Bird & Bird

UK & EU Data Protection Bulletin: March 2019

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
18 February	**Update to the ICO – FCA Memorandum of Understanding** In February the UK's Information Commissioner's Office (ICO) announced, and the Financial Conduct Authority (FCA) signed, an updated Memorandum of Understanding setting out the terms of their "future working relationship in areas of mutual regulatory interest". The ICO and FCA have agreed, where permitted, that the ICO will alert the FCA to potential breaches of legislation regulated by either party. They also agreed to communicate regularly on issues of mutual interest and to consult one another on issues that may have significant implications for the other. The Memorandum also provides for further exchanges of information (where permitted by law) and for each regulator to request information from the other. The Memorandum goes on to set out the purpose and legal basis for this information sharing. The ICO and FCA have agreed to consult and co-ordinate in respect of reviews, calls for evidence and recommendations where appropriate, and to work together where there is a major incident of mutual interest at an FCA regulated firm. As part of this cooperation, where there are areas of overlap, the two parties will work to ensure that the most appropriate body commences and leads investigations. The Memorandum is to be monitored by both parties and will be reviewed biennially.
28 February	**Nuisance Calls and Banned Directors** Since legislation was introduced 15 years ago, ICO investigations into nuisance marketing have led to 16 company directors being banned from running a company for more than 100 years between them. These include Keith Hancock of LAD Media (4 years), Shaun Harkin of Easyleads Ltd (6 years) and Aaron Stalberg of Lead Experts (6 years). The most recent ban issued by the Insolvency Service was an 8 year ban given to Richard Jones after his two companies made 220 million automated nuisance calls and failed to pay the fines issued by the ICO. During the case the ICO blocked an application by Mr Jones to have the businesses wound up and the case was then referred to the Insolvency Service. The ICO has said "This is typical of the type of case we refer to the Insolvency Service". In December 2018 new legislation (Privacy and Communications (Amendment) Regulations 2018) came into force giving the ICO the power to hold directors and other company officers personally liable for such fines. The partnership with the Insolvency Service looks set to continue as the ICO and Insolvency Service both pledge to work closely to clamp down on directors like Richard Jones.

7 March

Advice for GPs handling subject access requests for medical records:

Since the GDPR came into effect last year there has been an increase in the number of SARs received by medical practices, as is the case in many other sectors. The ICO has acknowledged the increase in workload this causes and so has suggested the following tips for dealing with SARs:

- Provide online access to patient health records – the ICO is working with organisations in the health sector looking at different options for this.
- Responses can be provided electronically and only need to provide paper copies where requested and where it is reasonable to do so.
- Where there is a large volume of information ask for clarification on what information would the patient or their representative deem as acceptable to satisfy the SAR.
- The cost of providing the initial copies must be borne by the GP practice but further copies can be charged for.

Often requests are made by legal representatives on behalf of patients and these need to be responded to in the same way. The BMA have produced a form that legal representatives can use when submitting requests. The ICO reminds GP practices to consider the following when responding to such requests from third parties:

- "Ask for evidence that the third party has the clear, specific authority of the data subject to exercise their right of access".
- If a GP thinks the request goes beyond what is necessary they can check that the patient is aware of what is being requested.
- If the practice is concerned that it is giving out "excessive information" the data can be provided directly to the data subject who can then choose what to pass on to their representative.

GP practices also receive requests from insurers, the mechanism for which is the Access to Medical Reports Act 1988 which allows practices to charge insurance companies a fee for access to patient information. The ICO expects insurers to use this mechanism and previously formalised this expectation with the industry.

The BMA has also updated its guidance regarding access to health records here.

Date	Description
5 March	**Data Protection (Charges and Information) (Amendment) Regulations 2019** The Data Protection (Charges and Information) Regulations 2018 (the "Funding Regulations"), enacted via the Digital Economy Act 2017, set out a requirement for data controllers to provide certain information and to pay a charge to the ICO. The Schedule to the Funding Regulations outlines various exemptions from this requirement. The Data Protection (Charges and Information) (Amendment) Regulations 2019 ("**Funding Amendment Regulations**") introduces a new exemption as follows: a. **Members of House of Lords**: The processing of personal data by members of the House of Lords (and those acting with their authority) for the purposes of exercising that member's functions; b. **Elected Representatives**: The processing of personal data by elected representatives (and those acting with their authority) where the processing is used solely for the purposes of standing for or fulfilling the office of elected representatives; and c. **Prospective Representative**: The processing of personal data by a person seeking to become (or remain) an elected representative (and those acting with their authority) in connection with any activity reasonably regarded as intended to promote or procure the election (or re-election) of that prospective representative. The Explanatory Memorandum to the Funding Amendment Regulations explains that the rationale for the new exemption is that *"the charges constituted a 'barrier to democracy' and that activity deriving from public office should not be liable to a charge"*. The new exemption took effect on 1 April 2019. It will result in a loss to the ICO's funding of approximately £720,000 per year based on the approximated 18,000 members of the House of Lords, elected representatives, and prospective representatives. The Explanatory Memorandum gave a useful insight that *"some elected representatives currently claim the cost of the charge as an expense [and therefore] this also represents a potential saving to the public purse"*.
6 March	**Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No.2) Regulations 2019** The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the "**Main Regulations**"): (i) transfer the European Commission's powers under the GDPR to make adequacy decisions to the UK Secretary of State; and (ii) contain transitional provisions which seek to enable personal data to continue to be transferred from the UK to countries in respect of which the European Commission made an adequacy decision before 29 March 2019. One such decision is that on which the Privacy Shield – i.e. the mechanism by which transfers of personal data from the European Economic Area ("**EEA**") can be legally made to US companies which have certified under that mechanism - is based.

According to the applicable Explanatory Memorandum, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No.2) Regulations 2019 (the "**Amendment Regulations**") *"correct a deficiency in the retained EU law and ensure it operates effectively after EU exit"* i.e. the Amendment Regulations *"amends the transitional provisions of the Main Regulations to provide that transfers of personal data from the UK in reliance on Privacy Shield can only take place after 29 March 2019 in a no deal scenario, if the certified Privacy Shield company has a privacy policy which includes a commitment to comply with the Privacy Shield Principles in relation to personal data transferred from the UK"*.

The only cost to UK businesses which is envisaged by the applicable Explanatory Memorandum is the cost of checking that their US counterparts' online privacy policies contain wording which extends the application of the Privacy Shield Principles to personal data received from the UK.

Other News

26 February

Argentina approve the UK as an 'adequate' jurisdiction for data transfer purposes

Argentinian data protection laws restrict the transfer of personal data to jurisdictions which do not offer adequate protection to personal data. All EU Member states are currently recognised as adequate jurisdictions under Argentinian data protection laws, but upon the UK's exit from the EU it will no longer benefit from this existing adequacy finding. Following a formal request from the UK, the Argentine Agency of Access to Public Information passed Resolution No. 34/2019 (published on 26 February 2019) to 'whitelist' the UK and Northern Ireland for data transfer purposes.

8 March

CIPL Issues White Paper on the Regulatory Sandbox Following Joint Roundtable with the ICO

Further to our prior posts regarding the ICO regulatory sandbox, the Centre for Information Policy Leadership ("CIPL") issued a white paper on Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice (the "White Paper") on March 8, 2019, following a joint roundtable with the ICO.

The White Paper sets out the key features of the regulatory sandbox and lists a series of relevant developments regarding the concept in data protection in different jurisdictions. It outlines the main benefits of sandbox participation for organisations, data protection authorities, society and economy, and individuals. The White Paper also identifies some key concerns from organisations, and points out the mutual trust as the key to success. In its White Paper, CIPL puts forwards with the practicalities of setting up the sandbox to maximise the prospects of success, including possible criteria for acceptance into the sandbox and safeguards to address apprehension by potential participants. The White Paper also discusses the relationship between the regulatory sandbox and data protection impact assessments and considerations surrounding the international application of the sandbox.

Separately the ICO has now opened its beta phase for the Sandbox and is accepting applications. For more information, see here.

14 March	**DIFC approve the UK as an 'adequate' jurisdiction for data transfer purposes** Dubai International Financial Centre (DIFC) data protection laws restrict the transfer of personal data to jurisdictions which do not offer adequate protection to personal data. All EU Member states are currently recognised as adequate jurisdictions under DIFC data protection laws, and the Commissioner of Data Protection for the DIFC has confirmed in a circular (issued on 14 March 2019) that the UK's adequacy status will continue to exist after its exit from the EU.
26 March	**AI: A top strategic priority for the ICO** The ICO is looking to develop a new auditing framework intended to provide a solid methodology to audit AI applications and ensure they are transparent and fair and to ensure that the necessary measures to assess and manage data protection risks arising from them are in place. It is informally seeking views to inform its thinking prior to the publication of a formal consultation, expected in January 2020. The final AI auditing framework and the associated guidance for firms is on track for publication by spring 2020. For more see here.

Europe

EDPB

Date	Description
12 February	**Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under GDPR** The aim of the guidelines is to "provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR". Articles 40 and 41 of the GDPR relate to codes of conduct and the accreditation of bodies to monitor compliance with codes of conduct. The public consultation on these guidelines closed on 2 April 2019. The guidelines are important for any bodies submitting codes, as they clarify the procedures and the rules involved in the submission, approval and publication of codes at both a national and European level as well as the requirements for the effective monitoring of compliance with a code. The guidelines are also useful for harmonisation purposes – the guidelines say that they should act as a clear framework for competent supervisory authorities, the EDPB and the European Commission to evaluate codes in a consistent manner and to streamline the procedures involved in the assessment process. It is noted that guidance on codes of conduct as a tool for transfers of data as per Article 40(3) of the GDPR will be considered in separate guidelines to be issued by the EDPB at a later date. **Admissibility of a draft code:** There are a number of conditions to be met before a competent supervisory authority would be in a position to undertake a full assessment and review of a code for the purposes of Article 40(5) of the GDPR. In summary, these conditions are as follows: • Include a clear and concise explanatory statement in the code; • Demonstrate that the representative body submitting the code is capable of effective representation; • Ensure the code precisely determines the processing it governs, the categories of relevant controllers or processors and the issues it seeks to address; • Make the territorial scope clear; • Ensure that the chosen supervisory authority is competent in accordance with Article 55 of the GDPR; • Identify the monitoring body and the mechanisms which enable that body to carry out its functions as per Article 41 of the GDPR (the guidelines go into some detail about the accreditation requirements for monitoring bodies); • Include information about the extent to which the consultation has been carried out (Recital 99 of the GDPR indicates that a consultation should take place with the relevant stakeholders including data subjects, where feasible);

- Confirm compliance with national legislation (in particular, where the code involves sectors governed by specific national laws or processing subject to specific national requirements);
- Use the language of the competent supervisory authority (and if the code is transnational, it code should be submitted in English too); and
- Use the checklist provided in Appendix 3 of the guidelines to help frame the submission of the draft code.

Criteria for approving codes:

The guidelines highlight that a body or bodies submitting draft codes should be able to demonstrate that their draft code:

- meets a particular need of that sector or processing activity;
- facilitates the application of the GDPR,
- specifies the practical application of the code to GPDR that does more than just re-state GDPR - it should aim to codify how the GDPR shall apply in a specific, practical and precise manner;
- provides sufficient safeguards and provides effective mechanisms for monitoring compliance with a code.

Submission:

The guidelines also contain guidance on the different stages of a submission for national code and a transnational code.

The guidelines explain that a competent supervisory authority should determine if a submitted code meets the admissibility criteria before it reviews the content of a draft code.

The EDPB explains that the review process should not serve as a consultation opportunity, so code owners should consult on the content of a draft code before submitting it for review. Under the review process, the competent supervisory authority is just required to provide an opinion on whether the draft code complies with the GDPR. Competent supervisory authorities may get in touch with code owners for clarifications and further information.

The guidelines can be found here.

12 & 13 March

EDPB 8th plenary session

On 12 & 13 March 2019 the European Data Protection Board (EDPB) met for their eighth plenary session. Matters covered in the session included the adoption of:

(a) the EDPB Opinion on the interplay between the e-Privacy Directive and GDPR (see below and here);

(b) a statement calling upon EU legislators to intensify efforts towards the adoption of the e-Privacy Regulation. The EDPB emphasised that 'under no circumstances' should the new e-Privacy Regulation lower the level of protection by the current e-Privacy Directive;

(c) a statement on the use of personal data during election campaigns. In the statement available here, the EDPB highlights a number

of key points which need to be taken into consideration when political parties process personal data in the course of electoral activities; and

(d) opinions on the Data Protection Impact Assessment lists submitted by the Spanish and Icelandic DPAs.

Opinion on Interplay between the e-Privacy Directive and the GDPR

On the 12 March 2019 the EDPB adopted an opinion on the interplay between the ePrivacy Directive and GDPR, in particular regarding the competence, tasks and powers of data protection authorities. The opinion was published in a response to a request from the Belgian DPA seeking more clarity in the area.

Overlap between GDPR and the e-Privacy Directive

This EDPB guidance acknowledges that while there is an overlap in material scope between the e-Privacy Directive and GDPR. There are numerous processing activities which trigger the material scope of the e-Privacy Directive and the GDPR – a key example is the use of cookies and similar technologies. Such overlap does not lead to a conflict between the e-Privacy Directive and GDPR. This is because Article 1(2) of the e-Privacy Directive expressly provides that the *'the provisions of this Directive particularise and complement Directive 95/46/EC (…)'*.

The e-Privacy Directive and the GDPR therefore work together because the e-Privacy Directive particularises i.e. renders more specific rules in some areas (for example on telecommunications traffic data or the storing of information on an end user's device). In such cases, these specific provisions of the e-Privacy Directive take precedent over the more general provisions of the GDPR in accordance with the principle *lex specialise derogate legi generali* - a legal principle meaning simply that specific law prevails over general law.

Accordingly, the EDPB Guidelines clarify that 'any processing of personal data which is not specifically governed by the ePrivacy Directive (or for which the ePrivacy Directive does not contain a 'special rule'), remains subject to the provisions of the GDPR.'

EDPB give the example of a data broker who engages in profiling based on cookie data but also other personal data obtained from other sources (i.e. non-cookie data). The placing or reading of cookies must comply with Article 5(3) of the e-Privacy Directive (as in accordance with the lex specialis principle, the special rule in the e-Privacy Directive applies). However GDPR will apply to the subsequent processing of personal data involved in the profiling and such processing must also have a legal basis under Article 6 GDPR.

Enforcement

The Belgian DPA raised two questions relating to enforcement where the e-Privacy Directive and GDPR intersect.

Question 1: Does the fact that the processing of personal data engages the material scope of both the GDPR and the e-Privacy Directive, limit the competences, tasks and powers of EU data protection authorities under GDPR?

The EDPB clarified that where processing engages both the e-Privacy Directive and the GDPR, EU data protection authorities are competent

	to scrutinize the data processing operations which are governed by national e-Privacy rules only if national law provides for this. However, the fact that a subset of the processing falls within the scope of the e-Privacy Directive, does not limit the competence of EU data protection authorities under the GDPR with regard to the processing operations which are not subject to the special rules contained in the e-Privacy Directive. **Question 2: When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the e-Privacy Directive, and if so to what extent?** The EDPB clarified that the body appointed by Member States for enforcing the national law transposing the e-Privacy Directive is exclusively responsible for enforcing the e-Privacy Directive. However, data protection authorities remain competent in regard to any processing operations performed upon personal data which is not subject to the more specific rules contained in the e-Privacy Directive. A data protection authority may take the fact there has been an infringement of e-Privacy rules into consideration when applying the GDPR (e.g. when assessing compliance with the lawfulness or fairness principle under GDPR). However, any enforcement decision must be justified on the basis of the GDPR, save in circumstances where the data protection authority has been granted additional competences by Member State law. **Co-Operation and Consistency Mechanisms** The EDPB clarified that the cooperation and consistency mechanisms available to data protection authorities under the GDPR concern the monitoring of the application of GDPR provisions. The GDPR mechanisms don't apply to the enforcement of the provisions contained in the e-Privacy Directive. The cooperation and consistency mechanism remains fully applicable where the processing is subject to the general provision of GDPR and not the 'special rule' in the e-Privacy Regulation.
26 March	**EDPB publishes fine from Polish Data Protection Authority regarding failure to provide appropriate notice. For more, please see our Bird & Bird update here.**
15 March	**EDPB LIBE Report on overview of the first 9 months of the implementation of GDPR** This report examines how the cooperation and consistency mechanisms have been working under GDPR and have concluded that they seem to work well in practice. Some interesting statistics arise from this report: • 642 procedures have been initiated to the EDPB to identify the Lead Supervisory Authority. Nearly half have been closed and there has been no dispute on the outcome. • The main topics giving rise to cross border complaints relate to the exercise of individual rights, consumer rights and data breaches • 45 one stop shop procedures have been initiated (with 6 reaching final decisions) • 44 mutual assistance requests have been triggered by supervisory authorities from 18 different EEA member states

- 28 consistency opinions have been provided by the EDPB on national lists for DPIAs and 1 opinion on a draft administrative arrangement for the transfer of personal data between financial supervisory authorities.
- Most supervisory authorities have increased their budget and headcount
- Total number of cases reported by supervisory authorities to the EDPB is just over 200,000, with total fines of €55.9 million (most of this being against Google).

For more see here.

Other EU News

Date	Description
7 February	**ENISA published a much anticipated set of guidelines describing the "state of the art" in IT security** The European Union Agency for Network and Information Security (ENISA) and TeleTrusT, a German IT Security Association, have co-operated to publish guidance on a starting point for technical and organisational security measures which organisations should consider adopting. Whilst the guidance has in mind how organisations should comply with Germany's IT Security Act it also aims to assist with the GDPR's provisions on "appropriate" personal data security measures (Article 32) and so provides a useful reference point in that regard. The guidance is comprised of 72 pages of security recommendations. The core of the document (its chapter 3) sets out useful checklists and reference points for different technologies and security scenarios, for instance password strength assessment, server hardening, disk encryption, router security and mobile device management. Copies in English are available here.
5 March	**Report of Global Privacy Enforcement Network Sweep 2018 - 'Privacy Accountability' was published** The Global Privacy Enforcement Network (GPEN) has conducted the '2018 GPEN Sweep', aiming to consider how well organisations have implemented the concept of privacy accountability into their own internal privacy programs and policies. The report concludes that whilst most organisations have a good understanding of the basic concepts of accountability, in practice there is room for improvement. Organisations need to ensure that they continue to monitor their performance to ensure they are adhering to the data protection standards laid out in the relevant laws and regulations, and ensure that they have clear, documented procedures in place to deal with data security complaints. According to the report, 356 out of 667 organisations that the GPEN contacted gave substantial responses to the GPEN Sweep, leading to the following positive observations: • A large percentage of organisations had appointed an individual or team who would assume responsibility for ensuring that their organisation complied with relevant data protection rules and regulations. • Organisations were generally found to be quite good at giving data protection training to staff. • A large majority of organisations actively maintain privacy policies explaining how they handle personal data, which are often easily

accessible.

- Organisations that did have monitoring programmes in place generally gave examples of good practice, noting that they conducted annual audits or reviews and/or regular self-assessments.
- Over half of the organisations surveyed indicated that they have documented incident response procedures, and that they maintain up to date records of all data security incidents and breaches.

However, there exist some negative observations as well:

- Organisations often failed to provide refresher training.
- A number of organisations indicated that their privacy policies may not necessarily be easily accessible, may lack key principles of data protection, may be outdated, or have no privacy policy in place for customers and the general public.
- More than 20% organisations were found to fall short in monitoring internal performance programmes in relation to data protection standards.
- A number of organisations indicated that they have no processes in place to respond appropriately in the event of a data security incident.

As a result of the investigation, individual GPEN members may contact organisations in their own countries to assess what remedial action they need to take to improve user controls over their personal information.

The report can be accessed here.

14 March

Dutch Regulator Publishes Guidelines for the Calculation of administrative fines under the GDPR

On 14 March 2019, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – '**AP**') published new Guidelines on Administrative Fines 2019 (*Boetebeleidsregels Autoriteit Persoongegevens 2019* – '**Guidelines**'). It is a clear sign that the Dutch regulator is preparing itself for a new phase in its enforcement of the new data protection regime set by the General Data Protection Regulation (GDPR) and the Dutch GDPR Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming* – **'UAVG'**). The publication of the Guidelines sends a clear message to organisations: fines are coming!

The full article from our Dutch team can be found here

Date	Description
16 January	**CJEU upholds disclosure of personal data to authorities for background check purposes** In January 2019, the CJEU provided a relatively flexible interpretation of GDPR principles applying to the disclosure of personal data to public authorities. Its ruling came in a German dispute concerning whether a company could lawfully turn over tax identification numbers (TINs) and related details of several senior managers and board members, to a public authority demanding such data in reply to the company's request for customs authorisation. Several of the company's managers and board members refused to consent to the disclosure, leaving the company and public authority needing another "legal basis" in GDPR Article 6 in order to turn over the data without individuals' consent. Unfortunately, the law which the public authority (the Köln Customs Office / "*Hauptzollamt*") was relying on in order to demand those details from the company (Deutsche Post), did not specifically set out what personal data it could demand as part of the process – casting doubt over claims that the processing in question was necessary for compliance with a legal obligation (GDPR Article 6(1)(c)). There were also doubts over the necessity and proportionality of the disclosure, in particular since the details being disclosed could be used for unrelated investigations; and that it had been originally collected by the company only for payroll tax deduction-related purposes. According to the CJEU, given that the authorization in process effectively delegated customs powers to Deutsche Post, a broad background check on relevant individuals in the company was warranted (not simply related to past non-compliance with customs rules). As for legal basis, the CJEU found that "the subsequent collection of that personal data by the customs authorities in order to make a decision on an application [of this nature] is clearly necessary to comply with a legal obligation that is incumbent on those authorities…". Perhaps interestingly, the judgment does not appear to specifically opine on whether the disclosing *company* could rely on that legal basis; its analysis is focused on the customs authority. The answer may be that the CJEU and Advocate General considered both of the controller and authority were bound by the same "legal obligation"; or alternatively, that only the receiving authority needed a legal basis for GDPR purposes. This is not a moot point, particularly in situations where EU-based authorities seek information from organisations outside their jurisdiction, when it may be clearer that the authority and company are not both bound by the same legal obligation. **The CJEU's ruling in the case (C-496/17 Deutsche Post AG v Hauptzollamt Köln) can be found here; the Advocate General's Opinion is here.**

Enforcement

UK ICO enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
27 February	Kevin Bunsell	Prosecution	Kevin was employed by Nuneaton and Bedworth District Council in Warwickshire and had been trained in data protection law as part of his role as Head of Building control. In July 2017, his partner applied for an administrative job at the council and due to the personal relationship, Kevin was not involved in the selection process. However, he accessed the council's recruitment system and emailed the recruitment packs of the nine rivals to both his work email address and his partner's personal Hotmail account. The Nuneaton Magistrates Court was told that once it had been discovered, Kevin Bunsell has resigned and despite his partner being successful, her employment had also been terminated because she had been appointed due to the invalid recruitment process. Bunsell was fined £660, ordered to pay £713.75 of costs and a victim surcharge of £66.
12 March	ICO Raids on two businesses		The ICO had searched two addresses as part of an investigation into businesses suspected of making live and automated nuisance calls. Following a year of investigations, two teams of ICO enforcement officers executed a search warrant in offices in Birmingham and Brighton. The two businesses are suspected of making millions of calls and have been the subject of over 600 complaints to the ICO. People who had received the call were unable to identify who the calls were form or opt out of them, which is illegal. Enforcement officers seized computer equipment and documents for analysis and the enquiries will continue.

15 March	Faye Caughey	Prosecution	A former administrator at Heart of England NHS Foundation Trust (HEFT) has been prosecuted for accessing medical records without the correct authorisation. An internal investigation found that Faye Caughey had inappropriately accessed the medical records without any business need to do so. The records related to seven family members and seven children known to her. Faye Caughey appeared before Birmingham Magistrates' Court and admitted the two offences of unlawfully obtaining personal data, in breach of s55 of the Data Protection Act 1998. She was fined £1000, ordered to pay costs of £590 and a victim surcharge of £50.
19 March	Vote Leave Limited	Monetary penalty	The Information Commissioner's Office (ICO) has fined Vote Leave Limited £40,000 for sending out thousands of unsolicited text messages in the run up to the UK's 2016 EU referendum. An ICO investigation found that Vote Leave sent almost 200,000 text messages promoting the aims of the leave campaign with the majority containing a link to its website. The investigation found that Vote Leave were unable to provide evidence that the recipients had given their prior consent to the electronic marketing. Vote Leave claimed that the information that it had used to contact the recipients was obtained from enquiries which had come through its website; from individuals who had responded via text to promotional leaflets; and from entrants to a football competition. However, the organisation said that following the conclusion of its referendum campaign it had deleted evidence of the consent relied upon to send the messages. Also deleted were details of the phone numbers the messages were sent from, the volume of messages sent, and the volume of messages received.
26 March	Grove Pension Solutions Ltd	Monetary penalty	An ICO investigation found that Grove Pensions Solutions Ltd were responsible for sending nearly 2 million emails promoting its services back in October 2017 without the necessary consents and were fined £40,000. The Pensions Company Grove Pension Solutions had instructed a marketing agent to use third party email providers to carry out hosted marketing campaigns that advertised the company's services. The company had sought specialist advice from a data protection consultancy as well as independent legal advice about the use of hosted marketing. However, the advice was inaccurate and it breached the regulations.

15 March	Jayana Morgan-Davis	Prosecution	A former administration assistant at a used car dealership has been prosecuted for unlawfully obtaining the personal data of customers and other employees. Jayana Morgan-Davis forwarded several work emails containing personal data of customers and colleagues to her personal email account in August 2017, weeks before resigning from her role. Jayana appeared before Birmingham Magistrates Court and admitted three offences of unlawfully obtaining personal data in breach of s.55 of the DPA 1998. She was fined £200, ordered to pay costs of £590 and a victim surcharge of £30.