Bird & Bird

UK & EU Data Protection Bulletin: April - May 2019

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
15 April	**The ICO has released its new code on age-appropriate design.** It imposes strict rules on information society service providers whose services are likely to be accessed by children. As drafted, compliance with the code may require substantial design and operational changes and organisations which are likely to be affected by its provisions should review carefully. This code is open for public consultation until 31 May 2019. For more please see our Bird & Bird update here.
29 April	**ICO call for views on a data protection and journalism code of practice.** The ICO issued a consultation on the upcoming data protection and journalism code of practice. This consultation, which ends on 27 May, is meant to be the first stage of the consultation process. Contributions will be used to draft and develop the code which will also be based on the detailed guidance already issued by the ICO on this topic. To help with the consultation process, the ICO made available a survey (available here) that can be completed by organisations wishing to express their view on this topic.

Date	Description
10 April	**Robin Rudd V (1) John Bridle (2) J&S Bridle Ltd [2019] Ewhc 893** This case relates to the Court exercising its discretion in connection with a subject access request. **Facts** In this decision, Mr Rudd, who is a doctor who specialises in the science of exposure to asbestos and who often acted as an expert witness for claimants in asbestos actions, brought a claim under S7 of the old Data Protection Act 1998 and sought an order requiring the defendants to comply with a subject access request. The defendant, Mr Bridle had been involved with the manufacture and use of asbestos cement products and was an active campaigner on issues relating to diseases caused by exposure to asbestos and J & S Bridle Ltd was his asbestos consultancy business run by Mr Bridle and his son. The complaint relates to a profound dispute between the parties and in particular, Mr Rudd claimed that Mr Bridle (along with other unknown individuals) was engaged in attempts, funded by the asbestos industry, to discredit him as an expert witness and/or to intimidate him from continuing to act for claimants in asbestos related cases. As a result of these actions, Mr Rudd sent a subject access request to Mr Bridle (and subsequently to J & S Bridle Ltd) seeking further information about the identities of the third parties who had been collaborating with him. Mr Bridle initially resisted but eventually after a delay, some third party comments were provided although the identities of these individuals were not revealed. Mr Bridle also claimed that a number of documents fell within the legal professional privilege, regulatory activity and/or journalistic exemptions. Mr Rudd felt that the responses were inadequate and he sought orders from the court to compel the defendants to provide further information. **Decision** The court exercised its discretion to order a further SAR response as it found the original responses to be inadequate. The case contains some interesting discussions as why it felt that tests for the exemptions had not been properly met as well offering guidance as to what information the data subject is entitled to regarding what the data controller knows about the source of the personal data. In doing so, the court gave guidance on the correct approach to assessing whether information contained in a document was a claimant's personal data and how to balance a claimant's right of access to his personal data against the rights of unnamed third parties. The court concluded that in this case, the data could be understood without revealing the identity of the source so that this was not the individual's personal data but that nevertheless, there is still a specific provision that requires the provision of information about sources, to the extent the data controller has such information, and which must be complied with, whether or not that information counts as personal data. The court ordered that the response to the SAR should include, amongst other things: (i) descriptions of the recipients, actual or intended of the personal data (ii) the identifying details of any person, firm or company other than the recipient of the personal data which had been redacted in the previous responses; and (iiii) any information available to the data controller as to the sources of the information set out in the provided information. Mr Justice Warby also concluded that Mr Bridle rather than his company was the appropriate data controller in this case.

11 November 2018	**Campbell V Secretary Of State For Northern Ireland (2018) [2018] Ukut 372 (Aac)** The Upper Tribunal considered whether a data subject's right of access to their personal data and to bring an appeal against the Secretary of State's national security certificate under s.28(4) Data Protection Act 1998 (DPA 1998) survive the data subject's death. Mr Campbell had made a subject access request to the Secretary of State under the Data Protection Act 1998. The Secretary of State applied section 28(1) DPA 1998, which contained an exemption that can be applied where necessary for the purpose of safeguarding national security, and issued a certificate under section 28(2) Data Protection Act 1998. Mr Campbell, as a person directly affected by the issuing of the certificate, exercised his right to appeal the certificate under Section 28(4) DPA 1998. Mr Campbell died shortly after lodging the appeal. Mr Campbell's widow tried to maintain the appeal. However, the Secretary of State objected to this. The Upper Tribunal concluded that Mr Campbell's right of access was a purely personal right which did not survive his death as a cause of action. The Upper Tribunal stated that "*the section 28(4) procedure is no more than a statutory appeal route, a procedural mechanism, for challenging the issue of a national security certificate in the substantive section 7 subject access request proceedings*" and that "*there is no freestanding right to bring a section 28(4) appeal*". It also held that the request itself cannot be seen as giving rise to a "cause of action" that would survive for the benefit of the deceased's estate under section 14(1) of the Law Reform (Miscellaneous Provisions) Act (Northern Ireland) 1937.

3 April	**Ticketmaster Data Breach Action** A £5 million data breach action was launched on 3 April against Ticketmaster following the company's security breach last June. The claim was issued at the High Court in Liverpool, on behalf of more than 650 claimants. It has been reported that more than two thirds of the claimants have suffered multiple fraudulent transactions while more than one third have suffered significant stress and heightened anxiety as a result of the breach. The law firm representing the claimants support that the claim was issued following "unsuccessful negotiations" to agree an out of court settlement with Ticketmaster, which maintains it is not liable for the breach and the subsequent damages suffered by those affected. In June 2018, Ticketmaster reported a security breach which is believed to have affected up to 40,000 UK customers and which appears to have been caused by malicious software on a product hosted by a third-party supplier. The breach resulted in the compromise of information including payment details and the affected customers have been offered a free 12-month identity monitoring service. The breach is believed to have occurred between February and June 2018 and the ICO had stated that the time when the incident occurred and was discovered would inform whether it should be dealt with under the 1998 or 2018 Data Protection Acts.
8 April	**DCMS releases new Code of Practice for Social Media Platforms** The Department for Culture, Media and Sport (DCMS) released a code of practice on 8 April 2019 with the aim to reduce bullying, insulting, intimidating and humiliating behaviours on social media platforms. For more information see our Bird & Bird update on MediaWrites here

Europe

EDPB

Date	Description
9 & 10 April	**Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects** On 9th and 10th April 2019, the European Data Protection Board (EDPB) held their 9th plenary session; during which they adopted the Guidelines on the Processing of Personal Data in the Context of Online Services (Guidelines) (for consultation). Article 6 (1) (a) to (f) GDPR contains the lawful bases on which controllers must rely to justify the processing of personal data. The lawful basis contained in (b) is the 'contractual necessity' lawful basis i.e. "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*". The Guidelines examine this ground in a wider context but also comment specifically on how it should be applied in the context of 'information society services', which are defined as *"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."* Note that, this does include services that are not paid for directly by the individuals who receive them, such as online services funded through advertising. By way of explanation of the scope of this lawful basis, the EDPB explains in the Guidelines that, "*if the specific processing is part and parcel of delivery of the request service, it is in the interest of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed*". In establishing whether it can rely on this lawful basis, the EDPB provides the following insight: **Is Processing Necessary?** "*Assessing what is 'necessary' involves a combined, fact-based assessment of the processing 'for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal'. If there are realistic, less intrusive alternatives, the processing is not necessary*". **Is Processing Necessary for Performance of a Contract with the Data Subject**? "*The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur*". The Guidelines confirm that merely referencing or mentioning the data processing in a contract is not enough to establish that the processing is necessary to perform the contract. In order to carry out the assessment of whether Article 6(1)(b) is applicable, it is suggested that the following questions can be of assistance: 1. What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?

2. What is the exact rationale of the contract (i.e. its substance and fundamental object)?

3. What are the essential elements of the contract?

4. What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

The example which the EDPB provides demonstrates how strictly this ground will be interpreted: an online retailer collects a customer's home address and credit card details when that customers buys a product for home delivery; the customer subsequently opts for collection point delivery; as such, the processing of his home address cannot be justified on the basis of the Article 6 (1) (b) lawful ground.

The EDPB provides useful insight on the implications on the Article 6 (1) (b) lawful ground of the termination of a contract; "*where processing of personal data is based on Article 6 (1) (b) and the contract is terminated in full, then as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing*". The EDPB recognises that retention of that personal data beyond contractual termination may be necessary for e.g. compliance with a legal obligation, however, if this is the case, the controller must have identified this on execution of the said contract and have informed the data subject of the same.

Is Processing Necessary for Taking Steps Prior to Entering into a Contract? The EDPB states definitively that unsolicited marketing would not fall within the scope of this aspect of the lawful basis.

The EDPB provides the following examples of what may, and what will not fall, within the scope of this lawful ground:

1. Processing for the purposes of 'improving the service' (e.g. the "c*ollection of organisational metrics relating to a service, or details of user engagement*") will not generally fall within scope;

2. Processing for fraud prevention (e.g. involving "*monitoring and profiling customers*") will not generally fall within scope;

3. Processing for online behavioural advertising will not generally fall within scope; and

4. Processing for personalisation of content "*may (but does not always) constitute an essential or expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases*". Whether this is the case will depend on things like the nature of the service, the expectations of the average data subject and whether personalisation is necessary for delivery of the service. By way of example, a news aggregation service (providing users with tailored content) may fall within scope; but hotel comparison website will likely not.

Date	Description
8 April	**European Commission publishes Ethics Guidelines for Artificial Intelligence** The Ethics Guidelines for trustworthy AI, drafted by an independent group of 52 experts chaired by Pekka Ala-Pietila of media company Sonoma were published on April 8. The guidelines feature a checklist for companies and developers to test if their AI technology is trustworthy. Commissioner for Digital Economy and Society, Mariya Gabriel, at the press conference announcing the publication affirmed that the "goal of the EU AI strategy is to provide AI based technologies that are both efficient and (Europe's added value) people focused. Ethics and economic development of AI are not mutually exclusive, rather the contrary". The guidelines, therefore, are focused on trust, considered to be a key element for acceptance and promotion of AI technologies. To this end, the guidelines propose seven conditions: 1. Human control and autonomy: citizens need to be informed when they are in contact with an algorithm and not a human being. 2. Privacy and data governance: any decision made by an algorithm should be verifiable and explained. 3. Diversity: make sure that no unjustified discrimination is in place. 4. Technological robustness, resistance and safety: AI applications have to be robust, reliable and safe. 5. Transparency: limits and capabilities have to be communicated clearly. 6. Societal and environmental welfare: potential negative impact of an algorithm. 7. Responsibility: if something goes wrong we need an appeal mechanism. Next steps: In summer 2019, the Commission will launch a pilot phase involving a range of stakeholders including industry, research institutes and public authorities to test the detailed assessment list drafted by the High Level Group. Stakeholders can sign up to the European AI Alliance and receive a notification when the pilot starts (Bird & Bird has already signed up). Based on feedback received from this pilot, a new version of the checklist will be published early 2020. The Commission will also evaluate the outcome and propose any new steps.

	In Autumn 2019, the Commission also plans to launch a set of networks of AI research excellence centres and to start discussions to develop a model for data sharing and making use of common data spaces. Link to European Commission Report webpage here.
27 March	**EU Cyber Security Act: What do you need to know?** On 29 May 2018, the Council of the European Union issued its proposal for the regulation of the European Union Agency for Network and Information Security ("ENISA") and information and communication technology cybersecurity certification (the "EU Cybersecurity Act"). The proposal had two areas of focus: the first being to strengthen the powers of ENISA by making it a permanent agency of the EU; the second was to establish a European cybersecurity certification framework to ensure the application of a common cybersecurity certification for information and communications technology ("ICT") goods. The proposal was adopted on 27 March 2019 and enters into force 20 days after its publication. For more, please see our Bird & Bird update from Simon Shooter and Stephanie Lopes **here**.

GDPR Enforcement

Date	Description
18 March	**The Danish Data Protection Agency recommends fining a taxi company 1.2 million Danish kroner (EUR 160,000)** For the first time since the GDPR came into effect the Danish Data Protection Agency ("DPA") has reported a taxi company to the police and recommended to impose on the company a fine of 1.2 million kroner. The taxi company was found to have breached the principles of storage limitation and data minimization as the company had kept customers' personal data for longer than necessary. Unlike many other EU countries, the Danish legal system does not provide for administrative fines as prescribed in Article 83 of the GDPR. Therefore, the sanctioning process under Article 83 is instead initiated by the Danish DPA filing a police report. Hereafter the Danish courts may impose a fine taking into account the Danish DPA's recommended level of fine. **The taxi company failed to comply with the 'storage limitation' principle** The recommendation followed a routine inspection in the Autumn of 2018 with focus on whether the taxi company had established procedures for deleting data and whether the company had observed its own procedures. According to the taxi company, all personal data provided by customers ordering a taxi (which includes name, telephone number, date, start and end time and the distance of the taxi ride, payment, GPS coordinates of where the ride started and ended, etc.) are anonymized after 2

years. After completing the anonymization, the data on the rides are kept for up to 5 years after the end of the ride for business development purposes.

However, during the inspection of the company it was revealed that the taxi company did not erase the customers' phone numbers in one of its systems. Therefore, despite having deleted the customers' names, the company was still able to identify the customers and the related data through their phone number for a period of 5 years after the taxi ride. During the inspection the DPA identified 8,873,333 rides having been retained for more than 2 years and which by virtue of the phone number were considered personal identifiable data.

The taxi company argued that the phone number was the key to their database and that it was necessary to retain the phone number for business development purposes. They admitted that the phone number could have been replaced by another ID number but that this was not possible retroactively.

The DPA found that the taxi company had violated GDPR art. 5(1) (e) (storage limitation) as the company's procedures for anonymization were insufficient. The DPA noted that the company itself had evaluated that personal identifiable customer data was not necessary to retain for more than 2 years. Further, the DPA found that the taxi company had violated GDPR art. 5(1) (c) (data minimization) as the retention of phone numbers was not necessary for the purposes of business development. The DPA also found other violations of the GDPR that were criticized but did not contribute to the decision to recommend a fine.

Comment

This is the first time the Danish DPA has recommended fining a company for not complying with the GDPR. The case is of particular interest, as it indicates at which level the Danish DPA believes the fines should be under the GDPR. In Denmark, the level of fines has generally been non-existent before the GDPR. The highest fine imposed to date is 25,000 Danish kroner (3,350 EUR). The decision does not in itself elaborate on the calculation of the recommended fine except that the DPA refers to the amount of personal identifiable information which has been retained for longer than necessary to serve the purpose.

The DPA's decision does not question the retention period of 2 years established by the taxi company. It is surprising that the taxi company did not at least try argue that retention of customer data was necessary for the defence of potential claims from customers (statute of limitation under Danish law for contractual claims is 3 years and under certain conditions up to 10 years) or to comply with requirements for retention of bookkeeping material (statutory retention of 5 years from the end of the accounting year). However, these arguments may not have changed the outcome as the taxi company - as emphasized by the DPA - in its retention policy had stated that it was unnecessary to retain customer data for more than 2 years.

8 April

Danish Data Protection Agency imposes Danish telecom provider a temporary ban on recording telephone calls without consent

On 8 April 2019, the Danish Data Protection Agency 'Datatilsynet' imposed TDC A/S a temporary ban on recording telephone calls and expressed serious criticism of TDC's non-compliance with the data protection rules. However, no fine has been recommended for the violation.

The decision followed a complaint lodged by a customer who had not consented to TDC's recording of his telephone conversation with customer service. With the decision, the DPA has enforced its long-standing practice that it requires consent from the affected persons to record telephone calls. According to the DPA, there were no circumstances in the specific case that could justify a deviation from this rule.

The decision, which is only available in Danish, can be read in full here.

What rules apply to the recording of telephone calls in Denmark?

- An organisation's recording of telephone calls must comply with the general data protection rules (principles, legal basis, etc.), as it is not subject to specific rules in the GDPR or the Danish Data Protection Act.
- In most circumstances it requires prior consent to record telephone conversations.
- However, in limited cases it is legal to record calls without consent for documentation purposes, e.g. based on an organisation's legitimate interest in documenting an oral agreement, but it will always depend on the specific circumstances of each case where it, among other things, is taken into account whether an agreement or a series of events can be documented by using other means.
- Consent must be given voluntarily by an active and unambiguous act and an organisation must provide specific information on what the data subject is consenting to. This can be achieved by having the person press a button. It is not sufficient if the person has to actively opt-out of having the phone conversation recorded.
- Further, organisations are obliged to - regardless of whether the recording is based on consent or a legitimate interest - provide information to the person being recorded. The organisation must therefore on its own initiative inform that the conversation is being recorded and what the purpose of the recording is. This can be achieved by playing a pre-recorded message where after the data subject can press 1 if he/she wishes to provide consent.
- The recording must be processed securely and deleted when the company no longer has a need for it.
- Data subjects are provided with certain rights under the GDPR. This includes the right to access the recording and the right to have the recording deleted.

21 March **Case C-673/17 Planet 49: Advocate General Opinion**

In March 2019, the Advocate General (AG) of the Court of Justice of the European Union (CJEU) gave an important opinion in relation to cookies and consent (ECJ C-673/17)

The AG puts a particular emphasis on the following points:

- He reaffirms that a clear, affirmative, action is necessary to express consent. Organizations can't use pre-ticked boxes to get consent for cookies (whether pre-or post-GDPR), this is also valid for toggle switch buttons in Consent Management Platforms (which we still see fairly often). The opinion also appears to reject any notion of "implied" consent by continued browsing which is still common practice in some jurisdictions. This may impact how companies place cookies and similar technologies (e.g. SDKs) both in a web and mobile environment.
- The information given to users must be sufficiently detailed so as to enable the user to comprehend how the cookies function. In the AG's view this includes information on which third parties are placing and/or accessing the cookies (i.e. partners) and on the duration of these cookies. In practice, this means that companies will have to insert a link to a page listing their partners in their cookie consent wording (or a similar way of making this information available).

It should be noted that the CJEU is yet to issue its decision. If followed, this Opinion can have a significant impact on industry and will certainly have important consequences on conversion rates for companies still relying on implied consent. Also note that during the second half of 2018, the CNIL (French Supervisory Authority) issued 4 decisions on Adtech companies emphasizing similar points, making the redrafting of cookie consent wording necessary when targeting the French market.

The opinion of the Advocate General is available here.

Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
04/04/2019	London Borough of Newham	Monetary Penalties	The Information Commissioner's Office (ICO) has fined the London Borough of Newham £145,000 for disclosing the personal information of more than 200 people who featured on a police intelligence database known as the Gangs Matrix. This matrix contained the personal date of 203 data subjects including approximately 80 of those data subjects who had a matrix score of zero.
05/04/2019	Shamim Sadiq	Prosecution	A former GP practice manager has been fined for sending personal data to her own email account without authorisation, following an investigation by the Information Commissioner's Office. Shamim worked at Hollybrook Medical centre in Derby, but was suspended on 3 November 2017 for unrelated matters. Shamim admitted unlawfully accessing personal data. She was fined £120, plus £364 in costs and a victim surcharge of £30. (Due to the timing of the incident, she was prosecuted under s.55 of the DPA 1998 rather than the new DPA 2018).
10/04/2019	True Visions Productions	Monetary Penalties	A television production company has been fined £120,000 by the Information Commissioners Office for unlawfully filming patients at a maternity clinic. TVP set up CCTV style cameras and microphones in examination rooms at Addenbrooke's Hospital in Cambridge for a Channel 4 documentary on stillbirths. Although TVP had the hospital trust's permission to be on site. TVP did not provide patients with adequate information about the filming or get adequate permission from those affected by filming in advance.

			Despite having posted limited notices advising of the filming near to cameras and on the waiting room tables. However, these letters did not provide adequate explanations to patients and on one occasion provided incorrect information, stating that mums and visitors would not be filmed without permission. The ICO found that a patient attending the clinic would not have reasonably expected there to be cameras in examination rooms and would expect to be made aware of any filming.
11/04/2019	Bounty (UK) Ltd	Monetary Penalties	Bounty UK, a pregnancy and parenting support club which provides information and markets offers and services to parents at different stages of a family's life, has been fined £400,000 for sharing personal data unlawfully. Bounty came to the attention of the Commissioner during the course of a general investigation into non-compliant practices of the data brokerage industry, in which Bounty were identified as a significant supplier of personal data to third parties for direct marketing. Bounty contravened DPP1 by sharing the personal data of over 14 million individuals to a number or organisations including credit reference and marketing agencies without informing those individuals that it might do so.
16/04/2019	Avalon Direct Ltd	Enforcement Notice	Avalon Direct Ltd, a company selling funeral plans, made almost 52,000 calls to people who were registered with the Telephone Preference Service (TPS) between 1 March and 20 November 2017. The unsolicited direct marketing calls were made to subscribers who had registered with the TPS at least 28 days prior to receiving the calls, and they had not given their prior consent to ADL to receive calls. The Commissioner requires that within 35 days of this Notice ADL shall not: 'Use [...] a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where the called line is that of: (a) a subscriber who has previously notified ADL that such calls should not made on that line: and (b) subscriber who has registered their number with the TPS and least 28 days previously and who has not notified ADL that they do not object to such calls being made.' The ICO has flagged that the funeral planning industry had been on its radar for a long while and wants people to ask their elderly relatives or neighbours if they are receiving nuisance marketing calls.

07/05/2019	Hall and Hanely Ltd	Monetary penalties	Hall and Hanely Ltd were fined £120,000 as being found responsible for the instigation of 3,560,211 direct marketing messages in relation to PPI (emails & texts) to individual subscribers without consent, in breach of Regulation 22 of PECR. H&H first came to the attention of the Commissioner following a large number of complaints being received about unsolicited direct marketing messages through the 7726 (SPAM) service along with a number of complaints being made through the ICO's own reporting tool. In total there were 1,257 complaints through the 7726 service and 96 made through the online reporting tool. The ICO found that in total 4,833,167 messages had been sent. .
10/05/2019	Her Majesty's Revenue and Customs (HMRC)	Enforcement Notice	Her Majesty's Revenue and Customs (HMRC) has been issued an Enforcement Notice for failing to get adequate consent to collect around 7 million callers' personal data since 7 January when using voice authentication (Voice ID) for customer verification. The Commissioner is satisfied that HMRC has contravened data protection principles1 by collecting, retaining and using biometric data through its Voice ID service, without having a lawful basis to do so under GDPR Articles 6 and 9. The Voice ID service authenticates customers when they call HMRC's helpline through their voice. The characteristics of a person's voice constitute biometric data. As part of the initial complaint, "Big Brother Watch" shared two transcripts detailing the experience of customers calling HMRC helplines. These show that despite explaining the benefits and how the Voice ID system worked, the recording did not give details of where customers could find further information. There was also no clear option available for callers who did not want to register.
10/05/2019	Farrow and Ball	Monetary Penalties	Last year, the ICO began taking action against organisations for non-payment of the data protection fee. Farrow and Ball had been issued a £4,000 fine for not paying their Tier 3 Data Protection fee of £2,900. Farrow and Ball had appealed against this fine for many reasons, including that the responsible person was on holiday. The first tier tribunal stated that although the non-payment of the fine was an oversight, the company should have had measures in place to prevent this from happening. The Tribunal dismissed the appeal and the penalty notice was confirmed.