Date	Description
UK	
ICO	
02 March 2017	**ICO Guidance for Consent in the GDPR** On 2nd March 2017, the ICO published draft guidance on consent under the General Data Protection Regulation. The consultation period for the guidance closed on 31 March 2017. ICO's proposal to issue guidance on consent is a good idea: it is unrealistic to expect many organisations to read the text of GDPR, so this will make more people aware of the requirements in GDPR. It will also help to show the ICO's thinking on provisions in GDPR which are unclear. There are good attempts to summarise and explain GDPR. However, the guidance is repetitive (so unnecessarily long). It also lapses into jargon in places. For those familiar with data protection this doesn't matter. However it risks making the guidance confusing or misleading for those who aren't. The frequent references to 'opt-in consent' is a good example of this. Some of the examples used to illustrate points are also badly chosen – leading to over-complicated analysis, or missing industry specific nuances relevant to that example. The guidance is an interesting first draft, but needs work. For the details, read on. **To opt-in, or not to opt-in?** Consent has to include an affirmative action by the individual. This is not new: the current Directive already states that the individual must 'signify agreement'. It is tempting to abbreviate the requirement for consent to be active as 'opt-in consent'. However, this can lead to confusion: the Regulation does not state that consent has to involve use of a tick box; consent can be affirmed in many ways. In the at-a-glance summary, the guidance state states that 'consent requires a positive opt-in'. This is unfortunate and risks confusing. (Elsewhere the guidance does make clear that this is just one way of obtaining consent, but the term risks misleading). **Renewing consent**

Date	Description
	If an organisation has already obtained consent, will it need to 'refresh' this in order to meet its obligations under GDPR? ICO draws attention to recital 171, which provides that there is no specific obligation to obtain new consent. However, if existing expressions of consent do not meet the standards set out in GDPR then they will not be valid: the organisation will need to ask for consent again, or find another justification to process personal data. **Real choice** The guidance summarises GDPR requirements that individuals must have a real choice for consent to be valid. They must also be able to revoke consent without detriment. Helpfully, the guidance does accept that data controllers can offer a benefit, or an incentive, to people who give consent – and, if someone withdraws consent, the loss of this benefit will not render the consent invalid (on the basis that the individual suffers a detriment). The guidance gives the example of a scheme giving money-off vouchers to customers who agree to receive marketing materials. If you withdraw consent you lose the vouchers, but this would not make the request for consent invalid. **Separate from terms and conditions** GDPR requires that consent must be 'distinguishable'. ICO explains this means that consent should be separate from terms and conditions. ICO also highlights the GDPR requirement that an individual should not be required to give consent, as a condition of signing up to a service, unless the processing for which consent is sought is necessary for that service. This does not automatically make the consent invalid: however, there will be a presumption that it is not freely given. **Granular** Recital 43 of GDPR provides that '*consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case…*'. By way of an example, an insurance company may ask for consent to process health information which is necessary for it to evaluate risk in a life insurance contract. It may also ask for consent to send email marketing from group companies. These are different processing operations and it would be appropriate for the company to ask for consent separately – so as to allow me to request a quote, whilst saying no to marketing. ICO calls this concept 'granular consent'. The example above is clear. However, it is easy to come up with difficult examples – for example, an organisation may carry out marketing by post, email and phone; it may also market its own products and those of third parties; and it may share lists with third parties: are these different processing operations, or are they all marketing? And if they are separate, how many options would the organisation have to present?

Date	Description
	ICO draws attention to this provision, but does not give examples of occasions when it would be appropriate to offer separate choices and when it would not. ICO merely notes that there is no need to offer separate choice if this would be 'unduly disruptive or confusing'. In so far as it goes this is useful, as it recognises that an excess of choice may not be helpful. **Revocable** It must be as easy to withdraw consent as it is to give it – simple mechanisms are needed. **Proof** The guidance repeats GDPR requirements that an organisation must be able to demonstrate that it has obtained consent. There are some helpful lists of what this may require – such as keeping details of the versions of forms used. **Public bodies and employers** ICO notes that they are unlikely to be able to rely on consent, because of the imbalance in the relationship between the organisation and the individual which makes it unlikely that consent is freely given. There can be occasions when consent is freely given (for example, support services offered by an employer). It would be useful if the guidance recognised that this could be the case in some occasions. **Children** GDPR provides that if an online service is provided to a child and personal data is processed based on consent, then reasonable attempts must be made to obtain verifiable parental consent. There is a section in the guidance covering these rules. It also notes that consent given by a parent will expire once the child is old enough to give consent for him or herself. **Naming all third parties** The guidance states that the consent must name all third parties who will be relying on consent. This is both unclear and problematic. It is not clear whether the guidance means that organisations who ask for consent to share personal data with other organisations cannot share data unless they have listed all third parties. Alternatively, the guidance could be considering the situation of organisations who do not have a direct relationship with the individual, but who want to rely on consent as a lawful basis for processing, and who need the data controller with the initial relationship with the individual to obtain consent which covers their processing of personal data. Whichever scenario is meant, the guidance is problematic: listing all third parties will be difficult for many businesses which rely on being able to share data, or which rely on others to obtain consent which covers their personal data processing. Use of data by direct marketeers and by medical researchers are two obvious areas which will be adversely affected by this.

Date	Description
	The guidance suggests that naming third parties is required for consent to be 'specific'. However, the Data Protection Directive also required consent to be specific and ICO did not previously suggest that this meant that all third parties had to be named. Recital 42 *does* state that for consent to be informed, the individual must be aware of the identity of the person to whom consent is given (amongst other matters). However, this does not necessarily mean listing all third parties: it may be possible to meet this requirement by a clear description of a class of persons and a mechanism to provide more detail on request. **Wrong** Some bits of the guidance are just wrong. For example, it says that the requirement that consent must be '*unambiguous*' is new (it isn't: it's in Article 6 of the Directive). The guidance also says that 'you are likely to need consent under e-Privacy laws for most marketing calls or messages…' in fact, most marketing calls do *not* need consent. **Data protection is not the only consideration** The guidance includes examples to illustrate the points made. Some of these are badly chosen – as the approach taken to consent is driven by non-data protection related considerations. ICO gives the example of: ➢ A company providing credit cards which asks customers to give consent for their personal data to be sent to a credit reference agency, to provide information on credit risk. ICO states that if the customer withdraws consent, the credit card company will still send the data, on the basis of its legitimate interests. On this basis, ICO advises not trying to ask for consent as it is misleading. Organisations providing credit cards are subject to duties of confidentiality (in addition to data protection obligations) which restrict their ability to share personal data. Although there are exceptions to this duty, which allow data to be shared where it is in the best interests of the bank, the limits of the exception are unclear, so it is typical to ask for consent in order to meet concerns about confidentiality. ➢ A healthcare provider, processing health data on the basis of implied consent. ICO chooses this example to illustrate the point that consent which meets the standard for another area of law (here: confidentiality) will not necessarily meet the requirements for consent under GDPR. ICO's conclusion is that ' *..assumed implied consent would not … qualify as explicit consent for special category data'*. The point is correct. However, the explanation is not clear and depends on use of industry jargon. The argument will be clear (and familiar) to those who deal regularly with health-care related data protection and confidentiality considerations (who will already know the point). It risks confusing the non-expert reader for whom the guidance is presumably written. **What about Brexit?**

Date	Description
	GDPR will, of course, come into force before the UK leaves the EU. However, after Brexit, there would be scope for the UK to change course if it wanted to – although there would be strong arguments for maintaining consistency in many areas (to allow consistency for business and to support UK claims to be an adequate country to which EU data can be transferred). The ICO appears to want to stay with the EU-pack – noting that it intends the guidance to evolve as future guidance is issued by European data protection authorities. **Style-buster**: Warning for those sensitive to the use of the English language: the draft guidance introduces some new (and not altogether good) phrases. Our top picks are: ➢ 'Doing consent' - let's hope this isn't also used from the perspective of the individual – imagine having consent done to you ➢ 'Consent mechanisms' - think Heath-Robinson contraptions ➢ 'Consent requests' – which sound overly social-media specific ➢ 'granular consent' (which sounds like a sweetener, but is good) and 'blanket consent' (which sounds cosy, but is bad) ➢ 'Consent as an organic, ongoing and actively managed choice'- which sounds like an advert for health-food ➢ '..keep your consents under review and refresh them' – which sounds like gardening advice ➢ 'Transparent privacy notices' – as opposed to ones which are translucent, or, even worse, opaque… **The Guidance is available here.**
03 March 2017	**ICO guidance on Big data, artificial intelligence, machine learning and data protection** In March 2017 the ICO published a discussion paper on big data, artificial intelligence, machine learning (collectively referred to as "big data analytics") and data protection. The paper is not formal guidance or a code of practice, but rather gives views on the implications of big data analytics for data protection law, and suggests some potential routes to compliance. We expect that the Article 29 Working Party will publish their GDPR guidance on profiling and consent later in 2017, and the principles in this paper may well be developed in that guidance. According to the ICO, big data analytics represents a step change from traditional personal data processing activities. In particular, the ICO identifies the use of algorithms, the opacity of the decision making process, the tendency to collect 'all the data', the repurposing of data sets and the use of new types of data as distinctive aspects of big data analytics that

Date	Description
	pose new compliance challenges. The paper identifies a number of specific challenges, including • maintaining the overall fairness of personal data processing given the intrusive effects of certain types of big data analytics, such as profiling; • aligning big data processing with the reasonable expectations of the individuals concerned; • explaining complex methodologies and algorithms in a way that ensures organisations are transparent about what they are doing, and can obtain consent from individuals that is properly informed; and • the issue of hidden biases in datasets leading to inaccurate predictions about individuals, or to discriminatory and unjustified decisions being made. Perhaps of most interest is the ICO's view on the new right in the GDPR which allows individuals to obtain an explanation of decisions based on automated processing. For example, such automated decisions could be made in the context of credit applications, recruitment activities or insurance. The challenge here is that machine learning algorithms may learn and make decisions in a way that is "without regard for human comprehension", rendering it extremely difficult to provide a meaningful response to an individual who is exercising this new right. The ICO says that organisations must exercise caution before using technologies to make decisions where the methodology cannot be expressed in an understandable way. The suggestion here seems to be that if a decision has a significant effect on an individual, and the decision making methodology cannot be explained, then the technology should not be used. Avoiding unintentional discrimination is crucial to complying with the law. By way of illustration, the paper refers to a study of a machine learning tool used in some US states to predict the future criminality of defendants. The study of the tool revealed that black defendants were falsely classified as future criminals on nearly twice as many occasions as white defendants, despite there being no intention to discriminate. However, it is not enough to detect discrimination in hindsight and take steps to improve the technology. Businesses must have robust measures in place to detect potential discrimination prior to the use of big data analytics, and analysts must build anti-discriminatory measures into the technology at the planning stage. The paper states that organisations can overcome these challenges by developing flexible and innovative compliance tools, including:

Date	Description
	• using anonymised data only, coupled with robust risk assessments to mitigate the risk of individuals being re-identified from the data; • putting in place new forms of privacy notices (e.g. videos, standardised icons, and 'just in time' notices) designed to help make complex information easier to understand; • putting in place internal and external "algorithmic auditing" processes, to enable third parties to check and monitor the behaviour of an algorithm and the potential for bias and discrimination within the decision making process; • using ethics boards within organisations which ensure the application of big data standards and principles and build trust with individuals; and • undertaking formal privacy impact assessments to identify and mitigate privacy risks and assess the proportionality of big data processing. The main conclusion of the paper is that whilst it is more difficult to apply data protection principles to big data analytics, tools exist and will continue to be developed to support compliance. The ICO's view is that the benefits of big data analytics will only truly be felt when data privacy is embedded in the methods by which such technologies are used. Therefore whilst the use of big data analytics represents a significant change in the nature of processing activity, there is no doubt that data protection authorities intend to enforce compliance with the law within the framework of existing principles. **The ICO's paper can be found here.**
06 April 2017	**ICO issues update setting out what GDPR guidance organisations can expect** To date, the ICO has produced a number of documents, namely: **Preparing for GDPR: 12 steps to take now** - a list of key issues that organisations should be thinking about now; **Overview of GDPR** - a living document which will be expanded and revised over time to cover relevant points as they develop. This document currently follows the structure of GDPR and will reference out to Article 29 Working Party Guidance and other ICO Guidance as applicable. New content will be highlighted at the start of the document.

Date	Description
	GDPR references have been incorporated into the ICO's Privacy Notices Code of Practice; and **Draft consent guidance has been issued for public consultation – for more information on what this guidance contains, please see our article below.** **ICO/Article 29 WP Guidance coming soon** The ICO has indicated that they will not duplicate the work of the Article 29 Working Party but will incorporate key points into the Overview mentioned above. New Guidance is expected from the Article 29 Working Party later this year about: • Administrative Fines • High Risk Processing and Data Protection Impact Assessments (Issued in April – see below) • Certification (Expected June) • Profiling (Fab lab workshop organised for early April) • Consent (Fab lab workshop organised for early April) • Transparency • Notification of personal data breaches (Fab lab workshop organised for early April) • Tools for International Transfers The ICO has confirmed that they are working on further guidance on contracts and liability which should be issued shortly as well as assessing the GDPR provisions on profiling (issued in March) and risk. Children's personal data and international transfers are also on the agenda. **More information is available here.**
06 April 2017	**ICO feedback request on profiling and automated decision making** In April 2017 the ICO published a paper requesting feedback on the new profiling and automated decision making provisions in the General Data Protection Regulation (GDPR). The paper is not formal guidance or a code of practice, but rather sets out the ICO's initial thoughts on the key areas of profiling it feels need further consideration, and requests feedback from interested parties. Some of the issues covered may be developed further when the Article 29 Working Party publishes its formal guidelines on profiling later this year.

Date	Description
	In the meantime, we highlight below some of the key points from the ICO's paper: • Organisations need to keep profiling activities under regular review to ensure that all the information obtained is relevant for the intended purpose, and that irrelevant data is not retained for longer than necessary; • As profiles tend to comprise derived or inferred data, rather than data collected from the individuals themselves, there is a risk that organisations will infer sensitive personal data from non-sensitive personal data (e.g. inferring the state of an individual's health from the contents of their shopping trolley). This presents a challenge as sensitive personal data can generally only be processed with the explicit consent of the individual concerned; • The GDPR requires that organisations provide individuals with meaningful information about the logic involved in an automated decision making process. The ICO interprets this requirement as meaning that information should be provided about how profiling might affect a data subject generally, rather than requiring information to be given about a specific decision. It also makes clear that this does not involve providing a detailed technical description, but rather involves clarifying the categories of personal data used, the source of the data, and why the data is considered relevant; • The GDPR gives individuals the right to object to profiling. Where they do so, organisations must demonstrate compelling legitimate grounds if they are to override the objection. The ICO states that individuals must be clearly told about their right to object to profiling and this explanation should not be concealed with a set of general terms and conditions. Organisations must therefore be ready to justify their processing activities in readiness for an objection; • In certain circumstances, individuals can object to decisions being made about them with are based solely on automated processing. The ICO interprets this to cover those automated decision making processes where a human exercises no real influence on the outcome of the decision; • The GDPR is concerned with profiling which has a "legal" or "significant" effect on an individual. The ICO interprets "significant" as meaning a consequence that is more than trivial and potentially has an unfavourable outcome. This appears to be a reasonably low threshold; • Organisations must carefully consider how to ensure profiling is fair and non-discriminatory and does not have an unjustified impact on individuals. The ICO highlights the fact that profiling is often a continuous, evolving process, with new correlations in data sets discovered all the time. This means businesses must introduce appropriate measures to correct errors and minimise the risk of bias or discrimination. Such measures might include algorithmic

Date	Description
	auditing, seals, codes of conduct and ethical review boards to underpin profiling safeguards; and • Before undertaking many profiling activities, organisations will need to undertake a Data Protection Impact Assessment (DPIA). The ICO gives credit scoring, insurance premium setting, location tracking, loyalty programs and behavioural advertising as examples of activities likely to require a DPIA. The ICO also says that DPIAs may be needed in the case of a decision making process which is only partially automated, if it results in a legal or significant effect on the individual. The paper asks a number of specific questions for feedback. If you wish to feedback, the deadline for responding is 28 April 2017. Alternatively, you can use the ICO's paper to issue spot ahead of the release of more formal guidelines later this year. **The ICO's paper can be found here.**
Cases	
24 January 2017	***Holyoake v (1) Candy (2) CPC Group Limited* [2017] EWHC 52** This is a useful first instance case on these topics. The case forms part of the wider dispute between Mr Holyoake and the Candy brothers and their company. Mr Holyoake made subject access requests to the other parties he subsequently claimed that the searches made were inadequate (because personal email accounts should have been searched) and that the other parties incorrectly relied on claims of legal professional privilege to avoid releasing material. In his judgment, Warby J concluded that: 1. There was no need to search personal email accounts. In some cases, if there was evidence that a director used a personal account for corporate business, the director may be obliged to allow the company to access his account to search for materials. However, there would have to be evidence to support this approach. 2. Material could be withheld from a SAR when it benefitted from legal professional privilege. There would have to be very strong evidence of wrongdoing to open up argument on this point and the court would only become involved to inspect material subject to a claim to LPP where there was credible evidence to point to wrongdoing or that those involved could not be trusted. This was not the case here. **The full judgment is available here.**

Date	Description
16 February 2017	***Dawson-Damer v Tayor Wessing LLP* [2017] EWCA Civ 74** On 16 February 2017, the Court of Appeal handed down its judgment in the case of *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74. <u>Background</u> The case concerned a contested subject access request made against the background of legal proceedings in the Supreme Court of the Bahamas concerning family trusts. Taylor Wessing LLP were legal advisers to the trustees and the data controllers of the requested data. They had initially rejected the subject access request on the basis that the requested information was exempt by virtue of paragraph 9 of Schedule 7 DPA 1998 (legal privilege ("LPP")). In the High Court, Taylor Wising's reliance on the LLP exemption was upheld, the Court having accepted that the exemption extended not only to information that would attract legal privilege in the UK courts but also to information in respect of which compulsory disclosure could be resisted in Bahamian proceedings. <u>Court of Appeal Judgment</u> On appeal, the Court of Appeal took a more narrow approach to the LLP exemption and held that the exemption can only be used to withhold personal data which would attract legal privilege in proceedings in the UK. The Court found that the exemption does not extend to privilege arising under other legal systems. The Court of Appeal also considered two other issues which were of general importance. Firstly the Court considered the construction of section 8(2) DPA which concerns the supply of copies of personal data where this involves a disproportionate effort. The Court found that disproportionate effort under section 8(2) is not narrowly restricted to the supply of copies, but extends also to other steps that are required in order to respond to requests. When considering disproportionate effort, the Court noted, however, that while there will be "bounds to a search", it is clear from the recitals to the Data Protection Directive that there are substantial public policy reasons for giving people control over their data through the system of rights and remedies contained in the Directive *"which must mean that where and so far as possible, SARs should be enforced"*. Finally, the Court considered the extent to which the appellants' motive in making the request (to assist in their litigation against the Trustee) was relevant to the exercise of the Court's discretion under section 7(9) DPA to order a data controller to comply with a request. The Court accepted that there is nothing in the DPA or the Directive that limits the purpose for which a data subject may request his data, or provides data controllers with the option of not providing data based solely on the requester's purpose. It further held that that suggestions to the contrary in the judgment of Auld LJ in

Date	Description
	Durant v Financial Services Authority [2004] FSR 573 have been misunderstood and taken out of context and do not establish that a request would be invalid if made for the collateral purpose of assisting in litigation. **The full judgment is available here.**
06 March 2017	***Deer v University of Oxford* [2017] EWCA (Civ) 121** On 3rd March 2017 the Court of Appeal delivered another significant judgment on the scope of data subject access rights in the joined cases of *Deer v University of Oxford and Ittihadieh v 5-11 Cheyene Gardens RTM Co Ltd*. The ICO intervened in both appeals because of the points of wider significance they raised. Issues considered included the definition of personal data, the scope and nature of the duty to conduct searches, the scope of the domestic purposes exemption under section 36 DPA, the relevance of motive and the scope and nature of the court's discretion under section 7(9) DPA to order compliance where a data controller is found to have breached its duties to respond to a subject access request. Personal data: During the course of the High Court proceedings in Deer, the trial judge, Harris HHJ QC, had reviewed a 64 page bundle of documents and had concluded that none of these documents contained personal data .In reviewing Harris HHJ's judgment, the Court of Appeal concluded that the he had on the whole taken too narrow a view of the scope of "personal data" for the purposes of the DPA. In particular, the Court of Appeal observed that information is not disqualified from being personal data merely because it was originally supplied to the data controller by the data subject or because the information is otherwise known to the data subject. The Court of Appeal also noted that information about a person's whereabouts on a particular day or at a particular time may also amount to that person's personal data. Proportionality of searches: The Court of Appeal noted that neither the Directive nor the DPA imposes any express obligation on data controllers to search for personal data in response to a subject access request but that such an obligation is necessarily implied. The Court also noted that, while section 8(2) DPA entitles a data controller not to supply a copy of information in permanent form if to do so would involve disproportionate effort, there is no express provision in the DPA which relieves a controller from the obligation to supply data on the ground that it would be disproportionate to do so. However, the Court also noted that, despite this, the EU legislature did not intend to impose excessive burdens on data controllers. The Court confirmed that the implied obligation to conduct a search was limited to a reasonable and proportionate search; the fact that a further and more extensive search might reveal further personal data did not mean that the first search was inadequate. Motive and the court's discretion: In Deer, the trial judge had indicated that if there were any *"errors of taxonomy"* in his analysis of extent to which withheld material constituted Dr Deer's personal data, he would in any event in the exercise of his discretion, not require the University to take further steps to comply *"as this would serve no useful purpose"*. In addition although Dr Deer had been awarded her costs up to a given date, these costs had been discounted by 25%

Date	Description
	because of the trial judge's assessment of her motive in pursuing the litigation. In considering the relevance of motive, the Court of Appeal confirmed that the right of access under section 7 DPA is not subject to any express purpose or motive test; neither is a data subject required to state any purpose when making a SAR. In relation to discretion, the Court expressly disagreed with the view expressed obiter by Auld LJ in Durant v FSA to the effect that the discretion conferred by section 7(9) was *"general and untrammelled"*; the Court found that this discretion was conferred for a purpose and the fact that the discretion is exercisable only after there has been a finding of a breach of section 7 should have a significant bearing on the way in which the court exercises its discretion. Nevertheless the Court concluded that in exercising its discretion, the court has to strike a balance between the prima facie right of the data subject to access his or her data and the interests of the data controller, having regard to the general principle of proportionality. In carrying out this balancing exercise the court could take account of a range of considerations, including the reason for making the request, whether the application to the court was an abuse of rights or procedurally abusive, and the potential benefit to the data subject. Domestic purposes exemption: In Ittihadieh, the subject access request submitted to the right to manage company of the building in which Mr Ittihadieh lived included a request for information about him held in a personal capacity by directors of the company (some of whom were also residents of the building). The domestic purposes exemption had been relied on to withhold data held by the directors in a private capacity. The Court rejected arguments that the exemption should be applied only to matters which went on inside the data controller's own household and did not therefore apply to interaction with the wider world, for example in the form of email communications with others. This was considered too narrow an approach. Instead the Court found that in construing the scope of the exemption it is necessary to strike a balance between the competing privacy entitlements of the data controller and the data subject. Activities of Mr Ittihadieh's neighbours relating to the management of the private block of flats in which they live, (including the processing of personal data relating to other residents) fell within the scope of the exemption because they directly concerned their private lives and directly concerned their households. **The full judgment is available here.**
Other News	
15 February 2017	**Cloud industry body sets up new data protection code** The Cloud Infrastructure Services Providers in Europe (CISPE), a coalition of cloud computing providers, has published a Code of Conduct designed to help customers to choose the right cloud infrastructure service for their specific needs. This includes giving confidence to customers that their cloud infrastructure provider is using appropriate data protection standards to protect their data consistent with European data protection law (including the upcoming GDPR). The Code is a voluntary instrument and a cloud infrastructure provider may choose to declare only specific cloud

Date	Description
	infrastructure services as adhering to the Code. Cloud infrastructure providers could either obtain certification by an independent third party auditors or self-assess compliance. All cloud providers that comply with the Code are listed on the CISPE Public Register (www.cispe.cloud/PublicRegister) and will be able benefit from the use of an approved compliance mark. The Code does not replace a contract between the cloud infrastructure provider and the customer, but the cloud infrastructure provider should assess whether service agreements offered to new customers contradict the Code before declaring their adherence. Those cloud infrastructure providers adhering to the Code must give customers the choice to store and process their data entirely within the European Economic Area. Providers must also commit that they will not access or use their customers' data for their own purposes, including, in particular, for the purposes of data mining, profiling or direct marketing. **The Code can be found here.**
EU	
A29WP	
04 April 2017	Art. 29 Working Party Opinion on Proposed E-Privacy Regulation. **More information can be found here.**
10 April 2017	Final Art. 29 Working Party Guidelines on Data Protection Officers. **More information can be found here.**
10 April 2017	Final Art. 29 Working Party Guidelines on the right to data portability. **More information can be found here.**
10 April 2017	Final Art. 29 Working Party Guidelines for identifying a controller or processor's lead supervisory authority. **More information can be found here.**
12 April 2017	Draft Art. 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) - Comments should be sent to the working party by 23 May 2017 at the latest. **More information can be found here.**

Date	Description
Cases	
26 January 2017	***Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* Case C 13/16** Background A taxi stopped at the side of the road in the city of Riga – one of its passengers opened the door which hit a passing trolley-bus. As a consequence of the accident, an administrative offence was recorded. The owner of the trolleybus – Rigas – initially initiated a compensation claim against the insurance company of the taxi-driver. The insurance company denied liability on the basis that the taxi driver was not responsible for the accident, but rather the passenger of the taxi. Rigas requested the name, ID document number and address of the passengers of the taxi, and copies of the documents recording the taxi driver and passenger's explanations of the accident. The police gave Rigas the passenger's name only on the basis that the Latvian DPA prohibited the provision of the other information. Rigas successfully challenged this refusal in the District Administrative Court which ordered the police to disclose the information initially refused. Rigas appealed this decision before the Latvian Supreme Court which, in turn, sought an opinion from the Latvian DPA. The Latvian DPA indicated that, *"the data could not be provided on the basis of Article 7(6) of the Law on the protection of personal data, given that the Administrative Infringements Code sets out the natural or legal persons to which or to whom the police may send information relating to a case. Thus, the disclosure of personal data relating to administrative proceedings leading to sanctions may be carried out only in accordance with paragraphs 3 and 5 of that article. In addition, Article 7 of that law does not oblige the data controller (in this case, the police) to process the data: it merely permits it to do so."* The Latvian DPA also referred to alternative means by which Rigas could obtain this data: making a request to the Civil Registry, or applying to the Latvian courts for the production of evidence pursuant to the Latvian Law on Civil Procedure. The Latvian Supreme Court referred the following questions to the CJEU: 1. Should 'necessary' under art 7 (f) Directive 95/4/EC (i.e. controller's legitimate interests*) "be interpreted as meaning that the National Police must disclose to Rīgas […] the personal data sought by the latter which are necessary in order for civil proceedings to be initiated"*? 2. Is the fact that the taxi passenger was a minor at the time of the accident relevant to question 1? AG Opinion The AG 'rephrases' the referring court's question to the following: under Directive 95/4/EC , is there *"a duty on the part of the controller of the data to disclose data enabling the identification of a person allegedly responsible for an administrative offence so that Rīgas […] can launch civil proceedings".* The AG answers this clearly: No. The AG goes

Date	Description
	onto state in fact that, *"the default rule underpinning that directive is that personal data should, in general, not be processed, so that a high level of protection of the right to privacy is ensured. The processing of personal data shall, by nature, remain rather exceptional"*. Art 7 sets out the exceptions to this rule i.e. thee circumstances in which processing may take place. Linked to this question is: (i) when do the conditions of Art 7 (f) apply? And (ii) What, and how much, personal data can the requester obtain under Art 7 (f)? The following are important observations made by the AG: 1. *"The Directive does not define legitimate interests. (15) Thus, it is for the data controller or processor, under the supervision of national courts, to determine whether there is a legitimate aim that could justify an interference with private life… There is no doubt in my mind that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest"*. 2. In terms of the balancing of interests, *"In order to meaningfully carry out that balancing, due consideration should in particular be given to the nature and sensitivity of the data requested, their degree of publicity, (24) and the gravity of the offence committed…The referring court indeed asks to what extent the fact that the taxi passenger was a minor at the time of the accident is relevant. To my mind, and given the particular circumstances of this case, it is not…Unless it is established precisely how the disclosure in this particular case were to endanger, for example, the physical or mental development of a child, I fail to see why the fact that the damage was caused by a minor should effectively lead to immunity from civil liability"*. 3. In terms of necessity, *"First, …the Directive require that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected, but also when further processed. Thus, it follows from those provisions that the data disclosed shall also be adequate and relevant for the realisation of legitimate interests. Second, common sense calls for a reasonable approach as to the data that should actually be processed. Data requesters should indeed be given useful and relevant information, which are necessary and sufficient for them to fulfil their own legitimate interests, without having to forward a request to another entity that might also possess that information"*. However, *"the precise scope of the data to be disclosed is a matter of national law"*. **The full Opinion is available here.**
09 March 2017	**Camera di Commercio, Industria, Artigianato, e Agricoltura di Lecce v Salvatore Manni (C-398/15)** On 9 March 2017, the CJEU ruled that an individual's right to be forgotten does not override the societal interest in an official public registry of company data. The ruling sets limits to the court's previous jurisprudence on the application of the right to be forgotten.

Date	Description
	Background The Lecce Chamber of Commerce, acting under Italy's implementation of an EU Directive, established a Companies Registry that contained company details, including the fact that M. Manni was the sole director of a construction company that declared bankruptcy in 1992. M. Manni alleged that public access to this data prejudiced his new business. He therefore sought to have the data delisted or anonymised. M. Manni's action was sustained by the lower court, which ordered the Chamber of Commerce to anonymise the data. On appeal, the Italian Supreme Court referred the matter to the CJEU. Relying on the right to be forgotten, as established in *Google Spain v Costeja*, M. Manni argued that the public interest in maintaining the data in identifiable form was low because the bankruptcy occurred more than a decade earlier and the historical record could be equally served by anonymous records. In September 2016, the Advocate General sided with the Chamber of Commerce, emphasizing the importance of such disclosures to establishing trust in the marketplace and protecting third parties from undue risk in transactions. On 9 March 2017, the CJEU offered its judgment. Judgment At root, the case centred on finding the appropriate balance between two competing legal rules. On the one hand was an obligation stemming from an EU Directive for Member States to maintain a public register of companies. On the other was the data protection principle, also derived from an EU Directive, which requires data controllers to keep personal data in identifiable form only for as long as necessary for the purposes for which it was collected. Thus, the question posed to the Court was whether an individual could "request the authority responsible for maintaining the Companies Register to limit, after a certain period has elapsed from the dissolution of the company concerned and on the basis of a case-by-case assessment, access to personal data concerning them and entered in that register". While emphasizing that the Data Protection Directive "seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons" and that the provisions of the DPD "must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter", the Court nonetheless ruled that M. Manni did not have the right to have his personal data erased. This case is important because it clarified the test for when the right to be forgotten is limited by a public interest. First, the Court ascertained the purpose for which the data was collected and stored in identified form. Next, it considered whether the Chamber of Commerce was required to delete or anonymise the data automatically because the data was no longer necessary for its original intended purposes. Only after conducting this assessment did the Court consider the

Date	Description
	individual's interest in the case. Thus, under the Directive, only where an individual can demonstrate compelling legitimate grounds will she be able to force the deletion of data that is otherwise lawfully held. In this case, because questions surrounding the legal rights of companies could arise long after the dissolution of a company, the data was still necessary for the purposes for which it was intended. Moreover, the Court provided helpful language for justifying the retention of personal data where it serves multiple potential (but not necessarily concrete) purposes: *"In view of the range of possible scenarios, which may involve actors in several Member States, and the considerable heterogeneity in the limitation periods provided for by the various national laws in the various areas of law, highlighted by the Commission, it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary."* **The full Opinion is available here.**
15 March 2017	***Tele2 (Netherlands) BV, Ziggo BV and Vodafone Libertel BV v Autoriteit Consument en Markt Case C-536/15*** This CJEU case relates to provision of phone numbers to directory enquiry service providers. The CJEU rejected an attempt to use data protection as a means of imposing barriers to the transfer of personal data between member states. European Directory Assistance is a Belgian company providing directory enquiry services. It asked Dutch operators, who assign telephone numbers, for the numbers of their subscribers. The Dutch law implementation of the EU telecoms package only required numbers to be provided to Dutch companies. A reference was made to the CJEU asking whether Dutch law should allow requests to be made by directory enquiry companies in any member state. The reference also asked if telephone subscribers must be offered an extra choice before their details were passed to directory enquiry providers in another country. The CJEU confirmed that a company in one member state could request subscriber numbers from operators in another member state. Further, there was no requirement for operators to ask for consent from subscribers just because the directory enquiry service provider was based in another country; they should not differentiate between directory enquiry service providers on this basis when asking for consent from subscribers. **The full judgment is available here.**

UK Enforcement				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty or prosecution**	**Description of breach**	**Summary of steps required (in addition to the usual steps)**
16 January 2017	**IT Protect Ltd**	Monetary penalty	IT Protect Ltd (the "Company") makes unsolicited marketing calls to elderly subscribers in an effort to sell call blocking devices to stop unwanted marketing calls. Between 6 April 2015 and 16 May 2016, 35 complaints about the Company were made to the ICO by subscribers registered with the TPS, and 122 complaints were made directly to the TPS. Complaints involved allegations that callers pretended to be from BT, and that calls were intentionally targeted at the elderly. The ICO wrote to the Company, and the Company replied, saying that it had purchased opt-in data from a third-party company, but that it had not carried out any due diligence to ensure that subscribers had given their consent to receive their calls.	Monetary penalty notice of £40,000.
18 January 2017	**Rebecca Gray**	Prosecution	Rebecca Gray was prosecuted for the offence of unlawfully obtaining data. She previously worked at a recruitment agency in Widnes, and emailed	£200 fine, £214 costs, £30 victim surcharge

			herself the personal data of approximately 100 clients and potential clients just before she was about to leave the recruitment agency for which she was then working, to start at a rival company. She then used the personal data to contact those persons in her new role.	
24 January 2017	**LAD Media Ltd**	Monetary penalty	LAD Media Ltd (the "Company") is a lead generator and data brokerage business, with operations covering financial services, debt management, and consumer claims. Between 6 January 2016 and 10 March 2016, 158 complaints were made to the 7726 spam reporting service or directly to the ICO about text messages received from the Company by subscribers, relating to writing off debt using government schemes. The ICO wrote to the Company following the complaints, and the Company replied, saying that it had purchased the data used to send the messages from a third-party supplier, and that the messages had then also been sent by a third-party supplier on its behalf. The Company provided evidence of the websites from which it had bought the data, and of the kind of opt-in statements upon which it had been relying.	Monetary penalty notice of £50,000.

1 February 2017	**Kavitha Karthikesu**	Prosecution	Kavitha Karthikesu, a newsagent operating CCTV on her premises, was prosecuted for failing to register her CCTV.	£200 fine, £439.28 costs, £20 victim surcharge
2 February 2017	**The Data Supply Company Ltd**	Monetary penalty	The Data Supply Company Ltd (the "Company") is a list broker (data broker). It sells information about individuals, which it has obtained from various sources, to organisations. They can then use this information in order to send direct marketing to those individuals. Between 19 June 2015 and 21 September 2015, 174 complaints were made to the 7726 spam reporting service or directly to the ICO about text messages received by subscribers about payday loans. After an investigation, the ICO discovered that the person who had sent those messages had bought the subscribers' data from the Company. The Company had sold that person 580,302 records of personal data. The Company claimed that it had obtained the data from financial institutions that had declined or were unable to assist individuals who had requested financial products, and it also identified a range of third party websites from where it claimed to have bought the data. Not all of these, however, were the websites of financial institutions, and none of the privacy notices on these websites identified the Company as a potential recipient of an individual's data.	Monetary penalty notice of £20,000.

10 February 2017	**NHS Digital (formerly known as HSCIC)**	Undertaking follow-up	This action concerned an ICO "follow-up" assessment of the actions taken by NHS Digital (the "Provider") in relation to an undertaking it signed on 19 April 2016 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Provider had taken appropriate steps and put plans in place to address and mitigate the following risks which had been highlighted: • the Provider has established and is now operating a system to process and uphold Type 2 objections; • the Provider has updated the fair processing information on its website; • by using its Data Access Release team and Data Release Register, the Provider identified recipients of data sets provided between January 2014 and April 2016 that were likely to contain records of patients who had registered a Type 2 objection and who were not covered by an exemption. A letter was sent to these patients on 19 July 2016; • four data sharing agreements were examined. Each was looked at in detail and, owing to	The Provider should take further action as follows: • make it clear that type 2 objections received before 29 April 2016 were not honoured before this date, and to assess the effectiveness of the programme of distributing material to GPs and other organisations to raise patient awareness of the failure to honour received objections.

			different reasons, no action was required in relation to the undertaking requirement for any of the four agreements; • one requirement of contacting the recipients of the relevant data was that data sets should be destroyed/deleted where possible. A log of destruction certificates has been kept; and • the Provider examined the National Data Guardian's (NDG) review of data security, consent and opt-outs, published 6 July 2016. The review demonstrated that the Provider will need to complete further work to fully address the following actions: • as well as relying on press coverage to raise awareness, the Provider published relevant information to the NHS Choices website on the right to opt-out of identifying information of patients being shared beyond their GP practice or the Provider itself. However, the requirement to actively inform patients affected by the incident has not yet been fulfilled.	
15 February 2017	**Digitonomy Limited**	Monetary penalty	Digitonomy Limited (the "Company") is a credit broker which makes introductions between borrowers and lenders in order to enter into loan agreements under different trading names. It is registered with the FCA. One of its business lines involves generating leads through affiliates, which send marketing text messages directing	Monetary penalty notice of £120,000.

			individuals to various websites that it owns. Between 6 April 2015 and 29 February 2016, 1408 complaints were made to the 7726 spam reporting service about the receipt of unsolicited direct marketing text messages sent by the Company. Between 6 April 2015 and 29 February 2016, a further 56 complaints were made direct to the ICO. When questioned, the Company explained that it did not purchase any data from third parties. Instead, it said that it had used affiliate marketing channels in order to acquire customers. The Company was unable to provide any evidence to the ICO that the individuals to whom the text messages had been sent had consented to their receipt. It was later discovered that the Company had instigated the sending of 5,900,940 text messages. However, it indicated that while it had attempted to transmit this number of text messages, only 5,238,653 were successfully transmitted.	
17 February 2017	**Cornwall Council**	Undertaking	This action concerned an ICO "follow-up" assessment of the actions taken by Cornwall Council (the "Council") in relation to an	N/A

		follow-up	undertaking it signed on 16 September 2016 to provide the ICO with a level of assurance that the agreed undertaking requirements had been appropriately implemented. The review demonstrated that the Council had taken appropriate steps and put plans in place to address and mitigate the following risks which had been highlighted: • the Council confirmed in November 2016 that over 83% of Council employees had completed their Information Governance training within a two year period; • the Council will now monitor compliance with the requirement to complete Information Governance training at least every two years, and Compliance reports are now being reviewed at the Information Governance steering group and by the Corporate Directors' Team on a monthly basis; and • new staff members who are responsible for the handling of personal data are now being asked to complete data protection training within their first week of employment.	
21 February 2017	**Pennine Care NHS Trust**	Undertaking	The ICO investigated a number of incidents of a similar nature. For example, in April 2015, a patient letter containing sensitive personal data was sent to the patients' neighbour. The envelope was not marked "private and confidential" or for "addressee only". The ICO also raised other	The data controller shall ensure that: (1) Procedures are put in place to ensure data breaches are acted

			information governance issues, particularly in relation to checking patient addresses before correspondence is sent and keeping records up to date. In July 2016, a letter containing confidential mental health information was sent to an outdated address. Staff had failed to check the Electronic Patient Record for the correct address and the ICO expressed concern as to the level of training undertaken by staff.	upon promptly; (2) Processes are standardised across all teams and staff duties are clearly defined; (3) Checking procedure are implemented in relation to sending patient correspondence; (4) Staff complete mandatory data protection training, and monitor the completion of such training.
28 February 2017	**HCA International Ltd**	Monetary penalty	Since 2009, HCA had routinely sent unencrypted audio recordings by email to India for the purposes of transcription. The audio recordings were of private consultations that took place with patients wishing to undergo IVF treatment. HCA was unaware that the server on which the records were stored was unsecure. In April 2015, a patient informed HCA that the transcripts, containing sensitive personal data, could be accessed via an internet search engine. The ICO's investigation found a number of contraventions of data protection legislation: • The recordings were unencrypted; • HCA had no guarantee that the server would be secure;	Monetary penalty notice of £200,000.

			• HCA has no guarantee that the recordings would be erased after they had been transcribed; • HCA failed to monitor the data processor's security measures; • HCA did not have a DPA-compliance contract with the data processor.	
3 March 2017	**Elaine Lewis**	Prosecutions	A former nurse accessed the medical records, containing sensitive personal data, of over 3000 individuals, without the data controller's consent. The ICO issued proceedings against Ms Lewis, and Ms Lewis pleaded guilty.	Ms Lewis was fined £650, ordered to pay costs of £664, and a victim surcharge of £65.
9 March 2017	**Media Tactics Ltd**	Enforcement notice	From November 2014 to June 2015, Media Tactics was responsible for over 22 million automated marketing calls to subscribers without their prior consent. Media Tactics did not identify the person who was sending or instigating the automating marketing calls.	The ICO required that Media Tactics cease making, or instigating, automating direct marketing calls, except (a) where the call is made to an individual who has notified Media Tactics that he or she consents to such communications; and (b) where the communication includes the name of the company and either the address of the company or a telephone number on which the company can be reached free of charge.
9 March 2017	**Media Tactics Ltd**	Monetary penalty notice	See the above facts.	Monetary penalty notice of £270,000.
14 March 2017	**Munee Hut LLP**	Enforcement notice	From May 2015 to March 2016, Munee Hut used a public telecommunications service to send approximately 64,000 unsolicited direct	The ICO required that Munee Hut LLP neither transmit, nor instigate the transmission of, unsolicited electronic

			marketing electronic communications to individual subscribers. Munee Hut had instigated the sending of unsolicited direct marketing text messages to subscribers without their consent.	mail unless the recipient of the electronic mail has previously notified the company of his or her consent to receiving such communications.
14 Match 2017	**Munee Hut LLP**	Monetary penalty notice	See the above facts.	Monetary penalty notice of £20,000.
15 March 2017	**True Telecom Ltd**	Prosecutions	True Telecom Limited has been prosecuted for processing personal data without having an entry in the Information Commissioner's register.	True Telecom Limited was found guilty and fined £400, ordered to pay costs of £593.75 and a victim surcharge of £40.
16 March 2017	**Data breach by barrister**	Monetary penalty notice	In January 2016, a local authority solicitor found that documents containing confidential and sensitive information could be accessed on the internet. The author of these documents was a barrister. The local authority solicitor informed the barristers' chambers. The barrister had created the documents on a password protected desktop computer, but the files were unencrypted. The Bar Council had issued guidance to barristers that a computer may require encryption of specific files in order to prevent unauthorised access to confidential information by shared users. In this case, the barrister's husband had access to the desktop computer and uploaded the files containing sensitive information to an online directory in order to back them up. The documents were accessible via an internet search engine. Six documents contained confidential and highly sensitive information relating to clients involved in court proceedings. Up to 250 individuals were affected by this	Monetary penalty notice of £1,000.

			incident, including vulnerable adults and children. The barrister's husband removed the files immediately, and the internet service provider removed the cached information the following day. However, the ICO's investigation found that the barrister did not have in place appropriate technical measures for ensuring that such an incident would not occur. In particular, the files containing sensitive information should have been encrypted.	
16 March 2017	**Gregory Oram**	Prosecutions	Gregory Oram, who worked at a recruitment agency, emailed the personal data of approximately 500 candidates to his personal email address as he was leaving to start a rival recruitment company. The data included personal information, including identification and qualification documents. Mr Oram pleaded guilty to the offence.	Mr Oram was fined £170, ordered to pay £360 prosecution costs and a £30 victim surcharge.
20 March 2017	**Norfolk County Council**	Monetary penalty notice	In April 2014, a removals company collected furniture as part of a Norfolk County Council ("**Norfolk**") office move. They removed filing cabinets which had been used by the children's social work team. The filing cabinets were not empty and the lack of written procedure meant that it was not clear whose responsibility it was to ensure the cabinets were empty. A member of the public bought one of the filing cabinets in a second hand office furniture shop. The documents that had been left in the cabinets contained sensitive personal information.	Monetary penalty notice of £60,000.

			An ICO investigation found that Norfolk failed to take appropriate organisational measures against the unauthorised processing of personal data. In particular, Norfolk did not have an adequate written procedure regarding how furniture disposal should be managed.	
27 March 2017	**Honda Motor Europe Limited**	Monetary penalty notice	In 2016, Honda sent around 300,000 emails to individuals seeking to clarify their marketing preferences. No "opt in" or "opt out" information was held for these individuals. Following receipt of a complaint made, the ICO wrote to Honda with details of the complaint. Honda replied, explaining that it was intended as a service email, not a marketing email. In particular, the email was designed to ensure that they were not keeping personal data for longer than necessary and that any opt-outs were up-to-date. The ICO asked further questions of Honda, but found that Honda was unable to evidence that the individuals to whom emails had been sent has consented to receipt of the messages. The ICO considered the emails direct marketing.	Monetary penalty notice of £13,000.
27 March 2017	**Flybe Limited**	Monetary penalty notice	In August 2016, Flybe sent emails to over three million individuals, asking them to clarify that their information was correct and to update any marketing preferences. The email also advised that, by updating their preferences, they may be	Monetary penalty notice of £70,000.

			entered in to a prize draw. An individual who received the email made a complaint to the ICO, as they had previously opted out of receiving marketing emails from Flybe. The ICO wrote to Flybe with details of the complaint, advising that organisations cannot email individuals to consent to future marketing messages as this would, in itself, be a marketing message. A third party agent had distributed the emails. The agent had a database of individual opt-in and opt-out preferences. On this occasion, Flybe instructed the agent to send emails to customers who had opted-out of receiving direct marketing from Flybe. In the body of the email, customers were given the option of clicking one of two buttons: (a) to update their preferences, and (b) to update their preferences and enter the prize draw. The ICO considered that the emails constituted direct marketing and, as Flybe were unable to evidence that the individuals had consented to receipt of the messages, Flybe had breached PECR.	
29 March 2017	**Wolverhampton City Council**	Undertaking follow-up	This action follows two separate incidents. In January 2016, the personal information of employees at 73 educational institutions was sent	The ICO advises that the Council continue to improve in the following areas:

			in error to an external recipient via email. In November 2015, the Council asked for a report to be produced by its payroll department, and the personal data of 9858 data subjects was sent in error to an external recipient via email. The ICO's investigation revealed that the Council does not have a reliable method for monitoring the completion of refresher training, an issue that seems to have remained unresolved following a 2011 audit and a 2012 follow-up audit of the Council, in which the issues concerning refresher training were particularly highlighted. The ICO's follow-up demonstrated that the Council had taken steps to address the requirements of the undertaking. Examples of such steps include: • The 'protecting information' e-learning module was carried out and the module was updated; • E-learning refresher training will take place every 12 months; • A series of communications were issued across the Council to raise awareness of the ICO undertaking.	• Monitoring and producing statistical reporting information for the protecting information e-learning module; • Managers should be provided with additional dashboard solutions that will provide them with information on which staff have completed the e-learning training; • The Council should consider producing a training plan to ensure the continuous awareness of the protecting information e-learning training.

30 March 2017	**Xternal Property Renovations Ltd EN**	Enforcement notices	Xternal Property made more than 109,000 calls to individuals registered with the Telephone Preference Service. The ICO received numerous complaints from such individuals.	Xternal Property Renovations Ltd EN shall neither use, nor instigate the use of, a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where the phone number is that of: (a) an individual who has notified the company that such calls should not be made on that line; and/or (b) an individual who has registered the number with the TPS at least 28 das previously.
30 March 2017	**Xternal Property Renovations Ltd MPN**	Monetary penalty notice	See the above facts.	Monetary penalty notice of £80,000.
30 March 2017	**PRS Media Limited t/a Purus Digital**	Monetary penalty notice	Between January and May 2016, 2,628 complaints were made to the GSMA's Spam Reporting Service about the receipt of unsolicited direct marketing text messages from, or on behalf of, PRS Media Limited. The ICO wrote to PRS Media with details of the complaints, to which no response was received. The ICO issued an Information Notice in July 2016. PRS Media responded, explaining that their website is a competition and prize draw website and that a condition of entry is that individuals must agree to marketing.	Monetary penalty notice of £140,000.

			The ICO reviewed PRS Media's privacy policy and terms and conditions and found them to be generic and unspecific. Individuals were not offered a preference as to how they may be contacted. The ICO asked further questions but received no further responses. The ICO found that PRS Media had sent a total of 4,357,453 text messages between January 2016 and May 2016. The ICO considered that PRS Media had contravened PECR.	