Bird & Bird

UK & EU Data Protection Bulletin: January 2019

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
December	**UK ICO updates its DPIA requirements** The ICO has updated its guidance and requirements for Data Protection Impact Assessments (DPIAs), as part of a broader update to its GDPR guidelines. The bulk of DPIA-related changes were to the ICO's list of activities for which a DPIA is mandatory. As reported in our October newsletter, the EDPB found that the ICO's draft list was overly strict, requiring DPIAs in situations that in the EDPB's view should only have been severe enough to merit a DPIA if additional risk factors were present. The ICO's latest changes implement that feedback, resulting in a list that should reduce the number of DPIAs that organisations will need to put in place in order to satisfy UK requirements. For example, whereas the ICO previously felt that DPIAs would be required by any business "tracking" individuals' geolocation or behaviour (e.g. online), this would now only trigger a DPIA if, for instance, the tracking data was also combined with other datasets, or the individuals in question were especially vulnerable. **The revised list of activities for which a DPIA is mandatory, in the UK, can be found here, with further guidance here.**
December	**ICO Regulatory Sandbox** Further to our post in our September newsletter, the ICO has published its report on the 65 responses received to its Call for Evidence regarding the creation of the ICO Regulatory Sandbox. The ICO quite clearly describes two restrictions on the scope of the sandbox: (i) the imposition of eligibility criteria for participation in the sandbox in the areas of *"innovation, public benefit and... 'fitness to participate'"*; (ii) the sandbox will not be used to *"provide test environments, dummy data sets or software tools"*; and (iii) the sandbox will not constitute any form of certification for compliance. However, beyond this, the scope of the sandbox remains undefined. Chris Taylor - a Head of Assurance at the ICO – asks for more views on, *"what you think the scope of any such sandbox should be - should we focus on particular innovations, sectors or types of organisations?"* Further, the ICO has scheduled a consultation workshop on 6 February 2019 with the objective of obtaining *"more detailed evidence, ideas and opinions"* from *"innovators working with personal data"*; presumably on, i.a. scope. The ICO states in its analysis that, *"We are currently of the view that the sandbox should be broad in scope and open to all sectors and to all types of innovation"*.

That being said, in its report, the ICO stated how encouraged it was by the support that it had received in response to the proposed launch; and in particular, by the minimal responses which viewed the ICO's approach to regulating as a barrier to innovation. Notwithstanding this, most of the key themes which the ICO pulled from the responses received are not noteworthy, aside from perhaps that: (i) some respondents were keen to encourage use of the FCA sandbox as a starting point for the development of this sandbox – the ICO is keen to distinguish the two given the former's lack of focus on personal data; (ii) some respondents raised the point that the sandbox shouldn't be the ICO's only form of public engagement; and (iii) some respondents sought *"Clarity over the relationship between our work with the sandbox and our wider regulatory action such as enforcement and requirements such as Data Protection Impact Assessments (DPIAs)"*.

UK Legislation

Date	Description
December	**Pensions cold calling: New restrictions now in force** As reported in our October newsletter, new regulations were anticipated to bring in an opt in regime for pensions cold calling. These new regulations were published on 19 December 2018 as the Privacy and Electronic Communications (Amendment) (No. 2) Regulations 2018 and came into effect on 9 January 2019. The new rules prohibit cold calling in relation to pensions, except where: • the caller is authorised by the Financial Conduct Authority, or is the trustee or manager of an occupational or personal pension scheme, and; • the recipient of the call specifically consents to calls from the caller, or has an existing client relationship with the caller such as might give rise to an expectation of receiving cold calls from that caller. **For more see: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/law-changes-on-pension-cold-calling/**

Other News

Date	Description
December/ January	**Brexit Update: draft Statutory Instrument; ICO, FTC and other guidance released** December saw the release of guidance from multiple agencies on the potential implications of Brexit on data protection rules: • The UK Government laid its draft Statutory Instrument (**The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019**) under the European Union (Withdrawal) Act 2018. Originally laid in December, the draft Regulations were replaced and relaid in January to address typographical errors. The progress of this legislation can be followed **here**. As well as amending a "UK GDPR" for use after Brexit, including conversion of potential fines into British pounds, the draft Regulations seek to preserve the validity of existing EU transfer mechanisms in UK law made out of the UK after exit day. Importantly, all existing adequacy decisions in place before exit will be recognised by the UK (including Privacy Shield), and SCCs will be considered valid even where these are unamended and are signed after exit day. BCRs already approved are also preserved, although changes are required to address the position of the UK under those BCRs. The Government is expected to release Keeling Schedules, demonstrating 'red line' amendments to the Data Protection Act 2018 and the UK GDPR. We will provide links to these in our bulletin once these become available. • The ICO has also released guidance on Brexit. This covers the effect on both UK to EU and EU to UK international transfers, and addresses other legal topics to be considered by UK businesses in the event of a no-deal such as extra-territorial scope and appointing an EU representative. The guidance can be found **here**. • The FTC has produced **FAQs** for Privacy Shield participants on the changes required to ensure that their certification also permits transfers from UK businesses following Brexit. In particular, the public commitment to Privacy Shield must be updated to include the UK as separate from the European Union. Model language for this is included in the FAQs. UK organisations reliant on Privacy Shield should ensure that this amendment is made by their US counterparts prior to exit day (whether following a no-deal Brexit or any transition period). • Some other countries have also produced guidance on the effect of Brexit. The Swiss Federal Data Protection and Information Commissioner has released **Brexit guidance** confirming that it recognises the UK as an adequate jurisdiction and does not intend to change this after Brexit. The Gibraltar Regulatory Authority also addresses the effect of Brexit on businesses in Gibraltar in its new **guidance**.

Europe

EDPB

Date	Description
4 December	**EDPB Issues Final Guidelines on the Accreditation of Certification Bodies** On 4 December, the EDPB adopted its final Guidelines on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/697). The guidelines are intended to provide a harmonised framework by which Member State data protection authorities can approve the creation of certification bodies. Certification bodies are an important element in GDPR's framework for cooperative regulation. The GDPR permits organisations to sign up to certifications as a way of demonstrating they are complying with many of the GDPR's requirements. Notably, the GDPR expressly references certification as a way of demonstrating compliance with GDPR's security, privacy by design and by default, and, for processors, Article 28 processing requirements. In addition, certifications may be used to overcome restrictions on international data transfers. Only certifications that have been issued in accordance with Article 42 will be useful for these purposes – which means that the certification must be issued by certification that have the ability to develop standards and enforce against organisations for non-compliance. For this to work, the certification bodies must be properly accredited by either Member State data protection authorities or national accreditation bodies (which are created pursuant to ISO/IEC 17065/2012 standards). The Guidelines are directed to the data protection authorities and accreditation bodies to ensure they apply harmonised standards when approving certification bodies. In a significant departure from the draft Guidelines issued in February 2018, the updated Guidelines include a detailed draft Annex, which sets out additional accreditation requirements that align with ISO/IEC 17065/2012. The draft Annex is open for public consultation until 01 February 2019.

4-5 December

EDPB holds its 5th Plenary Session

In its press release the EDPB has highlighted the three main areas of discussion during this session:

1. Opinion on Japan draft adequacy decision

In this opinion the EDPB focuses on the provision of sufficient warranties for an adequate level of data protection. The EDPB outlines that to achieve this level of protection the Japanese framework does not necessarily need to replicate that of the EU but welcomes the increased convergence between both frameworks.

The EDPB expressed some concerns in particular with regards to data transfers from EU to Japan and asked for clarifications.

Finally the EDPB reiterates its view that this adequacy decision is of utmost importance as it is the first decision of this kind under the GDPR and it will set a precedent for further decisions.

2. DPIA lists

Opinions were adopted by the EDPB on Data Protection Impact Assessments (DPIA) lists submitted by 4 countries (Denmark, Croatia, Luxembourg and Slovenia). These lists, highlighting the processing activities for which a DPIA is mandatory, are important to ensure the consistency of the application of the GDPR across the EEA according to the EDPB.

The 4 new opinions are in line with the first 22 opinions adopted during the EDPB's 3rd plenary session in September and will help establishing common criteria across the Member States.

The EDPB expressed its satisfaction in achieving not "full harmonisation" but "more consistency" for the implementation of the GDPR through these opinions on DPIAs.

3. Guidelines on accreditation

A revised version of the WP29 (the body replaced by the EDPB) guidelines were adopted (see earlier commentary).

Date	Description
December	**EU-U.S. Privacy Shield Update**

a) Privacy Shield Passes Second Annual Review

On 19 December, the European Commission concluded that the Privacy Shield framework continues to ensure an adequate level of protection for personal data transferred to participating companies. The Commission's second Annual Report acknowledged measures taken by US authorities to address the Commission's concerns from the first Report a year earlier. Addressing concerns with commercial protections afforded under the framework, the Report highlighted US efforts to increase oversight over commercial practices. These measures included:

- A requirement for Privacy Shield applicants to delay publicly listing their participation until the US Department of Commerce ("DoC") has finalised its review of the application.
- The introduction of processes by DoC to better monitor compliance, such as random spot checks (including of more than 100 certified companies), monitoring of public reports concerning data handling, and the use of technical tools to scan the web for false claims of certification.
- The referral of more than 50 cases to the Federal Trade Commission ("FTC") for investigation and enforcement.

The commercial review also took into account initiatives to develop a US federal data privacy law.

On the government access side, the Report noted the appointment and confirmation of three new members to the Privacy and Civil Liberties Oversight Board, as well as the continued protections afforded by Presidential Policy Directive 28 ("PPD-28"), which restricts the purposes for which data can be accessed for national security. Although PPD-28 was not enshrined into legislation as the Commission had previously recommended, neither was the executive directive withdrawn, as the Commission feared the Trump administration might do.

While recognising these positive steps, the Report was critical of the US government's failure to appoint a permanent Ombudsperson to oversee compliance with the government access provisions. However, recent reports indicate that the Trump Administration has committed to appoint a permanent Ombudsperson.

b) European Commission Publishes Report on Privacy Shield Protections from Automated Decision-Making

In October 2018, the European Commission released the outcome of its study on Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield. For background, unlike the GDPR, the Privacy Shield framework does not include provisions governing significant automated decisions. Rather, the adequacy decision required the European Commission to start "*a dialogue on automated decision-making, including an exchange on the similarities and differences in the EU and U.S. approach in this regard*".

The study first noted the significant divergence between GDPR's omnibus protection from automated decision-making in all sectors

compared to the US approach, which includes sector-specific legislation as well as constitutional and civil rights protections from discrimination on the basis of protected classes. Despite the differences in approach, the study concluded that significant protections exist in US law, at least in areas where automated decisions are likely to be most consequential. US protections include:

- Credit reporting and lending acts provide rights to an explanation of decisions and an ability to contest;
- Equal protection statutes, such as the Civil Rights Act and the Fair Housing Act allow individuals to challenge automated decisions when based on protected characteristics, such as race, ethnicity, sexual orientation, etc.;
- The Due Process Clause of the Constitution provides procedural and substantive protections against government decisions affecting rights and entitlements; and
- The Federal Trade Commission Act (and similar state statutes) protects consumers against automated decisions that are "unfair or deceptive".

18 December

Draft Ethics Guidelines for AI Released by the European Commission

The European Commission's High-Level Expert Group on Artificial Intelligence (the 'AI HLEG') has published a first draft of Ethics Guidelines for Trustworthy AI (the 'Guidelines'). The Guidelines are the first of two deliverables being prepared by the AI HLEG to support the European Commission's implementation of its vision for AI (as set out in its Communications of 25 April 2018 (available here) and 7 December 2018 (available here)). The AI HLEG emphasises that the aim of the Guidelines is to offer guidance on the "concrete implementation and operationalisation" of AI, rather than being another attempt to establish core values and principles for AI. They are aimed at all organisations developing, deploying or using AI and, once complete, will incorporate a mechanism enabling organisations to voluntarily sign-up to the Guidelines.

The Guidelines are predicated on the basis that, whilst AI can have "tremendous" benefits for individuals and society, it also gives rise to risks which must be minimised by adopting a "human-centric" approach to AI (namely, AI should be used with the goal of increasing human well-being). The AI HLEG considers the concept of "Trustworthy AI" to be the "north star" in pursuit of this, and uses the Guidelines to establish a three-part framework for this, consisting of: (i) Ethical Purpose; (ii) Realisation of Trustworthy AI; and (iii) Assessment of Trustworthy AI.

Chapter 1: Ethical Purpose

The AI HLEG sets out the following key guidance for ensuring that AI systems have an ethical purpose:

- AI must be human-centric. This means that it should have an “ethical purpose” which reflects fundamental rights, societal values and the ethical principles of Beneficence (do good), Non-Maleficence (do no harm), Autonomy of Humans, Justice, and Explicability.

- The possible effects of AI on individuals and the common good should be evaluated in light of fundamental rights, ethical principles and values. Extra consideration should be given where vulnerable individuals are involved (e.g. minorities, children, people with disabilities) or where there is an imbalance in power or information (for example, in the employment or consumer context).

- Organisations should be vigilant for areas of 'critical concern'. In the Guidelines, AI HLEG flags: identification without consent; covert AI systems; certain types of citizen scoring; and lethal autonomous weapon systems as areas of critical concern, but notes that this was an area of disagreement between members. The AI HLEG specifically seeks input on this point.

Chapter 2: Realisation of Trustworthy AI

The AI HLEG sets out the following key guidance for the realisation of Trustworthy AI:

- The following requirements for Trustworthy AI should be incorporated from the earliest design phase (explanation of each of these requirements is set out on pages 14 to 18 of the Guidelines):

  - Accountability;
  - Data Governance;
  - Design for all;
  - Governance of AI Autonomy (Human oversight);
  - Non-Discrimination;
  - Respect for Human Autonomy;
  - Respect for Privacy;
  - Robustness;
  - Safety;
  - Transparency.

- Technical and non-technical methods of implementing these requirements into the AI system should be considered at all stages of development (namely, when assembling the team working on the AI system, the AI system itself, the testing environment and the potential applications of the AI system).

- Information relating to the AI system's capabilities and limitations should be provided to individuals in a clear and proactive way, ensuring that realistic expectations are set. Ensuring that decisions of the AI system are traceable is also key.

- Trustworthy AI should be part of the organisation's culture, and information should be provided to stakeholders on how Trustworthy AI is implemented into the design and use of AI systems. Trustworthy AI can also be included in organisations' codes of conduct and ethical guidelines.

- Stakeholders should be involved in the design and development of the AI system, and diversity should exist in the teams responsible for developing, implementing and testing.

- AI systems should be auditable and, as far as possible, designed to enable individual decisions to be traced and explained.

- A specific process for accountability governance should be put in place.

- Managers, developers, users and employers should be made aware of, and trained in, Trustworthy AI.

- There might be fundamental tensions between different objectives (e.g., correcting bias might conflict with privacy principles). These conflicts should be communicated and documented.

- Research and innovation should be fostered to further the achievement of the requirements for Trustworthy AI.

Chapter 3: Assessment of Trustworthy AI

The AI HLEG sets out the following key guidance for assessing Trustworthy AI:

- An assessment list should be adopted when developing, deploying or using AI, and adapted for the specific use of the AI system. In this Chapter, the AI HLEG sets out an example assessment list, establishing criteria to determine whether the requirements described in Chapter 2 are met. The AI HLEG specifically seeks input on this point.

- The AI HLEG stresses that the assessment list must be tailored to the specific use case in which the AI system is being deployed. The AI HLEG will develop examples of tailored assessments for (i) healthcare diagnosis and treatment; (ii) automated driving/moving; (iii) insurance premiums; and (iv) profiling and law enforcement, for inclusion in the final version of the Guidelines. The AI HLEG specifically seeks input on this point.

- An assessment list will never be exhaustive, and that ensuring Trustworthy AI is a continuous process of identifying requirements, evaluating solutions and ensuring improved outcomes throughout the entire lifecycle of the AI system.

The draft Guidelines are available here [hyperlink:

https://ec.europa.eu/futurium/en/ai-stakeholders-consultation/draft-ethics-guidelines-trustworthy-ai]. The AI HLEG is accepting feedback on the draft Guidelines until 1 February, here [hyperlink:

https://ec.europa.eu/futurium/en/ai-stakeholders-consultation/stakeholders-consultation-draft-ai-ethics-guidelines]. A final version of the Guidelines is due to be published in March 2019.

4-5 December

EDPB holds its 5th Plenary Session

In its press release the EDPB has highlighted the three main areas of discussion during this session:

1. Opinion on Japan draft adequacy decision

In this opinion the EDPB focuses on the provision of sufficient warranties for an adequate level of data protection. The EDPB outlines that to achieve this level of protection the Japanese framework does not necessarily need to replicate that of the EU but welcomes the increased

convergence between both frameworks.

The EDPB expressed some concerns in particular with regards to data transfers from EU to Japan and asked for clarifications.

Finally the EDPB reiterated its view that this adequacy decision is of utmost importance as it is the first decision of this kind under the GDPR and it will set a precedent for further decisions.

On 23 January 2019, the Commission has adopted its adequacy decision on Japan, allowing personal data to flow freely between the two economies on the basis of strong protection guarantees. Japan agreed to put in place additional safeguards to protect the data including a set of supplementary rules that address some of the key gaps between the regimes, additional assurances regarding access by Japanese public authorities for criminal law enforcement and national security purposes and a complaints handling mechanism. The decision will be reviewed again after two years. For more see here.

2. DPIA lists

Opinions were adopted by the EDPB on Data Protection Impact Assessments (DPIA) lists submitted by 4 countries (Denmark, Croatia, Luxembourg and Slovenia). These lists, highlighting the processing activities for which a DPIA is mandatory, are important to ensure the consistency of the application of the GDPR across the EEA according to the EDPB.

The 4 new opinions are in line with the first 22 opinions adopted during the EDPB's 3rd plenary session in September and will help establishing common criteria across the Member States.

The EDPB expressed its satisfaction in achieving not "full harmonisation" but "more consistency" for the implementation of the GDPR through these opinions on DPIAs.

3. Guidelines on accreditation

A revised version of the WP29 (the body replaced by the EDPB) guidelines were adopted. These guidelines aim at providing guidance on the interpretation of Article 43 of the GDPR. In particular, to help Member States authorities establishing a consistent view for the accreditation of certification bodies. A new annex has been added to the guidelines providing the additional requirements to consider for supervisory authorities.

EU Legislation

Date	Description
December	**e-Privacy Regulation: Disagreement continues** A progress report published by the Council of Minister highlights the continued disagreement between EU Member States on the draft e-Privacy Regulation. The Report outlines the area of contention in addition to the concessions which the Austrian Presidency have proposed in order to overcome the disagreement. The key dilutions proposed by the Austrian Parliament include: (a) The removal of the privacy by design rules in Article 10 in relation to cookies and similar technologies. These draft rules required all browsers and apps to provide users with choice as to cookies on installation or subsequent changes to cookie usage. According to the Report, the removal of these provisions was based on '*the burden for browsers and apps, the competition aspect, the link to fines for non-compliance, but also the impact on end-users and the ability of this provision to address the issue of consent fatigue, thus raising doubts about its added value'*. (b) Making the processing of electronic communications data more permissible by introducing a ground for further processing of metadata for compatible purposes (thus avoiding the need for GDPR level consent). This ground takes inspiration from the lawful basis of legitimate interest under the GDPR. Other areas of contention include the wider treatment of cookies and similar technologies in particular around the permissibility of cookie walls and the policy considerations this poses; in addition to the role of European Regulators in enforcing the new Regulation.
11 December	**The new Electronic European Communication Code ("EECC") Directive was adopted:** This code expands the regulation of electronic communications to more services; it needs to be implemented into national laws of EU member states by 21 December 2020. It recognizes that the traditional telecommunications service should not be the only one to carry the burden of regulation and that Over the Top providers which deliver services across an IP network (OTT's) should also be regulated. Indeed, Recital 15 of the EECC notes that end-users must be protected when using "functionally equivalent services" and a new definition of "electronic communications service" is adopted at art.2(4). The new definition encompasses the notion of "interpersonal communications service" (art.2(5)), which is: "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiative or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor

ancillary feature that is intrinsically linked to another service" (art.2(5)).

As a result of this new framework, the rules requiring confidentiality of communications and restricting use of traffic and location data by providers of electronic communications services, among others, will now be applicable to OTTs.

Interestingly, Recital 16 of the code recognises that personal data can count as "remuneration" for the provision of electronic communications services: "the concept of remuneration should therefore encompass situations where the provider of a service requests and the end-user knowingly provides personal data within the meaning of [the GDPR]. [It] should therefore also encompass situations in which the end-user is exposed to advertisements as a condition for gaining access to the service, or situations in which the service provider monetises personal data it has collected in accordance with [the GDPR]".

This recital clarifies what "normally provided for remuneration" actually means in the context of electronic communication services. However, the concept of services being paid for by advertisers is not new. This is in line with the long standing position of the CJEU in various cases in the audio visual context (e.g. C-352/85 - Bond van Adverteerders v State of the Netherlands) in which the ECJ confirmed that the service does not need to be paid for by those for whom it is performed. The position of the Court in these cases was that services are "normally provided for remuneration" if they are provided in return for payments made by advertisers.

Cases

Date	Description
December	**Facebook Like Button: Advocate General Finds Co-Controllership between Website Operator and Facebook.** In this case Verbraucherzentrale NRW pursed a claim against the German e-commerce company Fashion ID for purported unlawful data collection through the Facebook 'like' button. In particular, the Facebook 'like' button purportedly collected data such as IP address regardless of whether the user clicked the link or whether the user had a Facebook account. In the Advocate General's Opinion, Facebook Ireland and Fashion ID were co-controllers jointly responsible for each other's processing on the basis that both Fashion ID and Facebook were pursuing commercial purposes in a way mutually complementary: 'Fashion ID and Facebook Ireland co-decide on the means and purposes of the data processing at the stage of the collection and transmission of the personal data at issue,' Fashion ID's liability would not, according to the Advocate General, however, extend to secondary processing by Facebook outside its knowledge and control.

Fashion ID was the party best placed to provide notice of the data sharing and the co-controllership to users.

The Advocate General also disagreed with submissions from the European Commission that those data subjects who were Facebook users may have consented to the processing, with the Advocate General finding it unreasonable that Facebook users should be subject to less robust protections:

'It thus appears that the defendant and Facebook Ireland co-decide on the means and purposes of the data processing at the stage of the collection and transmission of the personal data at issue,'

The Court concluded that the consent and information obligations of Fashion ID should be the same vis-à-vis the data subjects irrespective of whether they had a Facebook account.

How the European Court of Justice will ultimately decide the case remains to be seen, but in light of the Advocate General's Opinion and the earlier European Court of Justice decision in Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd (Case C-210/16) a designation of co-controllership is likely. The CJEU's press release can be found here.

Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
November	**Multiple**	**ICO issues fines to businesses in various sectors for non-payment of data protection fee** The ICO has issued the first fines for non-payment of data protection fees (under the Data Protection Act 2018) to data controllers in multiple sectors including: construction, finance and health. All data controllers (including organisations, companies and sole traders) must register and pay the associated fee or face a fine of up to £4,350. More than 900 notices of intent to fine have been issued by the ICO since September 2018 and more than 100 penalty notices have been issued. Data controllers are advised to review their registration status to avoid facing such enforcement. You can search the register here and join the register here.	
13/12/18	**Tax Returned Limited**	Monetary Penalty: Direct Marketing	The London based company was fined £200,000 for instigating direct marketing through a third party provider. 14,800,000 messages were sent without the appropriate consent resulting in 2,146 complaints to the ICO. The company's argument that consent was obtained through policies on third party websites was rejected by the ICO who found the wording of these policies to be insufficiently clear. This is another example of the negative outcomes of insufficient due diligence when engaging third party marketers. The notice can be found here.

09/01/19	**SCL Elections Limited**	Criminal fine	SCL Elections Ltd (linked with Cambridge Analytica) was fined £15,000 (+ £6000 costs and a £170 victim surcharge) for failing to comply with an enforcement notice issued in May 2018 (pursuant to S47(1) Data Protection Act 1998). This enforcement action is part of the ICO's wider investigation into data analytics for political purposes.

Other notable enforcement actions

Date	Description
January	**The French DPA (CNIL) has issued its first sanction under GDPR fining Google €50 million** You can find our perspective here.