Bird & Bird

UK & EU Data Protection Bulletin: September- October 2018

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
September	**ICO publishes updated guide to NIS Regulations and registration reminder for Digital Service Providers**

The ICO has recently updated its Guide to the Network and Information Systems Regulations 2018 (NIS Regulations). The guide is aimed at 'relevant digital service providers' as defined under the NIS Regulations which includes certain online market places, online search engines and cloud services. The NIS Regulations derive from European Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the EU, known as the NIS Directive. The Guide explains the ICO's role as the UK's competent authority for these organisations. Other organisations covered by the NIS Regulations such as operators of essential services, should look to their own competent authorities for specific guidance although some parts of this guidance may of general use (e.g. in respect of the interaction between NIS and GDPR). The Guide includes links to relevant sections of the NIS Regulations, the NIS Directive, other relevant ICO guidance, guidance produced by the National Cyber Security Centre (NCSC) and guidance produced by the European Union Agency for Network and Information Security (ENISA).
GDPR and the NIS Regulations address different things: GDPR concerns personal data whilst the NIS Regulations address the security of systems, but there is considerable overlap as security considerations are relevant to both and most organisations covered by the NIS Regulations will be data controllers (as well as data processors in some situations).

The NIS Regulations apply to fewer organisations: you need to be an operator of essential services or a relevant digital service provider to be caught by the obligations (although it is expected that the NIS Regulations will also have a knock-on impact for suppliers to relevant digital service providers and operators of essential services). NIS incidents can be (but are not always) a personal data breach under GDPR, which is reportable to the competent authority (under NIS) and the ICO (under GDPR). If you are a relevant digital service provider, the ICO's NIS reporting tool allows you to indicate whether personal data has also been compromised.

As the GDPR and NIS are separate laws, organisations may face regulatory action under both pieces of legislation. The ICO has a range of enforcement powers under the NIS Regulations which are similar to those under GDPR, including information and enforcement notices, inspection powers and the ability to issue penalty notices. The level of fines will depend on the nature of the contravention but fines of up to £17 million are possible for any material contravention which the ICO determines has caused, or could cause, an incident that results in a threat to life or in significant adverse impact on the UK economy.

A link to the Guide can be found here. For more information on the NIS Regulations, contact Simon.Shooter@twobirds.com or James.Mullock@twobirds.com

Date	Description
Autumn	**ICO Regulatory Action Policy** With a view to enabling organisations *"to predict how [the ICO] will carry out its regulatory activity"*, the ICO has developed a Regulatory Action Policy (**RAP**) on which it sought views via a public consultation which closed on 28 June 2018, and to which 80 responses were received. A revised (undated) RAP now appears on its website which appears to have taken account of comments made during the consultation which *"...sets out a risk-based approach to taking regulatory action against organisations and individuals that have breached the provisions of the data protection, freedom of information and other legislation ... As with earlier versions of the policy it focusses on areas of highest risk and most harm and the principles we apply in exercising our powers."* The ICO confirmed to us that this is the final version which was laid before Parliament on 19 July and further changes are not expected. Among other things, the RAP sets out: the criteria which the ICO will apply when deciding which type of regulatory action to take when faced with a breach of information rights obligations (including aggravating and mitigating factors to consider); the criteria which the ICO will apply when deciding whether to issue Information Notices, Assessment Notices, Enforcement Notices, or Penalty Notices; and, perhaps more importantly, how the ICO will calculate the amount of a penalty to be imposed. The ICO states that, *"Generally, the amount will be higher where: vulnerable individuals or critical national infrastructure are affected; there has been deliberate action for financial or personal gain; advice, guidance, recommendations or warnings (including those from a data protection officer or the ICO) have been ignored or not acted upon; there has been a high degree of intrusion into the privacy of a data subject; there has been a failure to cooperate with an ICO investigation or enforcement notice; and there is a pattern of poor regulatory history by the target of the investigation."* The current version of the RAP can be viewed here.
October	**ICO updates advice on GDPR exemptions** The ICO has updated its guidance on the exemptions under the GDPR and DPA 2018 which includes a checklist for those relying on exemptions. Whether organisations can rely on an exemption generally depends on the purposes for processing personal data. Some exemptions apply in the context of a particular purpose. Others apply where compliance with the GDPR will be likely to prejudice the relevant purpose, prevent, or seriously impair an organisation from processing the data in a way which is necessary for the purpose. The available exemptions are split into categories with further explanations: crime, law and public protection; regulation, parliament and the judiciary; journalism, research and archiving; health, social work, education and child abuse; finance, management and negotiations; references and exams. There is also section on dealing with subject access requests where the data requested includes personal data of third parties. The guidance encourages those who rely on exemptions to review this reliance in the context of the new law. More information can be found here.
October	**The UK ICO's International Strategy 2017-2021** The ICO's International Strategy 2017-2021 contains some timely reminders on how the ICO intends to deal with the challenges of Brexit,

Date	Description
	increased globalism and changing technology. Part 1 of the Strategy Paper sets out the main challenges and priorities for ICO between 2017 - 2021. These can be summarised as follows: 1 **Challenge: Ensuring the ICO operates as an effective and influential data protection authority at European level while the UK remains a member of the EU and when the UK has left the EU or during any transitional period.** In order to meet this challenge the ICO intend to (a) provide expert advice to the UK Government on Data Protection; and (b) continue strong engagement with the European Data Protection Board ('**EDPB**') in addition to strengthening bilateral relationships with EU regulators and other relevant organizations such as the Council of Europe, Members of the European Parliament and other specialist working groups. The strategy rightly recognises that the UK's direction on Brexit will be driven by the outcome of the Brexit negotiations. 2 **Challenge: Maximising the ICO's relevance and delivery against its objectives in an increasingly globalised world with rapid growth of online technologies.** The ICO wants to ensure that it has the global reach and influence to protect UK data across boundaries. In order to meet this challenge the ICO will (a) continue to engage with leading privacy networks and data protection authorities and develop new networks where the opportunity exists; (b) continue to play a leading role in international enforcement co-operation; (c) develop new relationships with think tanks, academic and civil society networks and (d) share information with other independent bodies responsible for enforcing and promoting freedom of information laws. 3 **Challenge: Ensuring UK data protection law and practice is a benchmark for high global standards.** The ICO wants UK data protection to continue to be recognized as a globally leading standard and the ICO to be an internationally influential regulator. In order to meet this challenge the ICO plans to engage in international work to promote global data protection standards and more long term the potential development of a global data protection and privacy agreement or treaty. In addition the ICO will work with businesses and stakeholders to turn the GDPR's accountability principles into a robust but flexible global solution. 4 **Challenge: Addressing the uncertainty of the legal protections for international data flows to and from the EU, and beyond, including adequacy.** The ICO recognize that safeguards for international data transfers remain a key goal of effective data protection. In order to meet this challenge the ICO will provide expert advice to the UK government on international data flows and explore the concept of the UK as a 'global data protection gateway' which has a high standard of data protection law which is interoperable with different

Date	Description
	legal systems. Part Two of the Strategy Paper covers the ICO structure, resourcing, engagement and evaluation. This can be summarised as follows: **ICO Structure**: The ICO intend to establish a new International Strategy and Intelligence Department, creating an ICO department with international activity as its core focus. Additional resources will be added to the ICO's international team to support the strategy. In addition, ICO will explore the possibility of staff exchanges and secondments with other data protection authorities. **Engagement:** The ICO will host a number of conferences and attend events that seek to promote the strategy's objectives. The ICO will also seek to agree revised or new agreements with other key data protection and privacy enforcement authorities globally in addition to promoting the ICO guidance to global audiences. **Measurement and evaluation:** The ICO is to develop a reporting mechanism to evaluate the value of its international activities and include a dedicated section on the topic in its Annual Report. **Comments** Overall ICO's International Strategy is a high level set of aims which does not set out detailed guidance on how UK data protection will change post Brexit. It is nonetheless encouraging to see ICO looking ahead and planning more generally for what its role will be in a post Brexit world. The recent election of Elizabeth Denham as Chair of the International Conference of Data Protection and Privacy Commissioners, illustrates that the ICO are already making significant progress on some of the objectives of the paper. For more information on the ICO's Strategies see here.

Date	Description
22 October	***Wm Morrisons Supermarket Plc v Various Claimants [2018] EWCA Civ 2339***

Court of Appeal upholds decision that Morrisons is vicariously liable for its rogue employee

On 22nd October, the Court of Appeal dismissed an appeal by Morrisons against an earlier High Court decision from 1 December 2017 that found it was vicariously liable for an employee's misuse of the data.

Facts

Back in 2013 and 2014, Mr Skelton, a disgruntled former employee of Morrisons, used his legitimate work access to steal and unlawfully post the personal details of nearly 100,000 employees on a file sharing website and also attempted to frame a colleague in the process. The data included their names, addresses, gender, dates of birth, national insurance numbers and bank details. He was charged with fraud, offences under the Computer Misuse Act 1990 and under Section 55 of the Data Protection Act 1998 (DPA) and was sentenced to 8 years in jail in 2015. Once Morrisons were alerted to the disclosure, they quickly took steps to take down the website and alerted the police. The ICO investigated but decided that no enforcement action was appropriate at the time.

However, on 24 November 2015, a Group Litigation Order was commenced by around 5,500 employees where a claim form was issued against Morrisons for damages and interest for misuse of private information, breach of confidence and breach of statutory duty owed under S4(4) of the DPA. The claimants argued that Morrisons was primarily liable under those heads of damage but if not, then Morrisons was vicariously liable for the wrongful conduct of Mr Skelton. The High Court didn't find Morrisons directly liable (instead it held Mr Skelton to be a third party data controller who has acted autonomously in handling the data) but it did conclude that there was a "*sufficient connection"* between the position in which Mr Skelton was employed and his wrongful conduct to find that Morrisons was vicariously liable for Mr Skelton's actions. However Justice Langstaff was troubled by his conclusion that by finding Morrisons vicariously liable, the Court could be regarded as "*an accessory to furthering Mr Skelton's criminal aims"* so he granted Morrisons permission to appeal.

There were 3 grounds of appeal: (1) that the DPA excludes the application of vicarious liability; (2) the DPA excludes the application of other causes of action (e.g. misuse of private information and breaches of confidence and the imposition of vicarious liability for breaches of the same; and (iii) that the Judge was wrong to conclude that the wrongful acts of Mr Skelton occurred during the course of his employment and that Morrisons was vicariously liable for those actions. However the Court of Appeal disagreed with the "*extensive and elaborate submissions*" on behalf of Morrisons and agreed with the High Court judge that "*the causes of action for misuse of private information and breach of confidentiality are not excluded by the DPA in respect of the wrongful processing of data within the DPA and the common law remedy of vicarious liability of the employer was not expressly or impliedly excluded by the DPA"*. On the last point, notwithstanding the fact that Mr Skelton had uploaded the personal details at his home using his own computer on a Sunday, several weeks after he had downloaded the data at work onto his personal USB stick and despite the fact that there was no evidence that any of the claimants had suffered any financial loss, the judges still found that there was a sufficient connection and agreed with Justice Langstaff's previous

Date	Description
	judgment where he considered that there was "*an unbroken thread that linked his work to the disclosure; what happened was a seamless and continuous sequence of events*." His actions were "*all part of a plan, as the research and careful attempts to hide his tracks indicate*." ***Implications for businesses*** Although this action related to the DPA rather than the GDPR, this judgment has significant implications for companies who suffer data breaches as a result of an employee's deliberate wrong doings even if the employee's motive in committing the breach was to harm the company and the company has not directly contributed to the breach. The Court of Appeal recognises that this decision potentially exposes other companies to the risks of a large number of claims for "*potentially ruinous amounts*". However, the Court of Appeal believes the answer lies in adequate insurance: "*the fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward by...Morrisons*." Businesses should therefore consider whether their current insurance policies properly protect them against this risk. Morrisons have said they will appeal to the Supreme Court. The decision determining the amount of any damages payable is still to come. The full decision can be found here.
8 October	***Lloyd v Google LLC [2018] EWHC 2599 (QB)*** ***Facts*** *– another attempt at Safari-based compensation, for all affected UK users* In this recent case, *Lloyd* sought to bring a representative action under CPR 19.6 seeking compensation for breach of the Data Protection Act 1998 cause by the 'Safari workaround' deployed by Google between 2011 – 2012, which allowed it to override settings in Apple's Safari browser software, so as to collect data about users. The same factual scenario had previously led to the *Vidal-Hall* litigation (ultimately settled), in which specific claimants brought individual actions against Google. Here, the claimant sought compensation in a representative capacity on behalf of a class of residents in England and Wales said to be affected by the Safari workaround. Before any such claim can be made, it must be served – and this case assessed whether permission would be given to serve proceedings, based on whether there was any realistic prospect of success. ***At issue*** *– did the claim disclose a basis for compensation under the DPA 1998?* Although the claimant had secured funding (through litigation funders) of up to £15.5 million pounds, the claimant did not provide any evidence of financial loss, damage or distress. In the letter of claim, a figure of £750 per individual was advanced. Given the potential size of the class, Google's estimated liability was somewhere between £1 and £3 billion. All parties accepted that Google's actions were in breach of data protection legislation: however, the parties disputed whether this should automatically give rise to compensation – was the mere fact a breach took place grounds for compensation, with some "loss of control/autonomy over personal data" being sufficient to cause liability for compensation under the 1998 Act. Also at issue (but arguably less interesting to data protection lawyers) was whether this type of "*opt-out*" representative action – where

Date	Description
	litigation takes place before all claimants are identified – could be litigated under the CPR. *Warby J: "In my judgment, it does not"* Having heard the arguments, Warby J: • rejected the claimant's argument that breach of data protection legislation must – as a matter of principle – be compensated: He took the view that the claimant had to show that the breach of the legislation had actually caused some damage; if the claimant could not show this, then other remedies (such as deletion or correction of data) may be appropriate, but compensation would not be awarded; • accepted that loss of control over data *may* give grounds for compensation but emphasised that the person alleging this would have to demonstrate that the breach had caused some form of irritation or interference with their life and the claimant had provided no evidence to this effect; • held that there was no authority to award damages to censure Google or to deprive it of profits; and • held that this type of representative action could not proceed, because it would not be possible to define the class with certainty given the differing levels of damage (Warby J considered that everyone in that class would react to the data protection breaches differently and would have made use of Safari in different ways and amounts). Warby J. noted that "*the main beneficiaries of any award at the end of this litigation would be the funders and the lawyers, by a considerable margin*". He denied permission to serve proceedings out of the jurisdiction on the basis that there was no real prospect of success for the claimant – both because no damage was suffered or claimed and because the court would inevitably refuse to allow this type of representative claim to continue. The case is an interesting cautionary tale: although the claim here failed, it does illustrate well the types of large claims which could be brought where large numbers of users are affected (for example, in a personal data breach) and the likely costs of dealing with such litigation. It also shows that litigation funders are alive to these possibilities: this is unlikely to be the last case of this type. The full decision can be found here.

Legislation

Date	Description
8 September	**Claims management cold calling: New restrictions** New UK legislation came into force in September aimed at curtailing nuisance calls from personal claims companies. The change, contained within Section 35 of the Financial Claims and Guidance Act 2018, was brought into effect on 8 September 2018 (by the Financial Guidance and Claims Act 2018 (Commencement No. 1 and Transitional Provision) Regulations 2018). Section 35 amends the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the 2003 Regulations") by amending regulations 21 and 24 and inserting a new regulation 21A. The main change creates a special class of unsolicited marketing calls relating specifically to claims management services ("cold claims calls") and prohibits people from making such calls unless recipient subscribers have previously opted in to receiving them. Previously, people had to opt out of these types of calls by registering with the free Telephone Preference Service or withdrawing their consent while on the call. There are further changes to regulation 24 of the 2003 Regulations to ensure that people making cold claims calls remain under a duty to provide recipients with their name and, if requested, their address and a contact number that is free to call. "Claim Management services" means the following services in relation to the making of a claim: (a) advice; (b) financial services or assistance; (c) acting on behalf of, or representing, a person; (d) the referral or introduction of one person to another; or (e) the making of inquiries. More here. Section 21 of the Financial Claims and Guidance Act 2018 also gives the Secretary of State powers to make regulations prohibiting unsolicited direct marketing relating to pensions and requires the Secretary of State to keep under review whether a prohibition on other consumer financial products is also appropriate. In July, the Government consulted on draft regulations for banning pensions cold calling which ended in August. The results of the consultation were published in October 2018. Again, the intention is to create an opt in regime which will prohibit cold calling in relation to pensions unless the caller is authorized by the Financial Conduct Authority or is a trustee or manager of an occupational or personal pension scheme and (a) the recipient of the call consents to such calls being made by the caller on that line; or (b) the recipient of the call has an existing client relationship with the caller, and the relationship is such that the recipient might reasonably envisage receiving pensions cold calls. HM Treasury has confirmed that the draft regulations on the ban will be published this Autumn (although this has not happened yet) and the prohibition itself will come into force 21 days after the day on which they are made. More here.

Other news

Date	Description
7 September	**The British Airways data breach: group compensation claims and GDPR / NIS overlap?** Not all 2018 data protection planning has been about GDPR compliance programs. On 7th September, the same day that BA announced that 380,000 customers had potentially been affected by a breach involving website and app customer data, SPG Law, the UK arm of US law firm Sanders Phillips Grossman, demonstrated considerable pre-planning by announcing the launch of a group compensation claim against the airline based on Article 82 of the GDPR. SPG Law's 'no win, no fee' claim will, it says, be brought by way of a Group Litigation Order action with an estimated £1250 available for each claimant. Whether or not regulators decide to fine BA, the company is one of the first to face the prospect of co-ordinated compensation claims since the GDPR took effect in May, a reminder that percentages of worldwide turnover are not necessarily the end of the story when quantifying data protection risks. By virtue of it being a critical infrastructure provider (and, interestingly, potentially also as a provider of a digital market place for travel services) BA is in the unenviable position of being subject to both the provisions of the GDPR and laws which implement the Network & Information Systems Directive (NISD). Since May 2018, NISD has imposed security obligations on Operators of Essential Services (OESs) and Relevant Digital Service Providers (RDSPs) and obliged them to notify regulators of security incidents under a regime which is separate to that introduced by the GDPR in the same month. It remains to be seen whether the cyber-attack which BA announced in early September is one which falls under the ambit of the UK laws which implement NISD as well as the Data Protection Act 2018. To do that the breach would have to have affected a network and information system on which BA service is deemed to rely. It will be interesting to see whether either of the two UK regulators with responsibility for overseeing BA's NISD obligations, the Civil Aviation Authority (which has responsibility for UK aviation OES companies) and the Information Commissioner's Office (which has responsibility for UK RDSPs) consider that to be the case. In short, the BA breach highlights the potential risks posed by group litigation in addition to GDPR fines and the need for those who fall under the NISD to ensure that their GDPR compliance programs were set broadly enough to also meet the requirements of that piece of law.

Date	Description
13 September	**Government issues its No Deal Technical Note on Data Protection**

On 13th September, the Government issued its No Deal Technical Note on Data Protection. This short note briefly sets out the Government's view on the actions UK organisations should take to enable the continued flow of personal data between the UK and the EU in the event that the UK leaves the EU on 29 March 2019 with no agreement in place. It does not address transfers of personal data for law enforcement purposes.

Transfers from the EU to UK Companies

- If no deal is agreed, then the UK will become a "third country" from a GDPR perspective and the data transfer restrictions in Chapter V of the GDPR will apply;
- The GDPR will be written into UK law by the EU Withdrawal Act. This will help demonstrate that the UK offers an "essentially equivalent level of protection" to EU data protection laws. However, the European Commission has not indicated a timetable for making an adequacy determination in respect of the UK, so this may not be in place by March 2019. Indeed, the Commission has stated that the decision on adequacy cannot be taken until the UK is actually a third country.
- In the absence of an adequacy decision, EU organisations will need to identify a legal basis for any transfers to UK companies acting as data importer. For many organisations, the most relevant alternative legal basis would be the Commission approved standard contractual clauses (although the Note does not mention that such mechanisms themselves are also subject to their own legal challenges).

Transfers from UK Companies to the EU

- The Note states that the UK will at the point of Brexit continue to allow the free flow of personal data from the UK to the EU (although this would be kept under review).

Transfers from UK Companies outside of the EU

- The Note however does not go into any detail about data transfer mechanisms that should be used to address data transfers from the UK to other non EU countries. However, the mechanisms for transferring data elsewhere would also need to be updated – for example, the US Privacy Shield consists of commitments given by the US to the EU (and parallel commitments given to Switzerland). Commitments would need to be given to the UK, before this could cover transfers of personal data from the UK post-Brexit.

A copy of the Note can be found here.

Bird & Bird are hosting a broader Brexit event on Tuesday 27th November. For more information, please contact Deanne Prudden on: +44 (0)20 7415 6000.

Date	Description
23 October	**International Conference of Data Protection & Privacy Commissioners opens its declaration on Ethics & Data Protection in AI for consultation** The International Privacy Commissioners Conference (ICDPPC) adopted a draft declaration on this on Tuesday 23rd October. The declaration is open for public consultation. Written contributions should be sent by 25th January 2019 directly via email to the following address: ExCoSecretariat@icdppc.org (Subject: ICDPPC Public Consultation). As would be expected, the declaration recites the ways in which AI must respect privacy and data protection rights (there is more on this below). It also, however, expressly recognises that AI systems can bring significant benefits for users and society and there is an emphasis on education and awareness raising so as to ensure that privacy and wider human rights concerns (which the declaration encourages data protection authorities to consider, as well as more traditional privacy concerns), are explicitly taken into account. The ICDPPC is to establish a permanent working group on Ethics and Data Protection in Artificial Intelligence which is to promote understanding of and respect for the principles in the resolution by all parties concerned – ranging from governments, system designers and individuals. The need for international engagement was emphasized. The declaration lists 6 key principles, each of which has a number of sub-recommendations. These are: 1 Fairness a Consider individuals reasonable expectations and ensure AI remains consistent with these and the purpose limitation principle b Take into consideration the impact AI will have both on individuals and on society at large (i.e. consider collective harms and benefits as well as the individual) c AI can be developed in positive and negative ways – certain uses should be limited 2 Continued attention and vigilance a Ensure accountability by audit, monitoring & impact assessment. Keep oversight methods under periodic review b Develop joint responsibility by all stakeholders – e.g. via standards and best practice sharing c Invest in awareness raising, education, research and training d Establish governance processes – e.g. use of trusted third parties or independent ethics committees 3 Improve transparency and intelligibility a Invest in research on explainable AI b Develop innovative communication methods c Promote auditable systems d Ensure informational self-determination – tell people when AI will be used

Date	Description
	e Inform about the purpose and effects of AI – so as to enable human control and continuous alignment with individuals expectations 4 Privacy by default and by design a Should be implemented during design and on an ongoing basis b Assess and document the impact on individuals and society c Identify specific requirements for ethical and fair use 5 Individual empowerment a Encourage exercise of individual rights & respect the right to object b Use education and awareness campaigns to promote rights c Respect related rights (e.g. freedom of expression and information and non-discrimination) d Use the capabilities of AI to facilitate engagement – e.g. via adaptable interfaces and accessible tools 6 Biases and discrimination should be reduced and mitigated a Respect international laws on human rights and non-discrimination b Invest in research into technical ways to identify and mitigate bias c Ensure data quality d Develop guidance and principles to address bias and discrimination and to promote awareness. More information and the full declaration can be found here.
October	**ICO partners with Unlock on guidance on processing criminal record data** With input from the ICO, Unlock, a charity aimed at supporting the rehabilitation of ex-offenders, has published guidance for employers on the processing of criminal record data. *Asking the question: Guidance for employers on the GDPR, data protection and the processing of criminal records data in recruitment* (the "**Guidance**") provides a helpful starting point for employers when considering criminal record checks as part of the recruitment process, both in respect of the General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018 ("**DPA 2018**"). After first reviewing the GDPR's data protection principles, the Guidance explores both the data protection and employment law considerations employers must bear in mind to compliantly process criminal record data, such as automated decision making, the Rehabilitation of Offenders Act 1974, and the requirement under the DPA 2018 for an appropriate policy document. The Guidance concludes with some practical points about the timing of such checks, with an encouragement for employers to join the U.S.-originating 'Ban the Box'

Date	Description
	campaign, aimed at removing questions from application forms about previous criminal history and thereby creating a fair opportunity for candidates with previous convictions to access employment. The Guidance is balanced and successfully hones in on some key considerations for employers based in England and Wales, where criminal record disclosures are processed by the Disclosure and Barring Service ("**DBS**"). Unfortunately, the Guidance does not pick up on some substantive and procedural nuances for employers located in Scotland and Northern Ireland, where the DBS's counterparts – Disclosure Scotland and Access Northern Ireland – can have varying requirements. More importantly, and despite repeating the need for employers to consider the necessity of processing as a cornerstone for compliance, the Guidance falls short in exploring necessity in more than just theoretical terms.

Europe

EDPB

Date	Description
3 October	**European Data Protection Board reviews national Supervisory Authorities' DPIA lists**

On 3 October 2018, the European Data Protection Board (EDPB) publicly released its "Opinions" on 22 draft national lists of processing activities that are considered to be sufficiently high risk that a data protection impact assessment (DPIA) is required, before an organisation can engage in such activities (per GDPR Article 35).

Organisations will welcome the EDPB's requests that certain activities be removed from lists, whenever the EDPB didn't consider them to be sufficiently high risk to warrant a DPIA. For example, according to the EDPB, the UK Information Commissioner's Office felt that DPIAs should be conducted whenever an organisation wanted to use of biometric data (for identification), genetic data, location data, or any personal data collected from third parties in the absence of clear notice. The EDPB disagreed with the UK authority: it held that a DPIA should only be required in those cases *if* aggravating risk factors were present.

However, the EDPB also did not shy away from suggesting additions to the lists. Biometric data and genetic data (in the presence of aggravating risk factors) were held to be missing from the German DPIA list, for example.

This marks the first official exercise of the GDPR's "consistency" mechanism under Articles 63 and 64, aiming to promote EU-wide harmonisation of the GDPR's interpretation and application. Nevertheless, the EDPB's review disregarded aspects of the lists which were particular to a submitting supervisory authority's local laws; and even in respect of list contents that could have cross-border relevance, "supervisory authorities have a margin of discretion with regard to the national or regional context". National supervisory authorities were instructed to ensure that their lists were non-exhaustive: it is clear that DPIAs may still be required in cases not included on the lists.

National supervisory authorities that refuse to fully follow an EDPB Opinion are required to appeal within two weeks from its receipt. Doing so would trigger the GDPR Article 65 EDPB dispute resolution process.

The 22 DPIA List Opinions are available here.

Date	Description
24 August - 23 October	**European Parliament committee publishes report on post-Brexit data flows; UK government confirms adequacy determination process has not yet started** On 24 August 2018, the European Parliament's "Civil Liberties, Justice and Home Affairs" Committee (a.k.a. LIBE) published a commissioned report entitled "The future EU-UK relationship: options in the field of the protection of personal data for general processing activities and for processing for law enforcement purposes". The report explores options and makes policy recommendations in respect of ensuring the future free flow of data between the EU and the UK, once the UK ceases to be a part of the EU. EU rules require that except in certain cases, continuity of protection of the data must continue even after personal data leaves the EU (to avoid circumvention of EU standards of protection, by offshoring data processing activities). This is the case both in respect of routine, day to day processing activities, but also for law enforcement. The study authors' main findings are that in order to help ensure continued free flow of personal data between the UK and EU, the European Commission should implement a so-called "adequacy determination" in respect of the UK; private sector organisations would then be able to continue to engage in data transfers covered by that Commission decision without further formalities. In contrast, the alternatives, such as relying on so-called "standard contractual clauses", are "generally resource intensive" and "unsuitable to set up a broad framework for data exchanges"; particularly for SMEs. However, the study found that an adequacy decision would not be sufficient: public sector data exchanges, including for law enforcement purposes, are conducted on the basis of a multitude of other legal instruments that will be impacted by Brexit. Therefore a "broader legal basis" in the form of a "bespoke legal agreement" would be needed for such transfers to continue. That bespoke agreement could also allow the UK to continue to participate in the development and implementation of common EU data protection policy (e.g., continued participation by the UK Information Commissioner's Office in the GDPR "one stop shop" mechanism; but also "homogenous application of EU case law in relation to data protection, including in the UK"). The authors concede that this could be politically contentious, and would also require revision of the UK's "Withdrawal Act". The study's authors warned that Commission adequacy determination is typically a lengthy process (the Court of Justice of the EU having criticised the lack of detail in the 2000 Commission adequacy determination that underpinned the now-invalidated EU-U.S. Safe Harbor scheme). They therefore called for a "standstill period" of at least 18 months, under which the UK would effectively continue to be treated as an EU Member State for data flow purposes, allowing continued exchanges of personal data while the adequacy determination process took place. Without one, the authors conclude that a temporary halt in EU-UK data transfers might be inevitable following Brexit. The authors also pointed to a possible complicating factor: the UK's extensive law enforcement and national security investigatory powers, principally to be found in the Investigatory Powers Act 2016. It "remains to be seen" whether that Act meets EU fundamental rights standards. If it does not, "this is likely to have a negative impact on a potential adequacy decision and on information flows between the EU

Date	Description
	and UK in general." In an appearance before a UK Parliamentary Committee on 23 October 2018, the UK's Minister for Digital and Creative Industries (Margot James MP) discussed data transfer issues, and noted that: • An adequacy decision is the UK government's primary goal, but discussions have yet to commence; the European Commission is not yet ready. • The UK government will however ensure there are "various provisions in place that should allow for the free transfer of data during the period in which we are discussing adequacy but have not yet secured it." These were set out in a "technical notice" dated 13 September 2018 (see earlier commentary). The European Parliament report can be found here. A transcript of the UK Minister's comments can be found here.
12 September	**EU plans fines over misuse of voter data to sway polls** The 2018 State of Union Address (delivered on 12 September 2018) began with European Commission President Jean-Claude Juncker stating that, *"We must protect our free and fair elections. This is why the Commission is today proposing new rules to better protect our democratic processes from manipulation by third countries or private interests"*, going on to outline measures designed to ensure that European Parliament elections going forward are conducted in a *"free, fair and secure manner"*. These measures have been presented against a backdrop of proposed electoral reform by the EU legislative institutions, the catalysts being, *"Recent cases [which] have shown the risks for citizens to be targeted by mass online disinformation campaigns with the aim to discredit and delegitimise elections. Peoples' personal data are also believed to have been illegally misused. In addition, attacks against electoral infrastructure and campaign information systems are hybrid threats that need to be addressed."* The measures proposed by the European Commission include: 1 **2014 Regulation on Party Funding Amendment**: which will empower the Authority for European Political Parties and European Political Foundations to impose financial sanctions for *"breaching data protection rules in order to deliberately influence the outcome of the European elections"*. Such sanctions would amount to 5% of the annual budget of the applicable European political party or foundation. 2 **Establishment of National Election Cooperation Networks**: which would include officials from national cybersecurity, data protection and law enforcement bodies, and would designate a contact point for cooperation with an EU-level network. The aim of this network set-up is to *"enable authorities to quickly detect potential threats, exchange information and ensure a swift and well-coordinated response"*. 3 **Increased Transparency on Online Political Targeting**: this would include making public information on expenditure incurred on online political campaigns, and the targeting criteria used to advertise to voters. The European Commission further recommends that national sanctions are imposed if these transparency rules are not adhered to. **Next steps: Get approval for these measures from the Council of the European Union and the European Parliament in order that they become law.**

Date	Description
13 September	**Stronger data protection rules for EU institutions and agencies** On 13 September 2018, the European Parliament approved updated rules governing the data processing by EU institutions, bodies, offices and agencies. The proposed Regulation is currently pending approval by the Council of the European Union. Until this update comes into force, this is governed by Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The rules have been updated to align them with GDPR. Rapporteur Cornelia Ernst (GUE/NGL, DE) said: "Three months after GDPR became fully applicable in the EU it is high time to make sure that the EU's institutions are bound by the same rules. This goes in particular for the EU's law enforcement agencies." However, there are differences. The maximum fine that can be issued by the European Data Protection Supervisory Authority against an infringing party is 500,000 EUR per year. The European Parliament's press release regarding this legislation can be found here.
September - October	**EU-U.S. Privacy Shield undergoes annual review as US authorities take action to firm up the data sharing framework** The EU-U.S. Privacy Shield framework ("Privacy Shield") permits the transfer of personal data from the EU to organisations that certify to the US Department of Commerce that they will comply with the Privacy Shield Principles. To address concerns that led to the invalidation of Safe Harbor, a predecessor agreement in place from 2000-2015, Privacy Shield is subject to an Annual Joint Review process and the framework includes key commitments by US authorities to limit government access to transferred data and to enforce compliance with the framework. The following sets out some of the most recent developments over the past couple months. **(i)** Privacy Shield undergoes annual review On 18-19 October, senior US government officials met with their counterparts from the European Commission and representatives from European data protection authorities and civil liberties groups in Brussels for the second Joint Annual Review of Privacy Shield. The review, as mandated by the Commission decision authorising the framework, required the officials to consider all aspects of the functioning of the Privacy Shield, including the operation of the national security and law enforcement exceptions to the Principles. A joint statement by Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross states that the outcome of the review will be published by the end of the year. Last year's Joint Annual Review (the framework's first) recommended a number of areas for improvement, including the need for more proactive monitoring of compliance by US authorities, greater legal protections for Europeans from US surveillance and the appointment of US officials in important government posts. Nearly 4,000 companies are currently certified under Privacy Shield. **(ii)** US Federal Trade Commission ("FTC") reaches settlements with four companies for Privacy Shield violations On 27 September, the FTC announced settlements with four companies for Privacy Shield-related violations. One company was alleged to have begun but never completed an application for certification. Nonetheless, the company claimed on its website that it was Privacy Shield-certified. The three other companies were alleged to have allowed their certifications to lapse, without removing statements on their websites that they remained certified. None of the companies received financial penalties as part of the settlement. Instead, the FTC's consent orders prohibit the companies from misrepresenting their participation in Privacy Shield. Two of the companies were required to

Date	Description
	either apply Privacy Shield protections to data they have collected, or return or delete the data within ten days. When a company certifies its compliance to the Privacy Shield, its public statement becomes binding and legally enforceable under US law, where the FTC has the authority to enforce "deceptive trade practices". The four settlements follow another similar settlement in July 2018 and three others in September of last year, bringing the total number of Privacy Shield enforcement actions to eight. All such actions have to date been of a technical nature: they have focused on whether companies accurately represented their certifications rather than investigating compliance by certified companies with the Privacy Shield Principles. **(iii)** The Trump Administration fills important government posts ahead of the Joint Annual Review On 11 October, the US Senate confirmed the Trump administration's appointment of three new members (including a new chairman) to the Privacy and Civil Liberties Oversight Board ("PCLOB"). PCLOB, the US agency tasked with ensuring that counterterrorism efforts are balanced against privacy and civil liberties, is referenced in Privacy Shield as one of the safeguards for European data transferred to the US. Until the Senate's confirmation, the agency had operated since 2016 with only one member – two short of the quorum it required to perform certain of its functions. PCLOB's lack of quorum was a significant area of contention between EU and US officials, as last year's Joint Annual Review called for the vacancies to be filled and a resolution of the EU Parliament called on the Commission to suspend Privacy Shield if the appointments were not made. The appointment of new members to PCLOB followed the confirmation, in May, of three new Commissioners to the FTC. The FTC is the agency with oversight over the commercial provisions of Privacy Shield.
10 October	**UK signs modernised convention 108** The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is the only existing international treaty on data protection. On 18 May 2018, the European Council adopted an Amending Protocol updating Convention 108 which was signed by 21 states (including the UK) on 10 October 2018 (entering into force once ratified by 5 member states). This update was developed in parallel with the GDPR to ensure consistency with the result that much like the GDPR there is an emphasis on transparency, proportionality and cooperation between supervisory authorities (including a duty to co-ordinate investigations). Council of Europe membership is significantly wider than that of the European Union and the EEA member states and includes a number of non-European states such as Uruguay. This modernised version of the convention is intended to better address the increasing use of technology and the globalisation of data by ensuring adequate safeguards and raising awareness of data protection. In particular the latter point has been emphasised with supervisory authorities now having a duty to educate those involved in processing personal data. See here for a copy of the Convention.

Enforcement

UK ICO enforcement

Date	Entity / individual	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
20 September	**Equifax Ltd**	Fined £500,000	The ICO found that the UK arm of the company failed to take appropriate steps to ensure that its American parent (processing the data on its behalf) protected the information. Thus Equifax was fined for failing to protect the personal information of up to 15 million UK citizens during a cyber-attack in 2017. More here.
25 September	**Clare Lawson (Nurse)**	Prosecution	The Nurse (working at Southport and Ormskirk Hospital NHS Trust) has been prosecuted for accessing patient's medical records without authorisation. Between 2014 and 2016 the nurse was found to have inappropriately accessed the records of more than 20 patients multiple times. She was fined £400, ordered to pay costs of £364.08 and a victim surcharge of £40. More here.
28 September	**Bupa Insurance Services Ltd**	Fined £175,000	Failing to have effective security measures in place to protect the customer's personal information. A Bupa employee was able to extract the personal information of half a million customers and offer it for sale on the dark web between January and March 2017. The inadequacies in the way Bupa safeguarded personal data were systemic and unexplained. More here.

Date	Entity / individual	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
1 October	**Oaklands Assist UK Ltd**	Fined £150,000	Making thousands of nuisance direct marketing phone calls. Oaklands assist Ltd made 63,724 calls over a two month period from May to July 2017 to people who had opted out of receiving marketing calls by registering with the TPS. A total of 59 complaints were made. More here.
08 October	**Heathrow Airport Ltd**	Fined £120,000	Failing to ensure that the personal data held on its network was properly secured. On 16 October 2017 a USB memory stick was found, which had been lost by a Heathrow Airport employee. The stick, which contained 76 folders and over 1,000 files, was not encrypted or password protected. The ICO investigation found various shortcomings in the field of data protection in corporate standards, training and vision. More here.
9 October	**Boost Finance Ltd**	Fined £90,000	For sending 4,396,780 nuisance emails from January to September 2017 about pre-paid funeral plans. Emails were sent to people who subscribed to Boost Finance affiliate's websites – however, insufficient information was given about who would be sending emails, meaning that consent was not valid. In addition, information about unsubscribing was not provided meaning that the conditions for the soft opt-in were also not met. More here.

Date	Entity / individual	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
25 October	**Facebook**	Fined £500,000	The ICO has imposed a (maximum) monetary penalty of £500,000 on Facebook Ireland Ltd and Facebook Inc. as part of her Office's investigation into Cambridge Analytica. The ICO said that the penalty would have been higher if the breach had happened after the entry into force of the GDPR. More here and here from Ruth Boardman. On 29 September, Facebook also announced that it had suffered a data breach which potentially affected up to 50 million of its users and the Irish DPA was notified. The ICO also issued a statement stating that it was making enquiries with Facebook to establish the scale of the breach and if any UK citizens have been affected – watch this space!

Other Enforcement News

Date	Entity/individual	Detail
1 October	**FCA fines Tesco Bank 16.4 million following 2016 cyber-attack**	The Financial Conduct Authority ('FCA') has imposed a fine of £16.4 million on Tesco Personal Finance plc ('Tesco Bank') for "failing to exercise due skill, care and diligence" in protecting customers against a 2016 cyber-attack. Technical deficiencies (namely, flaws in Tesco Bank's debit card design) and operational deficiencies (namely, shortcomings in Tesco Bank's financial crime controls and Financial Crime Operations Team) resulted in a cyber incident lasting for more than 48 hours and the loss of £2.26 million from personal customer accounts. The FCA found that the incident was 'largely avoidable'. The FCA determined that Tesco Bank had breached Principle 2 of the FCA Principles for Business by failing to exercise "due skill, care and diligence" to: • Design and distribute its debit card; • Configure specific authentication and fraud detection rules;

Date	Entity/individual	Detail
		• Take appropriate action to prevent the foreseeable risk of fraud; • Respond to cyber-attack with sufficient rigor, skill and urgency. • In addition to emphasizing the importance of institutions implementing appropriate cyber-crime controls, the FCA stressed the importance of organisations having response plans that are "clear, well designed and well-rehearsed". • It is important to note that the figure of £16.4 million is inclusive of a series of discounts. In light of Tesco Bank's (i) "high level of cooperation" with the FCA; (ii) "comprehensive redress programme" through which customers were fully compensated; and (iii) success in blocking of a large percentage of unauthorised transactions, Tesco Bank was granted 30% credit for mitigation. Additionally, Tesco Bank agreed to early settlement of the matter with the FCA, which enabled it to benefit from a further 30% discount. If Tesco Bank had not been able to benefit from these reductions, Tesco Bank would have received a penalty of just over £33.5 million. • It is not yet known whether the Information Commissioner's Office is also investigating the incident, but this should serve as a reminder to organisations operating in regulated sectors that security breaches have the potential to attract multi-pronged regulatory action. • The Final Notice imposed on Tesco Bank by the FCA is available here and the FCA's accompanying press release is available here.