Bird & Bird

UK & EU Data Protection Bulletin: Highlights November 2019 - January 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

Information Commissioner's Office (ICO)

Date	Description
14 November	**Updated ICO Guidance on Special Category Data** In November, the ICO announced that it had updated its Guidance on the processing of Special Category Data. This includes data revealing a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, and biometric data (where used to uniquely identify someone) and data concerning health, sex life or sexual orientation. The majority of these categories are not defined further but there are specific definitions for genetic data, biometric data and health data. The Guidance looks at what these different categories include before taking a more detailed look at the relevant conditions for processing such data both under the GDPR and Schedule 1 of the DPA 2018. Some high level points to note include: • **Biometric data:** The Guidance provides some helpful guidance on what is and isn't biometric data. It clarifies that all biometric data is personal data, as it allows or confirms the identification of an individual but will only be special category data when it is being processed *"for the purpose of uniquely identifying a natural person"* which is often, but not always, the case. The Guidance also clarifies that the processing of digital photographs of individuals is not automatically biometric data even if being used for identification purposes. Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if the controller carries out "specific technical processing". Usually this involves using the image data to create an individual digital template or profile, which in turn is used for automated image matching and identification. If biometrics are being used to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, then the data will be special category data and the controller will need to comply with Article 9. The ICO is also planning on producing more detailed guidance on biometric data in due course. • **Special category data can include inferences:** Special category data includes personal data **revealing or concerning these** details. It may be possible to infer or guess details about someone which fall within the special categories of data. Whether or not this counts as special category data and triggers Article 9 depends on how certain that inference is, and whether you are deliberately drawing that inference. If you can infer relevant information with a reasonable degree of certainty then it's likely to be special category data even if it's not a cast-iron certainty. But if it is just a possible inference or an 'educated guess', it is not special category data (unless you are specifically processing to treat someone differently on the basis of that inference) - even if that guess turns out to be right. The Guidance provides the example of a job applicant listing in their CV that they are a trustee for a deaf charity. Other people involved with the charity are often deaf but this doesn't necessarily mean the applicant is deaf. This wouldn't be special category data even if the individual is in fact deaf. However, if the company has other information which confirms that the individual is deaf, then this would be special category data. The Guidance also helpfully clarifies that it is inappropriate to treat all names which may infer religion or ethnicity as special category data in every instance but if you hold this information to specifically target on this basis, then you are processing special category data. Any profiling which infers ethnicity, religion, politics, health etc if likely to be special category data – the key question is not whether the inferences are correct but whether you are using an inference linked to one of the special categories to influence your decision in any way.

Date	Description
	• **Interplay between GDPR and DPA 2018:** The Guidance reminds organisations that in order for processing of special category data to be lawful, you always need to identify an Article 6 basis for processing and an Article 9 basis for processing together with any associated DPA Schedule 1 conditions where required. • **Lawful Basis of Processing:** In terms of understanding which lawful basis is most appropriate, the ICO recommends starting out by considering whether you could reasonably get explicit consent for your processing (although flagging that consent is not always be appropriate, particularly in the public sector). If there are good reasons why consent won't work, then you can then consider the other Article 9 conditions. You should focus on your purpose for processing, ensuring that the special category data is actually necessary for that purpose. If the only relevant condition is substantial public interest, you should go on to consider the specific substantial public interest conditions in the DPA 2018. If the purpose is not covered by any of the conditions, and you cannot obtain valid explicit consent, you cannot process the special category data. The ICO states that it doesn't matter how good your reason for processing might be. In practice, you need to change your plans to either avoid using special category data, or else obtain valid explicit consent. The only potential exemption from Article 9 is the public interest exemption for journalism, academia, art or literature and the ICO cannot authorise the use of special category data in the absence of a condition • On the specific lawful bases, some interesting comments include: ○ **Legitimate Interests (Art 6(f)):** Where reliance is placed on this ground, the controller must specifically consider the risks associated with special category data in its legitimate interests assessment and more robust safeguards may be required. ○ **Manifestly Made Public (Art 9(e)):** The term '*manifestly made public*' is not defined by the GDPR so it is helpful that the ICO has provided some further guidance on this term. In its view, it "*clearly assumes a deliberate act by the individual – its not enough that its already in the public domain – it must be the person concerned who took steps to make it public*". There is a different between assenting to or being aware of publication and the individual actively making it available and the key message is that the ICO states that organisations should be very cautious about using this condition to justify the use of special category data obtained from social media posts. For example, you might also find it hard to show that someone has manifestly made information public if, for example, they made a social media post for family and friends but default audience settings made this public. The data must also be "*realistically accessible to a member of the general public*" – information is not necessarily public just because you have access to it. The Guidance also recommends that for accountability purposes, you should keep a record of the source to help demonstrate that it was manifestly made public. It is worth noting however UK case law supports a broader interpretation of this condition: For instance, in *NT1, NT2 v Google [2018] EWHC 799* , the judge held (when addressing the wording of similar condition under the Data Protection Act 1998 in connection with the processing of criminal offence data) that "*it did not require a deliberate decision or "step" by the data subject "to make" the information public but rather (a) the taking by him of a deliberate step or steps, as a result of which (b) the information is "made public". A person who deliberately conducts himself in a criminal fashion runs the risk of apprehension, prosecution, trial, conviction and sentence. Publicity for what happens at trial is the ordinary consequence of the open justice principle.* " In other words, if you commit a crime, you then put this information into the public domain.

Date	Description
	○ **Necessary to establish, exercise or defend legal claims (Art 9 (f)):** This ground appears to have been widely interpreted by the ICO – for instance, the Guidance provides the example of a beauty salon taking a patch test to check if a client will have an allergic reaction to hair dye – although there is *no actual or expected court claim*, the purpose is to establish that the hairdresser is fulfilling her duty of care to the client and to defend against any potential personal injury claims in the event of an adverse reaction. • **Appropriate Policy Document:** Many of the DPA 2018 conditions require the data controller to have an "*appropriate policy document*" in place to outline compliance measures and retention policies with respect to the special category data that is being processed and the Guidance provides a template policy to address this. It also reminds controllers to keep records of any special category data that is being processed including documentation relating to categories of data, the conditions for processing the data, how you satisfied a lawful basis for that processing and specific details about whether you have followed your retention and deletion policies. • **DPIAs:** A DPIA is required for any high risk processing which means you are more likely to need one for special category data. The Guidance confirms that that this will be needed if you plan to process special category data on a large scale; to determine access to a product, service, opportunity or benefit; or which includes any genetic or biometric data (if in combination with any other criteria in EDPB DPIA Guidelines). • **Other points to consider:** Given the particular risks associated with special category data, the Guidance reminds organisations to think about the following: ○ **Transparency:** Include the categories of special category data being processed in your privacy notice (but there is no need to specify the condition you are relying on)**.** ○ **Rights related to automated decision-making:** Ensure that you have the explicit consent of the individual or can identify a substantial public interest condition if you using special category data to carry out this type of processing which might have might have a '*legal or similarly significant effect'* on the individual. ○ **Security:** Enhanced security measures may be required for special category data ○ **Data Minimisation:** Only process the minimum amount of special category data required for the specified purpose. ○ **DPO:** Appoint a DPO if your core activities require large scale processing of special category data. ○ **EU representative:** Consider appointing an EU representative if you are not established in the EU but you offer services to, or monitor, individuals in the EU member states, and you process special category data on a large scale. You may need a representative even for occasional small-scale processing of special category data, unless you can show that it is low risk. Likewise organisations not established in the UK may need to appoint a UK representative under equivalent provisions in UK data protection law applicable post the Brexit transition period. A link to the Guidance can be found here.
2 December	**Draft ICO Guidance on AI-assisted decisions** On 2 December 2019, the ICO and the Alan Turing Institute issued guidance on the explainability of AI-assisted decisions. The guidance,

Date	Description
	which forms part of ongoing efforts to address the implications of transparency and fairness in AI decisions, provides good practice guidance on AI explainability, but is not a statutory code of practice. The aim of the guidance is to give practical advice to organisations to help them explain the processes, services and decisions delivered or assisted by AI, to the individuals affected. The audience of the guidance is mixed and it includes DPOs and compliance teams and technical teams, as well as senior management. Although the point of departure is the GDPR and the transparency requirements established by the GDPR, the information contained in the guidance is broader and covers wider points which go beyond GDPR obligations. The guidance is split in three parts, which are interconnected, but each of which has a separate role. Part 1 sets out the legal context and the relevant GDPR provisions, the main types of explanations that should be provided to individuals and the principles that organisations should follow to ensure that AI-assisted decisions are explainable. The guidance identifies the following types of explanation: a) **Rationale explanation,** which should describe the reasons that led to a decision, delivered in an accessible and non-technical way; b) **Responsibility explanation**, which should explain who is involved in building, managing and deploying the AI model and who is the contact point for a human review of the decision; c) **Data explanation**, which should set out what data has been used and how, including what data has been used to train and test the AI system; d) **Fairness explanation**, which should describe the steps taken to ensure that the AI-assisted decisions are unbiased and fair; e) **Safety & performance explanation**, which should describe the steps taken to maximise accuracy, reliability, security and robustness of the decisions and behaviours of AI systems; f) **Impact explanation**, which should explain the impact of the use of AI and of its decisions on an individual and on wider society. The guidance further advises organisations to be transparent and accountable, consider the context in which they implement AI models and reflect on the impact that the AI system has on individuals and wider society. Part 2 of the guidance sets out the practicalities of explaining AI-assisted decisions and contains guidance on how to select the appropriate explanation types and how to present this to individuals. This part provides more detailed information on what information should be provided as part of each explanation type and also contains technical guidance on the explainability of specific AI models and supplementary explanation tools used for black box methods. The final part of the guidance examines the various roles, policies, procedures and documentation that organisations can put in place to comply with the rest of the guidance and to ensure that they provide meaningful information to individuals. This part contains information that is also useful for accountability purposes and internal governance. The guidance recognises that several roles will be involved in providing an explanation, from product managers and AI developers to DPOs, compliance teams and senior management. It also clarifies that if the AI model is sourced from a third party, the organisation using it will be controller of the data processing and will have the primary responsibility for ensuring that appropriate explanations are provided to individuals. The guidance was open to public consultation until 24 January 2020.
10 December	**Information Commissioner consults on subject access guidance** The UK Information Commissioner has issued a consultation on new, draft, guidance on dealing with subject access request. The call for

Date	Description
	comments closes on Wednesday, 12th February 2020. As with other recent guidance from the ICO, the draft is long (77 pages). However, it is accessible and worth reading. Much of the draft consolidates earlier guidance and it does not contain "surprises". However, there are some helpful clarifications which practitioners will find of use. There are also some omissions in the guidance: 1. It concentrates on exemptions under the UK Data Protection Act 2018, but does not comment on the exemption set out at Article 15(4) which provides that the right to obtain a copy shall not adversely affect the rights and freedoms of others. It would have been useful to have commentary on how this may impact requests involving multiple data subjects' personal data – and requests involving commercially confidential information; 2. There is now a large body of law in the UK addressing important topics such as when a request may be considered disproportionate and how to treat requests were the main motive of the request is to obtain information for litigation. These are not addressed at all in the guidance, which focuses on the text of the GDPR and the 2018 Act. The cases are still relevant and this is a missed opportunity to make the guide even more useful to its target audience of data protection officers/ specialist privacy teams in organisations. **When are requests valid** ICO reiterates that there are no formalities for a request to be valid – this can include verbal [sic] requests and those made via social media sites. Therefore, there is an onus on organisations to ensure that channels of communication are monitored and that staff in public facing roles are trained to recognise requests. **Identifying individuals** Controllers should check that they are releasing data to the actual data subject – reasonable identity checks are appropriate, but controllers should not request more than is reasonable: asking for utility bill from an employee who makes the request in person would be excessive. Requests can be made via a third party, provided they are authorised to make the request. ICO states that it is the responsibility of the third party to provide this authority – which could be a specific written authority or more general power of attorney. If there is no evidence of authority, then the controller is not obliged to respond. **Subject access request generator sites** The same rules apply to online access portals such as Tapmydata, We're David or Chommy etc – so the identity of the applicant should be confirmed, and the third party should make clear how it is authorised to make the request. Helpfully, ICO also notes that the controller is not obliged to take proactive steps to "discover" a SAR – so if the controller cannot access a SAR without paying a fee or signing up to a service, then it has not "received" the SAR and so the obligation to respond will not have started. Similarly, if the only way for the controller to respond is via payment of a fee or acceptance of the portals ts & cs, then the controller should provide information direct to individual instead. **Locating information**

Date	Description
	ICO notes that it will be difficult to deal with SARs without information management systems which allow information to be retrieved and redacted. The guide repeats earlier comments that subject access has been a feature of data protection law since the 1980s – so organisations should already have such systems in place. **Timing to respond** Controllers usually have one month to respond. They can have longer if a request is "complex" or if they have received a number of requests from the individual – ICO gives the example of a controller which has received a SAR, erasure request and portability request simultaneously from the same individual. This is a fairly common situation so is helpful to note. The guide notes that a request will not be complex simply because the individual has requested a large amount of information or the controller is dependent on a processor in respond. Examples of "complex" requests would be: – Technical difficulties in retrieving information – e.g. where data has been electronically archived; – Applying an exemption that involves large volumes of particularly sensitive information; – Specialist work involved in redacting information or communicating it in an intelligible form. **Bulk requests** Claims management companies (and others) may submit bulk requests. Here ICO notes that each individual request within the one bulk request has the same status. However, ICO says it will have regard to the volume of requests received and steps taken by the controller to ensure requests are dealt with. It will also take into account the size and resources of the controller and - where reasonable – will exercise discretion in enforcement. **Tricky questions about searching for data** The guide notes that where an organisation has tried to permanently discard data and has no intent to access it again, then ICO will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate such data. However, data moved to a deleted email folder does NOT fall into this category. The guide also notes that there is no need to instruct staff to search personal devices or private emails unless the controller has reason to believe they hold relevant data. **Exemptions** There is no obligation to comply if a request is manifestly unfounded. Here the guide repeats previous commentary from ICO that this will be the case if an individual clearly has no intention to exercise their right of access – e.g. where an individual makes a request but then offers to withdraw it in return for some form of benefit from the organisation. ICO also accepts that requests made with malicious intent do not have to be honoured – examples given are: – requests made solely to try to cause disruption or harass – if there is an explicit statement that applicant intends to do this

Date	Description
	– if the applicant makes unsubstantiated accusations – for example, targeting a particular employee where there is a personal grudge – if the applicant systematically sends different requests as part of a campaign with the intent of causing disruption – e.g. weekly access requests. The guide also looks at the most commonly used exemptions – in particular what happens when one person's personal data also relates to another, living, individual. Here, the guide notes that if the information is held in confidence in relation to that other individual, then it will usually be reasonable to withhold it – however, this cannot just be a question of looking to see if documents are marked "confidential": the context and substance of the material must be assessed. **Guidance on special cases** There are detailed sections looking at the special UK rules for unstructured manual records held by public authorities; credit files and the rules for health data; educational data and social records.
8 January	**Information Commissioner consults on draft Code of Practice on Direct Marketing (the 'Code')** On 08 January 2020 the UK Information Commissioner published its draft Code of Practice on Direct Marketing (the 'Code'). The Code will be open for public consultation until 4 March. At over 120 pages the Code is long, covering traditional e-marketing but also newer tools increasingly relevant to marketers today such as social media and adtech. The Code is essential reading for those engaging in direct marketing activities in the UK. Much of the Code consolidates earlier guidance and won't come as a surprise to organisations with knowledge of the exiting rules. However, there are some important clarifications and updates to previous guidance particularly in relation to in-app marketing messages, refer-a-friend schemes, and marketing via social network platforms. <u>Headline points to note include:</u> **End of refer-a-friend schemes?:** According to ICO, it is difficult reconcile refer-a-friend schemes with the requirements of GDPR as organisations won't know what the referring individual has told their friends about the processing and will not be able to verify whether the friend provided GDPR standard consent. The restrictions in the Privacy and Electronic Communications Regulations ('PECR') also apply regardless of whether the organisation messages the friend directly or 'instigates' the individual to send or forward the messages on its behalf. ICO, thus, conclude that refer-a-friend schemes breach PECR. Refer-a-friend schemes are effective tools widely used by advertisers and valued by consumers, as such ICO's comments on this front won't be welcome and pushback from marketers can be expected. It would be worth stakeholders exploring if a more pragmatic position could be reached with ICO for organisations that do not abuse these programs. **Custom audience initiatives:** Many organisations use custom audience services whereby the organisation shares email addresses or other direct identifiers with a social network provider which the network provider then matches with its user base to allow the organisation to advertise via the social media platform. According to ICO, it is likely that consent is the appropriate lawful basis for advertising via custom audiences, as it is difficult to see how

Date	Description
	custom audience tools 'would meet the three part test of the legitimate interest basis' It is not, however, clear why ICO conclude this. Under GDPR direct marketing is recognised as processing which can be based on legitimate interest. Further, while in its update Report on Adtech and Real Time Bidding, ICO cites Article 29 Working Party ('A29WP') Guidance noting that behavioural targeting is unlikely to be justified on the basis of legitimate interest - such A29WP views often relate to scenarios where there's wide volumes of data collection across sites with little consumer awareness. In contrast, standard custom audience targeting generally works very differently: it does not depend on building large profiles, but just allows a marketer to reach an individual they already know in a different (ad-supported) medium. In taking the view it has, ICO is following the conservative German approach, but this is not typical of the position across Europe where custom audience is currently possible on the basis of legitimate interests. For look-a-like audiences, i.e. the advertiser asking the social network to build a list of individuals who 'look like' the advertisers own customers - ICO consider that the advertising organisation and social network will both be joint controllers. As the advertiser won't have a direct relationship with the individuals in the look-a-like audience, they will need to be satisfied that the social media platform has the appropriate transparency information in place. The Code's position on custom audience is not exclusive to social media, and will also apply to similar tools in other contexts such as subscription TV and video on demand services. **Service messages:** Consent is not required under PECR for genuine service/operational messages. According to ICO, in determining whether a communication is a service message, key factors will be the phrasing, tone and context of the message. If the message has an active promotional element it is likely to be direct marketing. For example a mobile network provider sending a text to a customer alerting them of reaching their data limit would constitute a service message, however if the message goes on to encourage the individual to buy more data or switch data plans that would cross the line and constitute direct marketing. However, the tone alone is not determinative. A message from a supermarket stating 'your local supermarket stocks carrots' is still, according to ICO, promotional in nature despite the 'non-sales' language used. **Electronic mail covers in-app messages and direct messaging on social media:** In an important change, ICO states that in-app messages and direct messages in social media 'are electronically stored messages' and treated akin to email for the purposes of PECR (thus requiring consent unless an exemption applies). The definition in Regulation 22 PECR refers to material being stored 'in the network or in the recipients terminal equipment' and as such is closely linked to traditional email rather than webmail type communications. The Code, unhelpfully, does not explain the reasoning for ICO's conclusion i.e. are in-app messages caught because the message is stored in the device (which does not seem correct from a technical perspective), or because ICO view the message as being stored, as opposed to being merely transmitted, in the network? Accordingly industry pushback on this point can be expected. The ICO is also silent on the European Electronic Communications Code ('EECC'), which will come into law on 21 December. The EECC will bring Over the Top communication providers , for the first time, within the scope of EU telecommunications regulation. These OTT services, which deliver services functionally equivalent to traditional electronic communication providers across an IP network but do not consist

Date	Description
	wholly or mainly in the conveyance of signals, will also be required to comply with the PECR rules on confidentiality of communications and restrictions on the use of traffic and location data. However, unlike the Code, the EECC does not seek to broaden the rules on email marketing to cover wider types of communications such as in-app messaging. **Incentivisation of consent:** While organisations should not coerce or unduly incentivise consent to marketing, some element of incentivisation is permitted - ICO give the example of joining a loyalty scheme, the whole purpose of which is to access money-off vouchers. However, when it comes to incentives, ICO warn organisations 'not to cross the line' and unfairly penalise those who refuse to consent to direct marketing. More prescriptive guidance from ICO on what these red lines are would be welcome, so as to avoid organisations finding out ex post through enforcement action. **Joint marketing activities:** Where an organisation is planning a dual branding promotion with a third party, it still needs to comply with PECR regardless of whether it has access to the data used. ICO give the example of a supermarket sending out a marketing email promoting a supported charity. Although the supermarket is not actually passing customer contact details to the charity it still needs to ensure there is appropriate consent from its customers 'to receive messages promoting the charity'. It is not clear whether the supermarket needs separate opt-in consent to send marketing about the charity. Further clarity on this point would be helpful. **Legitimate interests:** Where consent is not required under PECR or GDPR organisations may be able to rely on legitimate interest for the marketing activity subject to carrying out a legitimate interest balancing assessment. ICO provide some helpful guidance for organisations carrying out these assessments in practice: (1) the fact that GDPR states that direct marketing may be a legitimate interest should help organisations satisfy the legitimate interest purpose test, provided the activity is carried out in compliance with e-privacy laws and other industry standards; (2) in the assessments, organisations should avoid undue focus on the presumed benefits of the marketing on customers (such as discounts or offers) as this is 'unlikely…to add much weight to the test'; (3) it is difficult pass the balancing test if individuals are not given a clear opt-out when their data was initially collected and (4) the balancing exercise must consider whether people would expect their data to be used as the organisation propose; the potential nuisance factor of unwanted marketing messages; and the effects the methods and frequency of the communications might have on vulnerable individuals. According to ICO, marketing activities which individuals were not told about i.e. so called invisible processing is particularly difficult to justify on the basis of legitimate interests, as are activities that collect and combine vast amounts of personal data for profiling purposes. **Making a service conditional on direct marketing:** In most cases, it is unlikely that organisations can make direct marketing a precondition to a product or a service (such as, to use an example from the Code, a train service making passenger wifi conditional on opt-in consent to marketing). However there are exceptions to this rule: ICO point to retail loyalty schemes operated purely for the purposes of sending members marketing offers. Operators of such schemes still need to be upfront and clear about the purposes of their processing, and to send marketing they must have consent from the scheme members where required by PECR. **Using special category data in direct marketing:** Organisations can only use special category data for marketing purposes - including drawing inferences about likely race, ethnicity, political beliefs, health or sexual orientation - if they have the individual's explicit consent. Helpfully, ICO note that merely having a list of customer names will not trigger Article 9 GDPR even if those names are associated with a particular ethnicity or religion unless the names are specifically used to target marketing based on those inferences. Similarly an organisation inferring special category data from a customer list due to the nature of the organisations' products - for example, where the organisation sells disability aids, doesn't trigger Article 9 GDPR unless specific information about the individual's condition is held or that

Date	Description
	the organisation specifically uses the data for marketing purposes. ICO's comments here are broader than those in its Update Report on Adtech and Real Time Bidding, where ICO suggests that the use of special category data in order to avoid serving ads against certain types of content would amount to the unlawful processing of special category data. ICO's more flexible approach in the Code is to be welcomed and is in line with the similarly pragmatic approach seen in the European Data Protection Board's 2019 opinion on video surveillance that notes video footage which captures information which could be indicative of disability or religious belief would only be considered special category data if it was actually being used to deduce special category information about the individual. Elsewhere on special category data, ICO unsurprisingly note that it will be difficult for marketers to use biometric facial recognition technology to display direct marketing to specific individuals given the challenges of complying with the lawfulness, fairness and transparency principles in GDPR. **Duration of consent:** The Code reminds organisations that consent to marketing does not last forever. The validity of consent depends on the particular circumstances of the case including (1) the context in which it was given; (2) the nature of the individuals relationship with the organisation and (3) the individuals expectations. Where an organisation obtains consent via a third party, ICO warn that while the individual may be happy to hear from the organisation when they gave the consent they are unlikely to expect to start to receive messages at a much later date. To add to the woes of data vendors, ICO repeats it's best practice recommendation that organisations do not rely on consent from third parties that is more than 6 months old. **Providing Notice for indirectly collected data:** Where organisations obtain data indirectly under Article 14 GDPR, the organisation must provide the privacy information within a reasonable period and at the latest within one month of obtaining the data or at the time of first communication or disclosure of the data (if sooner). Helpfully ICO confirm that where an organisation buys in data from a data vendor it can send out the privacy information alongside the marketing materials. Therefore organisations that act promptly within the notification timeline in Article 14, may be less reliant on their data vendors providing the full list of Article 14 transparency information to the individual (although where required by PECR organisations still need to rely on the vendor to obtain consent for sending the communication). **Disproportionate effort exemption to giving notice:** Article 14(5)(b) GDPR provides an exception from the requirement to give notice where it would involve disproportionate effort. Some regulators have read down this exemption suggesting it only applies in the context of archiving, research, or statistical processing (an interpretation which is not supported on a literal reading of GDPR). The Code does not say this. The Code notes that if the processing has a minor effect on the individual then it may not be proportionate to put significant resources into informing individuals. However, the comments are cautionary - particularly in the big data/data mining context - with ICO warning that organisations are unlikely to be able to rely on disproportionate effort exemption where they are collecting personal data from various sources to build an extensive profile of an individual's interests and characteristics for direct marketing purposes. **Public information ≠ fair game:** The Code reminds us that just because information is publicly available does not mean it is fair game. As ICO note 'an individual may want as many people as possible to read their social media post but that does not mean they are agreeing to have that data collected and analysed to profile them to target…direct marketing campaigns'. In such contexts, GDPR is applicable and organisations are still required to provide privacy information to individuals unless an exemption applies. Buying additional contact details: According to the Code, 'in most instances buying additional contact details for existing customers is likely

Date	Description
	to be unfair, unless the individual has consented'. It doesn't matter how clearly this practice is explained in the privacy notice. The rationale here is that individuals should have a free choice about which channels they use for direct marketing and an organisation buying in alternative contact details erodes this. **Tracing/data cleansing:** The Code confirms that using data vendors to cleanse marketing databases of deceased individuals is permitted as GDPR only applies to living data subjects. However, organisations are unlikely to be able to justify tracking services to find the new addresses of individuals' who have moved. For example, ICO state that a university would not be allowed to use a data broker to find updated address details for its alumni. This is a conservative view worthy of review in the consultation. **Pixel tracking in email:** In line with ICO's recently updated Guidance on Cookies, the Code reminds organisations that if pixels or similar devices are being placed in email marketing messages so as to measure open rates or similar metrics then consent will be required under Regulation 6 PECR (i.e. under the cookie consent rule). This is in addition to the consent required under Regulation 22 PECR required for the sending of the email marketing message itself. This is a widespread practice which has generally flown under the radar but organisations will now need consent for tagging email messages in this way. The soft opt-in won't help organisations either: the exemption can only cover the sending of the message and will not extend to placing the cookie. **Cookie walls:** According to the Code, and in line with ICO's previous Cookie Guidance, cookies walls i.e. requiring users to consent to cookies before they can access a website, 'in many circumstances' won't be 'appropriate'. As in the Cookie Guidance, ICO have not totally prohibited cookie walls which reflects the fact that this is a difficult area given the policy considerations in play, notably the fact that many websites and e-commerce platforms rely on targeted advertising to monetise otherwise free content. For organisations for whom this is a particularly important issue, the public consultation on the Code may be another shot to re-lobby ICO on this matter. **DPIAs:** The Code promotes use of DPIAs. It considers that they are required for any direct marketing which targets children, which involves large scale profiling or wealth profiling. It also recommends them for any use of new technology, and suggests that a DPIA will likely be required for profiling, data matching, invisible processing (which, somewhat oddly, ICO considers includes online advertising in general, notwithstanding informed consent requirements for cookies), use of location data and running loyalty schemes. Indeed, ICO suggests that it is likely that all direct marketers will need to carry out a DPIA and that completing these will help bring broader financial and reputational benefits and build trust and engagement with individuals. DPIAs are unavoidable for processing which poses a high risk and, in this situation, a rigorous analysis of the impact of the processing and ways to mitigate risk is appropriate and helpful. However, suggesting this level of documentation and analysis for the wider types of direct marketing suggested by ICO is excessive and risks producing a counter-productive, box-ticking, culture.
22 January	**Information Commissioner publishes Age Appropriate Design Code** **Online services with a UK connection need to be (re)designed with kids in mind** On 22nd January 2020, the UK Information Commissioner published her Age Appropriate Design Code. The code applies to organisations in the UK. It also applies on a worldwide basis to organisations that monitor kids in the UK, or where it's apparent that they intend to offer online services or goods to kids in the UK. The code is not limited to child-directed sites: it applies whenever it's more likely than not that

Date	Description
	under 18s will use the site. The code is expected to be fully effective from Autumn 2021. **The code is much wider than parental consent requirements** The GDPR contains rules requiring organisations to obtain parental consent in order to process data of kids below 13 – 16 (depending on the age selected by different EU member states). The scope of the code is much wider than this: it requires online services to be designed with the best interests of the child in mind. This must be the primary consideration in all associated processing of personal data. It is to be achieved through 15 key principles – which link to privacy by design and by default; transparency; and accountability. The code states that where online services are likely to be accessed by kids a DPIA is mandatory. Impact on children is to be considered at every stage and cannot be "bolted on" as an after-thought. Existing DPIAs must be updated to achieve this. **What is the status of the code and what are the sanctions for non-compliance?** The UK Data Protection Act 2018 places an obligation on the Commissioner to produce the code. Failure to comply with the code is not automatically a breach of the law. However, both the Commissioner and the UK courts are required to take it into account. As the Code represents the Commissioner's view on what is required when processing children's personal data, failure to comply with the code may well lead to sanctions under data protection legislation. The Commissioner notes that this is an enforcement priority for her and that she will engage in pro-active audits. **The code applies to most websites, apps, online games and connected toys** The code applies to "information society services" which are likely to be accessed by kids. This would include websites and apps making products or services available online; news sites; games; education sites; messaging; content streaming; and connected toys and devices. "Information society services" are services provided by electronic means, at a distance and at the individual request of the particular user. The services must be provided "for remuneration" – which would include services which are free to the user because they are ad-funded. Counselling and preventive services are excluded. Processing which isn't subject to the GDPR (e.g. processing by law enforcement authorities) is also not affected. There is a useful flow chart at the end of the code, to give guidance on scope. The code covers data collected from the chid, but also data inferred from this information or inferred from the child's behaviour online. **The code applies to all online services "likely" to be accessed by under 18s** The code is deliberately not limited to child directed sites. It applies to online services if it is more likely than not that under-18s will access them. Here, the Commissioner recommends a common sense approach, looking at the nature of the service and how it is accessed. Market research or user provided evidence can be taken into account. The measures which a site takes to prevent kids accessing it can also be relevant. **On the internet, no-one knows you are a kid** The code does not prescribe how organisations should assess visitors age. It puts forward a range of options, from self-declaration, through to use of AI and requirements for provision of official ID documents. The code acknowledges that requirements to provide additional

Date	Description
	information to prove age may present privacy risks – the approach taken should reflect the risks of the service and should seek to incorporate privacy by design and data minimisation principles. For lower risk online services, self-verification may be sufficient: for high risk online services, independent verification may be appropriate. The code acknowledges this is a challenging and developing area. **Age- appropriate design must be appropriate to the age of the child** The code is not about one approach for kids and another for adults. Age appropriate design means just that. The code divides children into 5 developmental ages – 0- 5; 6 – 9; 10 – 12; 13 – 15; 16 – 17. It provides guidance in an appendix on developmental factors for each age group. In multiple parts of the code, it provides suggestions on how to tailor design with these different ages in mind. To take an example, a primary school child may actively need to be deterred from changing high privacy default settings, whereas a teenager might be better supported by clear and neutral information which helps them make their own decision. **Best interests of the child** The key principle in the code is that the child's best interest must be the primary consideration when designing online services. The UN Convention on the Rights of the Child is relevant in determining this. The Commissioner recognises the importance of children being able to access information and the importance of play (including online play). The child's best interest is not the sole consideration: commercial interests are also allowed and are relevant. However, if there is tension between these, the bests interests of the child must come first. The code draws a strong link between this principle and fair and lawful processing under the GDPR. Conversely, one of the 15 principles prohibits uses of personal data which are detrimental to the interests of the child. This would include processing which has been shown to be detrimental to the child's well-being, or where studies suggest that this could be the case. The code refers to compliance with other codes which contain requirements to prevent harm to children (such as the CAP Code on marketing, the press and broadcast codes and the OFT guidance for online games). The code also makes a point of noting that this principle will restrict use of "stickiness" – features designed to make it hard for a user to disengage. **Privacy by design and by default: data minimisation, limited data sharing and profiling, default settings and nudging** Relevant services must collect and retain the minimum personal data necessary to provide the service. Kids must be given choices over any processing which is not necessary. For example, a music streaming platform's core service, for which processing is "essential", is the track download; whereas ancillary services such as providing recommendations or sharing users' playlists would be non-essential processing that should be defaulted-off unless the child opts-in. On this point, the Commissioner warns she'll look "very carefully" at claims that a privacy setting cannot be provided because the personal data is needed to provide the core service. Accordingly organisations which over interpret "*essential service*" do so at their peril. Processing of geolocation data is singled out, both as an example of this and as one of the 15 principles in its own right: geolocation data collection should be switched off by default, unless there is a compelling reason to collect data. If data has to be collected (e.g. to provide map based services), then this should only be while necessary for the service and the user should have to make an active choice to share

Date	Description
	beyond this. The service should use an obvious sign to show location data is being collected. Profiling should be switched off by default unless there is a compelling reason to allow it – and it should only be used if there are measures to protect users from harm. The code gives the example that if you profile to serve personalized content or ads, then you must ensure no detrimental content is served. Any personal data you process to protect the child and to ensure content is suitable cannot then be used for incompatible purposes; commercialising data collected to protect children (or using it to target ads) would fall foul of this. The code also reminds us that profiling for targeted ads at under 13s is likely to need parental consent under art.8 of the GDPR. Relevant services should not share data – even intra group – unless they can demonstrate a compelling interest, taking into account the best interests of the child. The code gives extreme examples of what is permissible: sharing with a school or police in the event of safeguarding concerns. However, selling data for commercial re-use is unlikely to be justifiable. Notwithstanding this last requirement, the code notes that targeted advertising is not banned – but must be turned off by default. In addition, sites cannot bundle multiple options for profiling in one request for consent – so there should be separate options to turn on personalized content and personalized ads. Where choices are offered, then the default option should always be the most privacy friendly. Kids will just accept whatever default settings are provided and therefore according to the Commissioner "*it is of utmost importance...defaults set are appropriate for children and provide them with adequate protection*". The code gives the examples of privacy settings for making content visible to others, or for allowing the service to use this for non-essential purposes (for example, marketing permissions) or for sharing it with others. Nudging children (via language or design) to change settings to a less privacy friendly option is not permitted: any nudging should be towards privacy friendly options and behaviours that support the child's well-being and health (such as pause buttons to combat excessive screen time). **Say what you do (in a way that kids can understand)** Privacy notices – and other information (such as terms & conditions or policies and standards) must be concise, prominent and in clear language suitable for the age of the child. Just in time notices when data is collected are recommended. This could mean multiple versions of a privacy notice – with options to explain that differently if its not clear, or to go into more detail if the information is too basic. Effective communication may mean cartoons or videos – or options to provide information by audio or in video. For very young children, information will need to be aimed at parents. **And do what you say** Relevant services must follow their own policies and standards – across the board and not just for privacy. So if you say you only display "content suitable for children" or that you "do not tolerate bullying" then you need to have adequate mechanisms in place to effectively deal with this. Kids (and the Commissioner) will say processing of personal data is unfair if you can't do this. If you only rely on back-end processes such as user reporting to identify behaviour which breaches your policies then that needs to be made clear in your policies. Further if the risks are high then "light touch" or "backend" processes may not suffice.

Date	Description
	Offer online tools These could range from prompts to explain more or easier ways to exercise subject access (for example links or buttons saying "I want to access my information"), through to alerts if children want to report a safeguarding issue. For sites where this is possible, such alerts should be prioritised. Parental controls may also be appropriate. However, relevant services should also include age appropriate information about these – and should include clear alerts or symbols to show if a parent is monitoring what the child is doing. The code recommends that relevant services also provide information to parents about the child's right to privacy – and that the child's expectations in this regard will grow as the child gets older. **Connected toys and devices need easy to use privacy controls** These could be on the device or online. Features to show when data is being collected (for example a light) are recommended. Clear information about the toy's use of personal data should be readily available including pre-purchase on the seller's website, at point of sale and on set-up. If devices are likely to be shared, then they should be designed so that different users can have different settings – with privacy friendly default settings for child users. Organisations cannot absolve themselves of responsibility just because they outsource the connected functionality of the product - although in these cases, there may be shared responsibility with the outsourced vendor. While the code applies to existing relevant services, it accepts that where products or toys are already on the market that there is no need to make changes to existing physical products. **Do (or redo) data protection impact assessments** GDPR makes these mandatory for processing which is "likely to result in a high risk". According to the Commissioner, this is inevitable where the code applies – so a DPIA is mandatory. The DPIA should take into account a wide range of risks to kids – not just privacy risks, but also psychological and developmental risks, as well as social and emotional risks. Readers who are parents may be re-assured that the risk of undermining parental authority also has to be considered; as does risk of excessive screen time. All of this involves an assessment of likelihood and severity of risk. The code notes that larger organisations will be expected to consult as part of their DPIAs – this could range from user surveys to a public consultation. Organisations offering child-focused services (or services which can be expected to be widely used by kids) will also be expected to take advice from experts in children's rights and developmental needs.

Date	Description
	Where organisations don't consult on DPIAs because they think it's unnecessary, disproportionate or just not possible, then they need to document their reasons for the decision and be prepared to justify the conclusion to the Commissioner. There is a template DPIA in an Annex to the Code. **Be ready to prove compliance** In line with the GDPR principle of accountability, organisations must not only comply with the code but must also be in a position to demonstrate compliance. Given the Commissioner intends to carry out audits proactively, affected organisations would be well advised to have an audit trail in place - such as DPIAs, internal policies, training records and privacy UXs - in case the Commissioner comes knocking. The accountability program should, according to the code, be driven by the DPO and be overseen by senior management at Board level.

UK Cases

Date	Description
6 November	**Dr Kaleem Siddiqui v Information Commissioner (EA/2019/0289)** The First Tier Tribunal (Information Rights) (the FTT) has held that the maximum penalty which can be imposed by the Information Commissioner under the Data Protection Act 2018 ('DPA 2018') on an organisation which fails to pay the annual data protection fee is 150% of the highest data protection fee (i.e. the tier 3 fee), rather than 150% of the data protection fee payable by the organisation in question (based, primarily, on its size and turnover). **Background** Dr Kaleem Siddiqui ran a medical practice specialising in medico-legal work until June 2017, which involved handling of personal data by Dr Siddiqui as a data controller. Although Dr Siddiqui ceased to perform the medico-legal work, he continued to hold personal data in digital form, and to respond to occasional queries about it. On this basis, he continued to be a data controller. Every organisation that processes personal information needs to pay an annual data protection fee to the ICO, unless they are exempt. The size of the data protection fee payable depends (primarily) on the size and turnover of the organisation, currently: £40 for tier 1 organisations, £60 for tier 2 organisations, or £2,900 for tier 3 organisations. Following a Notice of Intent, the Information Commissioner issued a Penalty Notice of £400 on Dr Siddiqui for failing to pay the relevant annual data protection fee (£40, as a tier 1 organisation) within the requisite timeframe. Dr Siddiqui did not dispute the Information Commissioner's legal right to issue the Penalty Notice, and his appeal to the Tribunal was confined to challenging the Information Commissioner's refusal of his request for the Penalty Notice to be 'waived', largely on the basis that the infringement was minor and the penalty disproportionate. The Information Commissioner had dismissed this appeal on the basis that no good ground was shown for waiving the Penalty Notice. **Interpretation of s158(3) Data Protection Act 2018** In the course of the appeal, an issue of interpretation arose – namely whether the size of the penalty imposed by the Information Commissioner was lawful in light of the wording of s158(3) DPA 2018. S158(3) DPA 2018 states that, in the context of a fixed penalty for non-compliance with the charges regulations: *The maximum amount that may be specified is 150% of the highest charge payable by a controller in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.* Under s158(1) DPA 2018, the Information Commissioner is obliged to publish a document specifying the size of penalties to be imposed for failure to comply with the charges regulations. In compliance with this requirement Information Commissioner has published a 'Regulatory

Date	Description
	Action policy' ('RAP') where the Information Commissioner sets out the fixed penalties applicable to a failure to pay a data protection fee: *Certain legislation provides for set penalties to be applied for failing to meet specific obligations (for example, a failure to pay the relevant fee to the ICO). Where those provisions apply, we will levy those penalties in accordance with the law. For the purposes of section 155 of the DPA, the fixed penalty payable by a controller for any type of failure to pay a data protection fee in accordance with the Data Protection (Charges and Information) Regulations 2018, are [sic]:* *(a) tier 1 (micro organisations), is £400;* *(b) tier 2 (small and medium organisations), is £600;* *(c) tier 3 (large organisations), is £4,000.* *We reserve the right to increase this amount up to a statutory maximum of £4,350 for data controllers in respect of a failure to provide the ICO with sufficient information to determine the appropriate fee/exemption, depending on aggravating factors (for example, a failure to engage or co-operate with the ICO).* The 'statutory maximum' of £4,350 referred to in the final paragraph of the extract represents 150% of the current tier 3 data protection fee (£2,900). A question arose over whether the limit imposed by s158(3) DPA 2018 was intended to be set at 150% of the annual data protection fee applicable to the controller in question (the view taken by Dr Siddiqui) or at 150% of the highest of the 3 charging tiers (the view taken by the Information Commissioner). If Dr Siddiqui's view was correct, then the maximum penalty which could have been imposed on Dr Siddiqui by the Information Commissioner would have been £60, rather than the £400 imposed by the Information Commissioner. **The Tribunal's Findings** The Tribunal dismissed Dr Siddiqui's appeal. The Tribunal found that, although the legislation could have been more clearly formulated, the Information Commissioner's interpretation of s158(3) is correct, s158(3) was not contravened by the imposition of a £400 penalty on Dr Siddiqui, and Dr Siddiqui had not demonstrated a reasonable excuse for failure to pay the data protection fee. The Tribunal's reasoning was as follows: • The language of s158(3) sets a single limit for all data controllers through use of the indefinite article ("a" data controller rather than "the" data controller) and reference to the "highest charge". The scope of the Tribunal's inquiry did not extend to assessing any apparent irrationality or unreasonableness of the penalties specified by the Information Commissioner in the RAP. • It was unlikely that Parliament intended to limit the penalties for failure to pay the tier 1 or tier 2 data protection fee at such low levels (£60 and £90, respectively, which the Tribunal noted would be similar to the level of fines imposed for parking or minor traffic offences). This would not have been consistent with Parliament's intention to create an effective regime for enforcing the data controller charges requirement. • The statutory construction principle against 'doubtful penalisation' (that a person should not be subjected to a detriment unless

Date	Description
	imposed by clear words), as s158 is penal legislation and must be interpreted strictly and the principle is outweighed by the other factors establishing the intention behind s158. The Tribunal's starting point regarding Dr Siddiqui's appeal against the Penalty Notice was to establish whether Dr Siddiqui demonstrates a reasonable excuse for his default (Farrow & Ball v Information Commissioner (EA/2018/0269)). Dr Siddiqui had not put forward any excuse for failure to comply with his duty to pay the charge, despite the reminder he received in the Information Commissioner's Letter of Intent, and had not asserted that the penalty would expose him to any real hardship. The Tribunal stated that, in any event, there is no power for the Information Commissioner to impose a lesser penalty or for the Tribunal to reduce the penalty imposed by the Information Commissioner. The First Tier Tribunal Decision is available here.
27 November	**Hall And Hanley Ltd v Financial Conduct Authority (Rev 1) [2019] UKFTT CMS-2019-0001 (GRC) - due diligence recommendations for electronic marketing when relying on indirect consent** Hall & Hanley ('H&H') is a claims management service that manages PPI claims on behalf of its customers. The Claims Management Regulator ('CMR', the regulator which has now been replaced by the FCA) determined that H&H had failed to conduct sufficient due diligence on various companies sending electronic marketing on its behalf to consumers over a number of years, and subsequently electronic messages were sent to consumers without the proper consents in place, in breach of regulation 22 of the Privacy and Electronic Communications Regulations ('PECR'). As a result, in March 2019, the CMR issued a fine of £91,000 which H&H subsequently appealed. This fine was upheld by Judge Herrington in the First Tier Tribunal (FTT) on 27 November 2019 and the appeal was dismissed. The FTT decision sets out the importance of due diligence when using personal data obtained by third party suppliers for electronic marketing and provides some practical guidance on reasonable steps to take. In addition to the CMR fine, H&H were also given a £120,000 fine by the ICO in May 2019 for sending 3.5 million text messages without the correct consent in breach of PECR rules. See our May 2019 newsletter for further information. In Judge Herrington's decision he set out some recommendations (the 'Recommendations') for other claims management firms with similar business models to follow to ensure sufficient due diligence when using personal data for electronic marketing collected by a third party. Despite these Recommendations being described as being suitable to similar firms to H&H, they are practical ideas that can be used as a starting point for any businesses buying in or using third party personal data for electronic marketing. The Recommendations on 'reasonable' steps to take are as follows and should be carried out before the data is purchased: 1. Ask the supplier for the source(s) of the data and the privacy notice covering the generation of these leads. The business should check the privacy notice for whether consumers would have had sufficient details of what they are consenting to. Would a customer have expected to have been contacted about that service and in that way? In H&H's case this was SMS marketing about PPI claims; 2. Review the messages used by a third party to obtain opt-in consent and the consent mechanism, and whether these are consistent with the privacy notice;

Date	Description
	3. Review an 'appropriate' sample of the data to be supplied prior to purchase (and use) to ensure there is sufficient evidence of points one and two above being complied with. H&H had used a sample size of 0.5% of the data obtained which the court deemed appropriate and a reasonable enough step to give a 'reasonable indication' of whether 'substantially all of the data purchased will be compliant'. However, on the facts of the case, H&H had actually failed to check any samples *before* they actually used the personal data which made the size of the sample irrelevant, so however large the sample was it was never going to be 'sufficient'. Judge Herrington described it as 'shutting the stable door after the horse has bolted'. Therefore, carrying out these checks retrospectively meant they had no practical benefit and were not appropriate, despite being argued by H&H as an 'industry practice'. Judge Herrington also went onto to say that just because this was widely done in an industry does not mean it will necessarily be compliant with the law, as was the case here; 4. Seek a warranty from the supplier to place a sufficient degree of responsibility on their part and ensure collection and supply is compliant with the law. There was discussion of the 'obligations' of each person in the chain of responsibility for supplying the data; contractual assurances alone are not enough to shift responsibility and are not a substitute for a purchaser carrying out their own due diligence; and 5. Seek guidance from the regulator on 'points of difficulty' or where clarification of the regulator's approach or on a point of policy is required. On the facts of the case H&H asked the regulator a lot of questions, including which 'checks' they needed to do. H&H had tried to pass a lot of decisions onto the CMR in order to 'shift' compliance responsibility onto the regulator. The court said that the regulator does not have a duty to prescribe precise steps to a company like H&H to ensure compliance. H&H could instead have asked the regulator for views on a proposed approach, for example. The regulator is not there to be a 'substitute' for a firm making decisions. This also included decisions that could have been informed by widely available guidance and also in letters and audit recommendations H&H had received previously. Additionally, there was some discussion on the validity of consent. Judge Herrington suggested that a company should adopt a policy on when consent becomes 'stale' and document the reasons for this decision. He stressed that this will depend on the circumstances but as the scope of indirect consent is 'carefully circumscribed' it will not be reasonable to rely on consent obtained a long time before it is relied upon. Another point on due diligence was basic items, like checking a company's ICO registration as a way to determine their compliance and also recording each due diligence step. A link to the FTT case can be found here

EU and Council of Europe

EDPB

Date	Description
15 November	**EDPB Publishes Finalised Guidelines on Territorial Scope** On 15 November 2019, the European Data Protection Board ('EDPB') published its finalized Guidelines on the Territorial Scope of the GDPR. The GDPR applies to: • European Economic Area ('EEA') established organizations (pursuant to Article 3(1) GDPR); and • on a long-arm, extraterritorial basis to organizations which are not established in the EEA but which offer to sell goods or services to or who monitor individuals in the EEA (pursuant to Article 3(2) GDPR). **The key updates introduced to the guidelines include:** **Article 3(1):** • The EDPB emphasises that Article 3 GDPR is designed to determine whether a specific processing activity - rather than an entity - falls within the scope of GDPR. The EDPB therefore stresses that while some of an organisation's processing activities may be caught by the GDPR, other processing activities may not be. • Where a controller's activities fall within Article 3(1) GDPR, this processing will not fall outside the scope of the GDPR simply because the controller instructs a processor in a non-EEA jurisdiction. The place of processing is not relevant in determining whether or not the processing carried out '*in the context of the activities of an EU establishment*', falls within the scope of the GDPR. **Article 3(2):** • The EDPB re-iterates through a number of examples that for the offer of goods or services under Article 3(2) GDPR to apply, the provision of services must be intentionally targeting individuals in the EEA: inadvertent or incidental provision of services to an individual who happens to be in the EEA is not enough. • Where a data processor is not established in the EEA only the processing which is *related* to the activities of the controller in targeting data subjects in the EEA will fall within the scope of the GDPR under Article 3(2). However, the bar for this is low, to take an example, according to the EDPB, if a controller caught by the 'targeting' criterion under Article 3(2) GDPR procures a non-EEA based data processor to host this data then the processing activity by the non-EEA based processor also falls within Article 3(2).

	• It is not clear from the GDPR whether non-EEA organisations that offer goods and services to data subjects because of their role working for a business in the EEA, as opposed to those that offer goods and services to consumers, fall within the scope of Article 3(2)(a). The revised EDPB Guidelines, unhelpfully, still offer no clarity on this point. **EEA Representatives:** • The EDPB provides welcome clarity on the liability of EEA representatives. The GDPR does not, according to the EDPB, establish substitutive liability for representatives: EEA representatives can only be held directly liable for their direct obligations under the GDPR i.e. - Article 30 and Article 58(1) GDPR - and not for the wider obligations of the data controller or data processor. **Interaction with International Transfer:** • The EDPB notes that they are continuing to assess the interplay between the territorial scope rules of the GDPR and the provisions on international transfer, and further guidance may be issued on this front in the future. You can find our full article on these guidelines here: https://www.twobirds.com/en/news/articles/2019/global/edpb-publishes-finalised-guidelines-on-territorial-scope
20 November	**EDPB Publishes Guidelines on Data Protection by Design and by Default** On 20 November 2019, the European Data Protection Board ("**EDPB**") published its draft guidelines on the principles of Data Protection by Design and Default (the "**Guidelines**") under Article 25 of the EU General Data Protection Regulation ("**GDPR**"). They give general guidance on the interpretation of the obligations of data protection by design and by default. In addition to covering these principles, the Guidelines also cover certification mechanisms for demonstrating compliance with Article 25 GDPR and enforcement by supervisory authorities. You can find our full article on these guidelines here: https://www.twobirds.com/en/news/articles/2019/global/edpb-publishes-guidelines-on-data-protection-by-design-and-by-default
2 and 3December	**EDPB 16th Plenary Session** On 2 and 3 December 2019, the EDPB held its 16th Plenary Session. During this session: 1. The EDPB adopted it Opinion (17/2019) on the ICO's draft accreditation requirements for a 'code of conduct monitoring body' pursuant to Article 41 GDPR. The overarching objective of the Opinion is to ensure that EEA supervisory authorities apply accreditation requirements for such bodies consistently. In proposing changes to the ICO's proposed requirements, the Opinion provide insight into how other Member States should draft their requirements, including: - addressing the Article 41 (2) GDPR criteria and EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under the GDPR; - periodically reassessing the requirements. The ICO proposed that such requirements would be valid for a period of 5 years. The EDPB did not challenge this length of time but requested that the ICO specifies what happens after the expiry of that period; - Expressing accreditation requirements in 'shall' terms as opposed to 'should' terms; and

- Ensuring the requirements describe the penalties and corrective measures which the monitoring body may impose for breach of the codes.

2. The EDPB adopted its response to a request from the Body of European Regulators for Electronic Communication ("**BEREC**") for guidance on how certain terminology relating to traffic management would be interpreted in the field of data protection and privacy. This was to assist BEREC in the revision of its guidelines on the net neutrality rules. In the letter, the EDPB raises concerns regarding the processing of domain names and URLs for the purposes of traffic management and billing (zero-rating offers).

3. The EDPB adopted draft guidelines on the 'Criteria of the Right to be Forgotten in the search engine cases under the GDPR' ("**Guidelines**"). The Guidelines update earlier guidance from the Article 29 Working Party on the implementation of the CJEU's judgement in Case C-131/12 (the *Costeja* case).

CJEU cases

Date	Description
11 December	**How legitimate is your CCTV?** On 11th December 2019, the Court of Justice of the European Union ("CJEU") rendered its decision in Case C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* on conditions under which the processing of personal data by way of CCTV may be based on legitimate interests (available here). Following a suite of unsuccessful measures taken by a co-owners' association to prevent vandalism and burglaries in a block of flats, the association made the decision to install three CCTV cameras in the common parts of the building. One resident – TK – objected to this on the grounds that it constituted an infringement of the right to respect for private life. The referring Romanian court asked the CJEU to determine whether national law – which permitted use of video surveillance to ensure the safety and protection of individuals, property and valuables without consent – was compatible with the Data Protection Directive and the EU Charter of Fundamental Rights and Freedoms, and whether a controller's legitimate interests to install CCTV cameras is necessary and proportionate to the purposes pursued. Recapping the three cumulative conditions for legitimate interest to be valid – namely, (1) the pursuit of a legitimate interest, (2) the need to process personal data for the purposes of said legitimate interest, and (3) that the fundamental rights and freedoms of the individual do not override said legitimate interest [40] – the CJEU went on to determine whether the conditions were met in the case. In respect of the first condition, the CJEU held that the interests of the controller must be "present and effective" as at the date of the processing and "must not be hypothetical at that date". The CJEU stressed, however, that it was not necessary to show that the safety of property and individuals was previously compromised [44]. For the second condition, the CJEU referred back to its decision in *Rigas* (Case C-13/16), that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. This means that the purposes pursued by the controller cannot reasonably be as effectively achieved by other means that are less restrictive of the fundamental rights and freedoms of data subjects [46–47] and must also be examined in conjunction with the data minimisation principle [48]. This balancing exercise must be carried out on a case-by-case basis and cannot be pre-empted by Member State law [53]. In this context, the Commission's arguments to the CJEU advanced the need for the controller to examine how the video surveillance would operate in practice, such as only at night or outside normal working hours [51].The Commission's arguments were offered as an example for the controller to consider rather than forming the *ratio* of the CJEU's decision. Finally for the third condition, the CJEU held that the seriousness of the infringement of the data subject's rights and freedoms is an essential component to the balancing test. Practically, this requires that the controller to balance the aim of the association to protect the

	property, health and lives of its inhabitants against the sensitivity of the data, the nature and specific methods of processing, the number of persons having access to the data, and the reasonable expectations of the data subject [55–59].
19 December	**Opinion of Advocate General upholds standard contractual clauses in Schrems 2** On 19th December 2019, Advocate General Saugmandsgaard OE gave his Opinion in *Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems and interveners (C-311/18)* (Schrems 2). He concluded that nothing in the analysis he had carried out led him to conclude that standard contractual clauses should be invalidated. The referring Irish court had also asked questions about the validity of the Privacy Shield decision. Here, the Advocate General concluded that it was not necessary for the Court of Justice of the EU to answer this question. The Advocate General did, however, conclude that the standard contractual clauses placed responsibility on supervisory authorities and on data exporters. The responsibility placed on the supervisory authority is to suspend data flows which rely on the clause, if the authority considers that the law to which the data importer is subject imposes requirements on the importer which go beyond restrictions necessary in a democratic society [140]. The Advocate General suggested that the data exporter has an obligation to consider if –given the laws applicable to the importer and the circumstances of the transfer – the clauses will be effective to provide adequate protection. This means examining the nature of the data, including if they are sensitive, the security mechanisms used, any processing of personal data which may be carried out by public authorities in the importing country, the relevant applicable laws and international commitments and the role of any independent data protection authority: the analysis would overlap with the factors which the Commission has to consider when reaching an adequacy decision under art.45 of the GDPR [135]. The Commission relies on expert opinions and takes several years to reach an adequacy decision; it will be difficult for exporters to do the same and this statement is a problematic point in a decision which, in other respects, is helpful for data exporters. This is- of course - not the final decision; that is to be given by the CJEU later this year. The Opinion is the latest stage in the actions by Mr. Max Schrems who, in 2013, filed a complaint with the Irish Data Protection Commission regarding data transfers to the US by Facebook Ireland in reliance on the EU-US safe harbor. That complaint led to the invalidation of the EU-US safe harbor by the CJEU. Following that decision, Facebook sought to rely on standard contractual clauses authorised by Commission Decision 2010/87 to transfer personal data to the US. The Commission decision allows supervisory authorities to suspend transfers of personal data in certain circumstances. Mr Schrems asked the Irish Data Protection Commissioner to suspend the transfer of personal data by Facebook Ireland to the US – again, on the basis that US law and practice in relation to national surveillance meant that there was not adequate protection for EU personal data. Rather than giving such an order, the Irish Data Protection Commissioner asked the Irish court to make a reference to the CJEU asking questions both about the standard contractual clauses the successor to safe harbor, the EU-US Privacy Shield. The Advocate General concluded that it was not necessary to answer the questions on the Privacy Shield and he advised the CJEU not to do so, in part because this was not necessary to allow the referring court to resolve the matter, and in part, because he considered it preferable for any question as to the validity of the Privacy Shield to be resolved as a result of an express reference on this point, which would allow other interveners to participate, allowing a more thorough and exhaustive consideration [181]. In case the Court preferred to consider the matter, however, the Advocate General did go on to provide comments on the Privacy Shield. He expressed doubts on the following points: • whether US signals intelligence activities could be in accordance with law, as they are not sufficiently foreseeable [266], [271]

- whether surveillance measures based on s.702 FISA and EO 12333 are defined sufficiently clearly and precisely as to prevent risk of abuse [289] and whether the safeguards limit access and use to that which is strictly necessary[292], [297], [301].
- whether the minimum safeguards for secret surveillance, listed by the European Court of Human Rights, would be met [303]
- whether the Ombudsperson regime would provide an effective remedy [339].

Given all of these factors, AG Saugmandsgaard concluded that he had doubts as to the whether the Privacy Shield met the requirements for adequate protection for personal data [342].

AG Saugmandsgaard also considered how laws relating to national security should be taken into account in assessing adequate protection for personal data. National security falls outside the competence of EU law, and the GDPR is inapplicable in this situation (Art.2(2)). However, Art.45(2)(a) expressly requires national security provisions applicable in third countries are taken into account when adequacy is assessed. Facebook Ireland had argued that it would be wholly unjustified if a third country were expected to comply with requirements that did not correspond to obligations applicable to Member States themselves. AG Saugmandsgaard noted that Member States all have commitments under the ECtHR – and that this should be the relevant comparator for assessment of adequacy [207]. AG Saugmandsgaard also noted that the standards under the EU Charter are stricter than those under the ECtHR – and that there are cases pending before both the CJEU and the ECtHR inviting the courts to reconsider previous case law [252].

AG Saugmandsgaard also considered whether the GDPR should apply to an electronic communications service provider which is required by law to make data available to public authorities for purposes of national security – or whether the reservation for areas outside the scope of Union law at Art 2(2) would be applicable. Here AG Saugmandsgaard noted that there were potential divergent approaches between the CJEU PNR, Tele2 Sverige and Ministerio Fiscal cases (the first suggesting that this would be seen as a national security matter, where GDPR would not apply; the latter suggesting that GDPR would be applicable) [214], [215]. The Advocate General concluded that the test should not look to the purpose of the processing, but at whether the activities are state activities in the field of national security [220].

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
2 December	Michelle Shipsey	Prosecution	Michelle Shipsey, a former Social Services Support Officer at Dorset County Council, has been sentenced to a 6 month conditional discharge (meaning that unless a further offence is committed within 6 months Mrs Shipsey will not be sentenced for this offence), ordered to pay costs of £700 and a victim surcharge of £20 following prosecution for unlawfully obtaining personal data. Mrs Shipsey had accessed social care records relating to four individuals she knew without any business need to do so. She admitted the offence at Poole Magistrates' Court after an internal investigation.
5 December	Dannyelle Shaw	Prosecution	Dannyelle Shaw, a former Reablement Officer at Walsall Metropolitan Borough Council, has been sentenced to a fine of £450, ordered to pay costs of £364 and a victim surcharge of £45 following prosecution for unlawfully obtaining personal data. Ms Shaw had accessed social care records relating to seven adults and nine children without any business need to do so. She admitted the offence at Wolverhampton Magistrates' Court after an internal investigation.
20 December	Doorstep Dispensaree Ltd	Enforcement notices & monetary penalties	Doorstep Dispensaree Ltd ('DD') was issued with a monetary penalty notice of £275,000 for failing to ensure the security of special category data. DD had stored approximately 500,000 documents containing names, addresses, medical information and prescriptions in unlocked containers at the back of its premises. The ICO conducted an investigation after being alerted to the breach by another regulator. After refusing to answer the ICO's questions the ICO issued an information notice. DD appealed this but was unsuccessful. After being provided with some information, the ICO went on to issue an enforcement notice, a notice of intent (for a proposed penalty of £400,000) and finally the monetary penalty of £275,000.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			Contraventions of GDPR • No protection from unauthorised or unlawful processing by third parties (unlocked containers in a yard accessible by the public). • No protection against accidental loss, destruction or damage (some documents were water damaged from exposure to the elements). • No appropriate technical or organisational measures (most policies dated from 2015 or were templates clearly produced after the breach). • No retention policy or reason for retaining (some documents dated from 2016). • DD's privacy notice did not contain all of the information required by Article 13 and/or 14 of the GDPR. • The ICO considered the breaches to be serious, negligent and repeated. Enforcement Notice The enforcement notice requires DD to: • Update all policies to ensure compliance with data protection legislation. • Appoint an "Information Governance Lead" or DPOO. • Provide mandatory data protection training to all staff within 6 months and hold refresher training. • Update the privacy notice for compliance with Articles 13 and 14 of the GDPR.
	DSG Retail Limited	Monetary Penalty	The ICO has fined DSG Retail Limited £500,000 under the Data Protection Act 2018 after a point of sale computer system was compromised as a result of a cyber-attack, that took place between July 2017 – April 2018, affecting at least 14 million people, and included payment card details. In issuing this monetary penalty for breaching security, the ICO highlighted concerns with the security measures which had been in place. Its concerns about the lack of commonplace security measures including: • Insufficient network segregation of systems from wider DSG corporate network • No local firewall • Inadequate approach to software patching

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			• No regular vulnerability scanning • Failure to correctly manage application whitelisting across Pos terminals • No effective system to monitor & log incidence or manage the security of its domain administration account • Use of outdated software systems • Pos system did not support point to point encryption • Failure to implement standard guides based on industry good practise The fine (which was the maximum possible under the DPA 1998) recognises the seriousness of the inadequacies in the security system, the number of affected individuals, the length of time the cyber-attack went on undetected and its status as a large nationwide retailer. The 110 also took into account, as an aggravating factor, a previous monetary penalty issued against another Dixon's subsidiary (Carphone Warehouse) in January 2018 for similar security breaches.

Information Tribunal Decisions

Fine for unsolicited telemarketing increased on appeal

In January 2019, the ICO issued a £80,000 fine to Alistar Green Legal Services (AGLS) for making unsolicited marketing calls to numbers registered with the telephone preference service (TPS), and imposed an enforcement notice requiring the company to stop making unsolicited marketing calls. The company appealed but the First-Tier Tribunal dismissed the appeal and increased the penalty by an additional £10,000.

The initial fine was based on complaints received both by the TPS and by the ICO, by individuals registered on the TPS who were receiving repeated marketing calls from AGLS. The fine was imposed on the basis of the seriousness of the breaches (e.g. failure to document consent, absence of a TPS licence).

AGLS's appeal lead to a further review of the evidence, which indicated that the scale of non-compliance and the number of complaints was larger than what the ICO had initially realised. It was also discovered that the director of AGLS had previously been the director of a company which had committed similar breaches.

The Tribunal increased the fine to reflect these issues. For more information click here.