Bird & Bird

UK & EU Data Protection Bulletin: July - September 2018

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
July	**ICO Annual Report 2017-18 published** The ICO said new laws and high profile investigations have helped put data protection and privacy at the centre of the UK public's consciousness like never before. Data protection and freedom of information complaints have increased and the sectors generating the most concerns were general business, health and local government. "Subject access requests" were the biggest reason for generating a request (42%). Recent enforcement activity included: • 26 penalties under PECR totalling £3.28m for breaches of electronic marketing laws relating to nuisance calls and spam text messages, along with 10 enforcement notices and the execution of three search warrants; • 11 fines totalling £1.29m for serious security failures under the Data Protection Act 1998; • A further 11 fines to charities totalling £138,000 for unlawfully processing personal data and an £80,000 fine issued to a data broking organisation; and • A total of 19 criminal prosecutions resulting in 18 convictions - a further 6 cautions were issued and 11 search warrants were executed. A summary of the report and the full report can be found here.
Summer	**Updated ICO guidance on International Data Transfers** The ICO has updated its guidance on International Transfers within its Guide to the GDPR. Much of the content is not new but interesting points to note are:

- New guidance will be forthcoming from the EDPB on international transfers and on territorial scope so the ICO Guide will be updated in line with this.
- The data transfer rules apply where the GDPR applies to the processing of personal data that you are transferring and you are sending it or making it accessible to a "receiver" to which the GDPR does not apply (potentially this means that if a 'receiver' is subject to GDPR because of GDPR's extra-territorial scope, that there is no need to put data transfer safeguards in place).
- In terms of safeguards that can be used for data transfers, the Guidance refers to the updated tables and application forms for BCR-C and BCR-P and notes that the Commission plans to update the SCCs in due course. It confirms that the existing SCCs continue to be valid (and where these are incorporated into existing contracts, will also continue to be valid once any new GDPR SCCs have been introduced). As for other possible safeguards, the ICO has not yet adopted any standard data protection clauses of its own (which can be approved by the Commission) and confirms that no approved codes of conduct or certification schemes are yet in use. The ICO also confirms it is not authorising any bespoke contracts at present, until further guidance has been produced by the EDPB.
- In terms of other exceptions (in the absence of an adequacy decision or other safeguard), the ICO makes it clear that "explicit consent" may not be a feasible solution given the high threshold for consent, reliance on contractual performance should only be done where the transfers are "occasional" and "necessary". This may impact many organisations (particularly in the travel industry) which had relied on this exception under the old rules for transfers of customer data to overseas hotels/transport companies. The ICO gives a similar example and states that if it is regularly sending customer data to a particular overseas destination, it should not rely on this exception and should consider using an appropriate safeguard such as standard contractual clauses instead.
- Finally, in respect of the exception which references legitimate interests, this is only to be relied upon in truly exceptional circumstances: There must be no adequacy decision, other safeguards or exceptions which can be used, the transfer must not be repetitive, it must relate to a limited number of individuals (no threshold but this will form part of the balancing exercise), the transfer must be necessary for the organisation's compelling legitimate interests (this requires a balancing test and the organisation's interests must outweigh the rights and freedoms of individuals), must include suitable safeguards to protect the personal data, the organisation must have informed the ICO (who will ask to see full details of the above steps) and it must have told the individual about the transfer and explained the compelling legitimate interests.

More information is available here.

11 July 2018 **ICO publishes findings, recommendations and actions following investigation into data analytics in political campaigns**

Following its high profile investigations into Cambridge Analytica and Facebook in May, the ICO has published a progress

report on its findings. The 42 page reports set out the details of the ongoing investigation into the "invisible processing" carried out as part of the EU referendum, and as part of the 2016 US presidential campaign. The report was prepared to provide an update to the DCMS select committee to inform their "Fake News" report (which was published prior to the summer recess).

The report sets out the action taken so far (including an enforcement notice to SCL Election Limited, and the ongoing criminal prosecution following the failure to comply with this notice, and the notice of intent to issue a £500,000 monetary penalty under the Data Protection Act 1998.) The ICO has in particular committed to carrying out audits of all the main political parties, credit reference agencies and Cambridge University Psychometric Centre, using their new assessment notice powers under the 2018 Act. Investigative work is expected to carry on until the end of October 2018.

The report can be found here.

14 August 2018 **ICO Blog provides advice on use of CCTV in taxis**

The ICO has written a blog post about the privacy implications around the installation of CCTV cameras in taxis by councils as *"a way to combat crime, and to protect drivers and vulnerable passengers"*. The ICO is particularly concerned with the continuous operation of such CCTV systems whilst taxi drivers' vehicles are running, meaning that footage is captured outside of the taxi drivers' working hours (e.g. capturing drivers picking up their children from school). This continuous operation is at odds with the requirement that the processing of personal data must be *"necessary for its purpose and proportionate"*; capturing the private lives of taxi drivers on CCTV could be in breach of their Article 8 Human Rights Act 1998 right. The ICO offers councils three key recommendations: (i) consider, prior to system implementation, whether a CCTV system would be *"a necessary, justified and effective solution"*; (ii) conduct a data protection impact assessment ("DPIA") – CCTV in taxis is considered by the ICO to likely be *"an intrusive surveillance system"*; and (ii) read the ICO's Code of Practice for Surveillance Cameras and Personal Information. Councils are also reminded of their statutory duty under the Protection of Freedoms Act to consider the Home Secretary's Surveillance Camera Code of Practice.

By 12 October **ICO Regulatory Sandbox**

The ICO has launched a 'call for evidence' on creating a regulatory sandbox. Such a launch constitutes the first phase of the consultation process with a formal consultation being launched later in the year. The call for evidence closes on 12 October 2018. The ICO has described this sandbox as "a safe space where organisations are supported to develop innovative products and services using personal data in innovative ways." It won't mean that such organisations are exempt from compliance with their data protection obligations but "they will have the opportunity to engage with us; drawing upon our expertise and advice on mitigating risks and data protection by design, whilst ensuring that appropriate protections and safeguards are in place." You can fill out the survey here.

Cases

Date	Description
28 June 2018	***B v General Medical Council [2018] EWCA Civ 1497***

The Data Protection Act 2018 contains 'third party information provisions', which apply where an individual makes a subject access request and where the individual's personal data includes personal data which relates to another individual. In this situation, the controller has to consider the interests of the two individuals – in particular, whether the third party has given consent for his or her personal data to be released or whether it is reasonable in all the circumstances to release the data without consent. These provisions are essentially the same as earlier provisions in the 1998 Data Protection Act. Those provisions have been considered in some detail by the Court of Appeal in this case.

Dr B is a GP who had treated P and diagnosed P with cancer of the bladder. P complained to the GMC about Dr B's treatment, claiming that Dr B's incompetence led to a delay of about one year in the diagnosis of his cancer. The GMC commissioned an independent expert to prepare a report as part of its investigations and the report concluded that Dr B's care did fall below the standard expected - but not seriously below - and that most reasonably competent GPs would not have suspected bladder cancer given the particular information available at the time. The GMC decided not to take further action against Dr B. Dr B was given a copy of the report, but it was not provided to P - who made a subject access request to obtain it. The GMC consulted Dr B, following the third party information provisions under the 1998 Act. Dr B objected to disclosure, but the GMC considered that, in all the circumstances, it would be reasonable to release the report notwithstanding. Dr B then applied to court to prevent disclosure. At first instance, the judge agreed with Dr B. The Court of Appeal (in a majority judgment) considered that the GMC's decision to release the report was reasonable and should stand.

The Court of Appeal confirmed that the third party information provisions are evenly balanced (para 70) and "*there is no sound basis for saying that one should load the exercise at the outset in favour of either the objector or the requester*". However if, having considered all the relevant factors, there were to be a "*perfect equilibrium with nothing to choose between them, in that situation.. this would be a presumption of the weak, tie-breaker type.. It is not a significant or substantive presumption to be applied at the outset*".

The Court of Appeal also considered whether the fact that information may be used in litigation against the third party was relevant and agreed that it was a relevant factor though disagreed about how much weight it should be given. The Court of Appeal also noted that its role was to determine if the controller had taken a reasonable decision.

The case is helpful in many ways - and its advice for controllers could be summarised as:

- act reasonably to balance all relevant factors;
- take account of the interests of both parties;
- if the scales are completely evenly-balanced, then withhold.

The full decision can be found here.

12 July 2018 ***Information Commissioner v Miller [2018] UKUT 229 (AAC)***

Where a freedom of information request would require a public authority to release personal data, then the authority must consider if release of the data could be made in compliance with data protection legislation. If data protection legislation would bar disclosure, then there is an exemption under FoIA.

In *Information Commissioner v Miller,* the Upper Tribunal Appeals Chamber rejected an appeal brought by the Information Commissioner in relation to an argument that data concerning five or fewer individuals should be exempt from disclosure under FoIA.

Facts:

A request was made under FoIA for the Department of Communities and Local Government (DCLG) to release data related to homelessness statistics between 2009-2012. DCLG refused to disclose the information relying on s.40(2). Their position was that the data set was sufficiently small that a motivated intruder would be able to identify the individuals concerned, making this personal data. Neither the First tier Tribunal nor the Upper Tribunal were convinced by this argument. The Upper Tribunal approved of the test applied by the First Tier Tribunal: whether the data was in a sufficiently anonymous form that it would not be possible to identify a living individual from not only the data in question, but also other information "*which is in the possession of, or likely to come into the possession of, the data controller*" i.e. what are the chances of an individual being identified? Judge Markus of the Upper Tribunal reasoned that "*the chance of a member of the public being able to identify the household and its members from the data is so remote as to be negligible*", she also held that it was "*quite fantastical to suppose that, several years later, there would be anyone sufficiently motivated to try to identify an individual to which the data related*".

This decision gives some practical guidance to authorities in considering whether to release (small) datasets. It is also worth noting that little evidence was added by the Commissioner or DCLG in support of their assertion that there was a risk of identification – and this was also relevant to the Tribunal. The full decision can be found here.

30 July 2018 ***Stunt v Associated Newspapers Ltd [2018] EWCA Civ 1780***

This case has resulted in a reference being made to the CJEU on whether the UK approach to data protection and processing for purposes of journalism mis-implements the Data Protection Directive.

James Stunt is the former son-in-law of Bernie Ecclestone. He had brought proceedings against Associated News for misuse of private information and breaches of the 1998 Data Protection Act. These were stayed and Stunt appealed against the stay, which was ordered under the Data Protection Act 1998 s.32(4). This section provides that for automatic stays in pre-publication cases unless and until the Information Commissioner determines that processing is not being carried out solely for journalistic purposes. The provisions under the 2018 Act are similar.

Stunt argued that the effect of the provisions in the 1998 Act was so draconian as to mean that the Act mis-implemented the Data Protection Directive. At first instance, Popplewell J. agreed that the provision would produce lengthy delay and his succinct summary of the difficulties is quoted by the Court of Appeal:

"The upshot is that once a data controller has made a claim that the two conditions in s.32(4) are fulfilled, the data subject cannot compel the Commissioner to embark upon a s.45 exercise, which if it takes place at all may well involve a lengthy process in which the data subject is largely a spectator, with the result that the stay is itself either permanent or of lengthy duration" ([40]).

However, Popplewell J at first instance, and the majority in the Court of Appeal, rejected the claimant's argument that this mis-implemented the Directive, noting that the this restriction on pre-publication restraint was within the margin of manoeuvre allowed to Member States, that the very availability of pre-publication restraint for data protection breaches would have a chilling effect on freedom of expression and the availability of damages later may be a sufficient protection. The Court of Appeal could not reach a unanimous decision and concluded that this would mean that a reference to the CJEU was appropriate.

The full judgment is available here.

14 August 2018 ***Xerpla Ltd v Information Commissioner [2018] UKFTT 2017_0262 (GRC)***

In *Xerpla Ltd v. Information Commissioner,* the First Tier Tribunal overturned an ICO decision from 2017 in which Xerpla, a direct marketing company, was fined £50,000 for sending 1.26 million email marketing communications without opt in consent (as required under the PEC Regulations).

Facts:

Between 6 April 2015 and 20 January 2017, Xerpla sent 1.26 million unsolicited direct marketing emails, promoting the products and services of third parties. The emails consisted of marketing material from a variety of organisations including providers of dog food, pet products, wine, motoring services, magazines, financial services, competition, insurance and boilers. They were sent to individuals who had subscribed to two websites operated by Xerpla and individuals had been told that by submitting their details they consented to receive Xerpla's email newsletters and offers from and on behalf of Xerpla's offer partners and from other similar third party online discount/deal providers. The Privacy Policy gave more detail on the types of marketing activity carried out. The ICO received 14 complaints in respect of these marketing activities. When originally investigating the matter back in 2017, the ICO felt that the consent had not been sufficiently informed and that the contravention was serious enough to justify a monetary penalty. This was also intended as a message that compliance with the PEC Regulations was important and the fine was a deterrent to other similar organisations.

Whilst this case predates the GDPR and the tougher consent requirements, there was still a requirement for the consent to be "freely given, specific, and informed" in order to be valid. However, the tribunal dismissed the ICO's arguments that insufficient consent existed here and found that that Xerpla's subscribers had *"consented to, and knew they were consenting to, the direct marketing of third party offers for all kind of products and services... That is why they subscribed..."* It was therefore considered obvious what was being consented to, given the services offered by Xerpla. The fact that Xerpla was providing the direct marketing itself (albeit in respect of third parties offers) together with the small number of complaints received was also a significant point in Xerpla's favour. As a result the tribunal overturned the monetary penalty issued by the ICO.

A full link to the case can be found here.

Other news

Date	Description
June - July 2018	**The Investigatory Powers Act 2016 moves towards fuller implementation: Update on the "state of play"** The Investigatory Powers Act 2016 (the "IP Act") is not yet fully in force and secondary legislation continues to be implemented to bring into force various aspects of it. Mandatory communications data retention is one of the most controversial aspects of the IP Act. It is under challenge in the courts and, as a result of previous legal challenges (including the Watson/Tele2 judgment), the government has had to consult on amendments to the Act. We set out below some of the most recent developments in this area over the past couple of months.

(i) Government response to consultation on the IP Act (full response here)

In June 2018, the Home Office released its response to the consultation on the Government's proposed response to the Watson/Tele2 ECJ judgment from 2016 regarding the retention of communications data provisions. While the Government received almost 800 responses to the consultation, more than 700 of them were the result of a campaign organised by the Open Rights Group. The primary change proposed by the Government, in direct response to the *Watson/Tele2* judgment, was to no longer permit an order requiring the retention of communications data for purposes falling below the threshold of "serious crimes". To counter public comments that the proposed definition of "serious crimes" was too expansive, thereby setting too low a threshold for communications data retention, the Government narrowed its definition to only crimes for which a person is capable of receiving 12 months in prison.

The Government also confirmed (and indicated it received positive feedback for) its intention to establish a new body called the Office for Communications Data Authorisations [(OCDA)] to independently assess requests for access to retained communications data (although an expedited procedure will exist for urgent requests) under the assumption that courts will not be nimble enough to take on this role.

(ii) Draft Data Retention and Acquisition Regulations 2018 published (here)

On 24 July 2018, the Government published the draft Data Retention and Acquisition Regulations 2018. These draft regulations amend parts 3 and 4 of the IP Act and follow from the Home Office response to the consultation. Now before Parliament, the draft Regulations are the Government's attempt to comply with the requirements of EU law with respect to the retention of communications data. For instance, Regulation 3 amends RIPA so that access to certain communications data may be authorised only for the purpose of prevention or detection of serious crime. Regulation 5 amends Part 3 of the IP Act to provide for independent authorisation of requests to access communications data conferring on the Investigatory Powers Commissioner a new power [(which will be exercised through OCDA)] to authorise communications data requests

(iii) The Investigatory Powers (Codes of Practice and Miscellaneous Amendments) Order 2018 (see here)

On 19 August 2018, the above Order came into force which introduces three revised codes of practice regarding the functions carried out under the IP Act's predecessor, RIPA, as well as making some amendments and updates to the public authorities authorised to use surveillance powers under RIPA. The codes of practice have essentially been updated to bring in line with the IP Act and cover current practice.

(iv) The Investigatory Powers Act 2016 (Commencement No. 7 and Transitional and Saving Provisions) Regulations 2018 published (23 July 2018) (see here)

The above Regulations published on 23 July 2018 bring into force the provisions in the IP Act connected with the "bulk acquisition" powers. These powers, outlined in Chapter 2 of Part 6 of the IP Act, permit the Secretary of State to issue warrants

requiring telecommunications operators to disclose specified communications data in bulk (i.e. metadata, such as sender, recipient, location, etc., but not content). The warrants permit not only the acquisition of communications data in the operator's possession, but also future communications data.

The Regulations have also brought into force provisions relating to the intelligence services' use and retention of "bulk personal datasets". These are databases containing the personal data of several individuals, the majority of which are unlikely to be of interest to the intelligence services. As with the bulk acquisition powers, the intelligence services must obtain a warrant to justify both the retention of bulk personal datasets and their examination.

Finally, the Regulations will bring into force as of 1 November 2018, the provisions governing the retention of communications data by telecommunications providers. In particular, these powers will permit the Secretary of State, with review by Judicial Commissioners, to require a telecommunications operator to retain certain communications data for up to 12 months, where such an order is proportionate and at least one of series of enumerated factors is present.

(v) The Investigatory Powers Act 2016 (Commencement No. 8 and Transitional and Saving Provisions) Regulations 2018 (20 August 2018) (see here)

The above Regulations published on 20 August 2018 bring into force provisions of the IP Act relating to the targeted interception of communications. Provisions regarding the interception of communications by the intelligence services and Defence Intelligence are already in force. These Regulations relate to interception by the other intercepting authorities: the National Crime Agency, the Metropolitan Police, the Police Service of Northern Ireland, Police Scotland, Her Majesty's Revenue and Customs, and a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

Please also see our case updates below for a link to the latest ECtHR decision on this issue in *Big Brother Watch and others v UK*.

August 2018 **Department for Education publishes updated GDPR toolkit for schools**

The Department for Education (DfE) has updated its GDPR guidance for schools, originally published in April 2018.

The toolkit has been revised to provide further guidance on safeguarding, retention, consent, Data Protection Officers, data breaches and the National Schools and Colleges Contract. Additionally the DfE has incorporated new resources into the toolkit, including an example of an employee-facing ICT Policy, a template agreement to vary National Schools and Colleges Contracts, and an example report produced by the ICO following an audit of a school.

The DfE emphasises that this is a living document, which will be continually reviewed and updated in light of feedback (which can be submitted via data.modernisation@education.gov.uk).

The DfE's updated toolkit is available here.

Department of Health and Social Care publishes the Initial code of conduct for data-driven health and care technology

The Department of Health and Social Care has published an initial (voluntary) code of conduct for data-driven health and care technology. This builds on the Department for Digital, Culture, Media and Sport's Data Ethics Framework. The code aims to clarify expectations on the health service and technology suppliers, and how accountability and liability is managed.

The code sets out 10 key principles:

1. Define the user
2. Define the value proposition
3. Be fair, transparent and accountable about what data you are using
4. Use data that is proportionate to the identified user need (data minimisation)
5. Make use of open standards
6. Be transparent to the limitations of the data used and algorithms deployed
7. Make security integral to the design
8. Define the commercial strategy
9. Show evidence of effectiveness for the intended use
10. Show what type of algorithm you are building, the evidence base for choosing that algorithm, how you plan to monitor its performance on an ongoing basis and how you are validating performance of the algorithm.

Specific details on how these principles should be met is set out in the code, which includes in many places suggested methods of ensuring GDPR compliance of such technologies (such as the need to carry out a DPIA). Feedback is being sought on the code via questionnaire. A copy of the code can be found here.

Europe

News

Date	Description
5 July 2018	**European Data Protection Board Clarifies Application of GDPR to Payment Service Providers:** On 5 July 2018, the European Data Protection Board (EDPB) provided a response to a letter sent by Sophie in 't Veld MEP about the revised Payment Services Directive (PSD2) and data protection. She said that there is a "*lack of clarity about the precise data protection provisions governing transactions carried out by account information services and payment initiation services*". On her question regarding 'silent party data' (e.g. where data subject A uses the services of a payment initiation service to transfer money to data subject B without there being a contractual relationship between the payment initiation service and data subject B), the EDPB said GDPR may allow for the processing of data subject B's data based on the legitimate interests of the controller or a third party to perform the contract with the data subject A. The EDPB emphasises that the processing must be necessary, proportionate, limited and determined by the reasonable expectations of the data subject and otherwise be in line with GDPR principles including purpose limitation, data minimisation and transparency. Regarding the processing of data subject A's data, the EDPB is of the view that the "explicit consent" referred to in PSD2 is a contractual consent which is not equivalent to consent under the GDPR. They note that recital 87 of PSD2 says that "[t]his Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider"(PSP). The standard of this contractual consent is set out under Article 94(2) PSD2, which mandates that PSPs only access, process and retain personal data necessary for the provision of their payment service with the explicit consent of the user. As such PSPs are required to: fully explain the purposes for which users' personal data will be processed; ensure that such clauses are clearly distinguishable from the other matters in the contract; and, seek explicit agreement to such clauses. Again, this provision relates to the standard of contractual consent required by PSD2 and is not the same consent under the GDPR (which must be freely given). In terms of GDPR, the EDPB considers that contractual necessity may be the relevant legal basis processing data subject A's

data under GDPR.

The EDPB noted that there may be relevant grounds for a "fruitful interaction" between data protection and financial supervisory authorities.

The letter is available here.

For further analysis see here.

10 July 2018

Examination of the Presidency text of the proposal published in the Council Register

The European Parliament's LIBE Committee adopted its report on the e-Privacy Regulation on 19 October 2017.

However, the draft has been delayed as it works its way through the legislative process.

Before the tripartite trilogue meetings between the Council, Commission and Parliament can commence, the Council must first adopt its general position.

The Austrian Presidency of the Council stated last month that it is likely that only a progress report is achievable before the end of 2018 (as opposed to adoption of the Council's general position). Accordingly, the trilogue meetings may only commence after the European Parliament elections in May 2019.

The Council's amendments to the ePrivacy proposal in the text of 10 July 2018 (Council document 10975/18) seek to dilute certain key provisions of the ePrivacy Proposal:

(a) The Council has written down the restrictions on the processing of communications metadata in a number of ways, including for example, allowing further processing of metadata for compatible purposes without the need for end-user's consent (a ground that appears similar to legitimate interest under GDPR). The Council see the amendments being necessary to future proof the regulation to ensure it is flexible enough to facilitate innovation and ensure European companies remain competitive.

(b) The LIBE Committee had introduced a ban on tracking walls i.e. making websites conditional on an end-user accepting cookies. The Council has amended Recital 20 to make tracking walls permissible for websites without direct monetary payment. It is difficult to easily reconcile this with Article 7 GDPR (Conditions for Consent) but the Council has invited views from delegates on the issue.

(c) The Council has deleted the requirements for privacy by design and by default for the use of cookies and similar technologies. This was the provision that proposed that at the time of software installation, the software provider is to

inform the user about the privacy setting options and, to continue with installation, require the end user to consent to a setting. The Council justify the deletion on the basis the rules are too burdensome for developers and are likely to lead to consent fatigue for individuals.

The Council's amendments have attracted considerable criticism from civil society organisations and privacy advocates. I t seems unlikely that the e-Privacy Regulation will now come into force before 2020.

19 July 2018 **EDPB: State of play of the One-Stop Shop**

During its second plenary meeting on 4th and 5th July, the European Data Protection Board ("EDPB") discussed the One-Stop Shop mechanism and the platform used to support it, namely the Internal Market Information System ("IMI").

Members of the EDPB reported a substantial but "manageable" increase in complaints received, with around 100 cross-border cases in IMI currently under investigation.

Claiming that the first results of the new procedures to deal with cross-border cases should not be expected until the last quarter of 2018, EDPB Chair Andrea Jelinek said that the "GDPR does not offer a quick fix in case of a complaint but [the EDPB is] confident that procedures detailing the way in with the authorities work together are robust and efficient."

More information is available here.

5 September **The European Commission launches the adoption of its adequacy decision on Japan**

The EU and Japan successfully concluded their talks on reciprocal adequacy on 17 July 2018. They agreed to recognise each other's data protection systems as adequate, which will allow personal data to be transferred safely between the EU and Japan.

Adequacy does not require the third country's data protection system to be identical to the EU's one but it must be essentially equivalent to EU standards. It involves a comprehensive assessment of the country's data protection framework, both of the protections applicable to personal data and of the relevant oversight and redress mechanisms available. The Article 29 Working Party (now the European Data Protection Board) set out the elements that must be considered when conducting the adequacy assessment in their Guidelines adopted in February 2018.

In order to meet these criteria, Japan has committed to implementing a number of additional safeguards to protect personal data transferred to Japan: for instance, the Japanese definition of sensitive data will be expanded, the exercise of individual rights will be facilitated, and the further transfer of Europeans' data from Japan to another third country will be subject to a higher level of protection. Japan also agreed to establish a system of handling and resolution of complaints, under the

supervision of the Japanese data protection authority (the Personal Information Protection Commission), to ensure that potential complaints from Europeans as regards access to their data by Japanese law enforcement and national security authorities will be effectively investigated and resolved.

The Commission has now launched its procedure for formally adopting this decision which involves, seeking an opinion from the European Data Protection Board, consultation of a committee composed of Member State representatives, update of the EU Parliament committees and adoption of the decision by the College of Commissioners. A commitment has been made by both parties to ensure the relevant internal procedures required to adopt an adequacy decision will be completed by the end of autumn 2018.

Adequacy talks are also ongoing with South Korea.

For more information and a link to the draft adequacy decision: http://europa.eu/rapid/press-release_IP-18-5433_en.htm

Cases

Date	Description
CJEU Cases	
10 July 2018	**Jehovah's Witnesses Community case** This case (Tietosuojavaltuutettu v Jehovah's Witnesses, C-25/17) was a referral from Finland concerning whether or not Jehovah's Witnesses were data controllers as a community or as individual members, when processing personal data in the course of door to door preaching. The CJEU confirmed that the individual members were data controllers under the Data Protection Directive. It also considered the role of the Jehovah's Witness Community and whether it was also a data controller. It found that a person "*who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing*" can be regarded as controller, whether or not it had written instructions to that effect. The fact that the community centrally organised, coordinated and encouraged the preaching activity in which personal data was processed was relevant and made them also responsible for the processing. This decision comes just a few weeks after the Facebook case (C-210/16) and whilst the CJEU did not explicitly state that the community was a joint data controller, it reiterated a broad definition of that concept although that did not mean that every data controller had the same responsibility or had to have access to the data to be a controller.

ECtHR Cases

28 June 2018

***ML & WW v Germany* (App. No. 60798/10 and 65599/10)**

The right to be forgotten (Art 8 ECHR) vs free expression rights (Art 10 ECHR)

This case concerned the refusal by the German courts to issue an injunction prohibiting a media outlet from continuing to allow Internet users access to documentation concerning the applicants' conviction for the murder of a famous actor which included their names.

The ECtHR approved the judgement of the German courts in finding that, while there was an engagement of Article 8 rights, this was undermined by the applicants' own behaviour in courting media attention when pursuing their appeals. A balance had to be struck with the media outlet's journalistic freedom under Article 10 of the Convention, which the Court noted was necessary in a democratic society. Notably the court did not consider search engines to have the same rights under Article 10.

The court ruled the interference with Article 8 rights to be proportionate. The court considered the seriousness of the interference with the reputation, how the material portrayed the applicants and the circulation of the material on the website. It found that the applicants themselves had perpetuated attention in the case and encouraged public interest. It found that the material on the website was balanced in its depiction of the applicants. Finally it noted that the circulation of the material on the website was small and therefore less significant.

The ECtHR found that both Article 8 and Article 10 were engaged, but that in these circumstances there had been no violation of Article 8. Therefore the German court had been within its margin of appreciation in finding the publication lawful.

The Judgement is not yet available in English but a summary can be found here.

13 September 2018

***Big Brother Watch and others v UK (App No. 58170/13, 62322/14, 24960/15.)* (see here)**

On 13 September the European Court of Human Rights gave its judgment in Big Brother Watch and others v UK. The judgment concerned the UK bulk interception regime under the Regulation of Investigatory Powers Act 2000, the predecessor to the Investigatory Powers Act 2016.

The Court held that in three specific respects the RIPA bulk interception regime and RIPA's provisions for acquiring communications data from telecommunications operators violated Article 8 (privacy) and 10 (freedom of expression) of the European Convention on Human Rights. The Court expressly did not hold that bulk interception per se was impermissible. But it said that a bulk interception regime, where an agency has broad discretion to intercept communications, does have to be

surrounded with more rigorous safeguards around selection and examination of intercepted material. It was also not persuaded that the acquisition of related communications data was necessarily less intrusive than the acquisition of content.

Do the specific aspects of RIPA that resulted in the violation have implications for the Investigatory Powers Act? Although the 2016 Act introduced, for the first time, prior independent review of bulk warrants, the ECtHR judgment focused on adequacy of safeguards in specific areas: selection and examination of intercepted material, use of related communications data, and journalistic privilege. In at least some of these areas the IP Act may be vulnerable.

Bird & Bird partner Graham Smith discusses this further in his Cyberleagle blog.

Enforcement

UK enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach	Summary of steps required (in addition to the usual steps)
2 July 2018	**Nobel Design and Build of Telford, Shropshire**	Prosecution fined £4500	Failing to comply with an information notice (fined £2000) and fined £2500 (for processing personal data without having notified) and ordered to pay costs (£364.08) and a victim surcharge (£170). (Criminal offence). More here.	No additional steps
6 July 2018	**STS Commercial Ltd**	fined £60,000	Allowing its lines to be used to send spam texts promoting payday loans to more than 270,000 people, without their consent. STS was previously investigated in 2015 for mass sending of spam texts. The ICO concluded that STS performed no due diligence on its marketing lists.[This case has since been removed from the ICO website].	No additional steps
6 July 2018	**AggregateIQ Data Services Ltd**	Enforcement notice	Processing data of UK individuals on behalf of UK political organisations for the purpose of behavioural advertising in the context of political campaigning. The notice can be viewed here.	The ICO was highly critical of AIQ and has instructed that AIQ must cease processing any personal data of UK or EU citizens from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purpose.

				Failure to comply with this notice will result in a fine of up to €20 million or 4% of the undertaking's gross worldwide turnover, whichever is higher.
18 July 2018	**The Independent Inquiry into Child Sexual Abuse (IICSA)**	fined £200,000	Sending a bulk email that identified possible victims of non-recent child sexual abuse. ICO investigation also found that the Inquiry breached their own notice by sharing the email addresses with an IT company without consent. The ICO and Inquiry received 22 complaints about the security breach. More here. The ICO took into account the following mitigating factors: • The Inquiry had apologies to the affected individuals • It had taken substantial remedial action	No additional steps
1 August 2018	**AMS Marketing Ltd**	fined £100,000	For making 75,649 nuisance marketing calls to people who had opted out of receiving marketing calls by registering with the TPS. The calls were made between 1 October 2016 and 31 December 2017. A total of 103 complaints were made to the ICO and TPS. More here.	No additional steps The ICO commented: Firms that buy in lists of data are duty-bound to check whether people are registered with the TPS. Firms that fail to make the proper checks, do so at their peril. The ICO can and will take action.
9 August 2018	**Lifecycle Marketing**	fined £140,000	For selling personal information belonging to more than one million people for political	No additional steps

	(Mother and Baby) Ltd (Emma's Diary)		campaigning. The information was used by Labour to profile new mums in the run up to the 2017 General Election. More here. Mitigating factors: • This was the only occasion LCMB shared personal data with any political party • Experian confirmed on 28 June 2017 that it had destroyed all the data in question	
4 September 2018	**London Borough of Lewisham**	Enforcement notice	Regarding 113 SARs outstanding (the oldest of which dates from 2013). Recovery plan to eliminate these by 31 July 2018 was not met. More here.	By Monday 15 October needs to respond to the 19 individuals who submitted SARs pre GDPR. Formal progress update to be provided to ICO at weekly intervals during notice period.
4 September 2018	**London Borough of Lewisham**	Enforcement notice	Regarding 113 SARs outstanding (the oldest of which dates from 2013). Recovery plan to eliminate these by 31 July 2018 was not met. More here.	By Monday 15 October needs to respond to the 19 individuals who submitted SARs pre GDPR. Formal progress update to be provided to ICO at weekly intervals during notice period.
4 September 2018	**London Borough of Lewisham**	Enforcement notice	Regarding outstanding SARs (the oldest of which dates from 2013). More here.	
4 September 2018	**London Borough of Lewisham**	Enforcement notice	Regarding 113 SARs outstanding (the oldest of which dates from 2013). Recovery plan to eliminate these by 31 July 2018 was not met.	By Monday 15 October needs to respond to the 19 individuals who submitted SARs pre GDPR.

			More here.	Formal progress update to be provided to ICO at weekly intervals during notice period.
5 September 2018	**Everything DM Ltd**	Enforcement notice and fined £60,000	For sending 1.42 million direct marketing emails on behalf of clients without being able to prove consent from the recipient. More here and here.	

Enforcement News

Trends report from the ICO	**Nuisance calls and messages**	Highest number of complaints about broadband calls for 12 months.	In July the ICO took a strong stance against nuisance calls and text messaging. They levied a fine of £100,000 against AMS marketing (see above). The ICO has also issued 13 third party notices and has 107 cases under investigation. You can view more detail on the recent action the ICO has taken to tackle nuisance calls and messages in their June report here	
New ICO Newsletter	**Nuisance marketing**		The ICO has launched a new e-newsletter that focuses specifically on action they have taken under the Privacy and Electronic Communications Regulations (PECR), as well as noticeable trends in reports they receive from members of the public. You can sign up to receive the newsletter here.	