Bird & Bird

UK & EU Data Protection Bulletin: February 2019

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
30 January	**ICO Regulatory Sandbox: Discussion Paper and Intention to Apply Survey** Further to our recent posts on the ICO regulatory sandbox, the ICO has now published its Sandbox beta phase discussion paper setting out its thoughts on how this might work in practice. The paper sets out the main purposes for the sandbox, (i.e. to support the use of personal data in public-interest-related innovative products, to help develop a shared understanding of compliance in particularly innovative areas, and to support the UK's innovation economy) and explains the test phase for the sandbox (which if successful will then be added to the ICO regulatory tool box. The idea is to involve around 10 organisations (from different sectors) in the test phase who have products or services which address specific data protection challenges central to innovation (such as those dealing with biometrics, IoT, wearable tech, cloud based products, AI or complex data sharing). The three key threshold eligibility criteria for entry into the sandbox are (i) innovation; (ii) public interest and (ii) data protection maturity and accountability. Successful applicants will sign up to a bespoke plan that will define how the sandbox will work for them and what support the ICO will provide. The sandbox will contain three different mechanisms (Advisory Mechanisms, Adaptive Mechanisms, and Anticipatory Mechanisms) which the ICO can use to support the innovation. In particular, there will be some enforcement comfort against accidental breaches of data protection legislation during the sandbox process provided the organisations are taking appropriate steps to try and comply with data protection legislation. The ICO sandbox team is bound by obligations of confidentiality (but notes that as a public authority, it is subject to FOIA, so it is important that any confidential or commercially sensitive information is highlighted. To the extent that any processing is likely to involve "high risk" processing and require a DPIA, the applicant will need to inform the ICO who will ask for details regarding risk mitigation considerations. The ICO may provide information advice in this regard but there is no formal requirement for the DPIA to be submitted to the ICO unless the risks have not been mitigated. Full details of the sandbox beta phase will be published by the end of March with applications opening in April. To help plan its resources and build the sandbox appropriately, the ICO is launching an 'Intention to apply' survey.
14 January	**ICO publishes proposed strategy for Openness by Design for consultation** The aim of the strategy is to improve public trust in the openness and accountability of public authorities, build confidence in the regulator's ability to identify good and poor practice and take action where necessary, and to help public authorities to improve their standards of openness and transparency.

The strategy's priorities mainly relate to building awareness, supporting transparency and developing international collaboration. Notably the strategy also aims to promote the reform of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) (more below).

The consultation closes on 8 March 2018.

28 January **ICO publishes '*Outsourcing oversight? The case for reforming access to information law*' and lays it before Parliament**

The report has been submitted to the Public Accounts Committee and the Public Administration and Constitutional Affairs Committee for their consideration as part of the ICO's wider strategy for openness by design (see above).

What is the ICO proposing?

1. Greater use of designation orders under section 5 FOIA to bring external suppliers under FOIA. In particular ICO recommends designation orders with respect to: contractors regarding the public functions that they take; and organisations exercising functions of a public nature.

2. Legislative reform of section 3 FOIA to provide greater clarity regarding what information is held on behalf of a public authority in the context of these outsourcing arrangements.

3. Reform the EIR to increase consistency with FOIA, for example including provisions in EIR to allow for designation orders such as those described above.

4. Introduction of a periodic review process to support the progressive expansion of FOIA (a procedure along the lines of that introduced to good effect in Scotland under section 7A FOISA).

5. The Government should conduct a comprehensive review of all proactive disclosure provisions regarding contracting and which affect the public sector. The report criticises the current framework as having failed and attributes this to little monitoring and enforcement.

If adopted, the changes could have a major impact on the applicability of Freedom of Information legislation to transparency obligations of external providers engaged in contracts with public bodies.

January 2019 **ICO refreshes its Guidance on Personal data**

The ICO has refreshed its guidance on the meaning of 'personal data'. The changes are not substantial, but the guidance should be borne in mind by organisations generally, as it includes some useful clarifications and working examples. As a reminder:

- Pseudonymisation does not change the status of data as personal data, although it can reduce the risks to the data subjects and help organisations meet their data protection obligations.

- Organisations should exercise caution when attempting to anonymise personal data (true 'anonymisation' can be difficult to achieve), and the act of anonymising data amounts to processing of personal data.

- The GDPR only applies to information which relates to an identifiable living individual - information about deceased individuals does not amount to 'personal data'.

- Information concerning a 'legal' rather than a 'natural' person is not personal data. Whilst information about a corporate entity (e.g. a limited company) with a separate legal personality does not constitute personal data, the GDPR does apply to personal data relating to individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable and the information relates to them as an individual.

- Types of online identifiers which constitute personal data under Article 30 GDPR include IP addresses; cookie identifiers; and other identifiers such as radio frequency identification (RFID) tags. The ICO extends this list to include: MAC addresses; advertising IDs; pixel tags; account handles; and device fingerprints.

- The fact that an organisation does know an individual's name does not automatically mean that the individual cannot be identified and is therefore not personal data. If the organisation holds any identifier, or a combination of identifiers, this can be sufficient to distinguish that individual from other members of a group.

- When determining whether an individual is indirectly identifiable, organisations should consider the means that are reasonably likely to be used to identify the individual taking into account, for example:
    - the costs and amount of time required for identification;
    - the available technology at the time of the processing; and
    - likely technological developments.

- When assessing whether personal data 'relates' to an individual, the following different meanings of the concept should be considered:
    - the data is about the individual;
    - the data is used to learn, evaluate, treat in a certain way, make a decision about, or influence the status or behaviour of the individual;
    - the data impacts, or has the potential to impact, an individual.

The guidance is available here.

Date	Description
November 2018 to January 2019	The Investigatory Powers Act 2016 (Commencements 9 and 10) Regulations 2018 and (Commencement 11) 2019 have brought into force the following provisions of the Investigatory Powers Act 2016. Summary of the changes:

Date	Reg	Effect	Primary legislation affected
		Commencement 9 (equipment interference warrants)	
Nov	2	Brings into force the power of law enforcement chiefs to decide to issue equipment interference warrants and the function of judicial commissioners to approve those decisions	Ss. 106, 107, 108, 111, 115, 129, 248 Schs. 6 and 8 of the IPA 2016
Dec	3	Brings into force provisions to allow law enforcement chiefs to issue equipment interference warrants	Ss. 106, 117, 123, 124, 125, 128, 231(9), 243, , 248, 271(1), Schs. 8 and 10 IPA 2016 Sch 2 RIPA 2000 Crime and Courts act 2013
Jan	4	Brings into force a prohibition on property interference authorisation applications under s. 93 Police Act 1997 where the purpose of the interference is to obtain communications, private information or equipment data, the applicant considers the conduct constitutes an offence under Ss 1 to 3A Computer Misuse Act 1990 and the conduct can be authorised by an equipment interference warrant.	s. 14 IPA s.93 Police Act 1997

Commencement 10 (appeals)			
Dec	2	Inserts section 67A into the RIPA 2000, which provides for a right of appeal on a point of law against decisions and determinations made by the Investigatory Powers Tribunal.	s. 242 IPA
Commencement 11 (authorisations for obtaining communications data)			
Jan	2	These Regulations bring section 11 (providing for an offence of unlawfully obtaining communications data) and Part 3 of the IPA 2016 (authorisations for obtaining communications data) into force. Certain provisions (for example, paragraph 55 of Schedule 10) are only commenced in relation to the functions commenced in Part 3 of the 2016 Act. This is because Part 1 of Chapter 2 of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act") will remain in force for a period of time after the commencement of Part 3 and associated provisions of the 2016 Act, in order to allow relevant public authorities to transition in an staged way from the processes under the earlier Act to the later Act, particularly in relation to the regime under section 60A (independent authorisation by the Investigatory Powers Commissioner). It is anticipated that Part 1 of Chapter 2 of the 2000 Act will be repealed at the end of 2019.	Ss. 2; 11; 61-68; 229; 243(1)(c) and 243(1)(h) (to the extent that paras (cza) and (czl)(i) are brought into force); 243(1)(i) and 243(2)(a),(b) and (c); Schs. 4 and 5 IPA 2016

13 February The UK Government has now issued Keeling Schedules for the Data Protection Act 2018 and the GDPR which show the changes which will be introduced (in an easy to read form) by the draft Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 in the event of a no deal Brexit: https://www.gov.uk/government/publications/data-protection-law-eu-exit

Date	Description
23 January	***Michael Cooper v National Crime Agency [2019] EWCA Civ 16 (Jan 23 2019)***

This recent Court of Appeal case is interesting as it considers the meaning of the term “necessary” which is a relevant criterion for many of the lawful grounds of processing under the GDPR.

Mr. Cooper had been employed by the predecessor to the National Crime Agency, the Serious Organised Crime Agency ("SOCA"). SOCA required that its staff maintained the highest professional standards of behaviour in and out of work. In April 2012, Mr. Cooper was charged with being drunk and disorderly in a public place and with assaulting police officer. Mr. Cooper reported this to SOCA, as he was required to do. Information about the matter was also shared by the local police force with SOCA in accordance with information sharing agreements. Mr. Cooper was aware of this and did not object to it at the time. Mr. Cooper was subject to disciplinary proceedings, which led to his being dismissed by SOCA. Separately, he was convicted of the offences but, acquitted on appeal. Mr. Cooper had been punched in the same disturbance and he called a medical expert who gave evidence that his behaviour could have been caused by a head injury. The Crown Court acquitted him but, as the Court of Appeal noted, "*this was not a ringing vindication of Mr Cooper. The Court found that Mr Cooper… was certainly disorderly, was uncooperative with the police… [and] was swearing appallingly in a public place…"* [34].

Mr Cooper had been concerned that information obtained during the course of the disciplinary investigation would be used in the subsequent prosecution (as was indeed the case) and that this meant that he would not be able to defend himself properly in the disciplinary investigation. For this (and other reasons) he appealed against his dismissal to the Employment Tribunal and the Employment Appeal Tribunal. He also argued that the data sharing between SOCA and the local police force breached the Data Protection Act 1998 and he brought separate proceedings in this regard. The Court of Appeal considered both the data protection proceedings and the employment proceedings – finding against Mr. Cooper on all of the data protection claims.

In relation to the meaning of "*necessary*", the Court of Appeal approved of the interpretation suggested by the judge at first instance – that it means "*more than desirable but less than indispensable or absolutely necessary"* [89], [90]. The Court also quoted Baroness Hale, in the case of ***South Lanarkshire Council v Scottish Information Commissioner*** [2013] UKSC 55, who suggested that *"in ordinary language we would understand that a measure would not be necessary if the legitimate aim could be achieved by something less"* [91]. In this case, the Court of Appeal concluded that there were legitimate reasons, in accordance with the Data Protection Act 1998, for SOCA to investigate Mr. Cooper's behaviour and it was "necessary" for them to obtain information about the incident from the local police in order to do this [96].

18 January ***Paul Shepherd v The Information Commissioner [2019] EWCA Crim 2***

This case looks at the interpretation of s.55(2) of the Data Protection Act 1998 and considers whether it imposes a legal or evidential burden of proof on a defendant. The ICO also asked the court to provide guidance on the new provisions under s.170 of the Data Protection Act 2018.

Facts:

In March 2018 the Appellant was convicted of three counts of unlawfully obtaining personal data contrary to s.55 of the DPA 1998. He worked for a tenancy management organisation in Islington and disclosed a report of the London Borough of Islington on the organisation's safeguarding of children and vulnerable young people. This report included personal data.

As a result, the appellant was convicted of three counts of unlawfully obtaining personal data contrary to s.55 of the DPA 1998. In the first instance the judge held that s.55(2) of the DPA 2018 imposed a legal burden on the defendant. In front of the Court of Appeal, Paul Shepherd argued that (i) as a matter of statutory construction, subparagraphs (b), (c) and (d) of s.55(2) of the DPA 1998 cast no more than an evidential burden on him, and (ii) if the subsection did impose a legal burden, it is an unjustifiable incursion into the presumption of innocence.

Analysis:

Under the 1998 Act subsection (2) began with the unusual words "*Subsection (1) does not apply to a person who shows…*". The DPA 2018 s.170(2) by contrast uses the more usual wording: "*It is a defence for a person charged with an offence under subsection (1) to prove…*". The court agreed with Mr Shepherd's counsel that this wording in the 1998 Act was deliberate. Mr Shepherd did not have a legal burden to prove that one of these subsections was made out. Instead there was a lower requirement, an evidential burden simply to raise one of these provisions, at which point the Information Commissioner must disprove it, to the criminal standard of proof. The Court of Appeal went on to contrast this with the DPA 2018 [54], quoting paragraph 490 of the *Explanatory Notes* which state:

"…. As worded, the section places a legal burden on the defendant to prove the relevant defences on the balance of probabilities"

Thus, the 1998 Act had a lower threshold for the defendant than does the 2018 Act.

The court concluded:

"…. we agree with the opinion that the new section imposes a legal burden of proof on the defendant. We express no view on whether s.170(2) is compatible with the defendant's art.6 rights."

The full decision can be found here.

30 January ***In Re an application by Lorraine Gallagher for Judicial Review (Northern Ireland)***

***R (on the application of P, G and W) (respondents)* v *Secretary of State for the Home Department and another (appellants)* [2019] UKSC 3**

Criminal disclosures: Supreme Court declares multiple conviction rule incompatible with Article 8 ECHR

In a 4-1 majority decision, the Supreme Court ruled that the multiple conviction rule – whereby the existence of more than one conviction will mean that all convictions, no matter their age or subject matter will be disclosable – is incompatible with Article 8 of the European Convention on Human Rights 1950 ("**ECHR**").

Facts

The respondents to the appeals (Gallagher, P, G and W) were convicted or received cautions or reprimands in respect of relatively minor offending:

- Gallagher: In 1996, Mrs Gallagher was convicted and fined £10 for one count of driving without wearing a seatbelt and £25 each for four counts of carrying a child under fourteen without a seatbelt. In 1998, she was again convicted and fined £40 each for two counts of the latter. She has no other convictions. In 2013 she applied for a position at a day centre for adults with learning difficulties which required an Enhanced Criminal Disclosure.

- P: In 1999, P, while homeless and suffering from undiagnosed schizophrenia, received a caution for the theft of a sandwich and, in the same year, convicted of the theft of a book worth 99p and failing to surrender to the bail granted to her after her arrest for that offence. Now qualified to work as a teaching assistant, P has not been able to find employment as a result of her disclosure obligation.

- G: In 2006, aged 13, G was arrested for engaging in sexual activity with two younger boys. The police record indicates that the sexual activity was consensual and "seems to have been in the form of 'dares' ... and is believed to have been a case of sexual curiosity and experimentation on the part of all three boys." G was given a reprimand in September 2006. In 2011, when working as a library assistant in a local college, G was required to apply for an Enhanced Criminal Disclosure as his work involved contact with children. The police proposed to disclose the reprimand with an account of the mitigation. G withdrew his application and lost his job.

- W: In 1982, aged 16, W was involved in a fight with a number of boys on his way home from school. He was convicted of assault occasioning actual bodily harm and received a conditional discharge. He has no other convictions. In 2013, aged 47, he began a course to obtain a certificate to teach English as a second language. He believes that his chances of obtaining teaching employment will be prejudiced by the need to obtain a criminal certificate for a job as a teacher.

In all four of the appeals, the respondents challenged the two related statutory disclosures scheme as being incompatible with Article 8 of the ECHR.

Statutory disclosure schemes (the "schemes")

The United Kingdom has two schemes for disclosing criminal conviction data, which operate in parallel.

The first scheme is under the Rehabilitation of Offenders Act 1974 for England & Wales and the equivalent legislation is Scotland and Northern Ireland. Under this scheme, there is no duty for an ex-offender to disclose information concerning his or her previous conviction where such convictions and cautions have become "spent", i.e. that the rehabilitation period for the conviction has expired. The ex-offender is for all legal purposes treated as a person who has not committed, charged, prosecuted or convicted of the offence. However, for thirteen specified purposes enumerated in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (and equivalent legislation in Scotland and Northern Ireland), the right of the ex-offender not to disclose a conviction or caution does not apply. Such specified purposes include assignment to work with children or vulnerable adults.

The second scheme is under the Police Act 1997, which governs disclosure by the Disclosure and Barring Service ("**DBS**") in England & Wales, Disclosure Scotland in Scotland, and Access NI in Northern Ireland. Sections 113A and 113B deal with Standard Disclosure and Enhanced Disclosures, respectively, which create a system of mandatory disclosures of all convictions and cautions on a person's record if certain eligibility criteria are satisfied.

Both schemes were modified in 2014 to limit the disclosure of certain convictions and cautions to four main categories: (1) convictions and cautions for any of a list of more serious offences; (2) convictions which resulted in a custodial sentence; (3) "unspent" convictions; and (4) all convictions and cautions where the person has more than one conviction. It is category (4) that is at issue in the present case.

Reasoning of Supreme Court

Giving the main judgment, Lord Sumption acknowledged that Article 8 ECHR was triggered and so it fell to the court to assess any interference with the right to respect for private and family life to be "in accordance with the law" (the "legality test") and "necessary in a democratic society" (the "proportionality test").

Tracing the case law of the Strasbourg Court, particularly the decision in *MM v United Kingdom* (App. No. 24029/07), Lord Sumption considered that the legality test was satisfied. Both schemes were sufficiently accessible and foreseeable as the rules governing disclosure of criminal conviction data under them are highly prescriptive, mandatory and leave no discretion, thereby permitting an assessment of their proportionality. On this last point, Lord Kerr disagreed, considering instead that the schemes' safeguards are not sufficient to guarantee against the risk of abuse or arbitrariness.

With regard to the proportionality test, Lord Sumption considered that legislation for disclosure by reference to pre-defined categories of offence, offender or sentence is justified and that the categories in respect of the schemes are proportionate However, there are two exceptions. The first exception is that the multiple conviction rule does not achieve its purpose of identifying serial offenders as it applies irrespective of the nature, similarity and frequency and the intervals between offences. In Lord Sumption's view "*a rule whose impact on individuals is ...capricious cannot be regarded as a necessary or proportionate way of disclosing to potential employers criminal records indicating a propensity to offend*." The second exception is that warning and reprimands for young offenders, which are designed to be instructive and avoid damaging effects later in life, should be excluded from the disclosable categories under the schemes. Speaking *obiter*, Lord Sumption considered that youth cautions should also be excluded in the same way.

Analysis

Despite the filtering rules introduced in 2014 by the government following the landmark case of *R (T) v Chief Constable of Greater Manchester Police* [2014] UKSC 35 to draw ever brighter lines between competing public interests – namely the rehabilitation of ex-offenders and the protection of members of the public against individuals who might do them harm – marginal cases such as those in the present decision continue to question the ongoing compatibility of the schemes against Article 8 ECHR.

The decision of the Supreme Court is a welcome one in restoring greater balance between the competing public interests mentioned above. However, both the majority and dissenting judgments recognise that the schemes are designed to place employers at the heart of determining the relevance of a conviction for a given role, which may not necessarily be in the best interest of a candidate who is an ex-offender. Conceding this point, Lord Sumption explained that "*[r]ealistically, it must be assumed that some employers will take the line of least risk, and decline to employ ex-offenders on principle, especially if there is an alternative candidate without a criminal record*." Likewise, Lady Hale accepted that "*employers are likely to take a precautionary approach if they have more applicants than posts available*."

Whereas the majority opined that employers "*must be trusted to exercise…judgment responsibly*" when making a final recruitment decision, in his dissenting opinion, Lord Kerr took the view that the four cases before the court "*represent the significant impact that the current policy choice has on a potentially substantial number of individuals*" and that such cases "*should not be consigned to the category of unfortunate casualties at the margins*."

Importance to businesses

Irrespective of where the line is drawn, this case is a reminder for employers investigating an applicant's criminal history that a heavy burden sits on the shoulders of the recruiter who must consider the relevance of a conviction to the role to be filled. The Supreme Court's decision will certainly lighten that burden by removing youth warnings and reprimands and, more helpfully, minor multiple offences from Standard and Enhanced Disclosure Certificates, thereby reducing the risk of a recruiter considering irrelevant convictions which would otherwise involve the excessive collection and use of personal data under data protection law.

From an employment law perspective, although a recruitment decision not to make an offer of employment based on unspent criminal convictions are unlikely to lead to employment claims, guidance – including those from NACRO and Unlock – as well as the case law suggests that when exercising discretion, employers should consider how relevant unspent convictions are to a specific role.

Furthermore, in their respective codes of practice, the DBS, Disclosure Scotland and Access NI require employers obtaining disclosure certificates as part of the recruitment process to have a written policy on the recruitment of ex-offenders, a copy of which must be provided to all applicants for positions where a disclosure will be requested. Such a policy will set out the employer's obligation to treat ex-offenders fairly and not to discriminate because of a conviction or other information revealed.

The full decision can be found here.

18 January

The Queen (on the application of Maha El Gizouli) v the Secretary of State for the Home Department ([2019] EWHC 60 Admin)

Is it lawful under the DPA 2018 for the Home Secretary to assist the US in bringing prosecutions against ISIS terrorists which may lead to the death penalty?

Facts

The claimant, Ms El Gizouli, is the Mother of a British national, Mr El Sheikh, who fought in, and is detained in, Syria and who, according to the Director of National Security in the Home Office, is believed to be a member of a group of terrorists associated with crimes committed during the conflict in Syria. The UK concluded that there was insufficient evidence to charge Mr El Sheikh. However, the US, did wish to charge Mr El Sheikh and asked the UK for information which would be useful for its investigations. In such cases, the UK usually seeks an assurance that information which the UK provides will not be used in proceedings where the recipient seeks the death penalty. In this case, the Home Secretary took the decision not to require such a commitment: this conclusion was reached after consideration that such a request would be turned down (and that even to request such a commitment could be counter-productive with current senior US leaders), and could also lead the US to detain Mr El Sheikh in Guantanamo Bay instead of trying him in a civilian court. Ms El Gizouli argued that the disclosure of information to the US was unlawful (on various grounds, including breach of the DPA 2018) and that any future disclosure should be prohibited. Ms El Gizouli failed on all grounds. So far as the DPA 2018 was concerned, the court noted that the government parties had given no consideration to the DPA 2018 before disclosing the information, but still considered the disclosure to be lawful.

Analysis

The main argument advanced by Ms El Gizouli was that Part 3 of the DPA 2018 must be interpreted in accordance with the Charter of Fundamental Rights of the European Union and, as this prohibits the death penalty, any processing which could lead to the death penalty must automatically be unfair and unlawful. The court rejected this. Although the Law Enforcement Directive refers to the EU Charter, measures which relate to freedom, security and justice only apply if the UK opts-in to them – so that the Law Enforcement Directive is relevant to some, but not all, processing of personal data for law enforcement purposes in the UK. In this case, disclosures of personal data by the UK to the US did not take place pursuant to any EU criminal justice measure and was outside the scope of EU law; the EU Charter therefore has no relevance to such processing. The court went on to note that the EU Charter is limited in its territorial scope: because Mr El Sheikh was in Syria, even if the EU Charter was relevant to interpretation of the DPA 2018, Mr El Sheikh would not be able to rely on the EU Charter.

<u>The case also considered a number of other provisions in the DPA 2018:</u>

- the obligation in the first data protection principle that processing must be "*fair*" is primarily concerned with transparency and openness: the fact that the US would use the information in capital proceedings would not make the disclosure "*unfair*";

- the obligation for processing to be "lawful" meant that the processing had to authorised by statute, common law or royal prerogative: failure to keep records prescribed by the DPA 2018 did not result in "unlawful" processing for purposes of the first data protection principle. Further, where the DPA 2018 required documentation to be kept, documentation kept for other purposes could meet this requirement, it did not require a "*bespoke set of documents*";

- information about acts of extreme religious violence would not be protected as special category data: *"these provisions* should not be interpreted to give a heightened degree of protection in respect of terrorist offences which advance *"a political, religious, racial or ideological cause" compared with non-ideologically driven crimes";*

- the disclosure by the police to prosecuting authorities overseas was not processing for an *"incompatible purpose";*

- the transfer of personal data to the US could meet the provisions in the Part 3 (albeit that notice had not been given to the Commissioner, as it should have been under s.75(1)(3)) either on the basis (1) that, as a matter of fact, there were appropriate safeguards in place; or (2) because there were "special circumstances" as provided for in s.76 – namely that the transfer was necessary in an individual case for law enforcement or legal purposes (s.76(1)(d) or (e)); and

- lastly, the court also concluded that, when considering if there were *"appropriate safeguards"* in place, what mattered was whether such safeguards were in substance in place – there was no requirement for the party transferring the data to give express consideration to this before the transfer.

The full decision can be found here**.**

24 January

Doorstep Dispensaree Limited v ICO (First Tier Tribunal, 24 January 2019)

This case concerns an appeal against an Information Notice which was issued against Doorstep Dispensaree Ltd on 25 October 2018 under the new Data Protection Act 2018. The ICO is currently investigating the company's compliance with GDPR following a report received from the Medicines and Healthcare Products Regulatory Agency (MHRA) and issued an information notice against the company after the company had failed to informally respond to the ICO's request for further information.

The Company appealed the information notice on two grounds: (i) that it was void for breach of S143 (6) Data Protection Act 2018 which provides that a person may not be compelled to incriminate themselves arguing that there were criminal investigations into the company by the MHRA and (ii) even if the information notice was not void, certain questions within in which would have the effect of compelling self incrimination should be removed.

The Tribunal found that an Information Notice does not require a person to provide information which would expose them to criminal proceedings but the Data Protection Act 2018 does not say that the ICO cannot serve an Information Notice in these circumstances nor that it is invalid if she does so. Moreover it was held that the company had provided very little evidence about the scope of the criminal investigation and thus the scope for self incrimination and that therefore the information requested was reasonably required for the ICO's investigations into GDPR compliance (which was entirely separate to the MHRA's investigation). The appeal was therefore dismissed.

For more see here.

6 February

Department for Business, Energy & Industrial Strategy publishes Brexit guidance for business

The Department for Business, Energy & Industrial Strategy ('**BEIS**') has published brief guidance for businesses on using personal data after the UK leaves the EU (with, or without, a deal).

The guidance predominantly focusses on the implications for transfers of personal data to and from the EU, highlighting that there will continue to be a free flow of data from the UK to the EU, and that the European Commission plans to reach an adequacy decision permitting transfers of personal data from the EU to the UK. In the context of a no-deal Brexit, the guidance clarifies that the BEIS would like the European Commission to adopt an adequacy decision in respect of the UK as soon as possible, but does not expect this to be in place by the exit date of 29 March 2019.

The guidance reiterates the six preparatory steps that the ICO has suggested businesses take in the event of a no-deal Brexit:

1. Continue to apply GDPR standards and follow current ICO guidance. Your Data Protection Officer can continue in the same role for both the UK and Europe.
2. Identify where you receive data into the UK from the European Economic Area (EEA). Consult ICO guidance and think about what GDPR safeguards you can put in place to ensure that data can continue to flow once we are outside the EU. Standard contractual clauses are one such GDPR safeguard, the ICO have produced an interactive tool to help businesses understand and complete standard contractual clauses.
3. Identify where you transfer data from the UK to any country outside the UK, as these will fall under new UK transfer and documentation provisions.
4. Review your structure, processing operations and data flows to assess how the UK's exit from the EU will affect the data protection regimes that apply to you.
5. Review your privacy information and your internal documentation to identify any details that will need updating when the UK leaves the EU.
6. Inform your organisation. Make sure that key people in your organisation are aware of these key issues. Include these steps in any planning for leaving the EU, and keep up to date with the latest information and guidance.

The guidance is available here.

Europe

EDPB

Date	Description
22 January	**EDPB Issues Report on the EU-U.S. Privacy Shield Second Annual Review** Following the EU-U.S. Privacy Shield's successful completion of a Second Annual Review by the European Commission at the end of last year, the European Data Protection Board ("**EDPB**") issued a report on the functioning of the Framework. The EDPB report has no legal effect, but may be taken into consideration by the European Commission in the next Annual Review. In addition, with challenges to the Privacy Shield framework currently winding through the courts, the EDPB's opinion on the Framework's functioning could indirectly affect its continued viability. On both the commercial and government access elements of the Framework, the EDPB report highlights the positive steps taken, while at the same time finding that some key concerns remain unaddressed. **a) Commercial aspects** On the commercial side, the EDPB praised efforts by the U.S. Department of Commerce ("**DoC**") to issue further guidance, improve the certification process, and, in combination with the Federal Trade Commission ("**FTC**"), to take enforcement against false claims of certification. However, the EDPB highlighted several areas of continued concern: • Substantive oversight: while DoC's checks have focused on whether certifications are genuine and/or kept up to date, there have not been any investigations into whether companies are actually complying with the Privacy Shield Principles. • Onward transfers: the EDPB highlighted that DoC should do more to ensure that certified companies are complying with onward transfer requirements when they share personal data with other organisations outside the EEA – including by asking certified companies to share their onward transfer contracts. • HR data: the EDPB report indicated that ambiguities in the interpretation of the HR provisions of Privacy Shield left the protections for such personal data uncertain. • Certification process: the EDPB noted that some of the entries on the Privacy Shield list are outdated.

b) Government access

On the government access side, the EDPB report welcomed the appointment of new members to the Privacy and Civil Liberties Oversight Board and the publication of clarifications on the scope of certain protections afforded by Presidential Policy Directive 28. However, the EDPB also reiterated concerns that U.S. statutory protections were not sufficient to prevent massive and indiscriminate surveillance. In addition, the EDPB took issue with the fact that a permanent Ombudsperson to monitor compliance had yet to be appointed.

January

EDPB release opinions on Liechtenstein and Norway's DPIA lists

Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) was adopted by the EDPB on 23 January 2019. The EDPB requests the Norwegian Supervisory Authority amend its list by stating that the types of processing listed are the ones that are likely to present high risks for the rights and freedom of data subjects. The full version of the Opinion can be found here.

January

The EDPB adopts opinion concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the GDPR.

The opinion was adopted in response to the EC's request for consultation submitted in October last year. It begins by stating that in the context of clinical trials being conducted in Europe, both legislations will apply simultaneously and that CTR constitutes a sectoral law containing specific provisions relevant from a data protection viewpoint but no derogations to the GDPR.

The Q&A addresses a number of topics including adequate legal basis, informed consent and its withdrawal, information of data subjects, transfers and secondary uses. Primary use of data is given a much broader interpretation than under WP19 Opinion 03/2013 on purpose limitation: all processing operations related to a specific clinical trial protocol during its whole lifecycle are to be considered the primary purpose.

When considering the legal basis however, EDPB considers it important to distinguish between processing activities. This applies particularly with respect to processing activities related purely to research which ought to be distinguished from those activities related to the purposes of protection of health, reliability and safety. These two main categories may fall under different legal baes:

Processing activity	Legal basis (Art 9)	Legal basis (Art 6)
Reliability and safety	Public interest (health) (Art.9(2)(i))	Legal obligation (Art.6(1)(c))
Research (1) – consent	Consent* (Art.9(2)(a))	Consent (Art.9(2)(a))
Research (2) - other	Public interest (health) (Art.9(2)(i)) - subject to MS law or Scientific research (Art. 9(2)(j) - subject to MS law (Art 89(1))	Public interest (Art.6(1)(e)) (for public bodies, subject to MS law) or Legitimate interests of the controller (Art.6(1)(f)) (subject to balancing tests)

*This GDPR consent to processing should not be confused with the informed consent to participate in the trial.

Consent is a double edged sword. While it provides a wide gateway for processing, there are several issues to consider:

- Controllers should consider whether all conditions for a GDPR valid consent can be met (i.e. freely given, specific, informed, unambiguous, and explicit). The imbalance of power between the parties could impact on the validity of consent, particularly where the data subjects are economically or socially disadvantaged, in poor health, institutionalised or otherwise vulnerable. For this reason the EDPB recommends against relying on this legal basis.
- GDPR consent can be withdrawn at any time. There is no exception for scientific research. Where consent is withdrawn, the controller shall stop the processing actions concerned and, unless there is another legal basis for the processing, shall proceed to delete the data.

All other research legal bases require some foundation in Member State law.

Secondary purposes should be viewed in terms of whether they are compatible with the primary purposes (e.g. archiving of the study data could be compatible with the primary purpose of conducting the trial). Where the purpose falls outside of this primary purpose, the Controller remains accountable for the lawfulness, and compliance of the processing activities. There are no exemptions.

While the CTR is not yet in effect (its projected application is estimated to occur in 2020), stakeholders in clinical trials should consider this advice and how it applies to their study protocols in order to avoid pitfalls in the future.

February

The EDPB has published two Brexit related information notes on: (i) Data transfers in the event of a no-deal Brexit and (ii) BCRs for companies which have the ICO as the BCR Lead Supervisory Authority.

On the BCR guidance, important points to note are:

• Groups headquartered in the UK wishing to apply for new BCRs will need to identify an appropriate BCR Lead Supervisory Authority in an EU Member State.

- Where current applications have only reached the review stage, the new BCR Lead Supervisory Authority will take over the application and formally initiate a new procedure at the time of a no deal Brexit.
- If a draft ICO decision for approving BCRs is pending before the EDPB, the Group needs to identify a new BCR Lead Supervisory Authority who will take over and re-submit a draft decision for the approval the BCRs to the EDPB.
- Authorised BCR holders: BCR holders need to identify the new BCR Lead Supervisory Authority.

The ICO also refers to this Guidance and notes that those with authorised BCRs may need to update their BCRs to reflect the fact that the UK will be a third country, including (but not limited to) situations where the UK entity of the BCR Group is the entity which accepts responsibility for and agrees to take the necessary action to remedy the acts of other BCR members outside the EU. However BCRs which have already been authorised prior to Brexit will remain valid.

For new BCRs, the proposed new "UK GDPR" continues to recognise BCRs as a valid transfer mechanism but with some UK specific changes: Data subjects must be able to lodge complaints with the ICO and in the UK courts and the ICO will also be the body with which the organisation must cooperate, report changes to the BCRS or legal requirements which are likely to have a substantial adverse effect on the BCR guarantees or provide audits to on request.

	More significantly, a UK entity will need to accept liability for any breaches of the BCRs by any member concerned which is not established in the UK. For organisations whose BCRs cover the UK and other EEA members, there will therefore be a need to additionally pick a UK entity as well as an EEA entity to accept liability.
February	The EDPB has also published its 2019/2020 work programme setting out its proposed Guidelines, consistency opinions and other planned activities. There is a long list of proposed Guidelines but those of particular interest include Guidelines on Connected Vehicles, video surveillance, targeting of social media users, children's data, concepts of controller and processor, legitimate interests, data subject rights and finalisation of the Territorial Scope Guidelines. Other possible topics include: Enforcement against controllers in 3rd countries, Approval procedure for ad hoc contractual clauses, Blockchain, Interoperability between BCRs and Use of new technologies, such as AI, connected assistants. For the full programme, see here. The EDPB also published its first overview on the implementation of the GDPR and the roles and means of national supervisory authorities 9 months on. In particular, this paper focuses at how One Stop Shop is working across the Member States, summarises head count and budget for supervisory authorities and also examines the main areas of enforcement and penalties issued to date. For more see here.

Other EU News

Date	Description
January	On Data Protection Day (28th January 2019) the Committee of Convention 108 published "Guidelines on Artificial Intelligence and Data Protection". The aim of these guidelines is to ensure that AI does not undermine the right to data protection. The guidelines are aimed at developers and legislators in particular but also include some more general guidance. These high level guidelines place an emphasis on safeguarding humans starting at the design stage and evaluating the risks to data subjects at every stage. Particular emphasis is given where AI decision making impacts an individual and the guidance for protecting data subject rights in this area includes: informing the user they are interacting with AI and giving them "meaningful" control over how their data is processed. The guidance also echoes some of the key principles from GDPR: transparency, accountability and lawfulness of processing to name a few. Interestingly in the guidance for developers the Committee highlights the potential for hidden biases and discrimination by AI, many facial recognition algorithms have been criticised in the past for accuracy which varied depending on the ethnicity of the user. The Committee suggests these biases can be avoided by utilising a "human rights by-design approach" and consulting experts and academic institutions whilst designing apps.
5 February	**European Commission recommends negotiating international rules for obtaining electronic evidence** In recognition of the increasingly international nature of crime such as human trafficking, the Commission has responded to the Council's October 2018 decision by recommending the negotiation of two international agreements on cross border rules to obtain electronic evidence:

- a new protocol to the Budapest Convention, covering law enforcement authority (LEA) access to data in approx. 60 countries

The additional protocol would further strengthen international cooperation including facilitating access to electronic evidence, enhancing mutual legal assistance and setting up joint investigations. The Commission is seeking a mandate to negotiate on behalf of the Member States to improve the compatibility of the protocol with EU law and implement stronger safeguards for the protection of personal data in a cross border context.

- a new bilateral agreement with the USA, covering direct requests by one party's LEAs for data stored/controlled in the other party's territory

Currently, the cross border cooperation with the USA is done on a voluntary basis which is often stifled by local law and procedures. The Commission proposes to negotiate an agreement with USA to facilitate the relationship by addressing legal conflicts by clarifying the obligations and rights of both parties while guaranteeing strong safeguards on personal data and respecting the fundamental right and principles of necessity and proportionality. The Commission also hopes to ensure timely access by reducing the period for supplying information to 10 days instead of the current average – 10 months),

EU Legislation

Date	Description
4 February	**Presidential Note on proposed compromises may pave the way for progress on the stalling ePrivacy Regulation** The ePrivacy Regulation has been stagnating as the Council continue to be in disagreement on multiple issues. The Romanian Presidency has proposed several changes which may be a positive step towards a consensus in the Council. The highlights include: • Consent should not be required for technical storage or access necessary and proportionate for the legitimate use of a service requested by the user (such as authentication session cookies or information society services cookies) • Consent should be requested for cookies for purposes other than where they are necessary for the provision of a requested service. • New consent processes proposed for combating 'consent fatigue' (consent for one or more services for a specific provider can be collected for use over multiple platforms in one interaction.) The full text of the proposed compromise can be read here.

European Cases

Date	Description
January **(CJEU)**	**In two recent Opinions, the CJEU Advocate General, Maciej Szpunar, discussed Google's obligations under the Directive 95/46/EC as part of its search engine activities:** **1. Google should limit the de-referencing to searches within the EU only (*Case C-507/17 – Google v CNIL*).** In *Case C-507/17*, the French data protection authority (the "CNIL") served formal notice on Google effectively stating that: when complying with a de-referencing request,(i.e. when a natural person asks for the removal of links to web pages from the list of results displayed following a search performed on that person's name), Google must apply the removal to all of its search engine's domain name extensions (i.e. internationally). Google's refusal to comply with this notice resulted in a fine of €100,000 by the CNIL. Google proceeded to lodge an application before the Conseil d'Etat (Council of State) to have CNIL's decision annulled. The Conseil d'Etat referred questions to the CJEU for a preliminary ruling on Directive 95/46/EC. In responding to questions raised by the Conseil d'Etat, the Advocate General has disagreed with the CNIL position. According to him, the Directive 95/46/EC (unlike the GDPR) cannot be interpreted to have extraterritorial scope beyond the EU. The Advocate General considers that '*A distinction must be made depending on location from which the search is performed. Search requests made outside the EU should not be affected by the dereferencing of such results*.' To apply the de-referencing request worldwide, EU authorities would be required to balance the interests between the fundamental right to be forgotten with the right to receive information which differs from one-third State to another. This they are unable to do. The Advocate General concludes as follows: '*the search engine operator is not required, when acceding to a request for de-referencing, to carry out that de-referencing on all the domain names of its search engine in such a way that the links in question no longer appear, irrespective of the location from which the search on the basis of the requesting party's name is performed*'. However, the Advocate General places a caveat on the above. The search engine operator must ensure a '*full and effective de-referencing within the EU*'. It means, in particular, the geo-blocking of IP addresses located in a Member State, to prevent access to de-referenced links by using a domain name outside the EU. **2. Google should accede to request for the de-referencing of sensitive data, provided that such de-referencing does not affect the right to access to information and the right of freedom of expression (*Case C-136/17 – G.C. and others v CNIL)*** In the second case, following a claim, the CNIL refused to put Google on a formal notice to de-reference various links to web pages published by third parties, from the list of results displayed following a search performed on that person's name. The web pages dealt with

different articles or pictures related to sensitive personal data (such as political opinions, religious or philosophical beliefs, sex life).

The interested parties challenged the CNIL decision in front of the Conseil d'Etat which referred various questions to the CJEU.

Regarding the applicability to a search engine operator of the prohibition on processing data falling within sensitive data, the Advocate General considers that such prohibition cannot apply as if it had itself placed sensitive data on the web pages. However, operator of a search engine is bound by such prohibition '*by reason of referencing [sensitive data, placed online by third parties] and, thus, through subsequent verification, when a request for de-referencing is made by the person concerned*'.

Addressing the question asked by the Conseil d'Etat as to whether an obligation is imposed on the operator of a search engine to systematically de-reference material, the Advocate General responded positively. The prohibition on processing of sensitive data stated in the first question requires the operator of a search engine like Google to accede to requests for de-referencing web pages on which sensitive data appear. Mr Szpunar adds, however, that, since the prohibition of such processing applies, the same goes for its exceptions, although the application of these exceptions by a search engine operator is more theoretical than practical.

Lastly, when determining whether such exceptions may apply, a search engine operator must take into account all the interests involved to ensure the protection of the right to access to information and the right of freedom of expression which may be breached by de-referencing. Before agreeing to the de-referencing request, a search engine operator must, therefore, balance the right to be forgotten (right to respect for private life and the right to protection of data) and the right of public interest to access the information concerned and the right of freedom of expression.

The both CJEU's press releases can be found here and here.

January

(CJEU)

Sergejs Buivids v Datu valsts inspekcija (C-345/17)

In this case the CJEU decided that processing for "journalistic purposes" can be interpreted broadly. This case related to an individual who was arrested, secretly videoed police officers while he was arrested, and then posted this footage on YouTube, Mr. Buivids argued either that the processing should be covered by the domestic purposes exemption, or that it should be seen as processing for journalistic activities. The CJEU held that because processing for domestic activities falls completely outside data protection law, this exemption must be interpreted strictly and did not apply here. The Court also held that such processing could be considered as being done for "journalistic purposes" even though the person recording it is not a journalist but that the exemption cannot be pushed so far as to mean that all material published online is therefore exempt.

The CJEU also summarised criteria, mentioned in Satakunnan Markkinapörssi and Satamedia, C-73/07 (16 December 2008), which should be taken into account in determining whether processing is for journalistic activities. These are:

- whether the processing contributes to a debate of public interest;
- the degree of notoriety of the person affected;
- the subject of the news report;
- the prior conduct of the person;
- the content, form and consequences of publication; and

	• the manner and circumstances in which the information was obtained and its veracity [66]. For more see here.
February **(ECtHR)**	**Grand Chamber Panel's decisions** The Grand Chamber panel of five judges has decided to refer two cases to the ECtHR. *Big Brother Watch and Others v UK* concerns complaints made by various individuals, journalists and rights organisations regarding bulk interception of communications, international intelligence sharing and the obtaining of communications data from telecom providers. *Centrum För Rättvisa v Sweden* concerns a complaint brought by a public interest law firm regarding bulk interception of electronic signals for foreign intelligence purposes.
January **(ECtHR)**	***Catt v United Kingdom (application no 43514/15) (Jan 24 2019)*** This ECHR Chamber judgment relates to a British National, Mr Catt who was a lifelong peace activist. In 2005 he started to participate in a number of disorderly protests but he was never convicted of any offences. In March 2010, he made a Subject Access Request to the Police and they disclosed a number of entries relating to his attendance at a number of demonstrations over a 4 year period. The information was retained in a database concerning "domestic extremism" and was contained in records of other individuals and in reports which mentioned him incidentally. Mr Catt asked for the records to be deleted but the police declined to do so. Mr Catt challenged this decision through the UK courts arguing that the retention was not necessary within the meaning of Article 8 (right to respect for private and family life) of the European Convention of Human Rights and eventually lost at the Supreme Court which found that the data retention was lawful and proportionate and that any interference with Mr Catt's privacy was minimal. Mr Catt then took his case to the ECHR. Whilst the Chamber understood that there had been good policing reasons for why such data had been collected, it found that the continued retention of such data was disproportionate as it revealed political opinions which required enhanced protection and that therefore there had been a violation of his Article 8 rights. The Chamber also took into account Mr Catt's age (he is now 94) and the fact that he had no history or prospect of committing acts of violence. It remains to be seen whether the UK government will challenge this decision and request a referral to the Grand Chamber (which it can do within the next 3 months).

Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
22/01/2019	NWR Limited	Enforcement Notice Direct Marketing	NWR Limited made 827,883 calls numbers that were registered with the TPS between May 2016 and May 2018. It was determined by the ICO that NWR Limited contravened regulations 21 and 24 of PECR. The commissioner issued an enforcement notice to stop the illegal marketing activity.
31/01/2019	Alistar Green Legal Services Limited	Monetary penalty Direct Marketing	The ICO has fined Alistar Green Legal Services Limited £80,000 following 213 complaints regarding nuisance calls between March and July 2017, 127 of which were to TPS subscribers. The Commissioner found that Alistar Green had contravened regulation 21 of the PECR and had made unsolicited calls for the purpose of direct marketing. The commissioner was satisfied that the company was taking measures to stop the practice and therefor did not issue an enforcement notice. A monetary penalty was issued to further the policy objective of preventing telemarketing breaches of PECR.
01/02/2019	Eldon Insurance Services Limited (GoSkippy Insurance) Leave.EU Group Limited	Enforcement notice Monetary Penalty Direct Marketing	As part of the ICO's ongoing investigations into the use of data analytics for political purposes, the ICO found that Leave.EU and Eldon Insurance (trading as Go Skippy Insurance) were closely linked. Systems for segregating the personal data of insurance customers' from that of political subscribers' were ineffective. This resulted in Leave.EU using Eldon Insurance customers' details unlawfully to send almost 300,000 political marketing messages. Leave.EU was fined £15,000 for this breach. Eldon Insurance carried out two unlawful direct marketing campaigns. The campaigns involved the sending of over one million emails to Leave.EU subscribers without sufficient consent. Leave.EU has been fined £45,000 and Eldon Insurance has been fined £60,000 for the breach.

07/02/2019	Magnacrest Limited	Prosecution DSAR	Magnacrest Limited pleaded guilty to an offence under section 47(1) of the Data Protection Act 1998 having failed to comply with an Enforcement Notice from the ICO. The notice related to a subject access request made by a member of the public dating from April 2017 which the defendant had failed to comply with. The company was sentenced to a fine of £300, and ordered to pay costs of £1,133.75, with a £30 victim surcharge.
08/02/2019	Keith Nicholas Hancock	Director ban	Mr Hancock received a 4 year director's ban following an ICO investigation that revealed breaches of e-marketing rules under PECR: more that 393,000 SMS messages were sent to members of the public without the appropriate consents. The company failed to pay the £20,000 fine and was subsequently wound up. The insolvency triggered further investigation by the revealing Mr Hancock, the sole director of the Company, had played a central role in the marketing campaign which led to a disqualification undertaking and the ultimate ban issued by the Insolvency Service.