joint statement issued on 7 February 2020. Noting that they had "become aware" that some IPs of failed financial services firms had attempted to sell the personal data of the firms' clients to CMCs, the authorities cautioned IPs that valid legal consent for sharing such personal data was highly unlikely to be found in the run-of-the-mill client contracts which had been entered into by the failed firm (unsurprisingly for data protection professionals). CMCs were also warned that their subsequent direct marketing to such clients may be in breach of PECR, and that it was highly unlikely that a CMC would be able to rely on its legitimate interests here. On this latter point, the authorities noted that a CMC is also obliged, under the FCA Handbook, to act honestly, fairly and professionally in line with the best interests of their customers. This means a CMC must be able to demonstrate how it has considered the fair treatment of customers and how its actions comply with privacy laws. Taking a dim view of the value added by fee-charging CMCs to claims before the free-to-use FSCS, the ICO and FCA stated they will take appropriate action where they find breaches of data protection legislation or the FCA Handbook. The FSCS is a statutory body from which certain eligible consumers of failed financial services firms may seek recourse for losses connected to the products or services obtained from the failed firm. The FCA is responsible for policing the conduct of and authorising financial services' firms and claim management companies.
19 February 2020	**ICO issues draft guidance on the AI Auditing Framework for consultation** The ICO has recently opened for consultation a lengthy set of draft guidelines on how to understand data protection law in relation to AI and suggested best practice recommendations for ensuring data protection compliant AI. It comprises auditing tools and procedures that the ICO will use in audits and investigations and also includes indicative risk and control measures that organisations can deploy when using AI to process personal data and to audit the compliance of their own systems. The guidance is aimed at those with a compliance focus, such as DPOs, internal counsel and ICO's own auditors but also technology specialists. This idea is that this will complement existing ICO resources such as those on Big Data, AI and Machine Learning (from 2014) and the ICO's Guidance explaining decisions made with AI produced in collaboration with the Alan Turing Institute. The Guidance focuses on the data protection challenges introduced or heightened by AI but does not provide generic ethical and/or design principles for the use of AI. It provides sections on how to deal with the following in AI systems: accountability, lawfulness, fairness and transparency of processing, security and data minimisation and facilitating the exercise of individuals' rights.

Date	Description
	The consultation closes on 1 April. For a copy of the draft Guidance and how to respond, please see here.
28 February 2020	The ICO has published guidance for organisations wanting to develop GDPR Codes of Conduct or Certification schemes and organisations can submit their proposals for such Codes or Schemes to the ICO for approval.

Date	Description
29 January, 2020	**Data Protection (Independent Complaint) Bill [HL] 2019-20** Baroness Kidron, a keen advocate of the ICO's recently published Age Appropriate Design Code of Practice, introduced a private members' bill in the House of Lords on 29th January. Its purpose is to amend the Data Protection Act 2018 (adding a 's.187A' after s.187) to grant representative bodies and organisations the power to exercise independent complaint and remedy rights on behalf of data subjects (in particular on behalf of more vulnerable groups which are listed below). It has only had its first reading so far which is just a formality, no debate is held over its content at this stage, so it has not gained much publicity nor commentary as of yet. There has been no indication of when its second reading will be, but details on its progress can be found here. It currently reads as follows: **"187A Independent complaint by representative bodies or organisations** (1) In relation to the processing of personal data to which the GDPR applies— (a) a body or other organisation which meets the conditions set out in Article 80 of the GDPR may, independently of a data subject's authorisation, exercise the rights of a data subject under Article 77, 78 and 79 of the GDPR (rights to lodge complaints and to an effective judicial remedy) if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing. (2) In relation to the processing of personal data to which the GDPR does not apply— (a) a body or other organisation which meets the conditions in section 187 subsections (3) and (4) may, independently of a data subject's authorisation, exercise some or all of the rights of a data subject set out in section 187(2) paragraphs (a), (b), (c) and (d) if it considers that the rights of a data subject have been infringed as a result of the processing. (3) In this section "data subject" includes but is not limited to data subjects who are or may be— (a) less aware of their rights; (b) less willing to identify themselves as complainants or unable to identify their rights due to vulnerabilities; (c) children; (d) elderly; (e) LGBT+ persons; (f) persons in strict religious communities; (g) women in public positions; and (h) women at risk of domestic abuse and violence."

<< Back to table of contents

EU and Council of Europe

EDPB

Date	Description
EDPB Plenary Sessions – January and February 2020	The EDPB held plenary sessions in January and February. A number of new documents and guidelines have been published, including: • Guidelines on the processing of personal data in the context of connected vehicles and mobility related applications. The guidelines are open for public consultation until 20 March. The scope of the guidelines covers personal data that is (1) processed in connected vehicles (2) exchanged between vehicles and personal devices such as smartphones or (3) data that is collected in the vehicle and shared with third parties, including data sharing with insurers for the purposes of usage based insurance.Key points to note from the guidelines are outlined in our article; • Guidelines on the processing of Personal Data through Video Devices (following public consultation) . We will provide a more detailed summary of these Guidelines in due course; • Opinions of Accreditations Requirements for Codes of Conduct Monitoring Bodies submitted by Spain, Belgium and France and for Certification Bodies submitted by the UK and Luxembourg; • Draft Guidelines (which will be submitted for public consultation) to provide further clarification regarding the application of Articles 46.2 (a) and 46.3 (b) of the GDPR which relate to transfers of personal data from EEA public authorities or bodies to public bodies in third countries or to international organisations where these are not covered by an adequacy decision. • The EDPB's contribution to the evaluation and review of the GDPR as required by Article 97. The EDBP's overall conclusion is that the application of GDPR in the first 20 months has been successful and it would be premature to revise the GDPR at this point in time although it does recognise ensuring that supervisory authorities have sufficient resources remains a concern and that some challenges remain.

Council of Europe cases

Date	Description
30 January 2020	**Breyer v Germany (application no.50001/12)** On 30 January 2020, the European Court of Human Rights ("ECHR") delivered its judgement in Breyer v Germany stating that the compulsory collection of sim-card registration data under the German Telecommunications Law (Telekommunikationsgesetz, or "TKG") and the subsequently sharing of it with law enforcement was not a violation of Articles 8 and 10 of the European Human Rights Convention. Although the Court accepted that there was an interference with the applicant's right to privacy, nonetheless it concluded that the interference was limited and pursued legitimate aims of national security and therefore there was no human rights violation. **Background** The applicants argued that the compulsory data collection requirements under sections 111,112 and113 of the TKG for pre-paid sim cards and the sharing of this data with law enforcement were incompatible with Articles 8 and 10 of the Convention for the Protection of the Human Rights and Fundamental Freedoms ("the Convention") due to the interference with their right to anonymous communication. Similar laws around sim card registration exist in some other EU countries, but they did not exist in Germany prior to the TKG. Section 111 of the TKG introduced an obligation on telecommunication providers to collect the telephone numbers, name, address, date of birth and device number of the sim card holder whereas sections 112 and 113 contained an automated and manual procedure to access the data stored under Section 111. Applicants had previously brought a constitutional challenge against the TKG in 2005 to the German Federal Court. They argued the storage and sharing of sim card registration data was a serious interference with their rights and most of the data related to innocent individuals. They further argued that the information in question was in most cases useless for investigations because criminals would be unlikely to use their real identities for registration and they would often purchase the prepaid sim cards in jurisdictions where there is no registration requirement. The Federal Court held that the obligation to maintain a database of subscriber information pursued a legitimate aim of criminal prosecution and the information contained did not include specific activities of individuals. Therefore, it was justified and constitutionally unobjectionable. The case was subsequently brought in front of the ECHR in 2012. The ECHR referenced its case law to stress the importance of people's right to respect for private and family life and that this necessitates sufficient legal safeguards to prevent the misuse of personal data contrary to the protection provided by Article 8. It agreed that there had been interference. However, when judging the necessity of the measures, it highlighted the discretion given to governments when pursuing national security. It noted that the authorities that could request access to registration data under the TKG were all part of law enforcement and this constituted a limiting factor as well as being clearly foreseeable. The ECHR also considered the review and supervision of information requests under the relevant sections of the TKG and ruled that "*legal redress against information retrieval could be sought under general rules*". Overall the German Government's measures were found to be proportionate in pursuing their legitimate aim and there was no violation of the Convention.

EU legislation

Date	Description
March 2020	**Presidency introduces 'legitimate interests' into amended proposal** The Croatian Presidency of the EU has issued an amended proposal for an e-Privacy Regulation, to be discussed during the meeting of the Working Party on Telecommunications and Information Society on March 5 and 12. Negotiations have been ongoing for a number of years and the previous Finnish Presidency had tried unsuccessfully to reach a political agreement last November. Currently, the Croatian Presidency is proposing to simplify the text of some of the core provisions and to further align them with the General Data Protection Regulation, which may prove to be a controversial move. Highlighted below are some of the most important amendments for industry in the latest draft. **What's new?** The key change in the latest draft is the addition of the legitimate interests of an electronic communications network, or service provider, as a potential lawful basis for the processing of electronic communications metadata such as location data. This can only be relied upon where the interests, or the fundamental rights and freedoms of the end-user, are not overriding. The legitimate interests of a provider of electronic communications networks or services to process electronic communications metadata could exist where such processing is necessary for: Detecting or stopping fraudulent or abusive use of, or subscription to, electronic communications services; Calculating and billing interconnection payments; or For the purposes of network management or network optimisation. However, crucially, the proposal does make it clear that the use of legitimate interests cannot be used in order to determine the nature or characteristic of an end-user or to build an individual profile on them. Furthermore, one of the main changes in the latest draft is the ability to rely on the legitimate interests of the service provider as the lawful basis for the collection of information from end-users' terminal equipment (including through the use of cookies and other tracking applications). The draft seems to focus on mobile phones and similar terminal equipment but leaves aside security issues that may arise from modems and routers. These obligations are particularly relevant in view of the forthcoming BEREC Guidelines on common approaches to the identification of the network termination point in different network topologies.

Under this proposal, providers would also be permitted to process an end-user's electronic communications metadata where it is necessary for the provision of an electronic communications service based on a contract with that end-user (and for billing related to that contract).

What remains unchanged?

As with the previous proposal, the new rules should not prohibit the processing of electronic communications data (content and metadata) without the consent of the end-user for the purposes of ensuring the security of electronic communications services, including availability, authenticity, integrity or confidentiality. This should cover processing for the purposes of checking security threats such as the presence of malware or viruses, or the identification of phishing.

When processing content, the provider of the electronic communications service may be required to consult the supervisory authority, but this will depend on whether consent is obtained from one user for the provision of a service to that user or from all parties to the communication. Only the latter will require consultation with the supervisory authority.

In addition to the new provisions discussed above, providers of electronic communications networks and services should continue to be permitted to process electronic communications metadata after having obtained the end-users' consent or in order to protect the vital interests of a natural person.

The ability to facilitate end-user consent through software settings remains in place as does the option to rely on consent, which would only now be useful in the context of profiling and determining the characteristics of a user now that legitimate interests have been introduced.

One of the other sections that remains in the latest draft is the obligation for electronic communications networks or service providers to, where necessary, implement appropriate security measures such as encryption and pseudonymisation to ensure the privacy of the end-user.

Next steps

It is notable that the Presidency text is moving further away from the European Parliament's position, which will make negotiations between the two legislative bodies more difficult if a Council agreement on this text is reached in the near future. We believe the work on this proposal may still have a long way to go. The amended proposal can be viewed here.

Other EU News

Date	Description
19 December 2019	**EDPS publishes Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data** The European Data Protection Supervisor adopted Guidelines on assessing proportionality of measures that limit the fundamental rights to privacy and data protection on 19 December 2019. The Guidelines complement the EDPS Toolkit. The fundamental rights under the Charter of Fundamental Rights of the European Union include rights to privacy and the protection of personal data. These fundamental rights must be respected by EU institutions and bodies including when they design and implement new policies or adopt any new legislative measure. The Guidelines are intended to provide EU policymakers and legislators with a common approach to the assessment of necessity and proportionality of legislative measures with respect to the right to privacy and to the protection of personal data. The Guidelines are based on the case-law of the CJEU and the European Court of Human Rights and Opinions of the EDPS, Article 29 Working Party and the EDPB. Any limitation to the exercise of the fundamental rights must, amongst other things, be necessary (which is the focus of the EDPS Toolkit referenced above) and proportionate (the focus of these Guidelines). The overall assessment proportionality is summarized as follows: 1. Assess the importance of the objective and whether the measure meets the objective; 2. Assess the scope, the extent and the intensity of the interference in terms of effective impact of the measure on the fundamental rights to privacy and data protection; 3. Proceed to the 'fair balance' evaluation of the measure; and 4. If the measure is not proportionate, then either the measure should not be proposed, or it should be modified (including by introducing safeguards) so as to comply with these requirements. The Guidelines provide a detailed methodology for each of these steps, including examples.
14 January 2020	**AI regulation – robustness and explainability** For a few years, a focus of the European Union has been AI. In the hope of becoming a global hub for AI research and applications, it has increased its investment into this area and set out a policy for AI development. At the same time, it is striving to provide a framework to

Date	Description
	regulate AI, to promote the EU as a thought leader in the ethical, societal and security implications of AI. In January this year, the Joint Research Centre (JRC, the European Commission's science advisory organisation) published a report on the "*Robustness and Explainability of Artificial Intelligence*". The report identifies four proposals to increase the transparency and reliability of AI and to ensure that personal data used in modelling is protected. The JRC proposed that the European Commission should develop: - a method for assessing the societal impacts of AI applications, akin to Data Protection Impact Assessments required under the GDPR - a standard framework for assessing the robustness and safety of AI models, to ensure that they are suitable for use, have been trained on representative data and are secured from malicious attacks and promote: - increased industry awareness on technical vulnerabilities of AI and how to solve them - an "explainability-by-design" approach for AI systems (analogous to the principle of data protection by design in the GDPR) The proposals rest heavily on the GDPR framework, suggesting similar principle-based regulation. The JRC's report was followed in February by a white paper from the Commission outlining policy options for how to regulate AI in the EU. The two recent publications further demonstrate the EU's commitment to regulation and development of AI. For more information on the Commission's white paper, please see here.
21 February 2020	**NOYB launches GDPRHub** Max Schrem's crowd-funded NOYB has launched a public wiki – GDPRHub – which is divided into a section on GDPR enforcement action, and a section on GDPR commentary. The former consists of 100+ decisions by national supervisory authorities and Member State courts regarding GDPR enforcement (the goal being to increase this to 500+ by the end of 2020). The latter consists of, "commentary on the first 21 GDPR Articles, profiles on 32 DPAs and profiles on 32 GDPR jurisdictions". NOYB claims that, "Every day we monitor more than 50 webpages in each Member State" in order to deliver this content. As is the nature with a public wiki, access is entirely public and anyone can contribute to, and edit, content

Date	Description
January 2020	In January, the European Data Protection Supervisor (EDPS) issued a "Preliminary Opinion" discussing scientific research under the GDPR, as well as broader issues around society's interest in researchers being granted access to data held by large companies and public bodies. Regarding the GDPR, the Opinion takes a close look at several important concepts, but ultimately reaches relatively narrow, restrictive positions on most. For instance, despite GDPR Recital 159 suggesting a broad interpretation of what counts as 'scientific research' (including technological development and demonstration), the Opinion takes a narrower, requirements-laden view, causing consternation among commercial organisations with keen R&D interests. It also proposed strict positions on the notion of 'broad consent' for research, and in regard to data being usable because it has been "manifestly made public by the data subject". Finally, the Opinion took the unorthodox position that a GDPR Article 6(4) "compatibility" assessment should be conducted before engaging in research "secondary uses" of data, even though GDPR Article 5(1)(b) would seem to set aside such a requirement (provided appropriate safeguards are in place). The Opinion also discusses GDPR legal bases, reiterating the now increasingly commonplace view that consent may not always be an appropriate GDPR legal basis for studies (particularly clinical studies into new treatments), even when an 'ethical' consent is obtained to the individual's participation in the study. For more see the Opinion.

<< Back to table of contents

UK Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
15/01/2020	Individual	Prosecution	Mr Kirk was a social care worker who has been prosecuted for passing personal data to a third party provider in breach of s.55 of the DPA 1998. Mr Kirk was fined and ordered to pay costs, totally nearly £800. Mr Kirk unlawfully disclosed referrals for residential and foster placements of vulnerable young people (16 to 18 year olds) to a third party provider. These disclosures included sensitive personal data, including potential identifier information and vulnerability risks.
02/03/2020	CRDNN Limited	Monetary penalty & enforcement notice	CRDNN Limited, a lead generator company, was fined with the maximum £500,000 fine under PECR for making more than 193 million automated nuisance calls. The automated calls gave subscribers the option to receive a further call about the product or service in question (typically regarding window and conservatory sales, boilers, debt management) which the company would then sell on as a potential lead. The company acted in collaboration with an Irish and a Polish company which were all owned by the same directors. However, no evidence of customer consent to receive the calls was found. There was also evidence that many of the recipients of the calls had also tried to opt out but that CRDNN had not facilitated it. The ICO also issued an enforcement notice to change its practices within 35 days to become compliant with the relevant rules.
04/03/2020	Cathay Pacific	Monetary penalty	Cathay Pacific Airways Limited has been fined £500,000 under the Data Protection Act 1998 for failing to protect the security of its customers' personal data. Between October 2014 and May 2018 Cathay Pacific's computer systems lacked appropriate security measures which led to customers' personal details being exposed.

<< Back to table of contents

First Tier Tribunal Cases

Date	Description
December 2019	**EA/2019/0054-0059: Leave.EU Group Limited and Eldon Insurance Services Limited v ICO** This case concerns appeals by Leave.EU (a political campaign company) and Eldon (an insurance company), both of whom were members of the same corporate group, in respect of a number of statutory notices: namely PECR fines (£60k and £45K), enforcement notices and assessments notices which were issued by the ICO following its large scale investigation into the use of data analytics for political purposes following the Cambridge Analytica scandal. It contains some interesting points regarding unsolicited direct marketing communications which may be of broader interest. In particular, these notices were issued as a result of the ICO's concern that the personal data of Eldon's insurance customers had been used in connection with political campaigning by Leave.EU and specifically she considered that Eldon had breached Regulation 22 of PECR by instigating the transmission of over 1 million unsolicited direct marketing communications, transmitted by Leave.EU, which advertised GoSkippy Insurance. The ICO had concluded that GoSkippy did not have the necessary valid consent from recipients to receive this information and issued a monetary penalty and enforcement notice against Eldon. A similar monetary penalty was also issued against Leave.EU as the transmitter of the unsolicited messages. Additional notices were also served on each party as well. In this case, the Appellants had tried to argue that the ICO's case against them had been based on errors of law and/or the inappropriate exercise of discretion (i.e. procedural unfairness similar to the arguments that Facebook had raised during its appeal against ithe ICO's £500,000 fine following the Cambridge Analytica investigation) but here these arguments were unsuccessful and all of the appeals were dismissed with the Tribunal concluding with the following points: • The Tribunal was not persuaded that the "Appellants' criticisms of the *twists and turns* of the ICO investigations are sufficient to establish a case of apparent bias". It agreed that there were some difficulties in the ICO's internal procedures and that the decision making paper trial leading to the Assessment Notices is lacking but that they did not find these inadequacies "*so flagrant, the consequences so severe, that the most perfect of appeals or re-hearings will not be sufficient to produce a just result*" and concluded that any procedural irregularities could be cured in the context of this full merits appeal. The Tribunal was satisfied that the ICO had exercised its discretion appropriately. • The Tribunal was satisfied that the content of the newsletter which constituted direct marketing by including the GoSkippy banner but also by associating Skippy the kangaroo with Mr Bank's (the majority shareholder of the group's parent company and sole subscriber of Leave.EU) business interest in GoSkippy insurance and his political views. There would be no other reason to include a kangaroo in a political newsletter other than to reinforce the association with Eldon's product. • The emails were also considered "unsolicited" on the basis that they contained information which could not have been in the contemplation of subscribers who had signed up to receive a political newsletter. The Tribunal also found that whilst Leave.EU had transmitted the communication, Eldon had instigated the transmission (in particular by controlling the timing, content, naming, extent and cessation of the Brexit discount message). Eldon had gone beyond mere facilitation and their actions represented a "positive form of encouragement" to transmit the relevant material. • The Tribunal agreed that there had not been a deliberate breach of PECR but that both companies knew or ought to have known that there was a risk that a contravention would occur but failed to take reasonable steps to prevent the breach. It also did not accept the argument that a person who sends out mass communications in breach of PECR is entitled to argue that the intrusion of privacy is mitigated by the number of people who did not open them or who deleted them without reading them.